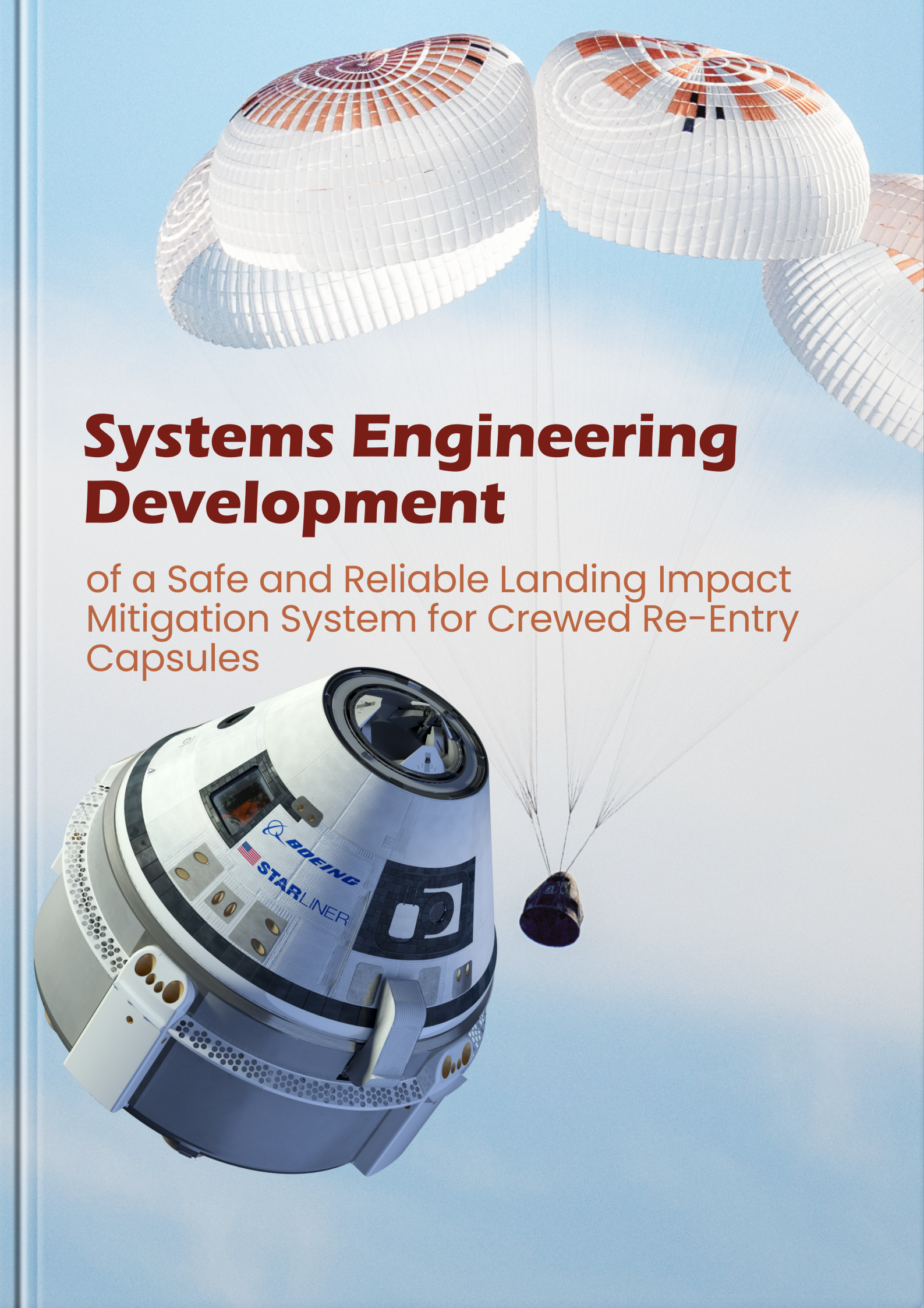


The image shows a Boeing Starliner capsule in a vertical orientation, with its nose pointing upwards. The capsule is white with blue and black accents. The word "BOEING" is printed in blue above "STARLINER" in black. A small American flag is visible on the side. The capsule is surrounded by several large, white, dome-shaped parachutes with orange and black patterns on their canopies. The background is a clear, light blue sky.

Systems Engineering Development

of a Safe and Reliable Landing Impact
Mitigation System for Crewed Re-Entry
Capsules



Contents

1.	Introduction	4
1.1.	Background and Context	4
1.2.	Scope and boundaries of the work	4
2.	Project Objective and Customer Brief	4
2.1.	Project Objective SMART	4
2.2.	Short summary of customer brief	5
3.	Requirement Specification	5
3.1.	Approach for Requirement Capture.....	5
3.2.	Requirement Specification	5
3.3.	Justification of requirements	5
3.4.	Requirement quality check.....	7
4.	System Architecture	7
4.1.	System boundary and context.....	7
4.2.	Rationale and feasibility linked to requirements	9
5.	Systems Engineering Methodologies	9
5.1.	Product Breakdown Structure (PBS)	9
5.2.	PBS diagram for the LIMS	10
5.3.	Quality Function Deployment (QFD)	10
5.4.	Trade-off Analysis	12
6.	Risk and Mitigation Plan	15
6.1.	Hazard identification Overview	15
6.2.	Hazard Identifications	15
6.3.	Fault tree analysis (FTA).....	16
7.	Verification and Validation Plan for Crewed Space Capsule	18
7.1.	V-Diagram and the Verification & Validation (V&V) Concept	18
7.2.	Maintenance Plan	21
7.3.	Quality and Standards	21
7.4.	Applicable Norms and Standards:.....	22
8.	Human Design and Human Factors	22
9.	Integrated Discussion.....	23
	References:	24
	Appendices	25
	Appendix A:	25
	Appendix B	34
	Appendix C.....	35

Table of Figures

Figure 1	System Diagram	8
Figure 2	QFD Diagram.....	11
Figure 3	Diagram (Custom Render).....	17
Figure 4	Modified Landing System FTA	18
Figure 5	V-Model of LIMS	18
Figure 6	Formal Verification and Runtime Monitoring Integration:	21
Figure 7	Trade-Off Support System (TOSS) for LIMS.....	34

List of Tables

Table 1	Requirement Specifications.....	6
Table 2	Functional Decomposition and Subsystem Integration	8
Table 3	Rationale and feasibility linked to requirements	9
Table 4	Trade-Off Evaluation Criteria and Rationale for LIMS Design Selection	13
Table 5	LIMS Evaluation Criteria Weights	13
Table 6	LIMS Design Alternatives Scoring Matrix	14
Table 7	Hazard Classification and Associated LIMS Requirements.....	15
Table 8	Linking Hazards to Safety Requirements	16
Table 9	Probability Calculation	17



Table 10 Alignment with Standards	19
Table 11 Verification Methods.....	19
Table 12 Analysis based Verification	20
Table 13 Inspection / Review Based Verification.....	20
Table 14 Applicable Norms and Standards	22

1. Introduction

1.1. Background and Context

The human-rated re-entry capsule must dissipate significant kinetic energy during descent, **reducing orbital velocity (~28,800 km/s) to survivable landing speed (~1.5 m/s)**. To achieve this, energy-attenuation systems typically parachute, airbags, retrorockets, and crushable structures are employed to limit impact loads. The Landing Impact Mitigation System (LIMS) is therefore a safety-critical subsystem that serves to reduce descent velocity and deceleration to human-tolerable limits, ensure fault tolerance (Evans *et al.*), and enable safe land or water touchdown. Initial specifications established functional requirements, including vertical velocity ≤ 7.5 m/s, peak deceleration $\leq 10g$, multi-stage deceleration with redundancy, and cross-environment compatibility. These were derived from stakeholder needs, NASA human-rating standards (Childress, Williams and Francisco, 2023), and systems engineering best practices (e.g. NASA SE Handbook, INCOSE guidelines).

1.2. Scope and boundaries of the work

This project focuses on the landing impact mitigation subsystem of the crew capsule, which includes the deceleration devices (main and backup parachutes, airbags, optional retro-propulsion), their inflation and control systems, and deployment sensors/logic based on altitude (SHEN, WANG and LIU, 2025), velocity, and descent phase. This includes the capsule structure, power systems, crew displays, and interfaces with environmental conditions such as high winds, rain, and rough seas. Human factors are addressed through deceleration limits, upright orientation after splashdown, and manual override provisions (Yu *et al.*, 2015). This scope does not include the complete spacecraft architecture, de-orbit/re-entry systems, orbital control, launch abort and post-landing recovery. This includes parachute deployment at 3400 m and an existing airbag system that LIMS can augment or replace. The reliability data provided will be used as is. The result is a high-level specification and architecture; Detailed design, manufacturing, and certification are out of scope.

2. Project Objective and Customer Brief

2.1. Project Objective SMART

S pecific	Design and document a landing impact mitigation system (LIMS) for the crew capsule that reduces vertical landing velocity to ≤ 7.5 m/s (≈ 25 ft/s) and limits vertical deceleration to ≤ 10 g, providing safe landing on land or water under nominal and abort scenarios, with the possibility of failure of redundant deceleration elements (parachutes and airbags/ retro-thruster) $< 6.1\%$, and includes health-and manual override capabilities.
M easurable	Maximum touchdown velocity ≤ 7.5 m/s and maximum crew vertical deceleration $\leq 10g$, with demonstrable single-failure-tolerant redundancy in the landing system. Define 10-15 verifiable system requirements with objective V&V methods and complete a verification matrix linking each requirement to its verification method.
A chievable	The goals are feasible using established aerospace heritage technologies (drogue-main parachutes, airbags, retro-thrusters, CMUS upright bags) and are supported by the summarized literature, NASA specifications, and reliability data.
R elevant	Landing load is the primary driver of crew safety and mission certification. A robust LIMS directly satisfies stakeholder expectations for safe human-spaceflight operations and aligns with recognized aerospace systems-engineering practices.
T ime-bound	All system performance targets, requirements updates, architectural definitions and validation evidence must be completed within the defined mini-project timeframe, requirement specifications will be prepared early in the schedule, and the final report will be delivered by the specified module deadline.

2.2. Short summary of customer brief

The customer is developing a human-rated space capsule and needs a robust landing impact mitigation system (LIMS) with redundancy. During re-entry, the capsule must slowdown from approximately 18,000 mph to a landing velocity of 5 ft/s, which requires a multi-modal deceleration system consisting of parachutes, airbags, retrorockets, and crushable structures. The baseline design includes two main parachutes deploying at 3400 m and an airbag system activating at ~1500 m. The team is tasked with designing an advanced LIMS that reduces impact forces, minimizes the risk of injury, and incorporates a fail-safe backup mechanism. Customer-specified reliability parameters include dual compressed-gas supply (failure probability 1×10^{-3} , maximum flow rate 0.012g/s), airbags with a minimum inflation period of 2 hours and overall cushioning system failure probability <6.1%. Power supply reliability is defined as 2×10^{-3} for the primary system and 7×10^{-4} for the backup. Additional failure probabilities include 4×10^{-3} per demand for both main and backup parachutes, 1×10^{-2} for retrorockets, 1×10^{-4} for manual valves, and 2.8×10^{-3} for powered valves.

3. Requirement Specification

3.1. Approach for Requirement Capture

Stakeholder requirements and mission objectives: All key stakeholders, including crew, engineers and mission planners, should be identified with their requirements for safety, payload security and system reusability; Stakeholder needs arise from expectations, constraints, risks, and life-cycle considerations, concepts of operations (ConOps) are used to translate mission scenarios into system functions (Encyclopedia, 2019).

Iterative requirements analysis: The NASA systems engineering process is applied to translate stakeholder needs into technical "to do" statements, supported by continuous stakeholder engagement to refine, validate, and verify requirement completeness and accuracy (NASA, 2006).

Requirement characterization and management: Each requirement is documented with its rationale, sources, and validation criteria, supported by hierarchical modelling using SysML or a requirements database (e.g., DOORS), with configuration control, versioning, and baselining maintained in accordance with NPR 7123.1 and the NASA Systems Engineering Handbook (Hirshorn, 2007).

3.2. Requirement Specification

Table 1 summarizes the key requirement categories with representative examples (ID from the initial LIMS specification). Each requirement is a testable "to do" statement, including functional, mission, interface, environmental, operational, human factors, logistics, physical, product assurance, and design needs. Includes technical values, rationale, standards, verification methods, and priorities according to NASA and SEBOK systems engineering guidance. It enables baseline traceability and supports iterative refinement with stakeholder validation to ensure complete and verifiable system definition.

3.3. Justification of requirements

The rationale for selected LIMS requirements is based on key engineering drivers including deceleration performance, redundancy, human safety, environmental resilience and maintainability. These considerations are consistent with NASA human-rating standards, historical capsule mission data, and current aerospace regulatory guidelines. For example, deceleration constraints arise from the need to reduce orbital velocity to human-tolerable landing speeds using multi-stage systems (Fasanella, 2008). Similarly, (Lee, McKinney and Corliss), fault tolerance and crew override provisions reflect best practices established in programs such as Orion and Gemini. Human biomechanical thresholds, environmental constraints (e.g. wind, sea conditions), and support requirements further shape the specification. A summary mapping of these engineering rationales to specific requirement IDs is provided in *Table A2 (Appendix A)*.

Table 1 Requirement Specifications

Requirement ID	Category	Requirement Statement	Technical Parameters/Values	Justification Summary	Verification Method	Priority
LIMS-FR-0001	Functional	The system shall reduce the capsule's vertical landing velocity to ≤ 7.5 m/s under nominal conditions.	Vertical velocity ≤ 7.5 m/s (≈ 25 ft/s)	- Reduces impact energy - Aligns with Orion safety criteria	Simulation and drop test validation	Critical
LIMS-FR-0002	Functional	The system shall limit the maximum vertical deceleration experienced by the crew to ≤ 10 g.	Max vertical deceleration ≤ 10 g	- Protects against spinal trauma - Follows human tolerance studies	Crash sled testing, CIAS test data	Critical
LIMS-FR-0003	Functional	The system shall incorporate redundant deceleration elements to ensure single-failure tolerance.	Redundant systems (parachutes/thrusters)	- Eliminates single-point failure - Required by NASA redundancy standards	FMEA, redundancy test	Critical
LIMS-FR-0004	Functional	The system shall implement a multi-stage deceleration sequence with ordered deployment.	Drogue $\rightarrow$ Main parachute sequence	- Smooth deceleration - Prevents instability	Staged deployment testing	High
LIMS-MR-0005	Mission	The system shall ensure safe landing capability for both land and water touchdown scenarios.	Compatible with land & splashdown	- Covers all mission profiles - Orion land contingency design	Simulation and field tests	Critical
LIMS-MR-0006	Mission	The system shall ensure safe landing capability during both nominal and abort descent trajectories.	Supports emergency abort trajectories	- Validated via PadAbort1 - Protects crew during aborts	Abort-mode scenario testing	Critical
LIMS-IF-0007	Interface	The system shall be integrated such that the LIMS remains protected until commanded deployment.	Stored internally; deploys only when commanded	- Preserves aerodynamics - Prevents thermal compromise	Structural & thermal analysis	High
LIMS-IF-0008	Interface	The system shall provide a safing interface to disarm or release parachutes after landing.	Pyro cutters or quick-disconnects	- Prevents capsule drag - Enhances recovery operations	Post-landing deployment sequence test	High
LIMS-EN-0009	Environmental	The system shall operate effectively under high-wind, rain, and rough-sea environmental conditions.	Environmental envelope (TBD)	- Ensures performance in real conditions - Wind tunnel & drop tested	Environmental chamber and drop tests	High
LIMS-OP-0010	Operational	The system shall execute fully automated deployment of deceleration devices based on sensor inputs (altitude and velocity).	Drogue @ $\sim 25,000$ ft; Main @ $\sim 9,000$ ft	- Removes crew burden - Validated in Orion automation tests	Sequence and logic testing	Critical
LIMS-OP-0011	Operational	The system shall provide real-time status indication and manual override capability for deployment.	Telemetry + cockpit alerts + manual switch	- Situational awareness - Backup control	Telemetry + override simulation	High
LIMS-HF-0012	Human Factors	The system shall limit crew impact acceleration to within safe biomechanical tolerance limits.	$G \leq 10g$; CIAS seats; restraints	- Protects human body - Reduces trauma	Biomech testing + crash simulation	Critical
LIMS-HF-0013	Human Factors	The system shall automatically upright the capsule to a stable orientation following splashdown.	CMUS with 5 air bags; "Stable1" position	- Prevents disorientation - Preserves air/comm systems	Splashdown orientation test	High
LIMS-LS-0014	Logistics Support	The system shall enable reuse or rapid refurbishment of landing mitigation components.	Modular, maintainable components; Kevlar parachutes	- Reduces cost - Enhances availability	Reuse inspection process	Medium
LIMS-PH-0015	Physical	The system shall fit within capsule mass and volume constraints without altering the external aerodynamic Mold-line.	Mass add $\leq X\%$; no Mold-line alteration	- Preserves re-entry dynamics - Compact packaging	CAD volume fitting + weigh-in	High

3.4. Requirement quality check

To ensure compliance with mission objectives and safety-critical performance limitations, a formal Requirements Traceability and Verification Matrix (RTVM) have been developed, aligning with the NASA Systems Engineering Handbook (NASA/SP-2007-6105 Rev2) (NASA) and INCOSE SEBoK guidance (Michael Ryan, 2023). RTVM defines each requirement using clear, measurable parameters and links it directly to its source purpose, verification method, criteria for compliance, and responsible subsystem. This structured approach ensures complete coverage, avoids ambiguity, and supports rigorous validation through testing, simulation, or inspection. Additionally, all requirements are expressed in active voice using the imperative "do" in accordance with NASA-SEH editorial standards for enforceability and clarity. Requirements avoid vague wording or implicit design solutions and instead provide quantitative limits (for example, "deployment within 3.0 ± 0.2 seconds"). A detailed traceability matrix showing this structure is presented in Table A3 (Appendix A).

4. System Architecture

4.1. System boundary and context

The Landing Impact Mitigation System (LIMS) is defined as a crew capsule subsystem that includes the components directly involved in landing load reduction such as parachutes, airbags, retrorockets, sensors and control units excluding avionics or propulsion unrelated to other flight phases (Fasanella, 2008). Its external environment includes the atmosphere, land/water interface, and recovery systems. Consistent with NASA Systems Engineering Practice (essp.larc.nasa.gov), Figure 1 shows the LIMS receiving inputs such as altitude, velocity, and environmental loads and generating outputs such as attitude corrections and parachute deployment. Internally, the LIMS capsule interfaces with structural hardpoints and crew systems (e.g., seats, displays). Defining this context ensures that interface requirements are fully identified and supports architectural decomposition.

4.1.1. Top-level System Architecture (Product Breakdown Structure)

The Landing Impact Mitigation System (LIMS) is a complex, multi-layered architecture designed to ensure the safe deceleration and touchdown of the re-entry capsule. Its design incorporates redundant deceleration mechanisms, inflation systems, sensor-driven logic, manual overrides and structural interfacing to withstand and reduce landing shock under nominal and off-nominal conditions (Tutt *et al.*). The architecture reflects NASA's systems engineering approach by ensuring safety through redundancy and operational flexibility in various landing scenario.

4.1.2. Functional Decomposition and Subsystem Integration

The Landing Impact Mitigation System (LIMS) is a hierarchical assembly of interdependent subsystems designed to manage controlled deceleration, impact attenuation, and structural protection during re-entry and landing. It consists of three main categories: deceleration, control and logic, and support subsystems, each carrying out integrated functions within the landing sequence. The deceleration subsystem consists of a sequential parachute system mortar-deployed drogue and pilot chute, followed by a pilot-deployed main chute with redundancies to ensure survivability under partial failure. This is complemented by a multi-chamber airbag assembly that includes crushable structures such as vented pressure regulation, or alternatively, honeycomb panels for passive energy absorption. Retro-propulsion modules can also be deployed using solid or throttleable thrusters to reduce terminal sink rate and landing torque just before touchdown (Tutt *et al.*). The control and logic subsystem integrates a barometric altimeter, IMU, GPS, and a flight computer to enable real-time sensor fusion and event-driven deployment logic. Fail-safe algorithms ensure redundancy, while manual override interfaces with visual cues and switches allow crew intervention if automation fails.

Support subsystems include aspirator-based inflation systems mixing high-pressure nitrogen with ambient air for efficient airbag deployment, telemetry units for real-time monitoring (e.g. load, pressure, acceleration), and structural components such as hardpoints and bay covers for load distribution and protection during re-entry. Together, these subsystems enable a flexible and adaptive LIMS that can ensure crew safety under nominal and off-nominal landing scenarios.

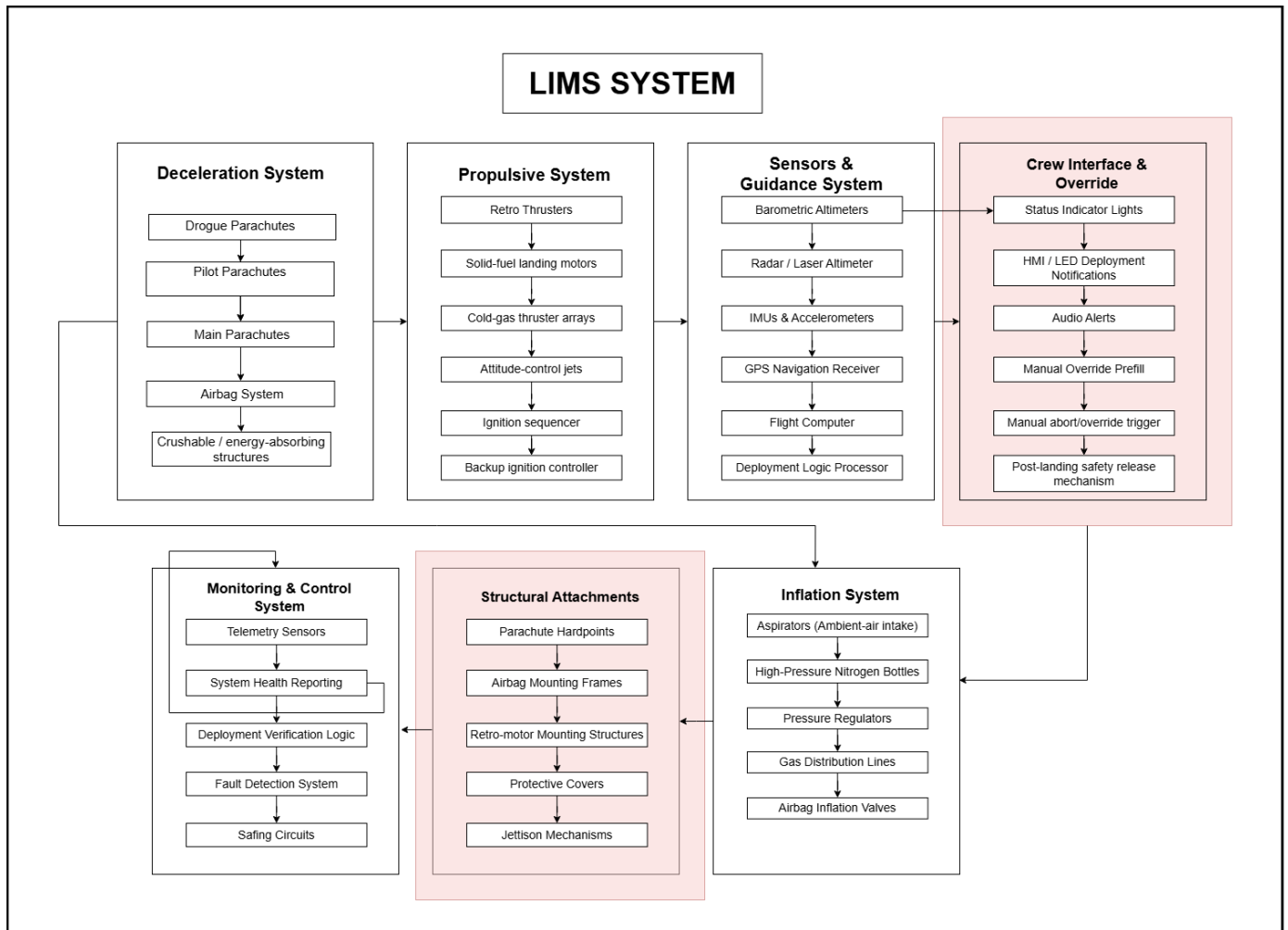


Figure 1 System Diagram

Table 2 Functional Decomposition and Subsystem Integration

Subsystem	Purpose	Key Components	Notes
Parachute System	Primary deceleration	Drogue, pilot, main parachutes	Redundant for single-failure tolerance
Airbag System	Final impact cushioning	Airbags, vents, shaping structures	Mass-efficient aspirators
Crushable Structures	Passive energy absorption	Honeycomb, crush struts	Optional for hard landing concepts
Retro-Thrusters	Final descent velocity reduction	Solid or throttleable rockets	Symmetric arrangement critical
Sensors and Guidance	Altitude estimation, event triggering	Altimeters, IMU, GPS, flight logic	Includes fail-safe triggers
Inflation Subsystem	Airbag inflation	Aspirators, nitrogen bottles	Mixed inflation for mass efficiency
Manual Interface	Human-in-the-loop control	Override switches, indicators	Mandatory per safety standards
Monitoring and Control	Data acquisition and telemetry	Pressure sensors, arming logic	Transmits to displays and recovery teams
Structural Integration	Load transfer and hardware protection	Fittings, covers, jettison mechanisms	Includes re-entry shielding

4.1.3. Textual Flow Diagram Description (System Interconnects)

At the heart of the LIMS system lies the control logic, which receives inputs from the sensor suite (altimeter, IMU, GPS). This logic controls deployment commands on parachute mortars, inflation valves, and retro-thrusters based on altitude and descent rate. Additionally, the manual override interface allows crew intervention. The inflation subsystem provides airbag activation using aspirators and high-pressure gas. After deployment, monitoring sensors record the dynamics of the impact, transmitting telemetry and data back to control circuits (Shook, Timmers and Hinkle, 2009). Structural enclosures ensure mechanical stability, while external casings protect components during high-velocity re-entry.

4.2. Rationale and feasibility linked to requirements

Table 3 Rationale and feasibility linked to requirements

Subsystem / Feature	Rationale	Feasibility	Linked Requirements
Parachutes (Primary Decelerators)	Multi-stage parachute systems are mass-efficient and reduce subsonic velocities to safe descent rates. Redundant design tolerates single-chute failures.	Highly mature technology with decades of heritage; validated in Orion testing and legacy programs.	LIMS-PH-0015
Airbags (Impact Attenuation)	Airbags dissipate remaining kinetic energy when parachutes are insufficient. Venting and anti-bottoming features prevent bottoming out and distribute loads evenly.	Demonstrated in Orion and other programs. Aspirator-based inflation reduces gas mass. Drop-tested and validated for space capsule use.	Performance (LIMS-PH-0015)
Retro-Thrusters	Provide extra impulse margin in hard landing or high sink-rate cases. Useful for soft landings and walk-away scenarios.	Proven in crew escape systems and planetary landers. Symmetric firing prevents rotation; can be throttled or pulsed.	Performance (LIMS-PH-0015)
Autonomous Control Logic	Automates event sequencing based on altitude, velocity, and sensed rates. Reduces crew workload and enables safe landing if crew is incapacitated.	Flight software with smart logic and multi-modal triggers used in Orion. Sensors and timers ensure reliable event sequencing despite failures.	Operability (LIMS-OP-0010/0011)
Indicators and Manual Override	Ensure crew situational awareness and allow intervention if automation fails. Boosts safety and crew confidence.	Required for human-rating; standard in crewed spacecraft. Manual deployment and cutaway capabilities support emergency handling.	Human factors (LIMS-HF-0012), Operability (OP-0011)
Health Monitoring System	Enables real-time system verification and recovery planning. Supports maintenance and continuous improvement.	Telemetry, safing circuits, and sensor data logging are standard practice. Used in Orion and similar systems.	Safety & reliability LIMS-PH-0015
Feasibility of Full Architecture	Entire LIMS uses proven, flight-tested components (parachutes, airbags, sensors, retrorockets). Design trades mass vs. safety.	Subsystems tested on Apollo, Soyuz, Dragon, Orion. Inflation systems with aspirators validated in drop tests.	All above; traceability to Section 3
Requirements Traceability	Each subsystem directly supports a verifiable system requirement, ensuring justified design.	Architecture is compliant with performance, safety, operability, and human factors requirements as specified in Section 3.	LIMS-PH-0015, LIMS-OP-0010/001, LIMS-HF-0012

5. Systems Engineering Methodologies

5.1. Product Breakdown Structure (PBS)

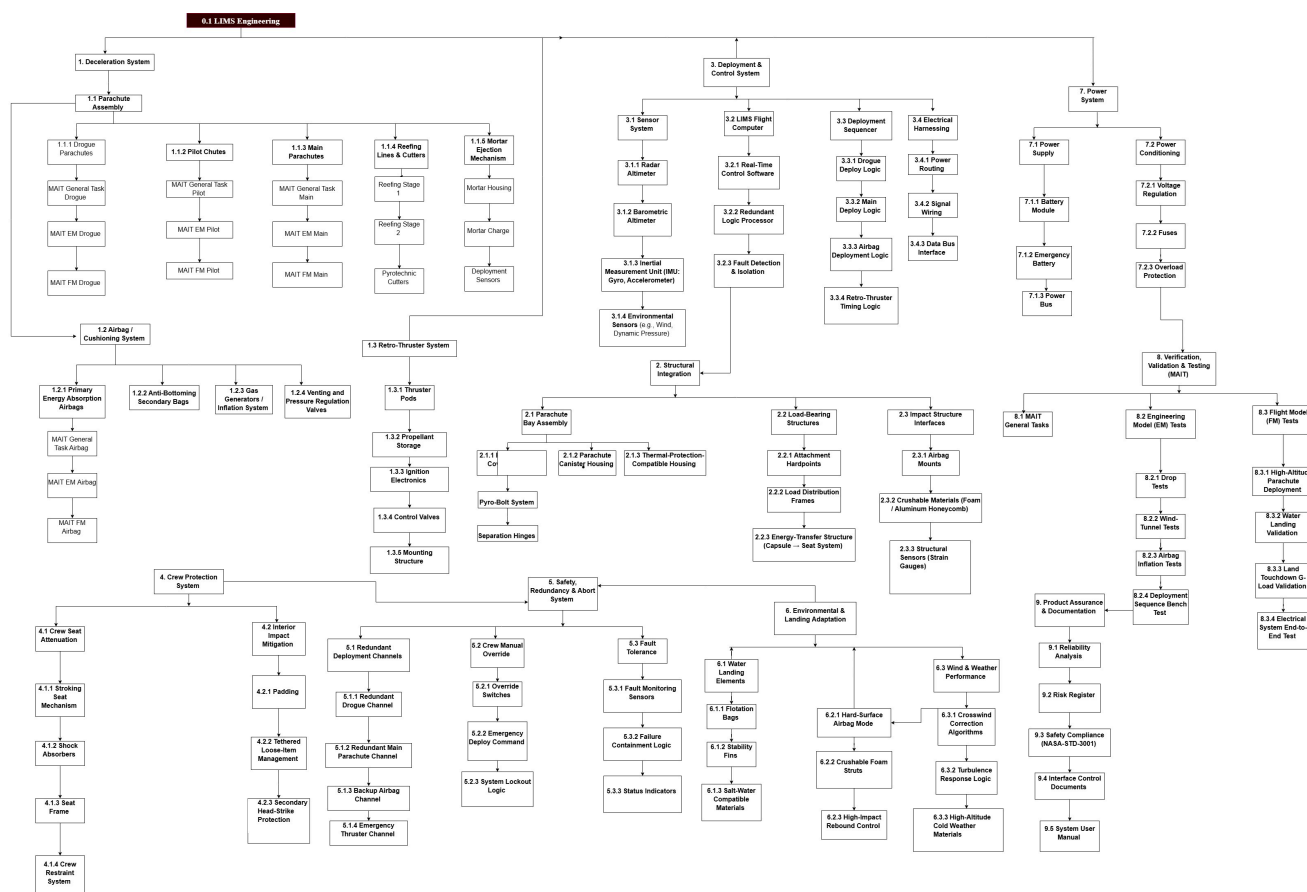
5.1.1. Description of the PBS method

A product breakdown structure (PBS) is a hierarchical decomposition of a system into its physical products or deliverables, starting with the top-level end item (for example, LIMS) and breaking it down into subsystems, assemblies, and components. According to NASA guidance, each PBS element should represent a specific, verifiable, and measurable product or capability, ensure completeness and enable scope control. The PBS is typically aligned with a deliverable-oriented work breakdown structure (WBS), which forms the basis of

technical, schedule, and cost planning. In the context of LIMS, applying PBS ensures that no critical components are overlooked and allows independent assessment of mass, power, and thermal feasibility per subsystem. This strengthens requirement traceability by linking PBS elements to performance criteria and enables concurrent development across system branches (Shook, Timmers and Hinkle, 2009). Overall, PBS provides a structured framework that converts high-level system requirements into concrete, manageable deliverables, supporting effective validation and system planning throughout the LIMS lifecycle.

5.2. PBS diagram for the LIMS

A product breakdown structure (PBS) provides a hierarchical decomposition of the landing impact mitigation system (LIMS) into its major subsystems and components. At the top level, LIMS includes several key product elements. Deceleration systems include primary equipment such as drogue and main parachute, and secondary energy-attenuation hardware such as airbags or retrorockets that are required to satisfy FR-0001 and FR-0002. The control and sensor subsystem includes the altimeter, deployment sensors, flight computer, and sequencing logic that enable the automated, safe staging required by the OP-0010 and OP-0011. Structural integration includes the parachute bay, attachment interface, and housing assembly that ensure compatibility with capsule geometry and physical constraints (PH-0015). The safety and recovery subsystem includes health-monitoring electronics, indicators, manual-override elements, and post-landing features such as a parachute cutter and up-righting bag (HF-0013). Finally, Support and Logistics includes renewable components, maintenance kits and storage solutions aligned with LS-0014. Refer Appendix C Document A1: QFD.



5.3. Quality Function Deployment (QFD)

The full QFD diagram provides a structured mapping between customer requirements (WHATs) and engineering specifications (HOWs) for a landing effects mitigation system. This ensures that design decisions including the size of parachutes, airbag systems, dumping mechanisms and redundancy paths directly address user expectations and mission-critical requirements. The QFD serves as a traceability tool linking

stakeholder requirements to engineering specifications and backup mechanisms within parachute-based landing systems (Shook, Timmers and Hinkle, 2009).

5.3.1. Roof Correlation Matrix

The roof section of the House of Quality presents the interdependencies between engineering characteristics, indicating whether improving one characteristic will support or conflict with another. The correlations are represented using the following symbols:

- ++ (Strong Positive Correlation) – Enhancing one HOW strongly improves another.
- + (Positive Correlation) – A supportive relationship, but with less influence than ++.
- None – No interaction between the characteristics.
- – (Negative Correlation) – Improving one characteristic degrades another.
- — (Strong Negative Correlation) – A strong conflict; improvement in one significantly harms the other.

These correlations help designers identify engineering trade-offs for example, increasing parachute area may positively influence terminal descent rate but negatively affect system mass or deployment time.

5.3.2. Relationship Matrix (Body of the HOQ)

This section quantifies how strongly each customer requirement influences each technical characteristic. QFD commonly uses a 9–3–1–0 weighting scheme:

- 9 (Strong Relationship) – The HOW has major impact on satisfying the requirement.
- 3 (Moderate Relationship) – The HOW contributes meaningfully but not decisively.
- 1 (Weak Relationship) – The HOW has minimal influence.
- 0 (No Relationship) – No meaningful link exists.

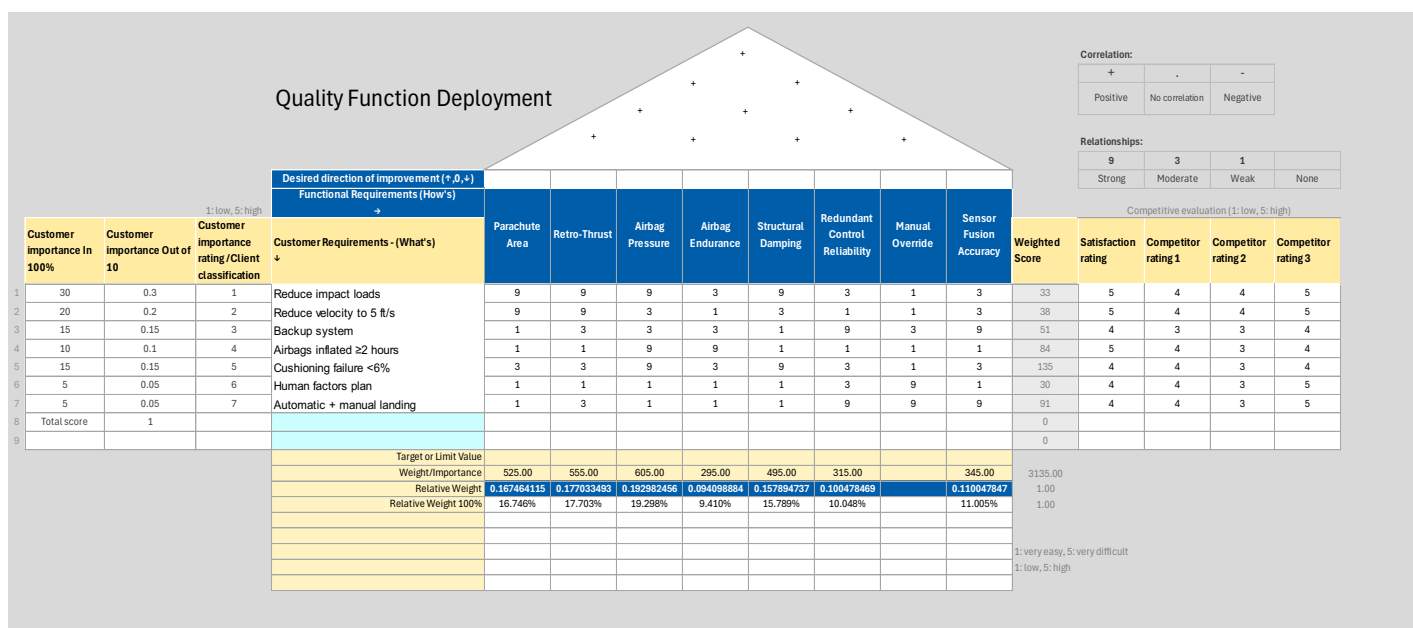


Figure 2 QFD Diagram

Comment In LIMS QFD, the strongest relationships are between key safety requirements such as limiting impact loads and meeting landing velocity targets and engineering characteristics such as airbag inflation pressure, retro-thrust capability and structural damping. These high-load correlations highlight that energy absorption and deceleration mechanisms are the primary design drivers for mission safety. Since these subsystems directly impact kinetic energy management and G-load reduction, they are central to meeting human-rating criteria and form the focus of engineering optimization in LIMS architecture.

5.3.3. Customer Requirements Selected

To systematically translate stakeholders' needs into engineering solutions, a QFD approach was applied. The analysis identifies key customer requirements such as safe deceleration, redundancy and human-factors

compliance and links them to measurable technical characteristics including parachute area, retro-thrust capability and sensor fusion accuracy. This process supported prioritization of design trade-offs and ensured alignment between system functions and mission-critical objectives. See Appendix A Table A3&A4 for a detailed representation of customer requirements (what's) and related technical characteristics (how's) used in the QFD matrix.

5.3.4. House of Quality (HOQ)

House of Quality establishes the relationship between each customer requirement and its corresponding technical characteristic using traditional QFD weighting values (9 = strong, 3 = medium, 1 = weak). Correlation "ceiling" identifies interactions, dependencies, and potential design conflicts. Notable examples include:

- Positive correlation between Parachute Area and Structural Damping
- Partial substitution relationship between Parachute Area and Retro-Thrust Capability
- Positive correlation between Airbag Pressure and Structural Damping
- Negative correlation between Parachute Area and mass budget (outside HOQ scope)

Weighted column totals were obtained by multiplying each requirement's importance rating by its corresponding 9/3/1 relational value. This process yield the following ranked technical characteristics:

1. Airbag Inflation Pressure – 19.298%
2. Retro-Thrust Capability – 17.703%
3. Parachute Area – 16.746%
4. Structural Damping – 15.789%
5. Sensor Fusion Accuracy – 11.005%
6. Redundant Control Reliability – 10.048%

These percentages reflect the relative impact of each feature on meeting the prioritized requirements.

5.3.5. Interpretation of QFD Results

QFD analysis identifies airbag inflation pressure, retro-thrust capability, parachute area and structural damping as the primary design drivers to achieve target impact load and descent velocity and should be prioritized in the early design stages. Moderately weighted factors such as sensor-fusion accuracy and redundant control reliability play important supporting roles in ensuring robust deployment and fault tolerance, requiring rigorous validation, especially under off-nominal conditions. Overall, the findings confirm that impact-energy management mechanisms dominate LIMS performance, while control and sensing systems provide the necessary support for safe, robust, human-rated landings consistent with aerospace systems engineering standards (Shook, Timmers and Hinkle, 2009).

5.4. Trade-off Analysis

QFD analysis identifies airbag inflation pressure, retro-thrust capability, parachute area and structural damping as the primary design drivers to achieve target impact load and descent velocity and should be prioritized in the early design stages. Moderately weighted factors such as sensor-fusion accuracy and redundant control reliability play important supporting roles in ensuring robust deployment and fault tolerance, requiring rigorous validation, especially under off-nominal conditions. Overall, the findings confirm that impact-energy management mechanisms dominate LIMS performance, while control and sensing systems provide the necessary support for safe, robust, human-rated landings consistent with aerospace systems engineering standards (Zapata, 2016).

5.4.1. Definition Of Alternative Design Options

Three landing concepts were shortlisted for evaluation:

Parachute + Airbag (Option A). A multi-stage parachute system slows the capsule, after which inflatable airbags cushion the touchdown. This concept provides better impact attenuation but introduces additional mass and deployment complexity.

Parachute + retrorocket (option B). After the vehicle is slowed by a parachute, a set of small retro rockets are fired just before touchdown to further reduce the descent velocity. Although more expensive and heavier than airbags, retrorockets offer higher deceleration capability and fault tolerance.

Parachute only (option C). The capsule uses a conventional drogue-and-main parachute system without additional impact mitigation devices. The concept is light and inexpensive but relies entirely on parachute performance to meet the 7.5 m/s touchdown requirement.

These options cover the major architectural choices for landing systems passive cushion, active propulsion and baseline parachute and provide a basis for comparison. Exotic concepts (for example, hovering landers) were discarded because they either violated mass/volume constraints or were not mature enough for Phase-A evaluation.

5.4.2. Selection of Criteria and Weighting

In accordance with the methodology, the critical evaluation parameters were first identified and assigned relative weightings prior to the scoring phase. These criteria were formulated to align with the formal requirement specifications and to reflect the prioritization articulated by the customer.

To ensure objective derivation of weighting factors, the Analytic Hierarchy Process (AHP) was used. This method involved the development of a pairwise comparison matrix based on Satie's 1–9 fundamental scale, which facilitates a systematic assessment of the relative importance of each criterion. For example, the criterion of safety was considered slightly more important than reliability and significantly more important than cost, complexity, and mass. The principal eigen vectors of the resulting comparison matrix were calculated to obtain normalized preference weights, as presented in Table 5. To verify the internal consistency of pairwise decisions, a consistency ratio was calculated according to the standard AHP method (Whitaker, 1987), supporting the reliability of the assigned weights.

Table 4 Trade-Off Evaluation Criteria and Rationale for LIMS Design Selection

Criterion	Rationale
Safety	Ability to limit touchdown velocity and crew deceleration (highest priority).
Reliability	Fault tolerance and redundancy; ensures that no single failure leads to unsafe landing.
Cost	Life-cycle cost including development, production and refurbishment.
Mass	Added mass affects launch performance; lighter systems are preferred.
Complexity	Integration and operation complexity; high complexity increases failure risk and cost.
Technology Readiness (TRL)	Maturity of the technology; low TRL increases development risk.

Table 5 LIMS Evaluation Criteria Weights

Criterion	Weight	Complexity	0.044
Safety	0.398	TRL	0.089
Reliability	0.269		
Cost	0.119		
Mass	0.081		

The resulting load plan places major emphasis on safety and reliability (together about 67%), reflecting the capsule's broader need to ensure

crew safety and tolerate subsystem failures. In contrast, cost, mass and technology readiness level (TRL) exhibit only moderate impact, while

complexity emerges as the least consequential criterion within the evaluation framework.

5.4.3. Trade-off Analysis Calculations

Each landing concept was evaluated using a 1–10 scale, normalized to 0–1, and weighted according to the criteria to calculate the final performance index. The table displays the weighted contribution of each criterion to the total score. The parachute+retrorocket option ranked highest overall with the best safety (0.400) and reliability (0.311) due to its dual-mode deceleration and redundancy, although it has lower cost (0.072) and mass (0.039) due to system complexity. Only the parachute system had the best cost (0.130) and mass (0.070) scores from the minimum hardware, but the lowest safety (0.267) and reliability (0.194) due to the lack of backup systems. The parachute+airbag option showed balanced performance, especially in cost (0.116) and reliability (0.272), but fell short of the safety margin of the retrorocket.

Table 6 LIMS Design Alternatives Scoring Matrix

Option	Safety	Reliability	Cost	Mass	Complexity	TRL	Total weighted score
Parachute + Airbag	0.311	0.272	0.116	0.054	0.033	0	0.787
Parachute + Retrorocket	0.4	0.311	0.072	0.039	0.05	0	0.872
Parachute Only	0.267	0.194	0.13	0.07	0.022	0	0.683

The total weighted score – 0.872 for retrorockets, 0.787 for airbags, and 0.683 for parachutes only – was obtained by adding the weighted values of each criterion corresponding to the final AHP step: applying weights to the normalized scores and aggregating them. To validate this, a Pugh matrix was applied using Parachute as a baseline, scoring "+" if better, "-" if worse and "S" if equal. The parachute+retrorocket option achieved the highest net positive tally, which aligned with the AHP result and was confirmed as the strongest candidate both quantitatively and qualitatively. Appendix B Chart 1 (weighted score chart) reinforces this, showing parachute+retrorocket as the top-ranked concept, airbag-assisted descent as the second, and parachute alone given the lowest priority due to limited risk mitigation.

5.4.4. Interpretation of Results and Preferred Option

Table 6 The results highlight Option B (parachute+retrorocket) as the top performing configuration, primarily due to its superior scores in safety and reliability. In contrast, Option C (parachute only) is ranked lowest, reflecting its lack of redundancy despite advantages in cost and mass. The table outlines the impact of weighting critical parameters and suggests that designs incorporating fault-tolerant mechanisms are preferred when crew safety is prioritized. A hybrid approach is also recognized as a potential enhancement for future iterations.

5.4.5. Trade-Off Support System (TOSS) for LIMSs

The Trade-off Support System (TOSS) developed for the Landing Impact Mitigation System (LIMS) applies a structured multi-criteria framework to compare viable landing concepts against weighted requirements for safety, reliability, mass, cost, complexity and technology maturity. As shown in Figure 5 (Appendix), the evaluation considers only parachute, parachute+airbag, and parachute+retrorocket configurations using normalized scores derived from mission and functional priorities. The analysis identifies the parachute+retrorocket concept as the highest performing option due to its superior safety margin, redundancy and ability to manage high-energy descent conditions. The parachute+airbag system performs moderately, while the parachute-only configuration ranks lowest due to its lack of redundancy and reliance on a single deceleration mode. Overall, the TOSS results (Appendix B, Figure 5) indicate that architectures with multiple, independent deceleration mechanisms are more suitable for human-rated missions. This provides a clear and defensible basis for choosing the parachute+retrorocket concept as the preferred LIMS architecture.

6. Risk and Mitigation Plan

6.1. Hazard identification Overview

Risk analysis for a Landing Impact Mitigation System (LIMS) begins with the systematic identification of potential events that could result in an unsafe landing. This includes both external threats, such as adverse environmental conditions, and internal threats, such as subsystem or component failures. This process typically involves performing a functional analysis (Whitaker, 1987), defining relevant measures of system effectiveness, and collecting supporting data for each design alternative prior to selection. *Table 7* summarizes the primary hazards identified for LIMS capsules.

Table 7 Hazard Classification and Associated LIMS Requirements

Hazard type	Examples and rationale	Linked requirements
External – Environmental	High winds, turbulence, dust or debris could cause parachute collapse; lightning could trigger unintended pyrotechnic events; hard or sloped terrain could puncture airbags.	FR-0001/0002 specify maximum touchdown velocity and deceleration; environmental constraints in DR-0018 require operation in extreme temperature and pressure.
External – Operational	Premature deployment due to erroneous altimeter readings; late deployment (e.g., due to sensor failure) leading to high impact speeds; ground operator error when initiating manual overrides.	OP-0010/OP-0011 require automatic deployment and status/manual override capability.
Internal – Structural/mechanical	Main or backup parachute packing or rigging faults; tangled lines; pyrotechnic squib failures; airbag leaks; thruster valve jams.	FR-0003 demands redundant decelerators; PH-0015 imposes mass/volume constraints impacting material selection.
Internal – Electrical/electronics	Power loss in deployment electronics; sensor failures; software errors causing incorrect sequencing; actuator motor stalls.	PA-0016 requires reliability targets and continuous health monitoring; OP-0011 requires status indication and manual abort.
Human factors	Crew impairments (e.g., disorientation) leading to improper manual override; training deficiencies.	HF-0012/0013 specify maximum crew g-loads and post-landing orientation.

Each identified threat can be traced to one or more system requirements, ensuring that the risk analysis is based on formal requirement specification rather than influenced by subjective judgment.

6.2. Hazard Identifications

6.2.1. Key Internal and External Hazards

A comprehensive threat to the Landing Impact Mitigation System (LIMS) has been identified, encompassing internal mechanical, electrical and human-factor threats as well as external environmental and operational threats. The analysis links each credible threat such as parachute deployment failure, retrorocket malfunction, airbag leak, sensor errors, power-system faults and adverse atmospheric conditions to the corresponding safety, functional, environmental and human-factors requirements. This structured mapping ensures that all critical risk sources are clearly addressed through design requirements, redundancy provisions, and reliability targets. The complete classification of threats and their detection capability according to system requirements is given in *Appendix A Table 5: Key Internal and External Hazards*.

6.2.2. Linking Hazards to Safety Requirements

Table 8 Provides Each threat is associated with one or more specific requirements, ensuring that design mitigations are aligned with security goals. This traceability allows targeted engineering solutions, such as redundancy measures, material selection and system reliability improvements, to be verified through testing and analysis.

Table 8 Linking Hazards to Safety Requirements

Hazard	Related Safety Requirement	Description/Implication
Parachute Failure	FR-0001: Safe landing velocity	Parachute failure threatens the ability to meet the safe landing velocity requirement, highlighting the need for redundancy (FR-0003).
Sensor Malfunctions	OP-0010: Automatic deployment operational requirement PA-0016: Reliability requirement	Sensor malfunctions affect automatic deployment, which is critical for system performance, and must meet reliability standards.
Rough Terrain (External Hazard)	FR-0005: Safe land and water landings HF-0013: Capsule upright orientation	External hazards such as rough terrain may impact landing safety, necessitating the need for requirements on safe land and water landings, as well as capsule stability.

6.3. Fault tree analysis (FTA)

Top event definition: In fault tree analysis (FTA), the top event is defined as "unsafe landing – injury or loss of crew", capturing the primary unwanted system outcome. The FTA method hierarchically explores how a combination of lower-level failures in hardware, software, and human interactions can lead to this top event. This structured approach aligns with aerospace systems engineering standard by revealing subsystem interdependencies and latent vulnerabilities.

Fault tree construction: FTA links the top event to its causes using logic gates: the OR gate indicates that the top event occurs if an input fails; AND gates require that all inputs fail simultaneously. This logic supports transformation into minimal cut sets and Boolean simplification, thereby facilitating risk quantification.

Baseline Landing System: LIMS employs a dual-parachute system (main and backup) for primary deceleration, complemented by airbags and retrorockets as secondary mitigation layers. The top event defined "unsafe landing with crew injury" occurs when both parachutes fail and at least one redundant system also fails, exposing critical pathways to mission failure.

minimum cut set as the smallest combination of component failures that causes the top event; If no failures occur in that set, the top event does not occur. Translating trees into Boolean equations (Whitaker, 1987) and using the top-down or bottom-up substitution method the minimum cut set is obtained:

1. $MCS_1 = \{M, B, R\}$ – Both parachutes fail, and the retrorocket fails.
2. $MCS_2 = \{M, B, A\}$ – Both parachutes fail, and the airbag fails.

The fault tree shown in Figure 3 shows the logical structure of this failure scenario. Specifically, the top event is connected through an OR gate to two subordinate AND gates, each representing a different minimum cut set that can give rise to an unsafe landing event. There are two minimum cut sets:

1. $\{M, B, R\}$ – Failure of the main parachute (M), backup parachute (B), and retrorocket (R).
2. $\{M, B, A\}$ – Failure of the main parachute (M), backup parachute (B), and airbag system (A). In this analysis, all basic events are assumed to be statistically independent.

In this analysis, all basic events are assumed to be statistically independent.

Quantitatively, assuming independence:

- $P(M \cap B \cap R) = P(M)P(B)P(R)$
- $P(M \cap B \cap A) = P(M)P(B)P(A)$

Total (baseline) $P(T) \approx P(MBR) + P(MBA)$.

This matches your earlier computation. Such formal Boolean logic + minimal cut set definition is standard practice in FTA.

The logic in Figure 3 leads to two minimal cut sets. The fault-tree handbook formally defines the

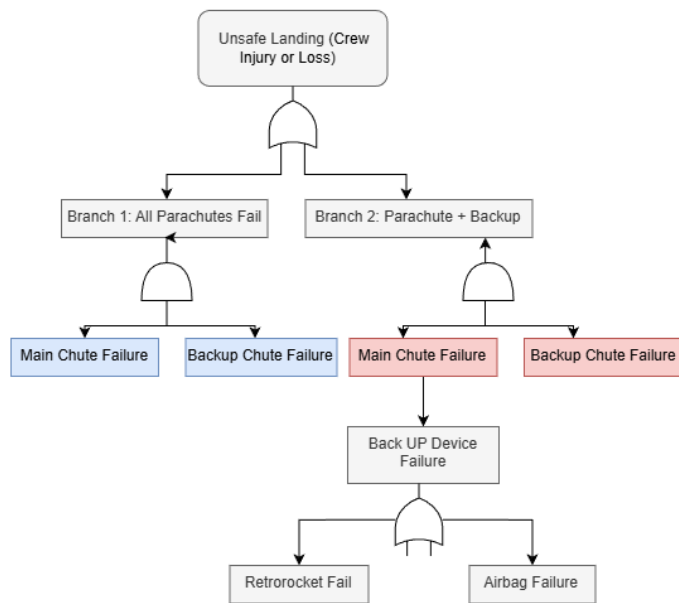


Figure 3 Diagram (Custom Render)

Table 9 Probability Calculation

Basic event	Approximate probability	Notes
Main parachute fails (M)	(4×10^{-3})	typical main parachute failure rate
Backup parachute fails (B)	(4×10^{-3})	like main parachute
Retrorocket fails (R)	(1×10^{-2})	thruster ignition or control failure
Airbag fails (A)	(6.1×10^{-2})	includes inflation failure or tear

6.3.1. Common cause failures

Common cause failures (CCFs) occur when multiple components fail due to a shared cause, such as manufacturing defects, improper installation, or environmental conditions. As defined in the NASA Fault Tree Handbook with Aerospace Applications, ignoring the CCF can lead to underestimating the probability of total system failure. For example, three components with independent failure probabilities of 1×10^{-3} result in a combined failure of 1×10^{-9} , but introducing 1% CCF increases this to 1×10^{-5} . To minimize CCF in landing systems, parachutes should be independently sourced and packaged, thrusters and airbags should be operated by separate electrical buses, and human factors such as maintenance procedures should be considered in the hazard analysis.

6.3.2. Risk-Reduction Strategy: Redundancy, Diversity and Separation

Redundancy: Add a tertiary parachute (T) and an additional retrorocket to prevent two thrusters failing simultaneously. Redundant units increase the number of failures required for the peak event. For three independent parachutes, the probability that all of them fail is $(4 \times 10^{-3})^3 = 6.4 \times 10^{-8}$. Two independent thrusters each with failure probability 1×10^{-2} produce a combined failure probability of $(1 \times 10^{-2})^2 = 1 \times 10^{-4}$. Two independent thrusters each with failure probability 1×10^{-2} produce a combined failure probability of $(1 \times 10^{-2})^2 = 1 \times 10^{-4}$. The probability of MCS involving thruster failure is therefore $6.4 \times 10^{-8} \cdot 1 \times 10^{-4} = 6.4 \times 10^{-12}$. The MCS involving airbag failure becomes $6.4 \times 10^{-8} \cdot 6.1 \times 10^{-2} \approx 3.9 \times 10^{-9}$. Summing these yields a new top-event probability $P_{top} \approx 4 \times 10^{-9}$, roughly three orders of magnitude lower than the baseline.

Probability calculations:

Assuming independent failures, the probability of each minimum cut set is the product of the original event probabilities. Common failure data used for specific aerospace components:

The probability of MCS_1 is $P(MCS_1) = P(M) \cdot P(B) \cdot P(R) = 4 \times 10^{-3} \cdot 4 \times 10^{-3} \cdot 1 \times 10^{-2} = 1.6 \times 10^{-7}$. The probability of MCS_2 is $P(MCS_2) = 4 \times 10^{-3} \cdot 4 \times 10^{-3} \cdot 6.1 \times 10^{-2} \approx 9.8 \times 10^{-7}$.

Since the cut sets are mutually exclusive, the probability of the top event is the sum: $P_{top} = 1.6 \times 10^{-7} + 9.8 \times 10^{-7} \approx 1.1 \times 10^{-6}$. This low probability suggests that the baseline design meets stringent reliability targets; however, improvement is possible.

6.3.3. Modified Landing System Fault Tree

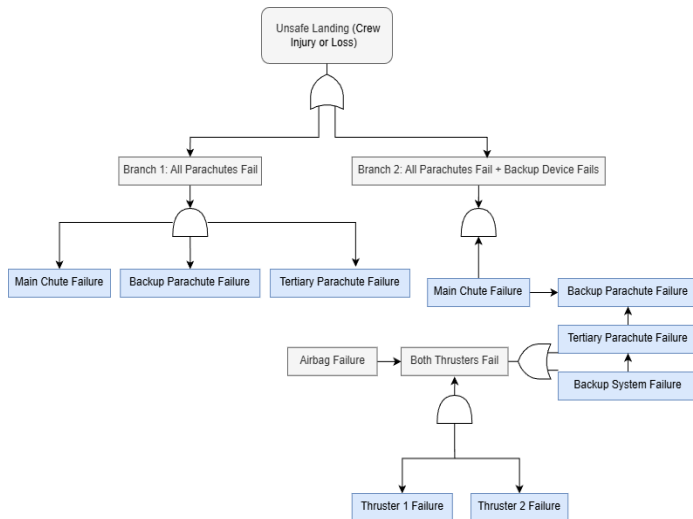


Figure 4 Modified Landing System FTA

Conclusion:

Applying fault-tree analysis to the LIMS capsule landing system shows how a top-down logic model

identifies combinations of failures that endanger the crew. The two minimum cut sets of the baseline design indicate that crew protection against single failures is strong; There is a backup system should both parachutes fail for an unsafe landing. Quantitative evaluation yields a probability of roughly 1.1×10^{-6} . Recognizing the risk of common cause failures emphasizes the need for diverse materials, independent suppliers, and physical separation, adding redundancy (a tertiary parachute and redundant thrusters) reduces the probability of a top-event by several orders of magnitude and aligns with NASA guidance on risk reduction through redundancy, diversity, and separation. Careful adherence to FTA construction rules and systematic derivation of minimum cut sets Providing engineers with a reliable way to evaluate and improve complex safety-critical systems (Shook, Timmers and Hinkle, 2009).

7. Verification and Validation Plan for Crewed Space Capsule

7.1. V-Diagram and the Verification & Validation (V&V) Concept

The V-diagram depicts the system lifecycle, with details from mission requirements to design on the left, and details mapping integration and V&V activities on the right. According to NASA guidance, early and independent V&V increases risk identification and reliability of results (Sutherland *et al.*).

7.1.1. V-Model Decomposition with Detailed V&V Steps

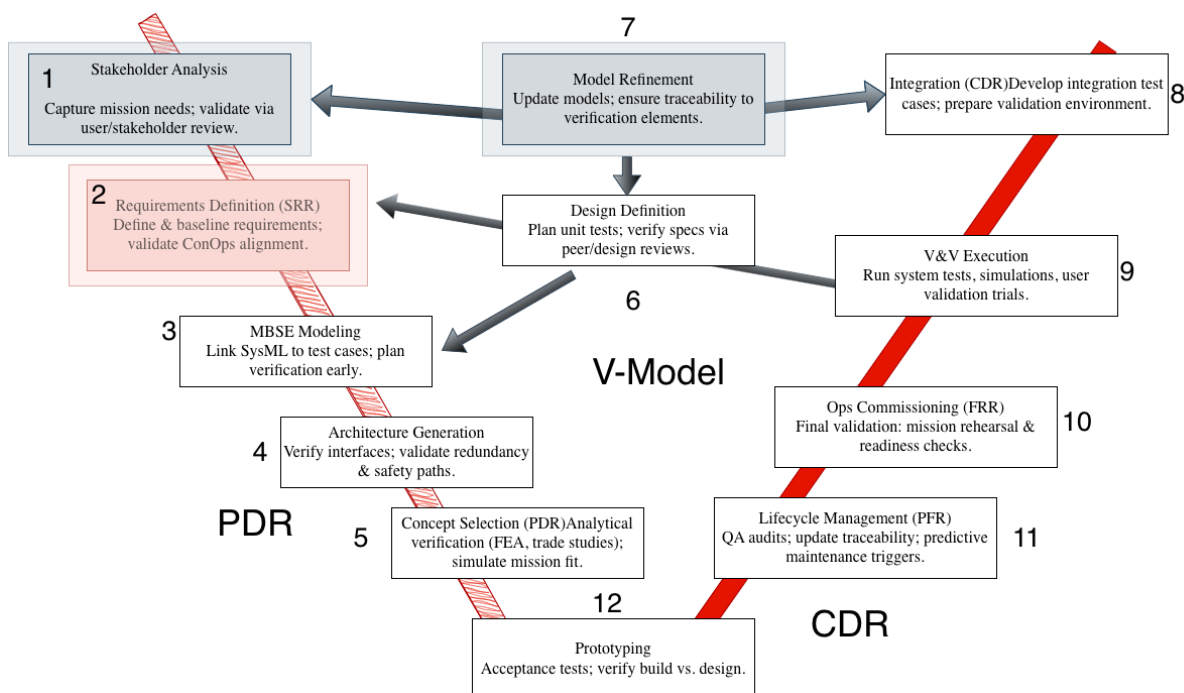


Figure 5 V-Model of LIMS

7.1.2. MBSE and the V-model

NASA's 2025 System Modelling Handbook extends the traditional V-model through the integration of model-based systems engineering (MBSE). MBSE employs SysML diagrams to represent requirements, design logic, analysis, and V&V artifacts, supporting a model-centric development approach. INCOSE (*insight_vol26-1_0329*) defines MBSE as the formal use of modelling to enable requirements, design, analysis and V&V across all life-cycle phases (Hart and Martin, 2015). Within SysML, the Requirements column directly supports specification development and V&V activities (*Nasa technical handbook*). In this scheme, MBSE is applied to generate verification and validation cases, requirements traceability matrix, and model-based test scenarios that link design elements to their respective validation steps. The handbook further provides metamodels and example diagrams for V&V configuration decomposition and indexing. Integrating MBSE strengthens maintainability, improves traceability, and enables early problem detection, reinforcing NASA's emphasis on independent evaluation throughout the development process.

7.1.3. Alignment with Standards

The V&V framework and MBSE integration described here conforms to the following key standards and guidance documents:

Table 10 Alignment with Standards

Standard / Guideline	Description
ISO/IEC/IEEE 15288:2015	Defines system life-cycle processes, requiring V&V to confirm design compliance and stakeholder fit
IEEE 1012:2024	Details V&V processes for systems, software, and hardware across multiple integrity levels
NASA Handbook 1009A (2025)	Extends MBSE with specific V&V requirements, planning, result documentation, and reporting
NASA SE Handbook (NPR 7123.1)	Describes the SE Engine, covering stakeholder engagement, requirements, verification and validation

7.1.4. Verification Methods

Test-Based Verification

Test based methods involve executing the system (or part of it) under defined conditions and observing the output, behaviour and performance. This is often the most direct and quantitative verification approach. As described in NASA's V&V guidelines (e.g., "Product Verification"), verification may include testing at the component, subsystem, and system levels.

Table 11 Verification Methods

Testing Type	Scope and Purpose	Key Features and Implementation
Unit Testing	Verifies individual components or software modules (e.g., thruster valves, flight control software) against their specifications	- Focus on functional correctness, performance metrics, and robustness to off-nominal inputs- Ensures each module behaves as intended under normal and edge-case conditions
Integration Testing	Verifies interfaces and interactions between subsystems (e.g., avionics, power, propulsion)	- Includes hardware-in-the-loop (HIL) and software-in-the-loop (SIL) simulations- Detects interface mismatches and communication issues- Artemis integration tests include interface verification, end-to-end communications, and countdown demonstration
System Testing	Verifies the complete capsule in a controlled, system-level environment	- Includes thermal vacuum tests, vibration tests, acoustic tests, structural static tests, and electromagnetic compatibility (EMC)- Conducted with flight-like hardware and software- Qualification tests must validate performance at worst-case thermal and vibration extremes
Acceptance Testing	Final validation of flight units prior to deployment	- Confirms workmanship, assembly quality, and basic functionality- Acceptance criteria include quantitative limits (e.g., heat shield thickness $\pm 5\%$, interface response time $\leq X$ ms)- Failures initiate corrective action and re-verification

Analysis-based Verification

Where physical testing is impractical, cost-prohibitive, unsafe, or cannot cover all combinations (e.g., extreme environments, rare fault conditions), analytical methods provide the necessary evidence. Such methods allow validation beyond tests or under complementary conditions.

Table 12 Analysis based Verification

Verification Method	Scope and Purpose	Key Features and Implementation
Mathematical Modelling and Simulation	Verifies compliance with design requirements where direct testing is impractical or incomplete	- Uses Finite Element Analysis (FEA), Computational Fluid Dynamics (CFD), orbital/flight dynamics, thermal and radiation models- Supports structural, thermal, aerodynamic, and environmental verification
Reliability, Risk, and Safety Analysis	Assesses system reliability and fault resilience under rare or hazardous conditions	- Includes Fault Tree Analysis (FTA), Failure Mode, Effects, and Criticality Analysis (FMECA), Monte Carlo simulations- Supports fault propagation analysis and redundancy/margin verification
Performance Budgeting & Parametric Analysis	Validates subsystem-level performance against design allocations	- Confirms mass, power, thermal load, bandwidth, latency, and response time budgets- Often conducted through MBSE-derived parametric models under nominal and worst-case scenarios
Verification by Similarity / Heritage	Reuses prior verification data for legacy systems with unchanged configuration	- Justified when heritage hardware/software has documented qualification evidence- Any modifications trigger additional analysis or re-testing to ensure ongoing compliance

Inspection / Review-Based Verification

Inspection and review-based methods systematically check design documents and components manually or through tools early in development. They provide a cost-effective way to detect problems before manufacturing or testing, reducing rework and improving design assurance.

Table 13 Inspection / Review Based Verification

Verification Subtype	Scope and Purpose	Key Features and Implementation
Design Reviews	Formal milestone-based assessments of system readiness at key lifecycle stages	- Includes Preliminary Design Review (PDR), Critical Design Review (CDR), Test Readiness Review (TRR), and Operational Readiness Review (ORR)- Evaluates completeness, consistency, traceability, testability, and maturity- Uses independent review boards or technical authorities to enhance objectivity
Peer Reviews and Walkthroughs	Informal yet structured reviews of technical artifacts by peers to detect early design flaws or documentation errors	- Applied to requirement specifications, architecture models, design drawings, software code, schematics- Identifies ambiguities, omissions, latent errors, non-testable or unclear requirements, and non-compliance with coding or design standards
Physical Inspections	Direct examination of hardware or assemblies for compliance with design and manufacturing specifications	- Includes visual and metrology-based inspection- Checks material conformity, workmanship quality, correct part installation, cable routing, labelling, and configuration- Equivalent to first-article or acceptance inspections in manufacturing environments
Documentation Reviews	Ensures quality and completeness of supporting documents critical to V&V execution and traceability	- Reviews traceability matrices (requirements ↔ design ↔ test), V&V plans, procedures, change logs, issue tracking, and test reports- Confirms consistency, completeness, and alignment across documentation sets

Formal Verification and Runtime Monitoring Integration:

A model-based validation approach was used for the Landing Impact Mitigation System (LIMS), where key requirements such as descent rate, parachute sequencing and impact attenuation were formally encoded and validated against safety properties. The verified model also generated runtime monitors to ensure real-time compliance. All system requirements were evaluated under a structured V&V framework (Bouhali *et al.*, 2024) aligned with ISO/IEC/IEEE 15288 using drop testing, ATD impact testing, environmental testing (*insight_vol26-1_0329*).

and fault injection to confirm performance, redundancy and robustness. The strategy ensured that all requirements were measurable, testable and traceable, mapped to validation methods meeting pass/fail criteria and documented in a controlled validation matrix. requirement-to-method

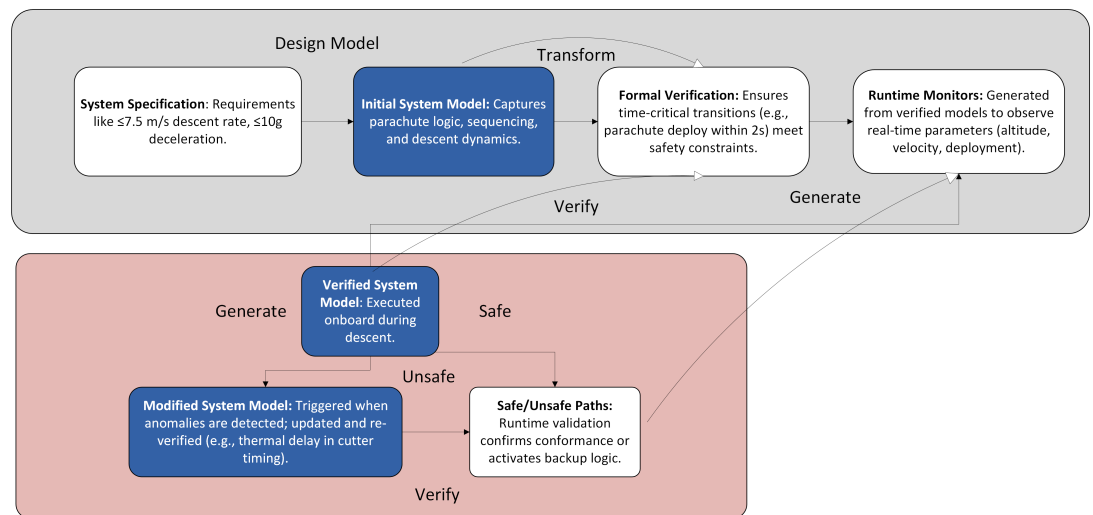


Figure 6 Formal Verification and Runtime Monitoring Integration:

traceability. Table A6 (Appendix) illustrates a multi-method V&V approach using thermal system testing to demonstrate how testing, simulation, and inspection collectively ensure design compliance

Key Recommendations: The V&V plan should specify at least one verification method (test, analysis, inspection, or demo) as required, with ≥ 3 methods for critical functions. All activities must follow defined criteria, maintain configuration controls and clearly track test article lineage. A complete V&V package covering reports, traceability, reviews and non-conformities should support certification and audits.

7.2. Maintenance Plan

A robust maintenance strategy is critical to maintaining safety, performance, and mission readiness throughout the capsule's entire lifecycle. Maintenance activities are classified as preventive, corrective, adaptive and predictive. Preventive maintenance includes scheduled servicing such as filter replacement, sensor calibration, software updates and seal inspection guided by use cycle and age-reliability analysis rather than MTBF alone. Safety-critical objects (for example, pyrotechnics) use non-destructive inspection and modular design for maintenance. Corrective maintenance addresses detected failures through fault isolation, component replacement, software patching, and emergency reconfiguration, followed by root cause analysis and re-verification to restore compliance. Adaptive maintenance modifies systems to meet emerging environments or standards, such as thermal optimization or technology upgrades, which require threat assessments and full V&V. Predictive maintenance uses real-time telemetry, diagnostics, and machine learning to predict failures and optimize servicing, reducing downtime and increasing availability (Weiss *et al.*). Together, these integrated strategies ensure long-term reliability and mission success and in more detail present in Appendix A.9Table.

7.3. Quality and Standards

These requirements are evaluated through quantitative metrics and verified through testing, analysis, and simulation: **Reliability (MTBF and Availability):** Critical subsystems – such as life-support, propulsion, and avionics – must achieve specified mean time between failures (e.g., $\geq 10^6$ hours) and meet defined availability thresholds to ensure mission readiness. Reliability is verified through reliability analysis, failure trend monitoring and lifecycle performance assessment. **Safety (risk of loss of crew/loss of vehicle):** NASA has defined an acceptable loss-of-crew (LOC) risk limit of 1 in 270 for a 210-day mission. This requirement informs the system architecture, requiring redundancy, fault tolerance, and proactive threat controls (Boyer, Bigler and Rogers). Compliance is demonstrated through probabilistic risk assessment and fault-tree analysis. **Usability and human-factors metrics:** The crew interface must support task completion with a high success rate ($\geq 95\%$) and low error rate ($\leq 10\%$) during acceptance testing and operational simulation (Rhodes, Adams and McCleskey). Usability is quantitatively evaluated using tools such as the System Usability Scale (SUS),

workload index, and situational awareness assessment. **Performance Criteria:** Mission-critical functions are validated according to defined limits, including re-entry g-load limits (≤ 4 g), communication latency (< 300 ms), and docking alignment tolerances. These parameters ensure mission feasibility and crew survivability in dynamic conditions. Maintenance and Support: Maintenance metrics such as mean time to repair (MTTR) are specified to guide support planning. Design access requirements are implemented to enable efficient servicing and modular replacement of components during scheduled or corrective maintenance tasks (Rhodes, Adams and McCleskey).

7.4. Applicable Norms and Standards:

Table 14 Applicable Norms and Standards

Standard / Guideline	Applicability
ISO/IEC/IEEE 15288:2015 – Systems and Software Engineering — System Life-Cycle Processes	Defines life-cycle processes; requires verification and validation within the Evaluation process. Provides a framework for aligning V&V with lifecycle stages.
IEEE 1012:2024 – Standard for System and Software V&V	Specifies V&V processes and rigor levels for software and hardware products. Guides the creation of V&V plans, including independence and documentation requirements.
NASA Handbook 1009A (2025) – Systems Modelling Handbook	Integrates MBSE and SysML with the NASA SE Engine; expands the scope to include V&V requirements, planning, results and reports. Provides metamodels and example diagrams for V&V cases and verification matrices.
ISO 9001:2015 – Quality Management Systems	Requires documented quality policies, procedures, audits and continual improvement. Ensures the V&V process is managed within a controlled QMS.
IEC 61508:2010 – Functional Safety of Electrical/Electronic/Programmable Systems	Provides safety lifecycle processes for safety-critical systems. Emphasises minimizing faults early and uses reliability/availability/maintainability/safety (RAMS) analyses. Mandates collaboration among systems engineers, designers and product assurance to ensure safe operation.
NASA-STD-8739 and NASA Software Assurance Standards	Provide software assurance requirements, verification independence, coding standards and test coverage criteria.
DO-178C / ED-12C (2012)	Avionics software certification standard; defines levels of rigor based on software criticality. Relevant for flight control and guidance software.
DO-254 (Design Assurance Guidance for Airborne Electronic Hardware)	Governs design assurance for electronic hardware. Applicable to safety-critical avionics boards.
ECSS Standards (e.g., ECSS-Q-ST-10 and ECSS-Q-ST-20)	European Cooperation for Space Standardization guidelines for product assurance and quality assurance. Provide additional criteria for quality control, reliability and documentation.

8. Human Design and Human Factors

Landing systems integrate physical and cognitive human factors to enhance crew safety, comfort, and performance during take-off and landing. Physically, energy-absorbing seats, strutting struts and passive damping keep impact forces within survivable limits while reducing vibration and acoustic risk (Boring, 2012). Interior ergonomics, visibility, accessibility and thermal comfort conform to human-systems integration standards, ensuring operational utility even under stress or after long missions. Cognitively, workload is reduced through automation and task simplification, supported by clear status indicators, go/no-go logic, multimodal cues and consistent crew roles. TLX-based workload analysis confirms low mental load during nominal operations, while training and communication protocols support decision making in nominal cases. Quantitative assessment of human reliability is performed using THERP, in which error-prone tasks such as manual override or chute deployment are integrated into fault trees and minimized through dual crew confirmation, automation backups, interlocks, and interface protection measures (Lam and Chan, 2023).

Crew input acts as a redundant safety layer, contributing to system fault tolerance and a high probability (>99.9%) of safe landing. The main design responses to physical, cognitive and reliability-related human factors are detailed in Appendix Tables A.10 to A.14.

Design Recommendations: For the Earth-return capsule focus on effective human-systems integration to ensure crew safety and mission reliability. Critical controls and basic data (altitude, velocity, system status) should be clearly displayed, with emergency functions centrally placed and easily identified. The ergonomic design – using tactile, color-coded controls and a high-contrast display – enhances usability under stress. Adjustable, impact-absorbing seats accommodate various crew sizes and maintain accessibility. Automation manages nominal descent, with manual override available for critical events, supported by onboard decision support. Stress-tested crew training, clear checklists and role clarity reduce human error possibilities (HEP). Continuous human-in-the-loop testing (e.g., VR, mockups) supports interface refinement. Further details are given in Appendix Table A.14.

9. Integrated Discussion

The systems engineering process for the LIMS Capsule maintained strict traceability between requirements, architecture, and validation throughout development. Each design decision was based on stakeholder needs, confirmed by a bi-directional traceability matrix. Tools such as QFD, trade studies, FTAs and V&V were iteratively applied to ensure consistent, data-driven results. QFD translated critical requirements such as $\leq 5\text{ft/s}$ landing speed and 99.9% reliability into architectural features such as parachutes, airbags and retrorockets, while trade studies balanced safety, mass and complexity (Li, Lockett and Lawson, 2020). The FTA identified high-risk elements (for example, airbag inflation, $P = 6.1 \times 10^{-2}$), prompting design mitigations such as dual inflation paths. Human error risk (HEP ~ 0.01) Informed interface design and crew redundancy. V&V links each requirement to physical testing or simulation (e.g., drop testing, thermal vac), ensuring full validation. Key insights include managing reliability-scale trade-offs, integrating human-system interactions, resolving subsystem interdependencies, and implementing configuration controls. Details are provided in Appendix Table A.15 (Architecture-Requirement Mapping) and Appendix Table A.16 (Technical Insights).

Conclusion: This project demonstrates that a structured, requirements-driven systems engineering (SE) approach enables the development of a safe, reliable, and certified landing impact mitigation system (LIMS) for a crew capsule. Based on formal requirements such as touchdown velocity $\leq 7.5\text{m/s}$, $\leq 10\text{g}$ deceleration, $\geq 99.9\%$ reliability, and full redundancy the final architecture (triple parachutes, retrorockets, airbags, stroking seats) was developed using QFD, trade-off studies (AHP, Pugh), and fault tree analysis. Human error and failure risks are minimized through redundant triggers, protected interfaces, and automation. The validation followed the V-model with drop testing, thermal/vacuum testing, software-in-the-loop testing, and human-factors validation. Human-system integration was already embedded, enabling automation with manual overrides. The SE process ensured that all design choices were traceable, risk-informed and test-validated providing a transferable model for future safety-critical aerospace systems.

References:

insight_vol26-1_0329

Nasa technical handbook

Boring, R.L. (2012) *Fifty years of THERP and human reliability analysis PSAM11*

Bouhali, I. *et al.* (2024) 'Model-based systems engineering and safety assessment: A workflow for mechatronic systems design', *Systems Engineering*, Available at: <https://doi.org/10.1002/sys.21791>.

Boyer, R.L., Bigler, M. and Rogers, J.H. *Probability of loss of crew achievability studies for NASA's exploration systems development*

Childress, S.D., Williams, T.C. and Francisco, D.R. (2023) 'NASA space flight human-system standard: Enabling human spaceflight missions by supporting astronaut health, safety, and performance', *NPJ Microgravity*, 9(1), pp. 31–2. Available at: <https://doi.org/10.1038/s41526-023-00275-2>.

Encyclopedia (2019) 'SEH 2.0 fundamentals of systems engineering',

Evans, C. *et al.* *Human rating the orion parachute system*

Fasanella, E.L. (2008) *Multi-terrain earth landing systems applicable for manned space capsules*

Hart, L.E. and Martin, L. (2015) *Introduction to model-based system engineering (MBSE) and SysML*

Hirshorn, S.R. (2007) *National aeronautics and space administration*

Lam, S. and Chan, A. (2023) *Human reliability analysis in aviation accidents: A review.*

Lee, T.J., Mckinney, J. and Corliss, J.M. *Airbag landing impact performance optimization for the orion crew module*

Li, T., Lockett, H. and Lawson, C. (2020) *Using requirement-functional-logical-physical models to support early assembly process planning for complex aircraft systems integration* Elsevier BV.

Michael Ryan (2023) *Guide to writing requirements*

NASA (2006) 'NASA procedures and guidelines',

NASA 'How to write a good requirement— checklist',

Rhodes, R.E., Adams, T.C. and McCleskey, C.M. *Space transportation system availability requirement and its influencing attributes relationships*

SHEN, X., WANG, X. and LIU, C. (2025) 'A review of airbag landing system for spacecraft', *Chinese Journal of Aeronautics*, 38(8), pp. 103569. Available at: <https://doi.org/10.1016/j.cja.2025.103569>.

Shook, L., Timmers, R. and Hinkle, J. (2009) 'Second generation airbag landing system for the orion crew module', Available at: <https://doi.org/10.2514/6.2009-2989>.

Sutherland, J. *et al.* *Systems engineering and the V-model: Lessons from an autonomous solar powered hydrofoil*

Tutt, B. *et al.* *A summary of the development of a nominal land landing airbag impact attenuation system for the orion crew module*

Weiss, B.M. *et al.* *Leveraging smart maintenance for satellite health preservation*

Whitaker, R. (1987) 'The analytic hierarchy process – what it is and how it is used', *Mathematical Modelling*, 9, pp. 161–176. Available at: [https://doi.org/10.1016/0270-0255\(87\)90473-8](https://doi.org/10.1016/0270-0255(87)90473-8).

Yu, H. *et al.* (2015) 'A new landing impact attenuation seat in manned spacecraft biologically-inspired by felids', *Chinese Journal of Aeronautics*, 28(2), pp. 434–446. Available at: <https://doi.org/10.1016/j.cja.2015.02.012>.

Zapata, E. (2016) *A quality function deployment method applied to highly reusable space transportation*

Appendices

Appendix A:

Table A1 Justification of requirements

Aspect	Justification Summary	Related Req. IDs
Deceleration Capability	Orbital velocity (~18,000 mph) must reduce to a few ft/s; justifies landing speed and g-load limits. Multi-system deceleration is historically validated.	LIMS-FR-0001, FR-0002, FR-0004
Redundancy & Fault Monitoring	NASA mandates single-failure tolerance and crew alerts; telemetry and manual overrides follow best practices (e.g., Orion, Gemini).	LIMS-DR-0017, OP-0011
Crew Impact Limits	Acceleration must remain within biomechanical thresholds (<12 g); seats and restraints mitigate trauma. FAA 2023 aligns with this.	LIMS-HF-0012
Environmental Robustness	Requirements address operation under vacuum, heat, wind, and sea states. Validated by Orion and SpaceX drop/wind tunnel tests.	LIMS-EN-0009, DR-0018
System Access & Maintenance	Maintainability built into design (modular, inspectable). NASA and FAA mandate support for inspection, repair, and diagnostics.	LIMS-LS-0014

Table A2 Requirement quality check

Req. ID	Requirement Statement	Type	Source Objective	Verification Method	Verification Criteria	Linked Subsystem
LIMS-FR-0001	The system shall reduce the capsule's vertical landing velocity to ≤ 7.5 m/s.	Functional	Crew Safety	Test (Drop simulation)	Velocity ≤ 7.5 m/s at impact	Parachute Assembly System
LIMS-FR-0002	The system shall attenuate landing impact forces to ≤ 10 g on crew vertical axis.	Safety	Human Tolerance Limit	Test + Simulation	Peak deceleration ≤ 10 g	Crew Seats, Shock Absorbers
LIMS-IF-0008	The system shall safely disarm parachutes post-landing to avoid dragging.	Interface	Crew Recovery Safety	Inspection + Test	Auto-release of parachutes within 5 seconds	Parachute Release Mechanism
LIMS-HF-0012	The system shall use impact-attenuation seats to limit injury risk.	Human	Crew Biomechanical Protection	Test	Force transmission $\leq$ max tolerable levels	CIAS (Crew Impact System)
LIMS-OP-0010	The system shall deploy automatically based on sensor logic during descent.	Operational	Autonomous Safety Deployment	Test + Simulation	Trigger logic works at 25k/9k feet	Descent Control Subsystem
LIMS-MR-0005	The system shall function safely in both land and water landings.	Mission	Redundancy in Touchdown Mode	Test + Analysis	Compliance in both terrain scenarios	Impact Attenuation, Floatation

Table A3 Customer Requirements (“Whats”)

Customer Requirement (CR#)	Description	Linked Req. IDs	Importance Summary
CR-01	Reduce impact loads to protect crew	LIMS-FR-0002, HF-0012	High – critical for injury prevention
CR-02	Limit terminal landing velocity ≤ 7.5 m/s	LIMS-FR-0001	High – vital for safe touchdown
CR-03	Provide fault-tolerant deceleration system	LIMS-FR-0003	High – ensures redundancy
CR-04	Airbag to remain inflated ≥ 2 hours post-landing	OP-0012, EN-0009	Medium – stabilisation after landing
CR-05	Cushioning failure probability $< 6\%$	LIMS-PA-0016	High – required for mission reliability
CR-06	Comply with human-factor constraints	LIMS-HF-0012	High – supports crew survivability
CR-07	Enable auto and manual deployment modes	OP-0010, OP-0011	Medium – ensures operational flexibility

Table A4 Technical Characteristics (“How’s”)

Technical Characteristic (TC#)	Description	System Influence
TC-01	Parachute Area	Controls terminal descent rate
TC-02	Retro Thrust Capability	Augments deceleration, reduces impact
TC-03	Airbag Inflation Pressure	Dictates touchdown load absorption
TC-04	Airbag Endurance	Supports post-landing stability
TC-05	Structural Damping	Reduces force transfer to crew
TC-06	Redundant Control Reliability	Mitigates logic failure risk
TC-07	Manual Override Functionality	Ensures off-nominal deployment
TC-08	Sensor Fusion Accuracy	Enhances timing via integrated data

Table A5 Key Internal and External Hazards

Hazard	Description and Potential Cause	Linked Safety Requirement(s)
Parachute deployment failure	Main or backup parachute fails to deploy due to mechanical jam, mis-rigging, or mis-timed release; may result from sensor or actuator malfunction.	FR-0001: Capsule must reduce vertical landing velocity to ≤ 7.5 m/s (loss of parachute jeopardises descent rate). FR-0003 : System must tolerate single-point failure via redundancy (failure of one chute must not be catastrophic).
Retrorocket failure	Thrusters misfire or do not ignite due to fuel leak, clogged valves, ignition circuit failure, or power loss.	FR-0001/FR-0004: Ensure safe landing velocity and multi-stage deceleration sequence; rockets are part of the second stage. OP-0010 : Automatic deployment must command thrusters at the correct time.

Airbag failure	Airbag punctures, leaks, or fails to inflate due to valve jam, gas generator fault or tear.	FR-0001/FR-0002: Cushions final impact and keeps deceleration within 10 g. FR-0005 : System must provide safe landing on both land and water; airbag aids water buoyancy.
Structural attachment failure	Failure of parachute risers, harnesses, or capsule attachment points due to overload, corrosion or material defect.	PH-0015 (structural integrity): Design must withstand loads with appropriate safety margins. FR-0003 : Attachments must not constitute single-point failures.
Sensor/altimeter malfunction	Barometric, radar or inertial sensors provide erroneous altitude/velocity data; control logic may trigger deployment too early or too late.	OP-0010: Automatic deployment logic must use accurate sensors; failure could violate FR-0001. PA-0016 (reliability): Sensors must meet reliability targets.
Electrical or power system fault	Loss of power bus, battery depletion or wiring short disables thrusters, airbags or controllers; single bus powering multiple backups introduces common-cause vulnerability.	FR-0003/PA-0016: Redundancy must not be nullified by common-cause power loss; components must meet reliability requirements.
Human error	Mis-packing of parachutes, incorrect installation, or erroneous manual override of deployment. NASA cautions that single human errors appearing in a minimal cut set indicate weak links that deserve prevention priority.	OP-0011: Manual overrides and status indicators must be intuitive and fail-safe. Quality and training requirements : Maintenance and packing procedures must be validated to prevent single-point human errors.
Fire or explosion hazard	Propellant leak, improper handling of retrorocket fuel, or short circuits could ignite, damaging the capsule or injuring crew.	FR-0001/FR-0005: Propulsion systems must be designed to prevent accidental ignition. EN-0009 : Components must operate safely across environmental conditions.
Toxic gas or smoke	Gas generator or airbag chemicals may leak into the cabin, creating toxic atmosphere.	HF-0012: Capsule environment must remain safe for crew; deceleration system must not introduce toxic substances.
External: atmospheric conditions (wind, turbulence)	High winds, gusts or turbulence can collapse parachutes, entangle lines, or cause oscillations.	FR-0003/FR-0004: System must tolerate adverse wind conditions and still meet deceleration requirements.
External: rough terrain or water conditions	Impact on rocky ground may puncture airbags; high sea state may flip or inundate capsule.	FR-0005: Must provide safe land and water landings; HF-0013 : Capsule must remain upright or self-right after landing.
External: lightning/electromagnetic environment	Lightning strike or strong electromagnetic fields can disrupt electronics or ignite propellants.	EN-0009: Systems must withstand environmental extremes (temperature, pressure, EMI).
External: debris or bird strike	Falling debris, hail, or bird strikes could damage parachute fabric or sensors.	FR-0003: Redundancy must accommodate damage to one element; materials must be resilient.
External: temperature extremes and contamination	Extreme cold, heat, dust or moisture can degrade parachute materials and sensors over time. The first step in Preliminary Hazard Analysis is to identify such hazardous elements.	EN-0009: Deceleration system must operate under specified environmental ranges; materials and electronics must be rated accordingly.

Table A6 Evaluation of LIMS System Requirements:

ID	Requirement Statement	Performance Criteria	Verification Method	Acceptability Criteria
LIMS-FR-0001	The system shall reduce the capsule's vertical landing velocity to ≤ 7.5 m/s under nominal conditions.	Vertical landing speed ≤ 7.5 m/s	Drop tests and high-fidelity simulation	Measured average descent speed ≤ 7.5 m/s in at least 95% of trials.
LIMS-FR-0002	The system shall attenuate impact such that max deceleration $\leq 10g$ in vertical axis.	Vertical deceleration $\leq 10g$	Accelerometer data from test dummies	Max g-force $\leq 10g$ in 100% of operational profiles.
LIMS-FR-0003	The system shall incorporate redundant deceleration elements.	Ability to land safely after failure of one decelerator	Fault-injection simulation, failure mode test	Safe landing verified in all tested failure modes.
LIMS-FR-0004	The system shall perform multi-stage deceleration (e.g., drogue + main chute sequence).	Sequenced deployment: 2+ stages	High-speed camera + sensor logs during deployment	Each stage triggers on time with full deployment.
LIMS-MR-0005	Shall support safe landing in both water splashdown and land touchdown scenarios.	Structural integrity on both terrain types	Terrain simulation + dual-scenario tests	No critical damage in either scenario across 3 trials.
LIMS-OP-0010	The system shall deploy automatically at correct point using sensor logic.	Altitude-triggered sequence automation	Altitude-simulated tests with barometric and GPS input	Fully autonomous deployment in all test cases.
LIMS-OP-0011	The system shall provide deployment status indicators and manual override capability.	Indicator display + manual abort switch	UI functional test + emergency drills	Status correct in all cases, override works in <5 seconds.
LIMS-HF-0012	Crew impact acceleration must be within survivable human limits using crew-centric safety (stroking seats, etc.)	Spinal g-load $<$ threshold; seat energy absorption	Anthropomorphic test dummies (ATD) + seat sensor logs	Max spinal g-load $\leq$ safe limit (validated by ATD data).
LIMS-EN-0009	Operate effectively in high winds, rain, and rough sea states.	Wind up to 35 knots; wave height up to 2m	Wind-tunnel and sea-state tank tests	Full system functional under specified atmospheric conditions.

Table A7 Test Execution, Verification Criteria, and V&V Deliverables

Aspect	Description and Implementation Considerations
Pass/Fail Criteria	Each test or analysis must define explicit pass/fail (or acceptability) criteria traceable to specific requirement IDs.
	Examples include thermal cycle limits, structural load tolerances, latency thresholds, performance margins, and error rates.
Results Documentation	Outcomes of all verification activities (tests, analyses, inspections) must be documented in formal reports.
	Each result must be linked to the corresponding requirement identifier for traceability.
Verification Matrix	A maintained Verification Matrix (also called Traceability Matrix) must map each requirement to:
	- Verification method(s)
	- Test/analysis IDs
	- Status (pass/fail)

V&V Deliverables	- Non-conformance disposition
	- Final acceptance outcome.
	This matrix is a controlled, baseline document.
	The complete V&V Package for certification or release should include:
	- Test reports and analysis reports
	- Inspection records
	- Configuration status
	- Final verification matrix
	- Non-conformance or waiver log
	- Reviewer signoffs and approvals

Tabel A8 Example V&V Implementation for Diagnostic Platform

V&V Method	Implementation for Thermal Requirement
Requirement	“The thermal cycler shall heat the sample to 95 °C ± 0.5 °C and hold for 30 seconds, with ramp-up time ≤ 5 s.”
Test	Empirical thermal cycle testing using calibrated thermocouples over multiple cycles; verify temperature, hold time, and ramp-up time across operational and worst-case ambient conditions.
Analysis	Thermal simulation (e.g., FEA or thermal model) to assess heat distribution and gradients under worst-case ambient extremes; verify thermal uniformity and margin compliance.
Inspection / Review	Design review of heater layout and insulation; inspection of assembled hardware for conformance to drawings (thermal contact, insulation, heater placement); review of traceability matrix.

Table A9 Maintenance Strategy Overview for LIMS

Maintenance Type	Purpose	Key Tasks	Safety/Feasibility Measures
Preventive	Avoid failures before they occur	- Replace CO ₂ scrubbers, filters after flight hours- Inspect & retorque fasteners- Apply software/firmware updates- Calibrate sensors regularly	- Non-destructive inspections (e.g. for pyro bolts)- Modular hardware design for easy access
Corrective	Restore functionality post-failure	- Isolate & repair failed components- Apply bug fixes with regression testing- Execute in-flight emergency repairs- Document & re-verify changes	- Formal root-cause analysis- Configuration management control
Adaptive	Modify system for new conditions	- Update software for lunar or new environments- Upgrade sensors or communication units- Implement new regulatory standard changes	- V&V of updated components- Hazard analysis of all updates
Predictive	Forecast & prevent future failures	- Monitor vibration, temperature, battery trends- Use ML-based analytics for fault prediction- Pre-empt component degradation	- Ground analytics dashboard- Data-driven trigger for maintenance actions

Table A10 Astronaut Role by Landing Phase

Landing Phase	Automated Functions	Crew Tasks	Manual Intervention Points
Approach Phase	- Drogue parachute deployment via onboard sensors	- Monitor system status	- Manual override of parachute deployment if automatic trigger fails (e.g., altitude not reached)
	- Attitude control via thrusters	- Oversee re-entry trajectory - Maintain capsule orientation	- Abort command if required
Braking Phase	- Main parachute deployment sequencing (e.g., drogues at ~25,000 ft, mains at ~9,000 ft)	- Monitor descent rate, altitude, and parachute status	- Deploy backup main parachute if inflation fails (e.g., by 3,000 ft)
		- Confirm deployment signals	- Initiate contingency descent if severe malfunction occurs
Descent Phase	- Capsule stabilization via thrusters	- Monitor backup systems (airbag pressure, retrorocket status)	- Manually trigger cushioning system if automatic sensors fail
	- Automatic arming of retrorockets/airbags	- Maintain situational awareness	- Communicate anomalies to ground
Touchdown Phase	- Retrorockets fire at low altitude (~<3 ft)	- Assume bracing posture	- Abort or early fire of retrorockets if terrain hazard detected
	- Post-landing safe mode initiation	- Confirm landing indicators	- Manual parachute release post-touchdown
		- Prepare for post-landing safing	
Contingency / Abort	- None (relies on pre-armed backup systems)	- Trigger remaining backups	- Damage control only (e.g., harness tightening, activating residual systems)
		- Brace for impact	
		- Execute emergency egress if needed	

Table A11 Physical Human Factors in Landing System Design

Category	Design Provisions	Outcome / Performance Target
Acceleration & G-Forces	- Peak deceleration limited to ~3–4 g during re-entry- Final impact reduced to ~0.5–2 g using retrorockets and energy-absorbing seats (e.g., CIAS)- Seats mounted on stroking struts	- Maintains spinal loads within NASA tolerances- Prevents injury; ensures survivable impact forces
Vibration & Shock	- Damped seating system tuned to avoid 4–8 Hz resonance- Parachute sway minimized via reefing and finlets- Retrorocket impulse buffered by seats and airbags	- Prevents motion sickness and loss of motor control- Cabin vibration kept <0.1 g in sensitive frequency bands
Visibility & Lighting	- Strategically placed windows for horizon and parachute visibility- Anti-glare coatings, dimmable interior lights, dusk landing aids (e.g., floodlights)	- Ensures situational awareness- Maintains visual acuity under variable lighting
Ergonomics & Reach	- Controls positioned within 5th–95th percentile reach- Suited reach verified; override switches gloved-operable- No foot pedals; all manual actions within seated reach	- Full accessibility during restraint- Quick manual intervention possible under stress or emergency
Noise & Acoustics	- Interior acoustic insulation- Helmets/headsets with attenuation- Pyrotechnics isolated via structural damping	- Peak impulse noise <140 dB- Continuous noise <100 dBA- Maintains communication and hearing safety
Thermal Comfort	- ECLSS maintains 20–25 °C and ~50% RH- Backup fans and coolant loops- Reflective insulation for post-landing heat	- Cabin remains within survivable and tolerable thermal limits- Avoids heat stress during delayed recovery

Air Quality & Atmosphere	- Redundant CO ₂ scrubbers and oxygen supplies- Backup chemical oxygen candles available	- Breathable atmosphere maintained through all descent phases, even in power-loss scenarios
-------------------------------------	---	---

Table 12 Key Cognitive Human Factors in Landing Design

Category	Design Provisions	Outcome / Benefit
Workload Management	- TLX analysis shows low-to-moderate load during nominal descent	- Reduces cognitive demand and multitasking
	- Crew roles defined (Commander: monitor; Pilot: comms/checklists)	- Ensures actions are simple and trained
	- Manual actions are minimal and time-buffered	
Situational Awareness	- Central flight display (altitude, descent rate)	- Maintains awareness of vehicle state
	- Status indicators for parachutes, retrorockets, airbags	- Enables immediate recognition of deviations or failures
	- Auditory callouts for key events	
Decision Aids / Go/No-Go	- Predefined altitude-based triggers (e.g., 3000 ft for backup deploy)	- Enables rapid decision-making with minimal cognitive processing
	- Simple checklists and visual cues (e.g., "MAIN CHUTE FAILURE" alert)	- Supports timely interventions
	- Crew has authority to override automation	
Training & Simulation	- Repetitive simulator training across nominal and emergency cases	- Builds procedural memory and trust
	- Cue-response procedures reduce need for real-time problem-solving	- Enhances response under stress
Communication Protocols	- Defined crew roles reduce radio traffic confusion	- Avoids distraction at critical moments
	- Internal comms via noise-cancelling mics	- Ensures synchronized crew performance
	- Ground comm lockout during final 30 seconds	
Fatigue & Stress Handling	- Assumes reduced cognitive function post-mission	- Mitigates effects of stress and fatigue
	- Increased O ₂ and thermal comfort during re-entry	- Ensures safety despite degraded human performance
	- Automation handles complex failures	
Redundancy & Recovery	- Backup displays, manual instruments (e.g., altimeter, stopwatch)	- Maintains operability in degraded mode
	- Glow-in-the-dark markings, low-power lights in blackout scenarios	- Prevents total situational awareness loss

Table A13 Human Reliability Elements and Design Responses

Aspect	Details	Mitigation / Design Response
Assessment Method	THERP used to assign Human Error Probabilities (HEPs) for each critical task	Applied standard HRA tables; adjusted using stress, time, training as Performance Shaping Factors
Typical HEP Values	Well-cued actions: 0.001–0.01; complex or untrained actions: 0.03–0.1	Limited interface complexity; minimized novel tasks

High-Risk Actions Identified	- Manual backup chute deployment	Audible/visual cues, redundant crew roles, automation backup
Fault Tree Integration	- Abort of retrorockets	
	- Post-landing chute release	
	Human failure paths (e.g., “crew fails to deploy backup”) embedded in overall FTA	Quantitative reliability improved via dual paths: human + automation
Error Tolerance Design	System does not rely solely on crew action for critical events	Redundant automatic triggers; guarded manual overrides
Commission Errors Prevention	e.g., disabling retrorockets at wrong time	Dual-crew confirmation; interlock logic; distinctive control design
Cross-Verification	Implemented two-person rule for critical actions	THERP-based risk reduction: omission error drops from 0.01 → 0.001
Interface Safeguards	Unique shapes, colours, tactile identifiers for critical controls	Prevents misidentification and accidental activation
Reliability Impact	Crew acts as a safety layer — risk of total parachute failure drops to $\sim 4e-7$	Exceeds 99.9% system success requirement
Human Recovery Paths	System tolerates minor human errors (e.g., redundant chute deployment or premature cut)	“Fail-soft” architecture allows system-level recovery
Training-Based HEP Reduction	All emergency procedures trained and rehearsed	Prevents high HEP due to unfamiliarity (HEP capped ≤ 0.01)
Human-In-The-Loop Redundancy	Actions like chute deployment, system inhibit, are both automated and manually accessible	Reduces single-point failure dependence
Design Rule	No single human action can lead to unrecoverable failure	Fault-tolerant design with automation catch-ups and manual overrides

Table A14 Key Human-System Design Recommendations

Category	Design Recommendation	Rationale / Basis
Interface Layout	Prioritize altitude, descent rate, and landing system status on primary displays; emergency controls (e.g., backup chute) must be distinct, guarded, and centrally reachable.	Reduces reaction time and error risk during time-critical scenarios; supports situational awareness.
Control & Display Ergonomics	Use color-coded (e.g., red/yellow), tactilely distinct controls; apply HUD or symbolic display for descent path; large font and high contrast for readability.	Ensures visibility under vibration, suit constraints, and variable lighting.
Seating & Restraints	Energy-attenuating seats with 5-point harnesses; adjustable geometry to fit 5th–95th percentile crew; include stroking mechanisms and head/lumbar support.	Distributes G-loads safely and maintains reach envelopes for critical control access.
Manual vs. Auto Control	Default to automation; retain manual override for critical systems (e.g., chute deploy, retrofire inhibit) with simplified single-action mechanisms.	Minimizes error in routine operations while allowing human recovery from anomalies.
Decision Support	Implement simple onboard advisory logic to suggest crew actions when anomalies arise.	Enhances human decision-making under stress; improves cognitive performance during off nominals.

Training Strategy	High-fidelity landing simulators; repeated practice of failure scenarios; cross-role competency; stress inoculation techniques (e.g., high G, task saturation).	Reinforces procedural recall and decision-making under pressure; lowers Human Error Probabilities (HEPs).
Crew Procedures	Standardized checklists for emergencies (e.g., “Parachute Fail”); posted in cockpit and rehearsed regularly.	Reduces cognitive workload; provides clear action steps during anomalies.
Crew Assignment & Prep	Assign roles based on simulator performance and operational experience; G-load exposure training recommended.	Ensures critical tasks are handled by the most proficient crew member; prepares crew for physical loads.
Iterative Human Testing	Conduct continuous human-in-the-loop testing (mock-ups, VR, live simulations) for interface refinement.	Captures usability issues before final production; supports user-centered design validation.
Workload and Mode Clarity	Use clear “Auto/Semi-Auto/Manual” indicators; always ensure mode awareness.	Prevents mode confusion and supports supervisory control structure.

Table A15 Architecture-requirement consistency across methods

Requirement ID	Requirement Summary	Architecture Elements Addressing it	Methods Ensuring Compliance
LIMS-FR-0001	Limit landing impact accel $\leq 10 \text{ m/s}^2$	– Parachute system (dual mains)	– Analysis (landing dynamics calculation)
		– Airbag cushions	– Test (drop test with dummies)
		– Stroking crew seats	
LIMS-FR-0003	No single-point failure (redundancy)	– Redundant parachutes (3 mains)	– FTA (safety analysis for fault tolerance)
		– Backup parachute	– Inspection (redundancy checklist)
		– Dual gas supply for airbags	
LIMS-HF-0012	Crew impact within human tolerance (seat design)	– Energy-absorbing crew seats (CIAS)	– Test (seat drop test, NASA standard)
		– 5-point harness	– Analysis (crew injury risk modelling)
LIMS-OP-0010	Automated landing sequence (no crew input needed)	– GNC software for auto deployment	– Simulation (end-to-end auto landing)
		– Altitude and timing sensors	– Demo flight (uncrewed test)

Table A16 Key Insights from the Integrated Systems Engineering Process

Topic Area	Technical Insight / Key Point	Numerical / Technical Detail
Structured SE Process	SMART requirements anchored design; iterative QFD $\rightarrow$ trade studies $\rightarrow$ FTA $\rightarrow$ V&V ensured coherence.	Added requirement after FTA: cushion reliability due to $p = 6.1 \times 10^{-2}$ airbag failure.
Requirements vs. Trade-offs	Reliability vs. mass constraints shaped subsystem choices (e.g., retrorockets + airbags).	Redundancy justified despite added mass; retrorocket timing set to avoid chute interference.
Human–System Interaction	Human error modelled via HEP integrated into FTA; interfaces designed for error tolerance.	HEP ≈ 0.01 for omission errors; critical controls uniquely shaped and guarded.
Safety & Redundancy	Risk-driven redundancy applied only to critical elements (parachutes, descent control, cushioning).	Reliability target $\geq 99.9\%$; triple parachute config tolerates one failure ($p = 4 \times 10^{-3}$ per chute).
Subsystem Interaction	Identified cross-effects requiring mitigation: pyro shock, thermal loads, timing conflicts.	Added electrical isolation, thermal shielding, and event-sequencing constraints.

Documentation & Control	Traceability matrix ensured all requirements mapped to architecture and V&V tasks.	Updates propagated across architecture diagrams, trade matrices, and FTA models.
Optimization vs. Satisficing	Used heritage parameters where optimal data unavailable; ensured robustness via sensitivity analysis.	Airbag performance assumed from Orion heritage values.
V&V and Testing	Multi-layered V&V essential for mission assurance.	Drop tests validated ≤ 4 g landing loads; partial-chute tests validated redundancy.
Interdisciplinary Coordination	Balanced constraints from mechanical, software, avionics, and biomedical domains.	Human G-tolerance informed seat angle and attenuation requirements.

Appendix B

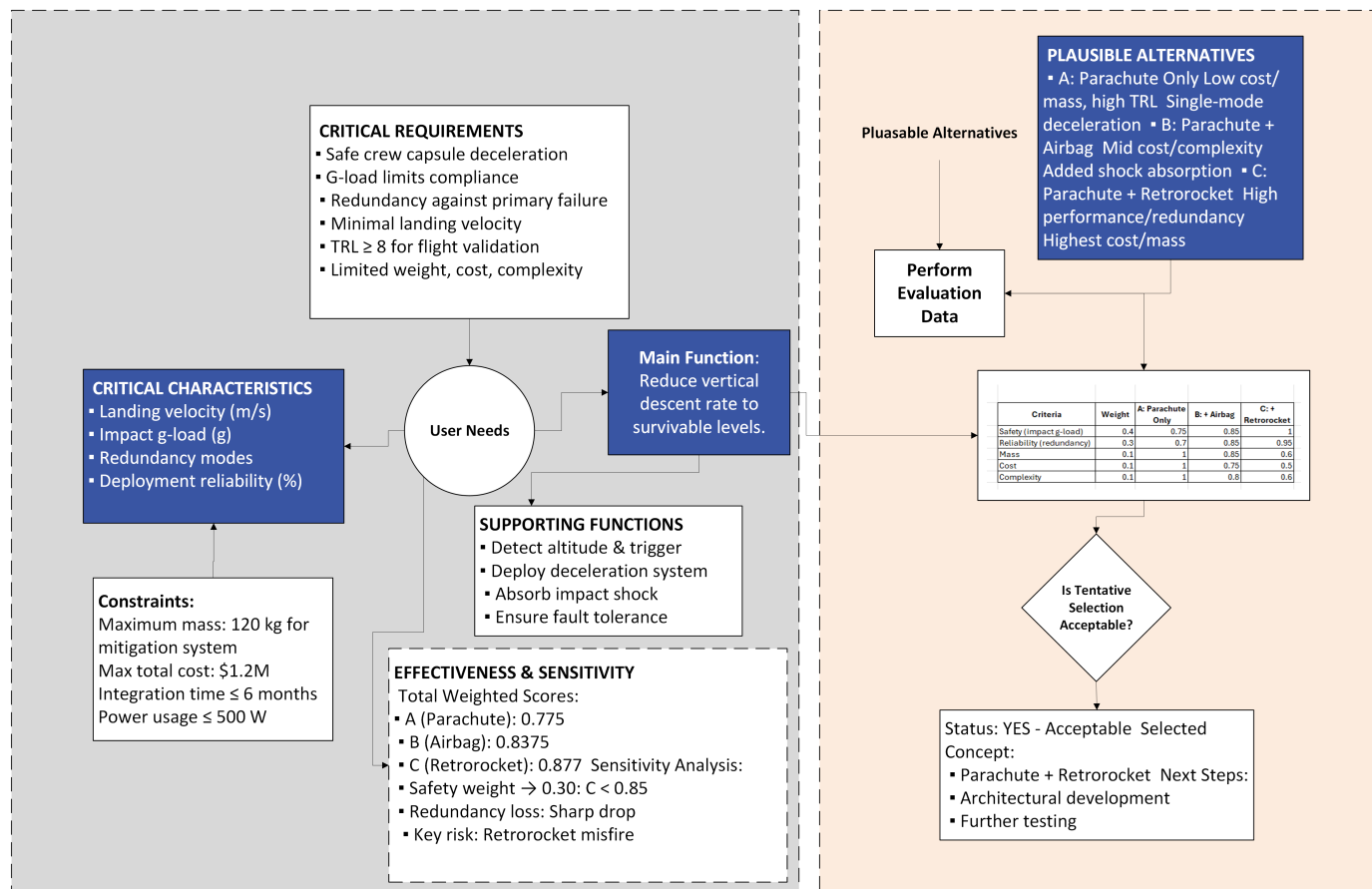


Figure 7 Trade-Off Support System (TOSS) for LIMS

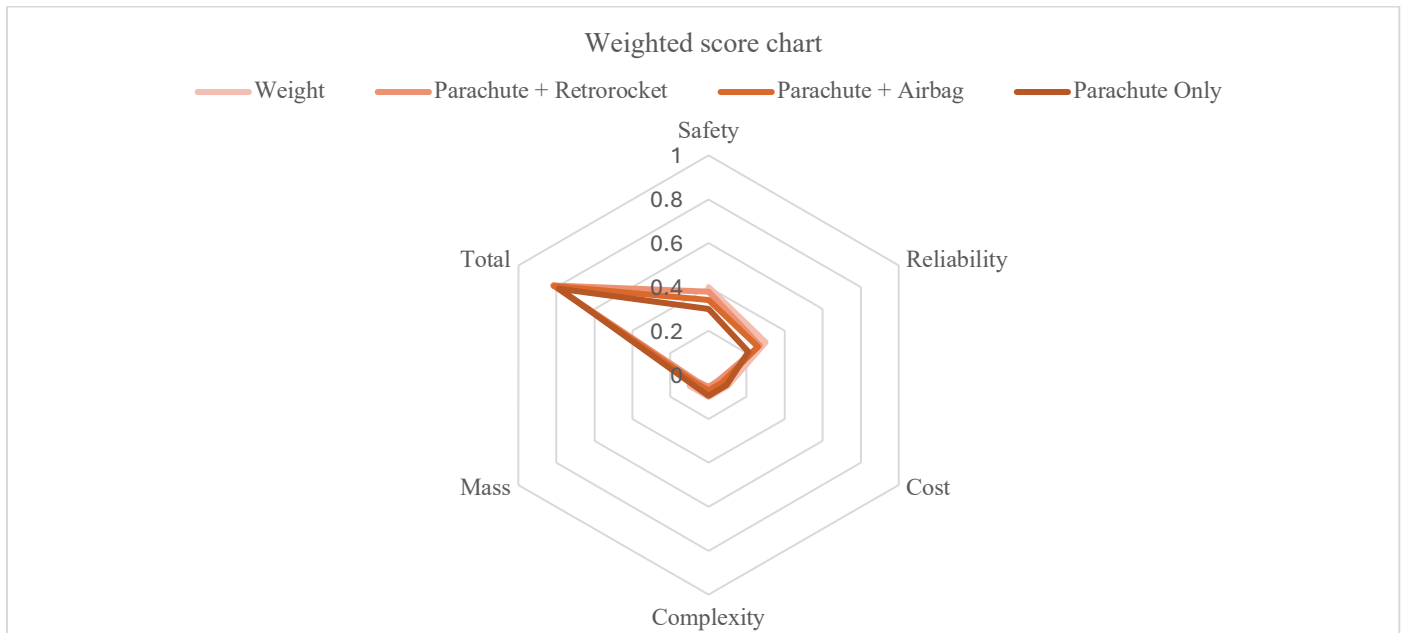


Chart A Weighted Score Chart

Appendix C

Document A1: QFD



QFD.xlsx

Document A2: PBS Structure



PBS.pptx

Student Self-reflection on performance

Describe how you have used AT LEAST ONE of the following sources of information to improve this piece of work:

- 1.) (PREFERRED) Feedback from previous assignment(s). This can be from the same module or from a previous module or previous year of study (e.g. comments from 1st year lab formal reports should be used to help improve your 2nd year lab formal reports).
- 2.) The marking criteria or rubric provided for this assignment.
- 3.) The Department Technical Writing Handbook for Students.

The Department Technical Writing Handbook for Students.

Are there any aspects of this work that you would specifically like the marker to comment/or advise on? For example: “I wasn’t sure if my figure formatting looked professional and would appreciate feedback on this aspect”

IMPORTANT DECLARATIONS AND REQUIREMENTS

Group Declaration:

We confirm that:

- All factors are fairly awarded
- Required documentation is attached
- All members had opportunity to contribute
- Professional conduct was maintained
- University procedures were followed

Signatures of ALL Group Members:

1. Name: Jagathguru Pazhanivel	ID:249057008 Signature: 	Date: 12/12/2025
2. Name: Bindushree Sanjeev Murthy	ID: 259045211 Signature: 	Date: 12/12/2025
3. Name: Fregin Sherofer Francis	ID: 249050172 Signature: 	Date: 12/12/2025
4. Name: Ekta Shanmukh Thakur	ID: 259053684 Signature: 	Date: 12/12/2025
5. Name: Avinash Raveendran Nair	ID: 249058062 Signature: 	Date: 12/12/2025

Module Convenor Use Only:

- Documentation Complete
- Factors Verified
- Procedures Followed
- Approval Granted

Title:	Peer Review and Individual Effort Factors		
Group:	New Group 9		
Date assessed:	12/12/2025		
Group Member and Student ID	Factor	Feedback <i>Group will need to provide a brief justification for the weighting factors awarded.</i>	Signature
	$0.00 \leq X \leq 1.10$		
Jagathguru Pazhanivel 249057008	1.10	Took a lead role and technical studies, data analytics, and research coordination organising research meetings, ensuring timely progress of analytical tasks, and maintaining high standards in methodology and reporting.	
Bindushree Sanjeev Murthy 259045211	1.10	Contributed to the development of key technical artifacts, including the QFD, WBS, V&V diagram, and system architecture diagram. Actively supported risk mitigation planning and played a crucial role in the technical refinement and structuring of the final project report. Demonstrated strong commitment by dedicating effective time to document construction and ensuring technical accuracy and coherence throughout.	
Ekta Shanmukh Thakur 259053684	1.10	development of the SMART analysis and contributed significantly to defining and refining the project scope. Ensured that objectives were Specific, Measurable, Achievable, Relevant, and Time-bound, aligning them with stakeholder needs and regulatory constraints.	
Avinash Raveendran Nair 249055249	1.10	Provided valuable contributions to the development of the maintenance plan and implementation of quality standards. Demonstrated a clear understanding of ISO 13485 requirements and ensured alignment with regulatory expectations.	

Fregin Sherofer Francis 249058062	1.10	Effectively carried out the human-centred design work and contributed to integrated discussions on human factors. Demonstrated strong awareness of usability, accessibility, and end-user needs, ensuring the device design aligns with clinical and user requirements. Their insights supported inclusive design decisions and contributed to a well-rounded conclusion grounded in user experience principles.	<i>7. Fregin Sherofer</i>
---	------	--	---------------------------