7.5.1 Engineering Process (Coarse → Fine)

Purpose. Establish a clear, auditable, and scalable process to design, build, verify, operate, and evolve the Sphere Space Station Earth ONE. The guiding principle is **coarse first, then finer**—we start broad to frame the whole system, then iteratively refine down to parts, interfaces, and procedures until the system is flight-ready and maintainable.

7.5.1.1 Foundations & Guardrails

- **Ethics, Safety, Transparency.** Adhere to project preamble; document every safety-critical decision; keep artifacts auditable.
- **Single Source of Truth (SSOT).** All specs, models, decisions, and approvals are maintained in the project's documentation space; changes only via controlled requests.
- **Configuration Management.** Version every artifact (requirements, CAD, code, models); trace from requirement → design → test → result.
- **Standards.** Apply MBSE (SysML/UML), ECSS/NASA-SE handbooks where applicable, RAMS practices, FMEA/FTA for hazards, ICD discipline for interfaces.

7.5.1.2 Coarse Layer — Vision to System Concept **Objective.** Align on what we're building and why; set bounding boxes.

Core outputs.

- Mission Objectives & Success Criteria (primary, secondary, stretch).
- System Concept of Operations (ConOps) incl. orbit, spin, docking, traffic, crew flows, emergency philosophy.
- Top-Level Requirements (TLRs): performance, capacity (~700 ppl), safety, sustainability, cost, schedule.
- Initial Architecture: segment breakdown (Structure, Power/Thermal, Life Support, Avionics/Comms, Attitude/Propulsion, Safety, Ops/Logistics).
- **LoD Levels (fidelity ladder):**
  - **LoD-0:** Back-of-envelope sizing, mass/power/heat budgets, first feasibility deltas.
  - **LoD-1:** Analytic models per discipline; strawman interfaces.

Gate: SRR (System Requirements Review). Approve TLRs, ConOps, initial budgets, risk register v1.

7.5.1.3 System Architecture & Trade Studies (Refinement 1) **Objective.** Choose the big rocks; prove feasibility with numbers.

Activities.

- MBSE model (SysML) with functional, logical, and physical views.
- Trades: reactor vs microreactor mixes; radiator geometry; deck gravity bands; docking topology; shielding options; escape system variants.
- Interfaces: draft ICDs between segments (mechanical, thermal, electrical, data, fluid).
- Preliminary Safety Assessment: hazard tree, fault containment regions, safe states, crew survival time budgets.
- Cost & Schedule envelopes; ops concept for assembly and resupply.

Outputs. Updated mass/power/thermal/radiation budgets; ICD set v0.1; hazard log v0.1; ops-timeline sketch.

Gate: SDR/Architecture Review. Approve chosen architecture and key trades.

7.5.1.4 Preliminary Design (Refinement 2) **Objective.** Turn architecture into validated preliminary designs per subsystem.

Activities.

- Subsystem PDRs (Structure & Decks; Power & Thermal; Life Support; Avionics/Comms; Attitude & Propulsion; Safety & Evac; Ground & Ops).
- Model maturation to **LoD-2:** coupled analyses (rotational dynamics ↔ structure; heat ↔ power; ECLSS ↔ crew loads).
- Digital Twin v1 (simulation backbone) for end-to-end performance runs.
- Preliminary test plans (qualification/acceptance); verification cross-matrix (req ↔ test/analysis/inspection/demo).

Outputs. Subsystem specs v1.0, ICDs v0.5, risk register v2, verification plan v1, draft manufacturing plans.

Gate: PDR. Converged preliminary design; cost/schedule re-baseline; go/no-go to detailed design.

7.5.1.5 Detailed Design & Build Readiness (Refinement 3) **Objective.** Lock drawings, parts, and processes; prove producibility.

Activities.

- Detailed CAD & drawings; tolerances; materials/finishes; process sheets.
- Parts lists/BOMs; long-lead procurement; supplier qualification.
- Software design to code complete for flight/ground; ICDs finalized.
- Design for Assembly/Integration/Service (DFx); human factors layouts for high-g and 1g decks.
- Safety: FMEAs to item level; red-team reviews; evacuation and fire suppression design finalized.
- Model maturation to **LoD-3:** integrated multi-physics models; HIL benches for critical loops (ECLSS, power, guidance).

Outputs.

- Released drawings (RFD/RFW processes ready), ICDs v1.0, work instructions, inspection plans, software CI/CD pipelines.

Gate: CDR (Critical Design Review). Design is buildable, safe, and testable.

7.5.1.6 Integration, Verification & Validation (V&V) **Objective.** Prove the system meets requirements and is flightworthy.

Build tiers.

- **EM/Breadboards:** early risk retirement.
- **QM (Qualification Models):** to limits and beyond (thermal-vac, vibration, EMI/EMC, radiation/SEU).

- **FM (Flight Models):** acceptance test regime; traceability to QMs.

Verification methods. Test, Analysis, Inspection, Demonstration (TAID). Maintain a closed-loop **Verification Matrix**.

System-level. End-to-end tests on spin rigs; emergency drills; power/thermal load shedding; fault injection; crew-in-the-loop sims.

Gates.

- **TRR (Test Readiness Review)** → start formal test.
- **QR (Qualification Review)** → qual complete.
- **FAR (Flight Acceptance Review)** → flight approve.

7.5.1.7 Launch, Assembly & Commissioning **Objective.** Safely deploy, assemble, spin-up, and commission the station.

Activities.

- Launch campaign & on-orbit assembly scripts; robotics tools; alignment & metrology.
- Incremental spin-up with telemetry guardrails; mode management & hold points.
- Commissioning tests: ECLSS stability, power/thermal steady-state, crew habitat checks, docking rehearsals, evacuation drills.

Gate: ORR (Operations Readiness Review). Authorize nominal operations.

7.5.1.8 Operations, Maintenance & Evolution (Refinement 4+) **Objective.** Keep it safe, efficient, and improving.

Practices.

- Reliability engineering (RCM), predictive maintenance (vibration/thermal analytics), spare strategy.
- Change management: ECR/ECO workflow; controlled rollouts; regression V&V.
- Post-flight/ops data into digital twin for continuous calibration.
- Periodic Safety Reviews; audit trails; incident investigation playbooks.

Gate: FRR (Flight/Operations Readiness for upgrades) per upgrade wave.

7.5.1.9 Cross-Cutting Disciplines & Checklists **Risk Management.** Identify → assess → mitigate; keep burn-down visible.

Human Systems Integration. Habitability, workload, health (radiation, rotation adaptation), emergency egress time.

Sustainability. Closed loops (air, water, waste), energy efficiency, recycling; environmental compliance.

Security & Resilience. Cybersecurity, physical security, fault tolerance, degraded-mode operations.

Compliance & Legal. Space law, export control, reactor licensing, debris mitigation.

Cost & Schedule Control. Earned value, critical path, contingency management.

7.5.1.10 Interface & Documentation Discipline

- **ICDs:** mechanical, thermal, electrical, data, fluid; unique IDs; auto-validation checks.
- **Design Books:** one per subsystem (requirements, rationale, calcs, margins, tests, as-built).
- **Review Datasets:** frozen snapshots at SRR/SDR/PDR/CDR/TRR/ORR/FAR; archived in SSOT.

7.5.1.11 Levels of Detail (LoD) Summary (Coarse → Fine)

- **LoD-0:** Concept sizing; 10–20% margins; feasibility only.
- **LoD-1:** Discipline analytics; key trades; preliminary ICDs.
- **LoD-2:** Coupled subsystem models; preliminary test plans.
- **LoD-3:** Integrated models; HIL benches; detailed drawings.
- **LoD-4:** Qualification/acceptance results; as-built configs.
- **LoD-5:** In-service telemetry-calibrated models; ops baselines.

7.5.1.12 Reviews (Quality Gates) — At a Glance

- **SRR** → requirements & ConOps approved.
- **SDR/AR** → architecture frozen.
- **PDR** → preliminary design mature.
- **CDR** → detailed design releasable.
- **TRR** → test campaign ready.
- **QR/FAR** → qualified & flight-accepted.
- **ORR** → operations authorized.

7.5.1.13 Minimal Template Set (Starter Kit)

- Mission Objectives Sheet • ConOps Canvas • TLR List • Risk Register • Architecture Block Diagram • Budget Sheets (mass/power/thermal) • Trade Study Template • ICD Template • Verification Matrix • Test Plan Template • Safety Case Outline • Review Checklist Pack (SRR→ORR) • Change Request (ECR/ECO) forms.

7.5.1.14 Success Metrics

- Technical: margins met, fault tolerance, RAMS KPIs.
- Programmatic: milestone hit rate, variance ≤ thresholds.
- Safety: zero loss-of-life incidents; risk exposure within limits.
- Sustainability: recycling efficiencies, energy intensity, waste KPIs.
- Operations: uptime, mean time to repair, anomaly closure time.

This document is living. All edits proceed via change control in the SSOT with full traceability from requirement to verification and operational evidence.

7.5.1.15 Appendices

Appendix A — Engineering Glossary (Detailed)

Scope. This glossary collects core terms used throughout the engineering process for Sphere Space Station Earth ONE. It follows an alphabetical order. Cross-references are indicated with arrows (→). See also the sections **Reviews**, **Levels of Detail**, **Interface & Documentation Discipline**, and **V&V** in this document.

A

- **Acceptance Test (AT).** Formal test performed on a Flight Model (FM) to show it meets acceptance criteria before delivery/launch. (→ Qualification Test, FAR)
- **Acceptance Review (FAR).** Flight Acceptance Review; gate confirming that hardware/software is accepted for flight. (→ Reviews)
- **AIT (Assembly, Integration & Test).** End-to-end process of assembling parts, integrating subsystems, and testing at each tier. (→ V&V)
- **All-Up Test.** System test with all subsystems active in mission-like configuration.
- **Anomaly.** Any unexpected behavior, result, or condition requiring triage, root-cause analysis, and corrective action. (→ NCR, MRB)
- **As-Built / As-Designed / As-Run.** Frozen configurations: manufactured/installed state; original design baseline; actual procedures executed. Used for traceability.
- **Avionics.** Spacecraft electronics for command, data handling, guidance, navigation, and control.

B

- **Baseline.** The authoritative, controlled definition of a configuration or requirement set at a point in time. Changes require approval. (→ CCB)
- **BOM (Bill of Materials).** Hierarchical list of all items needed to manufacture and assemble a product, with part numbers and revisions.
- **Breadboard (EM).** Early experimental hardware (Engineering Model) used to validate principles; not flight-like in form or finish. (→ QM, FM)
- **Budget (Mass/Power/Thermal/Radiation).** Allocated resources per subsystem with margins; tracked from early sizing through operations.
- **Burn-Down Chart.** Visual tracking of risk or work remaining versus time; used for risk retirement and schedule focus.

C

- **CBE (Current Best Estimate).** The latest realistic estimate of a parameter before margin; paired with growth allowance. (→ Margin)
- **CCB (Change Control Board).** Authority that reviews and approves changes to baselines, ICDs, and requirements. (→ ECR/ECO)
- **CDR (Critical Design Review).** Gate confirming detailed design is producible, testable, and safe. (→ Reviews)
- **Commissioning.** Post-assembly activation and calibration to transition to nominal operations. (→ ORR)
- **Common-Mode Failure.** A single cause leading to multiple failures simultaneously, often violating redundancy assumptions.
- **ConOps (Concept of Operations).** Narrative of how the system is used over its life cycle—modes, users, environments, and scenarios. (→ SRR)
- **Configuration Management (CM).** Governance and tooling for identifying, controlling, tracking, and auditing all configuration items.
- **Contingency Mode.** Predefined degraded mode to preserve safety and assets when nominal performance is not possible. (→ Safe State)

- **Coriolis Effects.** Apparent forces in rotating frames affecting crew perception and fluid flows in spin gravity habitats.
- **COTS (Commercial Off-The-Shelf).** Non-custom components procured as-is; usually require environment qualification.
- **Crew Survival Time (CST).** Minimum guaranteed time for crew survival after a critical failure, given emergency provisions.
- **Critical Item List (CIL).** Catalog of safety-critical parts and processes requiring special controls.
- **Critical Path.** The sequence of tasks that determines the project's minimum schedule; any delay here delays the whole.

D

- **Datum (Mechanical).** Reference feature used for locating and aligning parts during inspection and assembly.
- **DFx (Design for X).** Design for Assembly/Integration/Service/Manufacture/Safety; methods to reduce cost and risk. (→ AIT)
- **Digital Twin.** High-fidelity, continuously updated model mirroring the as-built system using telemetry and test data. (→ V&V)
- **Deviation / Waiver (RFD/RFW).** Formal permission to depart from a requirement (waiver) or from the design during build (deviation). (→ CCB)
- **Degrees of Freedom (DoF).** Independent parameters defining motion or state of a system.
- **Docking Envelope.** Spatial/kinematic limits and alignment tolerances for capture and berthing operations.
- **Downmass / Upmass.** Mass returned from orbit / mass launched to orbit; key logistics constraints.

E

- **ECLSS (Environmental Control and Life Support System).** Air, water, waste, thermal comfort, and pressure control systems for crewed habitats.
- **ECO / ECR.** Engineering Change Order / Request; proposal and approval workflow for modifying baselines. (→ CCB)
- **EM (Engineering Model).** Early hardware used for functional trials; not qualified for flight. (→ Breadboard, QM, FM)
- **EMI/EMC.** Electromagnetic Interference / Compatibility; design and test to ensure mutual non-interference. (→ Qualification)
- **End-to-End Test.** System test from stimulus to response across all relevant interfaces and modes.
- **Evacuation Time.** Maximum allowed time to reach safe refuge or escape vehicle from any point in the habitat. (→ Human Systems Integration)

F

- **FAI (First Article Inspection).** Complete verification that the first produced unit meets all drawing and spec requirements.
- **FAR (Flight Acceptance Review).** Gate approving flight readiness of production units, closing open actions and NCRs. (→ Acceptance Test)
- **Fault Containment Region (FCR).** Architectural boundary within which faults are isolated to prevent system-wide propagation. (→ FDIR)
- **FDIR (Fault Detection, Isolation & Recovery).** Automated and procedural mechanisms to detect, locate, and recover from faults.

- **FMEA (Failure Modes & Effects Analysis).** Bottom-up hazard analysis identifying failure modes, effects, and mitigations. (→ FTA)
- **FM (Flight Model).** The unit intended to fly, built to flight standards and passing acceptance tests. (→ QM)
- **FRR (Flight/Operations Readiness Review).** Gate authorizing a specific operation or mission phase. (→ ORR)
- **FTA (Fault Tree Analysis).** Top-down analysis modeling combinations of faults that lead to hazards or top events.

G

- **G-Level / Partial-g.** Effective gravity from rotation at a given deck radius and spin rate; defines human factors constraints. (→ Spin Gravity)
- **GCR (Galactic Cosmic Rays).** High-energy background radiation in deep space; key driver for shielding design. (→ SPE)
- **Gate (Quality Gate).** Formal milestone with entry/exit criteria (SRR, PDR, CDR, TRR, QR, FAR, ORR). (→ Reviews)
- **GSE (Ground Support Equipment).** Non-flight equipment used to build, test, and operate flight hardware on ground.
- **Growth Allowance.** Planned margin to accommodate expected mass/power increases as designs mature. (→ CBE, Margin)

H

- **Hazard Log.** Controlled list of hazards, causes, mitigations, verification, and status across the lifecycle. (→ Safety Case)
- **HIL (Hardware-in-the-Loop).** Test setup coupling real hardware with simulated environments for closed-loop verification. (→ SIL, MIL)
- **Hold Point.** A planned pause in a procedure requiring explicit authorization to proceed; used in critical operations.
- **Human-Rating.** Meeting stringent safety and reliability criteria for crewed missions.
- **Human Systems Integration (HSI).** Integration of human factors across design—workload, habitability, health, and emergency egress.

I

- **ICD (Interface Control Document).** Controlled specification of all mechanical, electrical, thermal, data, and fluid interfaces. (→ ICWG)
- **Incident.** Event that disrupts nominal operations; may or may not cause damage. (→ Anomaly, Mishap)
- **Ingress / Egress.** Entry to and exit from zones, vehicles, or modules; must meet timing and clearance requirements. (→ Evacuation Time)
- **ICWG (Interface Control Working Group).** Cross-discipline forum that authors and maintains ICDs under change control.
- **Inspection.** Verification by measurement, visual checks, or instrumented methods against drawings and specs.
- **IPT (Integrated Product Team).** Multidisciplinary team responsible for a product or subsystem across its lifecycle.

J

- **Jitter.** Small, rapid variations in signal, pointing, or motion that can degrade performance; controlled by design and damping.

K

- **KPI (Key Performance Indicator).** Quantified measure reflecting progress or performance in technical or programmatic domains.

L

- **Launch Campaign.** Coordinated sequence of pre-launch activities including rehearsals, fueling, and integration with the launch vehicle.
- **LBB (Leak-Before-Burst).** Design philosophy ensuring a detectable leak precedes catastrophic rupture. (→ Safety Case)
- **Level of Detail (LoD).** Fidelity ladder for models and designs from coarse (LoD-0) to in-service baselines (LoD-5). (→ Levels of Detail)
- **Life-Limited Part (LLP).** Part with a certified service life after which it must be removed or overhauled.
- **Lockstep Redundancy.** Parallel identical processors/components operating in sync for fault detection and voting. (→ Redundancy)

M

- **Margin.** Performance headroom carried to account for uncertainty and growth; tracked and protected at every gate. (→ CBE)
- **MBSE (Model-Based Systems Engineering).** Formalized application of models to support requirements, design, analysis, and V&V. (→ SysML)
- **Metrology.** Measurement science applied to alignment, geometry, and tolerances during AIT.
- **MIL / SIL.** Model-in-the-Loop and Software-in-the-Loop test stages before HIL. (→ HIL)
- **Mishap / Near-Miss.** An accident with damage/injury / a narrowly avoided mishap; both are reportable with corrective actions.
- **MRB (Material Review Board).** Authority to disposition non-conformances (use-as-is, rework, repair, scrap). (→ NCR)
- **MTBF / MTTR / Availability.** Mean time between failures; mean time to repair; fraction of time system is operational.
- **Mode (Nominal/Degraded/Safe).** Discrete configurations governing behavior, protections, and authority limits. (→ Safe State)

N

- **NCR (Non-Conformance Report).** Record of deviation from requirements/specs discovered in build or test; triggers MRB action.
- **Nominal.** As planned and expected, within specified tolerances.
- **N+1 Redundancy.** Having one more unit than required for function to tolerate a single failure. (→ Redundancy)

O

- **ORR (Operations Readiness Review).** Gate authorizing routine operations after commissioning. (→ Reviews)
- **Operations Concept.** See **ConOps**.
- **Ops Handbook.** Authoritative procedures, flight rules, and mode definitions for operators and crew.
- **Outgassing.** Release of gases from materials in vacuum; managed via bake-out and materials selection.

P

- **PDR (Preliminary Design Review).** Gate confirming the design meets requirements at preliminary maturity. (→ Reviews)
- **PFM (Protoflight Model).** Flight-representative unit used for both qualification-like and acceptance-like testing under combined regimes.
- **Power/Thermal Balance.** Condition where generated power and rejected heat meet steady-state limits across modes. (→ Budgets)
- **Precession / Nutation.** Slow and oscillatory changes in spin axis orientation affecting pointing and g-uniformity. (→ Rotational Dynamics)
- **Predictive Maintenance.** Maintenance scheduled based on condition monitoring (vibration, temperature) rather than fixed intervals. (→ RCM)
- **Protocol (Telemetry/Commands).** Defined messaging structures and link layers used for commanding and data return.

Q

- **Qualification (Qualification Test).** Demonstration that design meets requirements with margin under worst-case environments. (→ QR)
- **QR (Qualification Review).** Gate confirming completion of qualification program and closure of findings.
- **Quality Escape.** Defect that passes through build/test gates undetected; addressed via corrective and preventive action (CAPA).

R

- **Radiation (SEE/SEU/TID).** Single-Event Effects (transients or damage), Single-Event Upsets (bit flips), and Total Ionizing Dose accumulation. (→ Shielding)
- **RAMS.** Reliability, Availability, Maintainability, Safety—key system attributes tracked across lifecycle.
- **Redundancy (Cold/Warm/Hot).** Standby off / powered standby / active parallel redundancy strategies. (→ FDIR)
- **RCM (Reliability-Centered Maintenance).** Maintenance planning focused on preserving functions and managing failure consequences.
- **Requirement (Shall/Should/May).** Binding / recommended / optional statements that are uniquely identified, testable, and traced. (→ Verification Methods)
- **Review Pack.** Frozen set of artifacts presented at a gate (agenda, minutes, action items, decisions, deltas). (→ Reviews)
- **Risk Matrix.** Likelihood × consequence grid used to prioritize mitigations; often 5×5 with color coding.
- **Rotational Dynamics.** Behavior of spinning structures including balance, modal coupling, and control interactions. (→ Spin Gravity)

S

- **Safe State.** Minimal-risk condition the system autonomously enters on serious fault—power-positive, thermally safe, crew safe. (→ FDIR)
- **Safety Case.** Structured argument with evidence that the system is acceptably safe for a given context; linked to hazard log. (→ Hazard Log)
- **Sabatier Process.** ECLSS reaction converting CO_2 and H_2 to CH_4 and H_2O for oxygen recovery and fuel by-product.
- **SDR / AR.** System Definition/Architecture Review; gate where architecture and key trades are frozen. (→ Reviews)

- **SEE / SEU.** Single-Event Effects / Upsets caused by energetic particles; mitigated by shielding, redundancy, and ECC.
- **Shielding (Areal Density).** Mass per area (g/cm²) of protective material against radiation; water/PE effective for GCR moderation.
- **SIL / MIL.** Software-/Model-in-the-Loop testing stages. (→ HIL)
- **Single Fault Tolerance (SFT).** Ability to tolerate any single failure without loss of critical function.
- **Spin Gravity.** Artificial gravity via rotation; characterized by radius, angular speed, and g-gradient. (→ G-Level, Coriolis)
- **SSOT (Single Source of Truth).** The authoritative repository for requirements, designs, and decisions. (→ Configuration Management)
- **SysML.** Systems Modeling Language used to capture MBSE architectures and traceability.
- **System-of-Systems (SoS).** Interconnected systems working together (e.g., station + vehicles + ground + logistics).

T

- **TAID (Test/Analysis/Inspection/Demonstration).** Verification methods used to close requirements. (→ V&V)
- **Telemetry.** Measured data sent from system to operators for monitoring and analysis.
- **Thermal-Vacuum (TVAC).** Test environment simulating vacuum and temperature extremes for qualification/acceptance.
- **TRL (Technology Readiness Level).** 1–9 scale expressing maturity from basic principles to flight-proven.
- **TRR (Test Readiness Review).** Gate confirming readiness to start a test campaign with defined objectives and resources.
- **Trade Study.** Structured comparison of options using weighted criteria, uncertainty analysis, and sensitivity.

U

- **Uncrewed Operations.** Automated or tele-operated modes without crew on board; require additional autonomy & FDIR.
- **Upmass / Downmass.** See **Downmass / Upmass**. (→ Logistics)

V

- **Validation vs Verification.** *Verification*: did we build the system right (against requirements)? *Validation*: did we build the right system (against user need)?
- **V&V Cross-Reference Matrix.** Requirements-to-evidence table showing TAID closure status and results.
- **Vibration Test (Sine/Random).** Structural/environmental tests to verify survivability and workmanship.

W

- **Waiver (RFW).** Approval to accept non-compliance permanently, with risk rationale and compensating controls. (→ Deviation)
- **Watchdog Timer.** Hardware/software timer that resets or reconfigures a system when not periodically serviced. (→ FDIR)
- **Work Instruction (WI).** Controlled, step-by-step procedure for a specific task with tools, torques, and hold points.
- **Worst-Case Analysis (WCA).** Analytical proof that performance meets requirements under simultaneous worst-case conditions.

X, Y, Z

- **µg / Zero-g.** Microgravity/near-weightlessness; contrasted with partial-g in spin habitats.
- **TBD / TBR / TBC.** To Be Determined / Resolved / Confirmed; placeholders tracked to closure with owners and due dates.

End of Appendix A.