7.4.4 HAZARD CATALOG — Cross-Project Hazard Catalog

Considers: EVOL-00, EVOL-01 **Version:** v1.0.0 (initial stable; derived from v0.1.0 DRAFT)

Scope: Unified hazard catalogue for Sphere Stations and Crafts covering Evolution 00 and Evolution 01. Acts as the SSOT for hazard definitions, mitigations, and V&V. > Naivety is inevitable — **dangerous naivety is not**.

SAFETY FIRST.

---

1) Nomenclature & Scales Hazard-ID (project-wide unique): `HZ-<Domain>-<Code>` Examples for **Domains**: AX (axial/Wormhole), DOCK, HULL, PWR, THM, GAS, FIRE, MMOD, RAD, CYB, OPS. **Codes**: short mnemonics, e.g., **PI**=Polar-Impact, **COL**=Collision, **EXP**=Explosion, **LEAK**, **VENTFAIL**; e.g., `HZ-AX-PI` (polar-impact) 1.

Severity (MIL-STD-882E) 1: - I Catastrophic — loss of life/total loss; - II Critical — severe injury/partial loss of critical systems; - III Marginal — minor injury/temporary failure; - IV Negligible — small mission impact.

Likelihood 1: - A Frequent; - B Probable; - C Occasional; - D Remote; - E Improbable.

Risk index (R): - qualitative assessment as **Severity × Likelihood**; detailed matrix in SSOT.

---

2) Hazards (EVOL-00 & EVOL-01)

1. **HZ-DOCK-EXP — Explosion at a docked craft causing blast and debris Loc:** Docking ring(s), wormhole rings. **S/L:** I / C. **Mitig.:** Blast-tolerant rings, crush collars, radial vent/burst-out panels, quick-release/jettison 3 **V&V:** Impulse/blast tests, verify vent capacity (choked flow) 3 **Refs:** ECSS-Q-ST-40C, ISO 14620-1, NASA-STD-3001 3
2. **HZ-FIRE-DOCK — Fire onboard a docked vehicle 4 Loc:** Dock adapters, ring compartments. **S/L:** II / C. **Mitig.:** Inert-gas flooding (Ar/N_2), non-combustible lining, hazardous-area zoning, automatic detachment 4 **V&V:** Measure O_2-reduction time ≤ target; material LOI/fire tests **Refs:** ISO 14620-1, NASA-STD-3001 4
3. **HZ-AX-COL — Collision in the wormhole axial approach Loc:** Entry/exit corridors. **S/L:** I / B–C. **Mitig.:** Active traffic management, collision-avoidance algorithms, abort corridors, protective shutters 5 **V&V:** Interlock tests, emergency stop drills, dummy impact tests 5 **Refs:** NASA-STD-3001; MIL-STD-882E 5
4. **HZ-AX-PI — Uncontrolled polar approach/impact Loc:** North/South polar approaches. **S/L:** I / B–C. **Mitig.:** Deployable guard nets and tethers, honeycomb bumpers, deflection cones, shutters closing ≤ 0.5 s; geofencing 6 **V&V:** Sled/drop tests, shutter-timing verification 6 **Refs:** ECSS-Q-ST-40C; MIL-STD-882E 6
5. **HZ-MMOD-TRANS — Transverse MMOD penetration Loc:** Wormhole tubes, windows. **S/L:** II / C–D. **Mitig.:** Stuffed-Whipple shielding + spall liner, sector isolation, radial vents, shutters 7 **V&V:** Ballistic tests, debris-mitigation analysis 7 **Refs:** ISO 24113; NASA-STD-8719.14 7
6. **HZ-MMOD-LONG — Axial MMOD penetration Loc:** Window tubes, open rings. **S/L:** II / D. **Mitig.:** Shutter cascades, fragment capture lamellae, segment locking 8 **V&V:** End-to-end shutter test ≤ 0.5 s 8 **Refs:** ISO 24113; NASA-STD-8719.14 8
7. **HZ-RAD-SPE — Solar particle event / CME radiation exposure Loc:** Windows/wormhole; low-shield zones. **S/L:** II / C. **Mitig.:** Storm mode (close shutters), move crew into

water/poly-shielded decks (e.g., Deck 013/014), minimise exposure time 9 **V&V:** Alert chain from space-weather feed to actuators 9 **Refs:** NASA-STD-3001 9

8. **HZ-VENT-FAIL — Vent/blow-out malfunction (fail to relieve pressure) Loc:** Hull-proximate vents/blow-off panels. **S/L:** II / D. **Mitig.:** Redundant vent paths, fail-open philosophy, periodic functional drills 10 **V&V:** Choked-flow calculation, relief time under limit 10 **Refs:** ECSS-Q-ST-40C; ISO 14620-1 10

9. **HZ-PT-FAIL — Bulkhead/door fails to close Loc:** Partition doors/hatches (PT-A/B, AL-C). **S/L:** II / C. **Mitig.:** Redundant actuators; door status interlocks; manual override; periodic close/open drills **V&V:** Timed closure tests; fault insertion on sensors/actuators **Refs:** ECSS-Q-ST-40C; ISO 14620-1

10. **HZ-GAS-CRYO — Cryogenic release / oxygen displacement Loc:** Fuel cells, cryo tanks, service lines. **S/L:** II / C–D. **Mitig.:** Leak-before-break design; oxygen depletion sensors; purge/vent routing; PPE and area zoning **V&V:** Helium leak tests; ODH calculations; functional vent tests **Refs:** ISO 14620-1; NASA-STD-3001

11. **HZ-GAS-TOX — Toxic gas release Loc:** Labs, waste-processing, propellant lines. **S/L:** II / C. **Mitig.:** Gas detection arrays; automatic isolation; scrubbers; emergency ventilation purge **V&V:** Detector calibration; gas-in-air tests; evacuation drill timings **Refs:** NASA-STD-3001

12. **HZ-FIRE-HAB — Fire in habitat modules Loc:** Hab decks, crew quarters, galley. **S/L:** II / C. **Mitig.:** Low-flammability materials (LOI), smoke detection, zoned suppression (wet/dry/inert), hot-work controls **V&V:** Material LOI/ignition tests; suppression timing; compartment integrity tests **Refs:** NASA-STD-3001; ISO 14620-1

13. **HZ-FIRE-ELEC — Electrical fire Loc:** Power bays, distribution panels, racks. **S/L:** II / C. **Mitig.:** Arc-fault detection; derating; cable routing segregation; automatic de-energise; clean-agent suppression **V&V:** Arc-fault injection; breaker trip profiling; suppression test **Refs:** NASA-STD-3001

14. **HZ-PWR-LOSS — Total/partial power loss Loc:** PWR generation, storage, distribution. **S/L:** II / C–D. **Mitig.:** N+1 generation; cross-ties; load shedding; black-start procedures **V&V:** Black-start drills; FMEA; HIL testing **Refs:** ECSS-Q-ST-40C; IEC 60812 6

15. **HZ-THM-CTRL — Thermal control failure / over-temperature Loc:** Thermal loops, radiators, heat-exchangers. **S/L:** II / C–D. **Mitig.:** Redundant pumps/loops; bypass valves; boil-off paths; over-temp interlocks **V&V:** Thermal balance tests; loss-of-flow tests; interlock verification **Refs:** ECSS-Q-ST-40C

16. **HZ-HULL-LEAK — Hull breach / progressive leak Loc:** External hull, penetrations, windows. **S/L:** I–II / C–D. **Mitig.:** Compartmentalisation; automatic isolation; patch kits; radial vents to avoid implosive flow **V&V:** Pressure decay tests; door/valve auto-close timing; patch drill **Refs:** ISO 14620-1

17. **HZ-HULL-DEPRESS — Rapid decompression Loc:** Any pressurised volume. **S/L:** I / C. **Mitig.:** Blast-relief panels; auto door closure; tethered PPE; emergency O_2 **V&V:** Blow-out panel tests; man-in-the-loop drills; timing analysis **Refs:** ISO 14620-1; NASA-STD-3001

18. **HZ-OPS-HUMAN — Human error / procedural deviation Loc:** All operations. **S/L:** II / C. **Mitig.:** Two-person rule; checklists; digital work-flows; poka-yoke interfaces; fatigue management **V&V:** Ops simulations; incident reviews; FTA of critical tasks **Refs:** ISO 31000 2; NRC FTA handbook 7

19. **HZ-CYB-SEC — Cybersecurity breach affecting safety Loc:** Control networks, HMI, gateways. **S/L:** II / D. **Mitig.:** Defense-in-depth; zero-trust; safety-rated independence; signed configs; offline fail-safe modes **V&V:** Pen-tests; red-team exercises; safety-separation verification **Refs:** NASA-8719.13 13; NASA 8000-series 14

20. **HZ-OPS-EVAC** — **Failed/slow evacuation Loc:** Hab decks, labs, docks. **S/L:** II / C. **Mitig.:** Wayfinding; lighting; muster points; drills with metered timing; mobility-impaired accommodations **V&V:** Evacuation timing; blocked-path scenarios; smoke studies **Refs:** NASA-STD-3001

21. **HZ-ROBOT-COLL** — **Robotic collision/kinematic failure Loc:** Autonomous/tele-op robots near crew/structures. **S/L:** II / C. **Mitig.:** Speed limits; soft-body compliance; geofenced workspaces; dynamic obstacle avoidance; e-stops; HRI training **V&V:** HIL simulation; sensor stress tests; fail-safe/rescue procedures **Refs:** IEC ISO 8373; NASA-STD-3000 series

22. **HZ-ECLSS-FAIL** — **Environmental Control & Life-Support failure Loc:** Life-support modules (ECLSS), habitat. **S/L:** I / D. **Mitig.:** Redundant subsystems with cross-connects; consumables stockpile; manual operation; health monitoring; maintenance **V&V:** Reliability modelling; failure-mode tests; integrated ECLSS simulations **Refs:** NASA-STD-3001; ECSS-E-ST-20

23. **HZ-BIO-CONTAM** — **Biological contamination/health risk Loc:** Laboratories, hydroponics, waste-processing. **S/L:** II / D. **Mitig.:** Zoning (BSL-like); UV/heat sterilisation; waste isolation; PPE; sampling **V&V:** Bioburden tests; surface/air sampling; decon validation **Refs:** NASA-STD-3001

24. **HZ-DOCK-DET** — **Failed detachment/undocking Loc:** Dock ring, adapter systems. **S/L:** II / C–D. **Mitig.:** Redundant latches; pyros as last resort; manual release paths; torque-limiters **V&V:** Detachment drills; torque/force logs; fault-injection **Refs:** ECSS-Q-ST-40C; ISO 14620-1

25. **HZ-DOCK-MISALIGN** — **Dock misalignment / hard-dock impact Loc:** Dock interface. **S/L:** II / C. **Mitig.:** Soft-capture; alignment cones; relative-nav sensors; abort corridors **V&V:** Contact-dynamics tests; software-in-the-loop **Refs:** NASA-STD-3001

26. **HZ-THM-ICE** — **Ice formation / shedding Loc:** Cryo lines, vents, exterior. **S/L:** III / C–D. **Mitig.:** Heat tracing; purge; drip-traps; shields **V&V:** Thermal cycle tests; visual inspections **Refs:** ECSS-Q-ST-40C

27. **HZ-PWR-ARC** — **Arc-flash / electrical shock Loc:** Switchgear, battery rooms. **S/L:** II / C. **Mitig.:** Arc-flash boundaries; insulated tools; remote racking; PPE; interlocks **V&V:** Incident energy calc; protection coordination; trip tests **Refs:** NASA-STD-3001

28. **HZ-PWR-BATT** — **Battery thermal runaway Loc:** Energy storage racks. **S/L:** II / C–D. **Mitig.:** Cell-level fusing; gas vents; fire breaks; thermal monitoring; isolation **V&V:** Abuse tests; propagation tests; detection response time **Refs:** NASA-STD-3001; IEC 60812 6

29. **HZ-STRUCT-FAIL** — **Structural member failure Loc:** Trusses, rings, mounts. **S/L:** II / D. **Mitig.:** Safety factors; load path redundancy; crack monitoring; QA/NDT **V&V:** Proof-load; fatigue tests; NDT schedule **Refs:** ECSS-Q-ST-40C

30. **HZ-PROP-LEAK** — **Propellant leak (non-cryo) Loc:** Manifolds, valves, lines. **S/L:** II / C. **Mitig.:** Double containment; leak detection; isolation valves; purge lines **V&V:** Helium leak test; sniffer surveys; isolation verification **Refs:** ISO 14620-1

31. **HZ-PROP-IGN** — **Unintended ignition Loc:** Engines, test stands, docks. **S/L:** I–II / C. **Mitig.:** Hazardous area zoning; purge; ignition interlocks; LEL/UEL monitoring **V&V:** Ignition source control tests; interlock validation **Refs:** ISO 14620-1; NASA-STD-3001

32. **HZ-COMM-LOSS** — **Loss of command/telemetry Loc:** Control rooms, comms links. **S/L:** II / D. **Mitig.:** Redundant links; local autonomy; degraded-mode ops; manual safe-states **V&V:** Link failover tests; degraded-mode drills **Refs:** NASA-STD-3001

33. **HZ-NAV-ERROR** — **Navigation error / bad state-estimation Loc:** Guidance & relative nav in docking/approach. **S/L:** II / C–D. **Mitig.:** Sensor fusion; plausibility checks; geo-fencing; approach cones; velocity caps **V&V:** Monte-Carlo sims; HWIL; flight-like tests **Refs:** NASA-STD-3001
34. **HZ-SW-FAULT** — **Safety-critical software fault Loc:** Autonomy, guidance, interlocks. **S/L:** II / D. **Mitig.:** Independent safety layer; static analysis; formal methods; diversified redundancy **V&V:** Unit/integration tests with coverage; formal proofs where applicable **Refs:** NASA-STD-8719.13 13
35. **HZ-EMC-INTERF** — **EMC/EMI interference impacts safety Loc:** Mixed-signal environments; high-power RF. **S/L:** III / D. **Mitig.:** Shielding; filtering; grounding; separation; EMC test plans **V&V:** EMC testing; injected fault currents; susceptibility scans **Refs:** ECSS-Q-ST-40C
36. **HZ-TOOLS-FOD** — **Foreign Object Debris (FOD) / tool control Loc:** Shops, docks, EVA prep. **S/L:** III / C. **Mitig.:** Tool tethering; FOD mats; kitting; sign-in/out; inspections **V&V:** FOD audits; surprise inspections; incident tracking **Refs:** NASA-STD-3001
37. **HZ-MED-EMERG** — **Medical emergency / delayed response Loc:** Hab/labs; EVA staging. **S/L:** II / C. **Mitig.:** Medical bay readiness; telemedicine; AEDs; drills; med-evac protocols **V&V:** Drill timing; inventory checks; scenario-based training **Refs:** NASA-STD-3001

---

3) Governance & Versioning

- **Owner:** safety-life-support (Catalogue), safety-reactor (Schotts/VENT), structure-architecture (AX/Wormhole).
- **Change process:** Hazard Review Board (HRB) monthly; changes tracked in SSOT.
- **SemVer:**
  - **MAJOR** — new Evolution covered (e.g., EVOL-02) ⇒ v2.0.0;
  - **MINOR** — content changes (new hazards/mitigations) ⇒ v1.1.0;
  - **PATCH** — typos/format fixes ⇒ v1.0.1.

Fußnotenliste