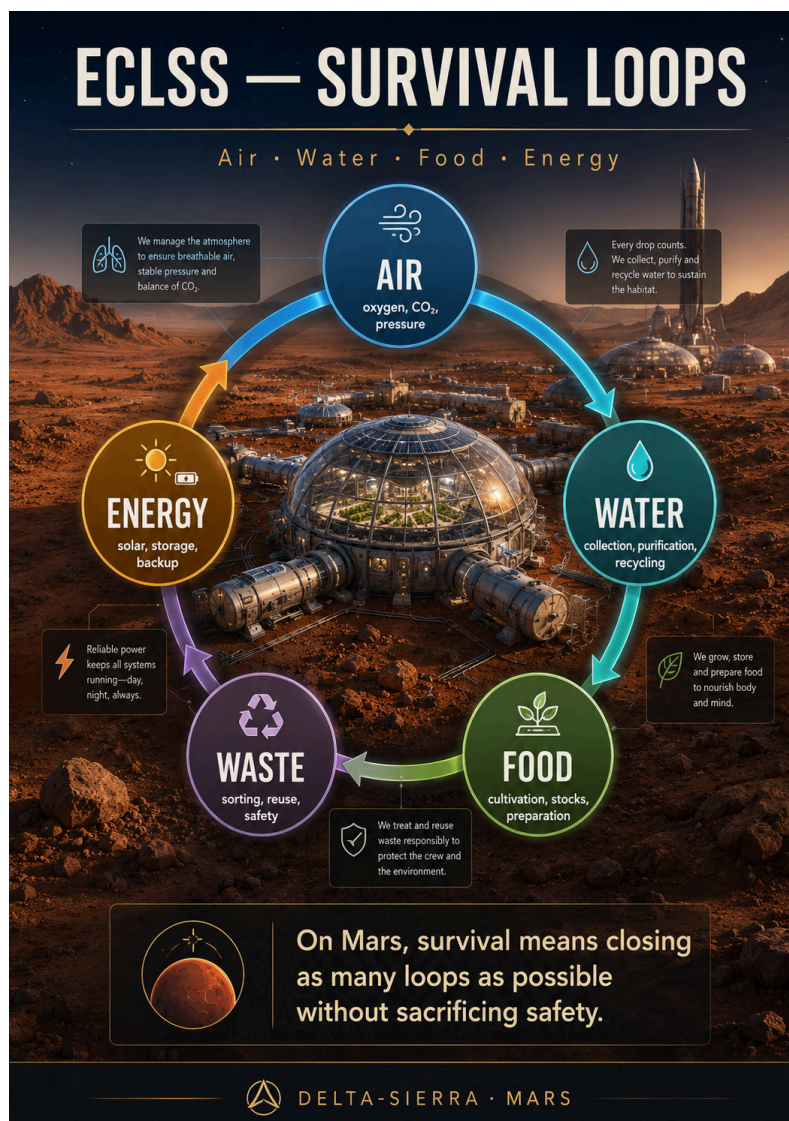


Survival & ECLSS: close loops without hiding failures



is a system of life-support functions, not one machine. It must maintain air, water, temperature, and quality while remaining controllable after faults.

The module separates ISS-demonstrated performance, long-duration goals, and Mars teaching scenarios.

1. Start from life-support functions

ECLSS is not one box but a set of functions: breathable atmosphere, potable water, thermal control, hygiene, waste processing, and monitoring. Equipment may change while the required function remains.

For each function, track inventory, flow, quality, and time to consequence. sensor failure and pressure-shell rupture evolve on different timescales and demand different responses.

System intuition

A vital system should be described as a measurable function before hardware is chosen. For each function, define the controlled variable, acceptable domain, sensor, action, backup path, and criterion. This prevents a hardware item from being confused with the survival function it performs.

Critical-stock endurance

$$t = S / q$$

1 — Concrete question	What operational question does this relation answer for critical-stock endurance?
2 — Intuition without symbols	Compare the verified usable reserve with the rate at which it is consumed to obtain a protection duration.
3 — Quantities first	S is usable stock, q is consumption rate, and t is endurance.
4 — Formula	$t = S / q$
5 — Read aloud	Read the relation aloud term by term: $t = S / q$.
6 — Symbols and meaning	S is usable stock, q is consumption rate, and t is endurance.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Use one resource unit for stock and the same resource unit per time for the rate; endurance is in that time unit.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Compare the verified usable reserve with the rate at which it is consumed to obtain a protection duration.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Use one resource unit for stock and the same resource unit per time for the rate; endurance is in that time unit. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: with usable stock $S = 120$ L and consumption $q = 8$ L/day, endurance is $t = 120/8 = 15$ days.
14 — Why the calculation works	Compare the verified usable reserve with the rate at which it is consumed to obtain a protection duration.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about critical-stock endurance under the declared assumptions.
18 — What the result does not	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.

prove	
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Usable stock increases by 10% while consumption remains 8 L/day. Recompute endurance. Detailed guided correction — open after attempting Detailed correction. The new stock is $120 \times 1.10 = 132$ L. Keep $q = 8$ L/day. Therefore $t = 132/8 = 16.5$ days. A 10% increase in the numerator increases endurance by 10%, from 15 to 16.5 days. Autonomous exercise. Build a second numerical scenario for “Critical-stock endurance” by changing at least two inputs in $t = S / q$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $t = S / q$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Trigger resupply, rationing or repair before endurance reaches the protected reserve.
21 — Mission decision	Trigger resupply, rationing or repair before endurance reaches the protected reserve.

Functional safety chain

robust function: identified variable → known limit → measurement → action → backup → recovery

1 — Concrete question	What operational question does this relation answer for functional safety chain?
2 — Intuition without symbols	A vital function is robust only when the crew knows what to monitor, when to act, how to fall back, and how to recover.
3 — Quantities first	The six terms are successive safety functions rather than numerical variables.
4 — Formula	robust function: identified variable → known limit → measurement → action → backup → recovery
5 — Read aloud	Read the relation aloud term by term: robust function: identified variable → known limit → measurement → action → backup → recovery.
6 — Symbols and meaning	The six terms are successive safety functions rather than numerical variables.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	This is a logical chain and has no single physical unit.

9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	A vital function is robust only when the crew knows what to monitor, when to act, how to fall back, and how to recover.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	This is a logical chain and has no single physical unit. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: oxygen partial pressure is measured at 18.8 kPa while the declared operational limit is 19.5 kPa. The safety chain must connect measurement < limit, alarm, backup action, then verified recovery above 19.5 kPa.
14 — Why the calculation works	A vital function is robust only when the crew knows what to monitor, when to act, how to fall back, and how to recover.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about functional safety chain under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. An oxygen measurement drops from 20.5 kPa to 18.8 kPa with a declared limit of 19.5 kPa. Decide whether the safety chain must activate and state the expected recovery condition. Detailed guided correction — open after attempting Detailed correction. 18.8 kPa < 19.5 kPa, so the threshold is crossed and alarm plus backup action must trigger. Recovery is not proved by the action alone: a verified measurement must return above the declared threshold, for example 20.0 kPa > 19.5 kPa. Autonomous exercise. Build a second numerical scenario for “Functional safety chain” by changing at least two inputs in robust function: identified variable → known limit → measurement → action → backup → recovery. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into robust function: identified variable → known limit → measurement → action → backup → recovery, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Reject an architecture that has measurement without action, backup without independence, or recovery without evidence.

21 — Mission decision

Reject an architecture that has measurement without action, backup without independence, or recovery without evidence.

One hardware item can support several functions; that interconnection must remain visible in common-cause analysis.

Design case — function and backup

Take the function “remove CO₂.” Write the sensor that detects drift, nominal removal capacity, saturation signal, backup path, and criterion for returning to normal mode. If the backup uses the same fan or power bus, it is not independent. This simple sheet turns a hardware list into a verifiable survival architecture.

Decision check. A useful design review asks whether the function can be demonstrated end to end: can the sensor detect the state, can the controller decide, can an actuator restore the variable, and can the crew verify recovery? Writing that chain for every vital function exposes hidden dependencies before hardware names dominate the discussion.

2. Atmosphere means pressure plus composition

A habitable atmosphere has total pressure and partial pressures. O₂, CO₂, water vapor, and contaminants must be monitored; correct total pressure can coexist with dangerous composition.

Pressure is also structural load. A 70 kPa difference over 1 m² produces 70 kN ideal resultant force. The atmosphere is both a life resource and a mechanical load.

Quantified balance

Total pressure and composition are insufficient when considered separately. An atmosphere can have correct total pressure but inadequate oxygen, or the reverse. Sensors must therefore distinguish pressure, gas fractions, temperature, humidity, and contaminants rather than reducing “air” to one reading.

Partial pressure in a gas mixture

$$p_i = y_i p_{\text{total}}$$

1 — Concrete question	What operational question does this relation answer for partial pressure in a gas mixture?
2 — Intuition without symbols	The fraction of one gas in the mixture applies the same fraction to total pressure to give that constituent pressure.
3 — Quantities first	p_i is constituent partial pressure, y_i is mole fraction, and p_{total} is total pressure.
4 — Formula	$p_i = y_i p_{\text{total}}$
5 — Read aloud	Read the relation aloud term by term: $p_i = y_i p_{\text{total}}$.
6 — Symbols and meaning	p_i is constituent partial pressure, y_i is mole fraction, and p_{total} is total pressure.

7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	p_i and p_{total} use the same pressure unit; y_i is dimensionless.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	The fraction of one gas in the mixture applies the same fraction to total pressure to give that constituent pressure.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	p_i and p_{total} use the same pressure unit; y_i is dimensionless. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: for $y_i = 0.21$ and $p_{\text{total}} = 70 \text{ kPa}$, $p_i = 0.21 \times 70 = 14.7 \text{ kPa}$.
14 — Why the calculation works	The fraction of one gas in the mixture applies the same fraction to total pressure to give that constituent pressure.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about partial pressure in a gas mixture under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Total pressure increases by 10%, from 70 to 77 kPa, while mole fraction remains 0.21. Recompute p_i. Detailed guided correction — open after attempting Detailed correction. $p_i = y_i p_{\text{total}} = 0.21 \times 77 = 16.17 \text{ kPa}$. Because mole fraction is unchanged, a 10% rise in total pressure produces a 10% rise in partial pressure: $14.7 \rightarrow 16.17 \text{ kPa}$. Autonomous exercise. Build a second numerical scenario for “Partial pressure in a gas mixture” by changing at least two inputs in $p_i = y_i p_{\text{total}}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $p_i = y_i p_{\text{total}}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Compare partial pressure with physiological limits rather than relying on total pressure alone.

21 — Mission decision

Compare partial pressure with physiological limits rather than relying on total pressure alone.

A pressure change shifts every partial pressure even if mole fractions remain temporarily unchanged.

Calculation case — atmosphere

Assume 70 kPa with 30% O_2 and 0.6% CO_2 in a teaching case. Partial pressures are 21 kPa O_2 and 0.42 kPa CO_2 . If total pressure falls to 60 kPa with fractions temporarily unchanged, they become 18 kPa and 0.36 kPa. The same percentage therefore does not represent the same physiological state when total pressure changes.

Decision check. For atmosphere control, the practical test is to calculate at least one off-nominal state. Change total pressure, oxygen fraction, and CO_2 independently and observe which sensor would first show unacceptable conditions. That exercise prevents one “green” indicator from being mistaken for proof that the whole atmosphere is safe.

3. CO_2 , humidity, and contaminants accumulate

Crew continuously produces CO_2 and water vapor. Removal systems need capacity for nominal operation, activity peaks, restarts, and some partial failures. Treatment flow must be compared with production flow.

Measurement is a barrier. A good scrubber with a bad sensor can allow silent drift. Calibration, , and cross-checks therefore belong to life support.

Space Academy · 12

Fermeture de l'eau / water-loop closure



A high percentage can still create tonnes of makeup

Water loop: collection, treatment, quality control, recovery and residual makeup.

Degraded mode

CO₂, water vapor, and contaminants are continuous source terms. Sizing must compare plausible maximum production with available removal and include regeneration, sorbent changeout, and maintenance intervals. Nominal capacity exactly equal to production leaves no margin for drift or an extra crew member.

Dynamic inventory balance

$$dM/dt = \text{generation} - \text{removal}$$

1 — Concrete question	What operational question does this relation answer for dynamic inventory balance?
2 — Intuition without symbols	An inventory rises when generation exceeds removal and falls when removal exceeds generation.
3 — Quantities first	dM/dt is inventory change rate; generation and removal are mass-flow terms on the same boundary.
4 — Formula	$dM/dt = \text{generation} - \text{removal}$
5 — Read aloud	Read the relation aloud term by term: $dM/dt = \text{generation} - \text{removal}$.
6 — Symbols and meaning	dM/dt is inventory change rate; generation and removal are mass-flow terms on the same boundary.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	All rates use the same mass-per-time unit.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system

	boundary and time basis from start to finish.
10 — Why this operation	An inventory rises when generation exceeds removal and falls when removal exceeds generation.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	All rates use the same mass-per-time unit. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: generation of 6 kg/day and removal of 8 kg/day gives $dM/dt = 6 - 8 = -2$ kg/day, so inventory decreases.
14 — Why the calculation works	An inventory rises when generation exceeds removal and falls when removal exceeds generation.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about dynamic inventory balance under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Generation increases by 10%, from 6 to 6.6 kg/day, while removal remains 8 kg/day. Recompute the balance. Detailed guided correction — open after attempting Detailed correction. $dM/dt = 6.6 - 8 = -1.4$ kg/day. The balance is still negative, but the resource debt is 0.6 kg/day smaller than the initial -2 kg/day case. Corrective action is still required if the trend persists. Autonomous exercise. Build a second numerical scenario for “Dynamic inventory balance” by changing at least two inputs in $dM/dt = \text{generation} - \text{removal}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $dM/dt = \text{generation} - \text{removal}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Treat a sustained negative balance as a measurable resource debt.
21 — Mission decision	Treat a sustained negative balance as a measurable resource debt.

A large cabin or buffer can slow concentration rise without correcting the flow imbalance.

Drift case — contaminant

A loop generates 0.25 kg/h of an equivalent contaminant and removes 0.24 kg/h. The difference looks tiny: 0.01 kg/h. Yet it accumulates 0.24 kg in 24 h and 7.2 kg in 30 days. The exercise shows why flow balance must close at adequate precision and why a small persistent drift can become a slow emergency.

4. Oxygen, electrolysis, and Sabatier

Water produces O₂ and H₂. Removed CO₂ can react with H₂ through chemistry to produce CH₄ and H₂O; recovered water can return toward electrolysis.

Sabatier stoichiometry



1 — Concrete question	What operational question does this relation answer for sabatier stoichiometry?
2 — Intuition without symbols	The reaction rearranges the same atoms between reactants and products, fixing ideal material proportions.
3 — Quantities first	CO ₂ is carbon dioxide, H ₂ hydrogen, CH ₄ methane, and H ₂ O water; coefficients are stoichiometric.
4 — Formula	CO ₂ + 4 H ₂ → CH ₄ + 2 H ₂ O
5 — Read aloud	Read the relation aloud term by term: CO ₂ + 4 H ₂ → CH ₄ + 2 H ₂ O.
6 — Symbols and meaning	CO ₂ is carbon dioxide, H ₂ hydrogen, CH ₄ methane, and H ₂ O water; coefficients are stoichiometric.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Coefficients are dimensionless; amounts are in moles and masses follow from molar masses.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	The reaction rearranges the same atoms between reactants and products, fixing ideal material proportions.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Coefficients are dimensionless; amounts are in moles and masses follow from molar masses. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Ideal stoichiometric case: 44 kg CO ₂ reacts with 8 kg H ₂ to produce 16 kg CH ₄ and 36 kg H ₂ O.
14 — Why the calculation works	The reaction rearranges the same atoms between reactants and products, fixing ideal material proportions.

15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about sabatier stoichiometry under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. CO₂ is increased by 10% to 48.4 kg, but only 8 kg H₂ remains available. Identify the limiting reactant and ideal products. Detailed guided correction — open after attempting Detailed correction. The ideal ratio requires 8 kg H₂ for 44 kg CO₂. With only 8 kg H₂, hydrogen remains limiting, so only 44 kg CO₂ can react. Products remain 16 kg CH₄ and 36 kg H₂O, with 48.4 – 44 = 4.4 kg CO₂ left over. Increasing a non-limiting reactant does not increase output. Autonomous exercise. Build a second numerical scenario for “Sabatier stoichiometry” by changing at least two inputs in CO₂ + 4 H₂ → CH₄ + 2 H₂O. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into CO₂ + 4 H₂ → CH₄ + 2 H₂O, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Size flows from the limiting reactant and keep real yield separate from ideal stoichiometry.
21 — Mission decision	Size flows from the limiting reactant and keep real yield separate from ideal stoichiometry.

Integration increases recovery but also creates interfaces. Safe design needs isolation so catalyst, compressor, or separator faults do not simultaneously compromise potable water and oxygen generation.

Safety reading

Oxygen can come from stored inventory, electrolysis, or a chain coupled to CO₂ processing. Each path has different dependencies on water, power, compression, and consumables. A safe architecture must isolate a failed subsystem without contaminating or stopping the entire loop.

Electrolysis-Sabatier coupling



1 — Concrete question	What operational question does this relation answer for electrolysis-sabatier coupling?
2 — Intuition without symbols	Water can supply hydrogen and oxygen, then hydrogen can feed Sabatier together with carbon dioxide.
3 — Quantities first	H ₂ O, H ₂ , O ₂ , CO ₂ and CH ₄ are linked by two atom-conserving reactions.
4 — Formula	$2\text{H}_2\text{O} \rightarrow 2\text{H}_2 + \text{O}_2$; $\text{CO}_2 + 4\text{H}_2 \rightarrow \text{CH}_4 + 2\text{H}_2\text{O}$
5 — Read aloud	Read the relation aloud term by term: $2\text{H}_2\text{O} \rightarrow 2\text{H}_2 + \text{O}_2$; $\text{CO}_2 + 4\text{H}_2 \rightarrow \text{CH}_4 + 2\text{H}_2\text{O}$.
6 — Symbols and meaning	H ₂ O, H ₂ , O ₂ , CO ₂ and CH ₄ are linked by two atom-conserving reactions.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Use moles for stoichiometric coupling, then convert to mass or flow with molar masses.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Water can supply hydrogen and oxygen, then hydrogen can feed Sabatier together with carbon dioxide.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Use moles for stoichiometric coupling, then convert to mass or flow with molar masses. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Ideal case: 36 kg water gives 4 kg H ₂ and 32 kg O ₂ by electrolysis. Those 4 kg H ₂ are half the 8 kg H ₂ required for 44 kg CO ₂ in the Sabatier reaction.
14 — Why the calculation works	Water can supply hydrogen and oxygen, then hydrogen can feed Sabatier together with carbon dioxide.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about electrolysis-sabatier coupling under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase electrolyzed water by 10% to 39.6 kg. Compute H₂ and O₂ output, then the amount of CO₂ compatible with all produced H₂ in Sabatier. Detailed guided correction — open after attempting

Detailed correction. $39.6/36 = 1.10$, so ideal electrolysis gives $4 \times 1.10 = 4.4$ kg H₂ and $32 \times 1.10 = 35.2$ kg O₂. Sabatier consumes $44/8 = 5.5$ kg CO₂ per kg H₂, so $4.4 \times 5.5 = 24.2$ kg CO₂. Associated ideal products are 8.8 kg CH₄ and 19.8 kg H₂O.

Autonomous exercise. Build a second numerical scenario for “Electrolysis-Sabatier coupling” by changing at least two inputs in $2\text{H}_2\text{O} \rightarrow 2\text{H}_2 + \text{O}_2$; $\text{CO}_2 + 4\text{H}_2 \rightarrow \text{CH}_4 + 2\text{H}_2\text{O}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change.

Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $2\text{H}_2\text{O} \rightarrow 2\text{H}_2 + \text{O}_2$; $\text{CO}_2 + 4\text{H}_2 \rightarrow \text{CH}_4 + 2\text{H}_2\text{O}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Never count the same recycled molecule twice in the overall material balance.

21 — Mission decision

Never count the same recycled molecule twice in the overall material balance.

Stoichiometry gives ideal masses; it does not give electrical efficiency, purity, or catalyst life.

Material case — oxygen

In an ideal balance, electrolyzing 72 kg water yields 8 kg H₂ and 64 kg O₂. If the 8 kg H₂ feeds Sabatier with 44 kg CO₂, the reaction makes 36 kg water and 16 kg CH₄; only half the original hydrogen returns after re-electrolysis of that water. The loop therefore still has an open boundary that must be identified.

5. Water: understand the 98% milestone

NASA reported ISS ECLSS demonstrated about 98% total water recovery with the Brine Processor Assembly, compared with roughly 93–94% beforehand. The aggregate result does not mean every stream recovers 98%.

Teaching case: $q = 20$ kg/person/day gross processed flow. For 100 people, 2,000 kg/day passes through the model. At $R = 0.98$, makeup = 40 kg/day; at 0.94, 120 kg/day. Difference = 80 kg/day or 29.2 t/year.

Make-up demand with recovery

$$M_{\text{makeup}} = q \times N \times (1 - R)$$

1 — Concrete question	What operational question does this relation answer for make-up demand with recovery?
2 — Intuition without symbols	Gross crew demand is reduced by the fraction actually recovered, and only the unrecovered part needs make-up.
3 — Quantities first	q is gross demand per person, N crew count, R recovery fraction, and M_{makeup} external make-up per time.
4 — Formula	$M_{\text{makeup}} = q \times N \times (1 - R)$
5 — Read aloud	Read the relation aloud term by term: $M_{\text{makeup}} = q \times N \times (1 - R)$.

6 — Symbols and meaning	q is gross demand per person, N crew count, R recovery fraction, and M_{makeup} external make-up per time.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	If q is kg per person per day, M_{makeup} is kg/day; R is dimensionless.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Gross crew demand is reduced by the fraction actually recovered, and only the unrecovered part needs make-up.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	If q is kg per person per day, M_{makeup} is kg/day; R is dimensionless. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: $q = 20$ kg/person/day, $N = 20$, and $R = 0.98$ gives $M_{\text{makeup}} = 20 \times 20 \times 0.02 = 8$ kg/day.
14 — Why the calculation works	Gross crew demand is reduced by the fraction actually recovered, and only the unrecovered part needs make-up.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about make-up demand with recovery under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase q by 10%, from 20 to 22 kg/person/day, keeping $N = 20$ and $R = 0.98$. Recompute make-up demand. Detailed guided correction — open after attempting Detailed correction. $M_{\text{makeup}} = 22 \times 20 \times (1 - 0.98) = 440 \times 0.02 = 8.8$ kg/day. A 10% increase in gross demand produces a 10% increase in make-up here, from 8 to 8.8 kg/day. Autonomous exercise. Build a second numerical scenario for “Make-up demand with recovery” by changing at least two inputs in $M_{\text{makeup}} = q \times N \times (1 - R)$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $M_{\text{makeup}} = q \times N \times (1 - R)$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Size make-up inventory from

demonstrated real-mode recovery, not the best laboratory figure.

21 — Mission decision

Size make-up inventory from demonstrated real-mode recovery, not the best laboratory figure.

Exercise 5

For 1,000 people, $q = 20$ kg/day and $R = 0.98$: yearly makeup?

Solution: $400 \text{ kg/day} \times 365 = 146,000 \text{ kg} = 146 \text{ t/year}$. q is a teaching assumption.

The 146 t/year result shows why 98% recovery is not autonomy. At 1,000 people the remaining two percent becomes a major logistics flow, and q must stay explicitly labeled as a teaching assumption.

Integrated case — 98% recovery does not eliminate losses

NASA demonstrated roughly 98% total water recovery on the ISS, compared with about 93–94% before the brine processor milestone. Use a teaching gross flow of 20 kg/person/day. For 20 people, gross flow is 400 kg/day. At 98% recovery, ideal makeup from unrecovered fraction alone is 8 kg/day or about 2.92 t/year. At 94%, it is 24 kg/day or 8.76 t/year. Four percentage points therefore change annual makeup by 5.84 t in this example.

Do not turn the teaching flow into a NASA requirement for a Mars colonist: 20 kg/person/day is only a loop-throughput assumption. Leaks, maintenance losses, rejected water, water embodied in processes or food, and contingency inventory sit outside that simple calculation. A headline recovery percentage never replaces a stream-by-stream balance.

Recovery-efficiency leverage

at 98%: 8 kg/day; at 94%: 24 kg/day; annual difference = 5.84 t

1 — Concrete question	What operational question does this relation answer for recovery-efficiency leverage?
2 — Intuition without symbols	A small drop in recovery percentage can multiply the make-up mass that must be supplied over a long mission.
3 — Quantities first	The comparison uses the same crew demand while changing only the recovery fraction.
4 — Formula	at 98%: 8 kg/day; at 94%: 24 kg/day; annual difference = 5.84 t
5 — Read aloud	Read the relation aloud term by term: at 98%: 8 kg/day; at 94%: 24 kg/day; annual difference = 5.84 t.
6 — Symbols and meaning	The comparison uses the same crew demand while changing only the recovery fraction.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Daily make-up is kg/day and the annualized difference is kg/year or tonnes/year.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this	A small drop in recovery percentage can multiply the make-up mass that must be supplied

operation	over a long mission.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Daily make-up is kg/day and the annualized difference is kg/year or tonnes/year. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: for 400 kg/day gross flow, 98% recovery requires 8 kg/day make-up while 94% requires 24 kg/day. The 16 kg/day gap is 5,840 kg/year, or 5.84 t/year.
14 — Why the calculation works	A small drop in recovery percentage can multiply the make-up mass that must be supplied over a long mission.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about recovery-efficiency leverage under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. With the same 400 kg/day gross flow, let recovery fall from 98% to 97%. Compute the new make-up and annual difference relative to 98%. Detailed guided correction — open after attempting Detailed correction. At 97%, the unrecovered fraction is 3%, so make-up is $400 \times 0.03 = 12$ kg/day. Compared with 8 kg/day at 98%, the difference is +4 kg/day. Over 365 days: $4 \times 365 = 1,460$ kg/year, or 1.46 t/year extra. Autonomous exercise. Build a second numerical scenario for “Recovery-efficiency leverage” by changing at least two inputs in at 98%: 8 kg/day; at 94%: 24 kg/day; annual difference = 5.84 t. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into at 98%: 8 kg/day; at 94%: 24 kg/day; annual difference = 5.84 t, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Treat a few lost recovery points as a major logistics consequence on a long mission.
21 — Mission decision	Treat a few lost recovery points as a major logistics consequence on a long mission.

System intuition

The ISS 98% milestone is demonstrated overall recovery in a specific architecture, not a promise that every Mars loop will lose exactly 2%. For engineering, convert the percentage into makeup mass, then add storage, quality control, maintenance losses, and outage scenarios.

The flow q must be defined: drinking water alone, total processed water, or loop throughput produce very different answers.

Logistics case — water

For 100 people, use a teaching processed flow of 20 kg/person/day. At 98% recovery, ideal makeup is 40 kg/day; at 94%, 120 kg/day. Over a year the difference is 29.2 tonnes. This does not define a real settlement flow; it shows the logistics sensitivity to a few recovery points at larger population.

6. Recovered water still needs qualification

NASA describes ISS processing with filtration, catalytic treatment, quality sensors, and reprocessing of unacceptable water. A recovery loop is therefore also a continuous quality-control system.

A false “good” sensor indication can be more dangerous than a filter that fails visibly. Sampling, calibration, acceptance criteria, and buffer storage limit propagation of one bad measurement.

Space Academy · 12

Compartmentage et refuge / compartmentation and safe haven



The safe haven must survive loss of another zone

Safe haven and degraded mode: sequence isolation, reserves, repair and return to service.

Quantified balance

Water quality is separate from mass recovery. A highly efficient loop that passes a critical contaminant is unusable. Define quality parameters, sampling frequency, sensors, confirmatory analyses, reprocessing capacity, and quarantine volume for suspect batches.

Produced-water acceptance

accepted water = produced water $\cap$ quality criteria

1 — Concrete question	What operational question does this relation answer for produced-water acceptance?
2 — Intuition without symbols	Producing water is not enough: it enters usable inventory only after the required quality criteria are met.
3 — Quantities first	Produced water is the process output; acceptance criteria represent the required verified quality conditions.
4 — Formula	accepted water = produced water $\cap$ quality criteria
5 — Read aloud	Read the relation aloud term by term: accepted water = produced water $\cap$ quality criteria.
6 — Symbols and meaning	Produced water is the process output; acceptance criteria represent the required verified quality conditions.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	This is a logical acceptance relation; individual quality measurements keep their own units.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Producing water is not enough: it enters usable inventory only after the required quality criteria are met.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	This is a logical acceptance relation; individual quality measurements keep their own units. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching qualification example: a 120 L batch meets a pedagogical conductivity limit of 5 $\mu\text{S}/\text{cm}$ at 4.8 $\mu\text{S}/\text{cm}$, but total organic carbon is 0.70 mg/L against a pedagogical limit of 0.50 mg/L. Volume is sufficient, yet the batch remains rejected because one criterion fails.
14 — Why the calculation works	Producing water is not enough: it enters usable inventory only after the required quality criteria are met.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about produced-water acceptance under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.

20 — Guided and autonomous practice

Guided exercise. After reprocessing, the same 120 L batch measures 4.6 $\mu\text{S}/\text{cm}$ and 0.40 mg/L against the same pedagogical limits. Apply the acceptance rule.

Detailed guided correction — open after attempting

Detailed correction. Conductivity: $4.6 < 5 \mu\text{S}/\text{cm}$, PASS. Total organic carbon: $0.40 < 0.50 \text{ mg/L}$, PASS. Both declared criteria are satisfied; in this teaching scenario limited to those two criteria, the batch can be accepted. This calculation is not a real drinking-water standard.

Autonomous exercise. Build a second numerical scenario for “Produced-water acceptance” by changing at least two inputs in accepted water = produced water n quality criteria. Compute the result, check units and order of magnitude, then state whether the mission decision should change.

Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into accepted water = produced water n quality criteria, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Keep produced, tested, and accepted water separate in both physical routing and inventory records.

21 — Mission decision

Keep produced, tested, and accepted water separate in both physical routing and inventory records.

A compliant measurement does not prove every possible contaminant was measured; the control plan must connect risk with analytical method.

Qualification case — water

Imagine a processor producing 500 L/day while 2% of batches are temporarily off specification. Even with excellent mass recovery, operations need buffer volume to isolate, reprocess, or analyze those batches. If laboratory confirmation takes 12 h, the buffer cannot be sized only from average consumption.

7. Food and waste: partial closure

Food combines calories, protein, micronutrients, water, shelf life, and acceptability. Crops can supply fresh food and contribute to gas exchange without instantly removing food logistics.

Waste retains water, carbon, nitrogen, phosphorus, and materials. Recovery requires energy, reactors, sanitation controls, and maintenance. Optimum closure can remain below 100% when marginal recovery costs exceed its value.

Degraded mode

Food creates a trade among shipped mass, water content, nutritional stability, crew time, fresh crops, and waste. Plants can provide variety and micronutrients without making the habitat automatically calorie-self-sufficient. The balance must count lighting energy, water, nutrients, volume, maintenance, and crop losses.

Wet-food mass from dry matter

$$m_{\text{food}} = m_{\text{dry}} / (1 - f_{\text{water}})$$

1 — Concrete question	What operational question does this relation answer for wet-food mass from dry matter?
2 — Intuition without symbols	Dry matter is only the non-water fraction of food; total food mass must include the water fraction.
3 — Quantities first	m_{food} is total wet-food mass, m_{dry} dry matter, and f_{water} the water mass fraction.
4 — Formula	$m_{\text{food}} = m_{\text{dry}} / (1 - f_{\text{water}})$
5 — Read aloud	Read the relation aloud term by term: $m_{\text{food}} = m_{\text{dry}} / (1 - f_{\text{water}})$.
6 — Symbols and meaning	m_{food} is total wet-food mass, m_{dry} dry matter, and f_{water} the water mass fraction.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	m_{food} and m_{dry} use the same mass unit; f_{water} is dimensionless.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Dry matter is only the non-water fraction of food; total food mass must include the water fraction.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	m_{food} and m_{dry} use the same mass unit; f_{water} is dimensionless. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: with $m_{\text{dry}} = 6 \text{ kg}$ and $f_{\text{water}} = 0.60$, $m_{\text{food}} = 6 / (1 - 0.60) = 15 \text{ kg}$.
14 — Why the calculation works	Dry matter is only the non-water fraction of food; total food mass must include the water fraction.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about wet-food mass from dry matter under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase water fraction by 10% relatively, from 0.60 to 0.66, while keeping 6 kg dry matter. Recompute total mass.

Detailed guided correction — open after attempting

Detailed correction. $1 - 0.66 = 0.34$, so $m_{\text{food}} = 6/0.34 = \text{about } 17.65 \text{ kg}$. Extra water raises wet mass while dry matter remains 6 kg: $15.0 \rightarrow 17.65 \text{ kg}$.

Autonomous exercise. Build a second numerical scenario for “Wet-food mass from dry matter” by changing at least two inputs in $m_{\text{food}} = m_{\text{dry}} / (1 - f_{\text{water}})$. Compute the result, check units and order of magnitude, then state whether the mission decision should change.

Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $m_{\text{food}} = m_{\text{dry}} / (1 - f_{\text{water}})$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Separate nutritional dry mass from total logistics mass before sizing stores and waste flows.

21 — Mission decision

Separate nutritional dry mass from total logistics mass before sizing stores and waste flows.

Reducing food mass can shift demand into water or energy; the optimum must be judged at system level.

System case — food

A 2.0 kg/day prepackaged ration at 46% water contains 1.08 kg dry matter. At 30% water, the same dry matter would weigh 1.54 kg/day. Shipped mass falls by about 0.46 kg/day, but the water loop must supply more at use. The system boundary must move rather than counting the saving twice.

Decision check. Food also couples to waste handling. Packaging, uneaten material, plant residues, nutrient solution, and sanitation loads become flows that consume storage and processing capacity. A crop system that reduces imported food mass can still increase electrical load and crew time, so the trade must remain multi-resource.

8. Fire, depressurization, safe haven

Fire combines heat, smoke, and toxic gases; combines atmosphere loss with structural danger. Both can require leaving nominal operation locally through compartmentation, hatches, masks, extinguishers, reserves, and .

A safe haven needs independent air, water, power, and communications for a defined duration covering detection, isolation, diagnosis, and repair. Emergency consumables should not share the same failure path they protect against.

Safe-haven scenario — 72 hours without external resources

Imagine an isolated refuge for six people over 72 hours. Start with functions rather than an arbitrary mass: pressure, oxygen, CO₂ removal, drinking water, temperature, control power, minimum lighting, communication, medical care, and sanitation. Give each function a stock or capacity, margin, and exit criterion. A refuge is not merely a stronger room; it is an isolatable miniature life-support system.

For direct drinking water, if a teaching scenario assumes 4 kg/person/day, arithmetic baseline is $6 \times 4 \times 3 = 72 \text{ kg}$ before margin. Adding 25% gives 90 kg. That mass does not include fire suppression or medical uses. A critical electrical load averaging 1.5 kW for 72 h requires 108 kWh useful; with an 85% storage chain, upstream stored energy is about 127 kWh. Two functions, two budgets, and two explicitly separate assumptions.

Three-day refuge water and energy

$$M_{\text{water}} = N q t k ; E_{\text{storage}} = P t / \eta$$

1 — Concrete question	What operational question does this relation answer for three-day refuge water and energy?
2 — Intuition without symbols	A refuge must cover both crew demand and critical energy for the whole protected duration, with an explicit margin.
3 — Quantities first	N is crew count, q essential water per person per day, t duration, k contingency factor, P critical power, and eta usable storage efficiency.
4 — Formula	$M_{\text{water}} = N q t k ; E_{\text{storage}} = P t / \eta$
5 — Read aloud	Read the relation aloud term by term: $M_{\text{water}} = N q t k ; E_{\text{storage}} = P t / \eta$.
6 — Symbols and meaning	N is crew count, q essential water per person per day, t duration, k contingency factor, P critical power, and eta usable storage efficiency.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Water is in kg or L; energy is in kWh when power is kW and time is hours; eta is dimensionless.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	A refuge must cover both crew demand and critical energy for the whole protected duration, with an explicit margin.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Water is in kg or L; energy is in kWh when power is kW and time is hours; eta is dimensionless. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: N = 6, q = 4 kg/person/day, t = 3 days, and k = 1.25 gives $M_{\text{water}} = 6 \times 4 \times 3 \times 1.25 = 90$ kg. For P = 1.5 kW over 72 h with $\eta = 0.85$, $E_{\text{storage}} = 1.5 \times 72 / 0.85 = 127.1$ kWh.
14 — Why the calculation works	A refuge must cover both crew demand and critical energy for the whole protected duration, with an explicit margin.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about three-day refuge water and energy under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.

20 — Guided and autonomous practice

Guided exercise. Increase refuge duration by 10%, from 3 to 3.3 days, keeping all other assumptions unchanged. Recompute required water and stored energy.

Detailed guided correction — open after attempting

Detailed correction. Water: $M_{\text{water}} = 6 \times 4 \times 3.3 \times 1.25 = 99 \text{ kg}$. Energy: 3.3 days = 79.2 h; $E_{\text{storage}} = 1.5 \times 79.2 / 0.85 = \text{about } 139.8 \text{ kWh}$. Both needs rise by 10% because duration enters both relations linearly.

Autonomous exercise. Build a second numerical scenario for “Three-day refuge water and energy” by changing at least two inputs in $M_{\text{water}} = N q t k$; $E_{\text{storage}} = P t / \eta$. Compute the result, check units and order of magnitude, then state whether the mission decision should change.

Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $M_{\text{water}} = N q t k$; $E_{\text{storage}} = P t / \eta$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Approve the refuge only if water, energy, air, communications, and access remain independent of the primary failure.

21 — Mission decision

Approve the refuge only if water, energy, air, communications, and access remain independent of the primary failure.

Safety reading

Fire and depressurization demand different responses in some respects: fire can require confinement, ventilation isolation, or suppression, while a leak requires volume isolation and pressure-loss management. A safe haven must remain habitable during repair without depending on the failure that triggered the emergency.

Refuge endurance

$$t_{\text{refuge}} = \text{stocks} / \text{emergency-use rate}$$

1 — Concrete question

What operational question does this relation answer for refuge endurance?

2 — Intuition without symbols

Useful refuge duration is set by the critical resource that is exhausted first in emergency mode.

3 — Quantities first

stocks is verified emergency inventory; emergency-use rate is the corresponding consumption rate; t_{refuge} is endurance.

4 — Formula

$$t_{\text{refuge}} = \text{stocks} / \text{emergency-use rate}$$

5 — Read aloud

Read the relation aloud term by term: $t_{\text{refuge}} = \text{stocks} / \text{emergency-use rate}$.

6 — Symbols and meaning

stocks is verified emergency inventory; emergency-use rate is the corresponding consumption rate; t_{refuge} is endurance.

7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Stock divided by stock-per-time gives time.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Useful refuge duration is set by the critical resource that is exhausted first in emergency mode.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Stock divided by stock-per-time gives time. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: a verified 90 kg stock consumed at 30 kg/day gives $t_{\text{refuge}} = 90/30 = 3$ days.
14 — Why the calculation works	Useful refuge duration is set by the critical resource that is exhausted first in emergency mode.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about refuge endurance under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase stock by 10%, from 90 to 99 kg, keeping emergency consumption at 30 kg/day. Recompute endurance. Detailed guided correction — open after attempting Detailed correction. $t_{\text{refuge}} = 99/30 = 3.3$ days. With the rate unchanged, +10% stock gives +10% endurance: $3.0 \rightarrow 3.3$ days. Autonomous exercise. Build a second numerical scenario for “Refuge endurance” by changing at least two inputs in $t_{\text{refuge}} = \text{stocks} / \text{emergency-use rate}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $t_{\text{refuge}} = \text{stocks} / \text{emergency-use rate}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Use the minimum of water, energy, oxygen, and critical-consumable endurance as the refuge endurance.

21 — Mission decision

Use the minimum of water, energy, oxygen, and critical-consumable endurance as the refuge endurance.

NASA's 30-day safe-haven concept is a studied architecture, not a universal duration; each mission must demonstrate its own recovery time.

Emergency case — safe haven

For eight people over 30 days, a 3 kW average vital load requires 2,160 kWh if no generation is available. With 80% usable stored energy and 90% conversion efficiency, nominal storage becomes $2,160 / (0.8 \times 0.9) \approx 3,000$ kWh. The exercise separates useful demand, usable depth, and conversion loss.

9. Martian dust: measurable contamination

In July 2026 NASA established a preliminary requirement of 0.1 mg/m³ as a 24-hour average for Martian particles below 10 µm in specified exposure scenarios up to 30 days. Uncertainty remains because authentic airborne Mars has not been returned for full human toxicology.

At that concentration, 100 m³ contains 10 mg suspended on average. Small mass can still matter for fine-particle inhalation, so airlocks, suit handling, cleaning, filtration, and monitoring form layered control.

scenario — dust, airlock, cross-contamination

NASA published in July 2026 a preliminary requirement for Martian particles below 10 µm: 24-hour time-weighted average below 0.1 mg/m³ for certain exposure scenarios up to 30 days. In a 150 m³ habitat that concentration corresponds to 15 mg of airborne mass at that average. A very small total mass can therefore matter when dispersed as respirable fine particles.

Contamination architecture aims to prevent dust from reaching habitable air: dirty and clean zones, suit cleaning, cleanable surfaces, filtration, measurement, and post-EVA procedures. Because authentic airborne Martian dust has not been returned to Earth, NASA explicitly describes uncertainty in the initial limit. Design should therefore preserve the ability to measure and revise rather than treating 0.1 mg/m³ as an immutable biological constant.

Total dust loading

$m = C \times V$

1 — Concrete question	What operational question does this relation answer for total dust loading?
2 — Intuition without symbols	Concentration multiplied by the affected air volume gives the total mass present in that volume.
3 — Quantities first	C is dust concentration, V air volume, and m total dust mass.
4 — Formula	$m = C \times V$

5 — Read aloud	Read the relation aloud term by term: $m = C \times V$.
6 — Symbols and meaning	C is dust concentration, V air volume, and m total dust mass.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	mg/m ³ multiplied by m ³ gives mg.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Concentration multiplied by the affected air volume gives the total mass present in that volume.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	mg/m ³ multiplied by m ³ gives mg. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: C = 0.10 mg/m ³ across V = 150 m ³ gives m = 0.10 × 150 = 15 mg suspended material.
14 — Why the calculation works	Concentration multiplied by the affected air volume gives the total mass present in that volume.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about total dust loading under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Concentration increases by 10%, from 0.10 to 0.11 mg/m³, for the same 150 m³ volume. Recompute total loading. Detailed guided correction — open after attempting Detailed correction. $m = 0.11 \times 150 = 16.5$ mg. A 10% rise in concentration gives a 10% rise in total loading at constant volume: 15 → 16.5 mg. Autonomous exercise. Build a second numerical scenario for “Total dust loading” by changing at least two inputs in $m = C \times V$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $m = C \times V$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Use this mass to plan

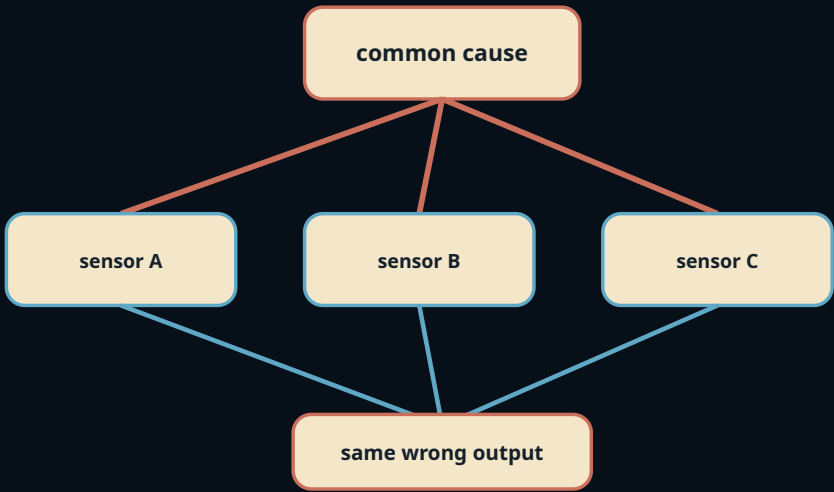
21 — Mission decision

containment, filtration, cleaning, and sampling without confusing it with inhaled dose.

Use this mass to plan containment, filtration, cleaning, and sampling without confusing it with inhaled dose.

Space Academy · 12

Arbre de cause commune / common-cause fault tree



Three identical sensors do not imply three independent failure causes

Redundancy and common cause: identify what can defeat two supposedly independent paths at once.

System intuition

Martian dust should be treated as a contamination flow: EVA ingress, deposition, resuspension, filtration, and removal. NASA’s new 2026 requirement provides a 24-hour average limit for particles <10 μm, while design must also address local peaks and toxicology uncertainty.

Time-weighted average exposure

C_TWA = (Σ C_i Δt_i)/(Σ Δt_i)

1 — Concrete question	What operational question does this relation answer for time-weighted average exposure?
2 — Intuition without symbols	Each exposure level matters in proportion to how long it lasts, so the average must weight concentration by time.
3 — Quantities first	C_i is concentration during interval i, Delta t_i its duration, and C_TWA the time-weighted average.
4 — Formula	C_TWA = (Σ C_i Δt_i)/(Σ Δt_i)

5 — Read aloud	Read the relation aloud term by term: $C_TWA = (\sum C_i \Delta t_i) / (\sum \Delta t_i)$.
6 — Symbols and meaning	C_i is concentration during interval i , Δt_i its duration, and C_TWA the time-weighted average.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Concentration-times-time divided by time returns concentration.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Each exposure level matters in proportion to how long it lasts, so the average must weight concentration by time.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Concentration-times-time divided by time returns concentration. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: 4 h at 0.10 mg/m ³ followed by 4 h at 0.20 mg/m ³ gives $C_TWA = (0.10 \times 4 + 0.20 \times 4) / 8 = 0.15$ mg/m ³ .
14 — Why the calculation works	Each exposure level matters in proportion to how long it lasts, so the average must weight concentration by time.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about time-weighted average exposure under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase the second-interval concentration by 10%, from 0.20 to 0.22 mg/m³, with durations unchanged. Recompute the time-weighted average. Detailed guided correction — open after attempting Detailed correction. Numerator = $0.10 \times 4 + 0.22 \times 4 = 0.40 + 0.88 = 1.28$ mg·h/m³. Total duration = 8 h. Therefore $C_TWA = 1.28 / 8 = 0.16$ mg/m³. A 10% increase during only half the exposure raises TWA by 0.01 mg/m³. Autonomous exercise. Build a second numerical scenario for “Time-weighted average exposure” by changing at least two inputs in $C_TWA = (\sum C_i \Delta t_i) / (\sum \Delta t_i)$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $C_{TWA} = (\sum C_i \Delta t_i) / (\sum \Delta t_i)$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Compare average and peaks separately: an acceptable average does not make an extreme peak acceptable.

21 — Mission decision

Compare average and peaks separately: an acceptable average does not make an extreme peak acceptable.

An acceptable average can hide a large airlock peak; sensor location and sampling strategy matter.

Exposure case — dust

A 24-hour time-weighted average can combine 0.20 mg/m³ for 2 h near the airlock and 0.05 mg/m³ for 22 h. The average is 0.0625 mg/m³. It is below 0.1 mg/m³ in this example, but the 0.20 peak can still matter operationally and for sampling strategy.

10. Radiation, EVA, and return time

Background radiation and solar events create shielding and exposure-time problems. EVA adds vacuum, dust, fatigue, thermal control, and suit dependence. These risks belong in schedules and return plans.

A better-shielded zone and decision rules can support radiation events. EVA needs consumables margin and a return path after credible faults. Survival is partly management of available time.

Quantified balance

Radiation and EVA become a time-to-shielding problem. A distant sortie adds return delay, mobility dependence, and possible simultaneous failure. Procedures must connect forecast, alarm, distance, degraded speed, accumulated dose, and shelter capability.

Degraded-mode return time

$$t_{\text{return}} = d / v_{\text{degraded}}$$

1 — Concrete question	What operational question does this relation answer for degraded-mode return time?
2 — Intuition without symbols	Distance to travel divided by the speed actually sustainable in degraded mode gives the minimum return time.
3 — Quantities first	d is return distance, v_degraded degraded speed, and t_return return time.
4 — Formula	$t_{\text{return}} = d / v_{\text{degraded}}$
5 — Read aloud	Read the relation aloud term by term: $t_{\text{return}} = d / v_{\text{degraded}}$.
6 — Symbols and meaning	d is return distance, v_degraded degraded speed, and t_return return time.

7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Distance divided by distance-per-time gives time.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Distance to travel divided by the speed actually sustainable in degraded mode gives the minimum return time.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Distance divided by distance-per-time gives time. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: at $d = 18$ km from shelter and $v_{\text{degraded}} = 6$ km/h, $t_{\text{return}} = 18/6 = 3$ h.
14 — Why the calculation works	Distance to travel divided by the speed actually sustainable in degraded mode gives the minimum return time.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about degraded-mode return time under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Distance increases by 10%, from 18 to 19.8 km, while degraded speed remains 6 km/h. Recompute return time. Detailed guided correction — open after attempting Detailed correction. $t_{\text{return}} = 19.8/6 = 3.3$ h, or 3 h 18 min. At constant speed, +10% distance gives +10% return time: $3.0 \rightarrow 3.3$ h. Autonomous exercise. Build a second numerical scenario for “Degraded-mode return time” by changing at least two inputs in $t_{\text{return}} = d / v_{\text{degraded}}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $t_{\text{return}} = d / v_{\text{degraded}}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Limit excursions so degraded return retains margin on oxygen, energy, thermal control, and fatigue.

21 — Mission decision

Limit excursions so degraded return retains margin on oxygen, energy, thermal control, and fatigue.

Travel-time calculation does not directly convert a radiation event into dose; it defines the operational response window.

Return case — EVA

A crew works 24 km from shelter. At 12 km/h nominal, return takes 2 h. If a failure cuts speed to 6 km/h, return takes 4 h. An excursion rule based on nominal speed can therefore double exposure time precisely when degraded operation is required. Distance limits must use credible degraded modes.

Decision check. A return-time rule should be written for nominal and degraded mobility. If a rover loses half its usable energy or a wheel failure halves speed, the allowed excursion radius may need to shrink before the EVA begins. The rule is therefore an operational control derived from physics, not a fixed distance painted on a map.

11. Medicine and human factors

Earth-Mars delay prevents instant telemedicine. Crew must recognize, stabilize, and treat conditions locally. Medical capability depends on water, power, sterilization, pharmacy, cold storage, and waste.

Fatigue, sleep, conflict, and maintenance workload affect risk. Technical redundancy can still fail operationally if each fault consumes too many hours of scarce expert labor.

Degraded mode

Mission medicine must classify what can be diagnosed locally, what can wait for Earth expertise, and what requires immediate action. Medical inventory is therefore a portfolio of capabilities: drugs, consumables, sterilization, imaging, blood or substitutes, procedures, and human skill.

Local clinical autonomy

available clinical time < communication delay $\Rightarrow$ local autonomy

1 — Concrete question	What operational question does this relation answer for local clinical autonomy?
2 — Intuition without symbols	If the medical action window closes before remote help can arrive, capability and authority must already exist locally.
3 — Quantities first	The comparison is between the clinically useful action window and the communications/support delay.
4 — Formula	$\text{available clinical time} < \text{communication delay} \Rightarrow \text{local autonomy}$
5 — Read aloud	Read the relation aloud term by term: available clinical time < communication delay $\Rightarrow$ local autonomy.
6 — Symbols and meaning	The comparison is between the clinically useful action window and the communications/support delay.

7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Both sides of the comparison use the same time unit.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	If the medical action window closes before remote help can arrive, capability and authority must already exist locally.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Both sides of the comparison use the same time unit. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: a clinical action must be decided within 20 min while usable remote support can respond only in 30 min. Because $20 < 30$, the crew requires local clinical autonomy.
14 — Why the calculation works	If the medical action window closes before remote help can arrive, capability and authority must already exist locally.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about local clinical autonomy under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. The clinical window increases by 10%, from 20 to 22 min, while support delay remains 30 min. Does the rule change? Detailed guided correction — open after attempting Detailed correction. $22 \text{ min} < 30 \text{ min}$, so the condition remains true. The larger window is still too short for remote support; local clinical autonomy remains required. If usable support were available in 18 min, the comparison would change. Autonomous exercise. Build a second numerical scenario for “Local clinical autonomy” by changing at least two inputs in available clinical time < communication delay $\Rightarrow$ local autonomy. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into available clinical time < communication delay $\Rightarrow$ local autonomy, produce a value with its unit or an explicit logical result, compare it with the reference case, and

21 — Mission decision

justify the following decision: Pre-identify actions that must be autonomous and train at least one qualified backup.

Pre-identify actions that must be autonomous and train at least one qualified backup.

Communication delay varies with geometry; the architecture must tolerate the range of delays and outages rather than one fixed value.

Clinical case — autonomy

A medical decision procedure requires four exchanges with an Earth specialist. At 18 min one way, a minimum question-answer cycle takes 36 min; four cycles can exceed 2 h 20 before human decision time. Any emergency with a shorter treatment window therefore requires local procedures, skill, and equipment.

Decision check. Medical autonomy can be decomposed into prevention, diagnosis, stabilization, definitive treatment, and recovery. Each layer has a different demand for training, consumables, sterile equipment, imaging, and communication. Mapping conditions to those layers is more useful than a single statement that the base “has a clinic.”

12. Redundancy and common cause

Two identical units sharing power or software are not independent barriers. Common power, contamination, configuration, or procedural errors can defeat both.

A degraded mode is deliberately less capable but stable: zones isolated, experiments postponed, consumption reduced. Defining these states early makes reserves and procedures concrete.

Safety reading

Useful redundancy separates causes. Two units on the same power bus, in the same dusty compartment, and running the same software can fail together. Diversity, isolation, independent monitoring, and repairability can matter more than unit count.

Common-cause risk

system risk ≠ product of individual risks when common causes exist

1 — Concrete question	What operational question does this relation answer for common-cause risk?
2 — Intuition without symbols	Two barriers are not truly independent when the same failure, operator, or environment can defeat both together.
3 — Quantities first	System risk depends on both individual failures and dependencies between barriers.
4 — Formula	system risk ≠ product of individual risks when common causes exist
5 — Read aloud	Read the relation aloud term by term: system risk ≠ product of individual risks when common causes exist.

6 — Symbols and meaning	System risk depends on both individual failures and dependencies between barriers.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Probability is dimensionless, but this relation is primarily a dependency warning rather than a numerical formula.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Two barriers are not truly independent when the same failure, operator, or environment can defeat both together.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Probability is dimensionless, but this relation is primarily a dependency warning rather than a numerical formula. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: two pumps each have a 1% individual failure risk over the period, but they share a power bus with a 5% loss risk. The naive product $1\% \times 1\% = 0.01\%$ therefore does not represent system risk because the common bus alone contributes at least 5%.
14 — Why the calculation works	Two barriers are not truly independent when the same failure, operator, or environment can defeat both together.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about common-cause risk under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Keep individual pump risk at 1% but reduce common-bus loss risk from 5% to 2%. Compare again with the naive product of individual risks. Detailed guided correction — open after attempting Detailed correction. The naive product remains 0.01%. Yet the common bus alone still contributes 2% simultaneous-loss risk, 200 times 0.01%. The system therefore still cannot be represented by the product of individual risks; the common cause must be modeled explicitly. Autonomous exercise. Build a second numerical scenario for “Common-cause risk” by changing at least two inputs in $\text{system risk} \neq \text{product of individual risks}$ when common causes exist. Compute the result, check units and order of magnitude, then state whether the mission decision should change.

Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into system risk $\neq$ product of individual risks when common causes exist, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Search explicitly for shared power, sensors, software, operators, and locations before crediting redundancy.

21 — Mission decision

Search explicitly for shared power, sensors, software, operators, and locations before crediting redundancy.

Independent probabilistic calculations are conditional models, never proof that common causes have vanished.

Common-cause case

Two backup pumps occupy the same compartment and share one controller. A liquid contamination event or software error can disable both. Adding a third identical pump in the same place increases component count without creating real diversity. The useful exercise is to identify physical or functional separation that breaks the .

Decision check. A strong redundancy review also asks whether maintenance can create common cause. Two channels may be independent in normal operation yet become coupled when the same technician, calibration standard, software update, or spare batch services both. Configuration control is therefore part of resilience.

13. Scale: 4, 20, 100, 1,000 people

At four people, one unit and reserve may cover a function. At twenty, spares and maintenance shape organization. At one hundred, medical, workshop, water quality, and multi-zone redundancy become infrastructure. At one thousand, 2% of a large stream becomes hundreds of kilograms per day.

Larger population adds skills while also increasing networks, interfaces, and common-contamination consequences. A settlement is not a mission multiplied by one factor.

14. Integrated exercise: 72 h without water recovery

Scenario: 100 people, emergency net demand 4 kg/person/day, zero recovery, separate 1,500 kg reserve. Demand = 400 kg/day. Three days consume 1,200 kg, leaving 300 kg or 18 hours at the same rate.

The number opens the real questions: can demand be reduced, is reserve quality verified, can repair finish before the deadline, is reserve physically independent, and what nonessential loads shut down automatically?

Scaling — when a loop becomes infrastructure

With four people, a single device may be watched directly by the whole crew. At twenty, the system becomes a service with scheduled maintenance and dedicated spares. At one hundred, a loop failure can affect people who do not operate it; distribution, isolation, compartmentation, and documentation become central. At one thousand, multiple trains, strategic inventories, workshops, and specialist teams become plausible, while new common causes appear: shared software, shared power, shared filters, or shared metrology errors.

Scaling is therefore not simply multiplying power by population. Take a teaching pump MTTR of eight hours. One pump makes the function unavailable for those eight hours after a fault. Two genuinely isolatable trains can preserve partial service, but not if both are disabled by contaminated common water or the same electrical failure. Useful redundancy requires independence of failure causes as well as duplicated machines.

- 4: integrated crew, simple stocks, little human depth.
- 20: specialization and first dedicated redundancies.
- 100: distributed services, compartmentation, institutional maintenance.
- 1,000: multiple trains, support industry, common-cause control.

End-of-module project — seven days in controlled degraded mode

A 20-person base loses one water-processing unit and must operate for seven days on inventory and reduced capacity. The teaching scenario assumes 5 kg/person/day of direct non-deferrable need and 3 kg/person/day of deferrable use. Minimum vital requirement is $20 \times 5 \times 7 = 700$ kg. Deferrable uses would add 420 kg. That separation immediately creates degraded-mode logic: 700 kg belongs to a vital function while 420 kg can be reduced or postponed according to the scenario.

Available inventory is 1,050 kg, of which 150 kg is reserved for medical and unforeseen events. That leaves 900 kg for routine operations. The 700 kg vital need leaves 200 kg, insufficient for all 420 kg deferrable uses. About 220 kg must therefore be rationed across seven days, or 31.4 kg/day. This does not mean people simply drink less; the scenario first reduces uses explicitly classified as non-vital. A safety rule emerges from the material balance before it becomes an organizational rule.

At the same time, the main CO₂-removal train is unavailable for ten hours while a backup provides 70% of nominal capacity. Without a detailed metabolic model, we do not invent a concentration. Instead, list the required information: CO₂ generation per person, habitable volume, ventilation, sorbent capacity, thresholds, and sensor dynamics. Knowing when the data are insufficient for a numerical answer is a safety skill. Inventing a metabolic rate merely to fill an equation would be less rigorous than declaring the missing input.

An unscheduled EVA then introduces a dust load. The base must isolate the airlock, clean the suit, monitor air, and replace a filter without shutting down the entire life-support system. Look for a common cause: if the same electrical bus feeds both main filtration and airlock filtration, one electrical fault can defeat functional separation. Redundancy on a diagram matters only when power, sensors, software, and consumables do not recreate a single failure point.

The final worksheet therefore has five columns: function, normal capacity, degraded capacity, buffer resource, and return-to-normal criterion. Water returns after repair and loop qualification; atmosphere after main train recovery and sensor confirmation; dust after cleaning, measurement, and consumable replacement. The project succeeds when the team can explain why the base remains inside a safe envelope for seven days, which activities are suspended, and which additional event would force refuge or evacuation.

Function	Nominal	Degraded	Buffer / decision
Water	8 kg/p/d in this scenario	5 kg/p/d vital	900 kg routine +150 kg reserved
CO ₂	main train	70% backup	watch trend, limit activity if needed
Dust	airlock + filtration	local isolation	filter, cleaning, air check
Power	full network	critical loads	shed deferrable functions

Protected vital-water reserve

$$M_{\text{vital}} = N q_{\text{vital}} t_{\text{protected}}$$

1 — Concrete question	What operational question does this relation answer for protected vital-water reserve?
2 — Intuition without symbols	Vital reserve is sized from minimum demand, crew count, and the duration that must remain protected independently of nominal operation.
3 — Quantities first	N is crew count, q_{vital} essential water per person per day, and $t_{\text{protected}}$ protected days.

4 — Formula	$M_{\text{vital}} = N q_{\text{vital}} t_{\text{protected}}$
5 — Read aloud	Read the relation aloud term by term: $M_{\text{vital}} = N q_{\text{vital}} t_{\text{protected}}$.
6 — Symbols and meaning	N is crew count, q_{vital} essential water per person per day, and $t_{\text{protected}}$ protected days.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	People times kg/person/day times day gives kg.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.
10 — Why this operation	Vital reserve is sized from minimum demand, crew count, and the duration that must remain protected independently of nominal operation.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	People times kg/person/day times day gives kg. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: $N = 5$ people, $q_{\text{vital}} = 20$ kg/person/day, and $t_{\text{protected}} = 7$ days gives $M_{\text{vital}} = 5 \times 20 \times 7 = 700$ kg.
14 — Why the calculation works	Vital reserve is sized from minimum demand, crew count, and the duration that must remain protected independently of nominal operation.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about protected vital-water reserve under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Increase protected duration by 10%, from 7 to 7.7 days, with crew and vital demand unchanged. Recompute the reserve. Detailed guided correction — open after attempting Detailed correction. $M_{\text{vital}} = 5 \times 20 \times 7.7 = 770$ kg. A 10% increase in protected duration raises the reserve by 70 kg, exactly 10% above the initial 700 kg. Autonomous exercise. Build a second numerical scenario for “Protected vital-water reserve” by changing at least two inputs in $M_{\text{vital}} = N q_{\text{vital}} t_{\text{protected}}$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria

Autonomous correction. The answer must show substitution into $M_{\text{vital}} = N_{\text{q_vital}} t_{\text{protected}}$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Prevent routine loads from consuming the protected reserve without explicit emergency authority.

21 — Mission decision

Prevent routine loads from consuming the protected reserve without explicit emergency authority.

Corrected drill set — independent check

1. 20 people, 10 kg/day/person gross flow, 98% recovery: makeup?

Gross flow is 200 kg/day; 2% loss is 4 kg/day. Across 365 days that is 1,460 kg, for this teaching flow assumption and this loss mechanism alone.

2. Why may two identical filters fail to provide useful redundancy?

Shared power, software, consumable batch, or common contamination can disable both. Physical duplication must be paired with functional independence.

3. A 300 kg reserve is consumed at 25 kg/day. Endurance?

Twelve days if flow stays constant and all reserve is usable. Medical reserves or minimum tank thresholds would reduce available inventory.

4. What must be checked after a water-loop repair?

More than whether the pump runs: flow, pressure, leakage, sensors, water quality, and stable return to nominal operation. A life-critical function is qualified by useful output.

5. Why does dust connect health with maintenance?

It can affect human exposure, seals, filters, surfaces, sensors, and EVA procedures. Contamination barriers therefore span several systems.

Deep practice workshop

For each survival scenario, identify the life-critical function and its time margin first: how long before pressure, CO₂, water, temperature, or medical capability leaves the acceptable range? Then build the resource balance and recovery path. The solutions emphasize operational decisions: detect, isolate, enter a degraded mode, repair, and requalify.

1. Water at 98%

20 people, 20 kg/person/day, 98% recovery. Makeup?

Reasoned solution: $20 \times 20 \times 0.02 = 8$ kg/day; 2,920 kg/year.

2. CO₂-equivalent drift

Production 4.0 kg/day, removal 3.95 kg/day for 60 days.

Reasoned solution: Accumulation = $0.05 \times 60 = 3$ kg.

A daily mismatch of only 0.05 kg appears tiny, yet integration over sixty days creates 3 kg of unremoved CO₂. Habitats therefore track cumulative imbalance as well as instantaneous flow.

3. Partial pressure

70 kPa at 30% O₂.

Reasoned solution: 21 kPa.

4. Dust

0.1 mg/m³ in 120 m³ perfectly mixed volume.

Reasoned solution: 12 mg airborne at the stated average.

The 12 mg is airborne mass in 120 m³ at the selected average concentration. It does not specify distribution near an airlock, inhaled fraction, or an individual crew member's exposure duration.

5. Safe haven

20 people, 30 days, 2 kg/person/day water makeup.

Reasoned solution: 1,200 kg makeup in this degraded-mode scenario.

The 1,200 kg comes from a degraded requirement of 2 kg per person per day for thirty days. A real safe-haven reserve also needs losses, medical uses, fire response, restart needs, and duration uncertainty.

6. Sensor vote

p=0.01 independent, 2-of-3 vote.

Reasoned solution: $3p^2(1-p)+p^3=0.000298=0.0298\%$.

Two-out-of-three voting greatly reduces independent one-percent errors, but the formula depends on that independence. Shared power, software, or calibration can fail all three sensors together and erase the theoretical benefit.

7. Delay

22 min one way: minimum question-answer loop.

Reasoned solution: 44 min before added decision or transmission delays.

Forty-four minutes is only the light-time round trip when each leg takes 22 minutes. A medical or engineering decision adds observation, human analysis, message preparation, and possibly another question cycle.

8. Combined-failure capstone

A 20-person base loses its main water processor for 72 h. Emergency mode recovers 90% of a 15 kg/person/day flow. What ideal minimum makeup stock is needed, and why is it insufficient for a procedure?

Reasoned solution: Deficit=20×15×0.10=30 kg/day, or 90 kg over 3 days. A real procedure must add margin, non-potable needs, fire and medical demand, startup, repair uncertainty, and the possibility that power or sensing fails too. Ninety kilograms is a calculation baseline, not a final safety reserve.

The 90 kg three-day deficit is the first line of a contingency budget, not the final reserve. The scenario also has to protect non-potable functional water and retain restart margin.

Additional advanced problems

1. Water buffer

Deficit 25 kg/day, repair estimate 5 days, 2-day margin.

Reasoned solution: Scenario minimum= $25 \times 7 = 175$ kg.

2. Atmosphere

60 kPa, O₂ 32%. pO₂?

Reasoned solution: 19.2 kPa.

3. Dust TWA

0.2 mg/m³ for 2 h then 0.05 for 22 h. 24 h average?

Reasoned solution: $(0.2 \times 2 + 0.05 \times 22) / 24 = 0.0625$ mg/m³.

The 24-hour weighted average is below the two-hour peak because the other twenty-two hours carry more weight. A compliant mean still does not describe a local peak or particle-size distribution by itself.

4. Safe-haven mini-project

8 people, 30 days, total vital load 3 kW average. Energy with no generation?

Reasoned solution: Crew count does not enter if 3 kW is already total load: $3 \times 24 \times 30 = 2,160$ kWh. Efficiency, reserve, and peak power must then be added.

The 2,160 kWh assumes 3 kW is already the total safe-haven load. Population affects other consumables but not this multiplication; defining the boundary avoids counting the number of people twice.

ECLSS incident laboratory — preserve life while the loop is degraded

This parity extension deepens the operational reasoning of the English curriculum without replacing the existing lesson. It is designed to make the learner explain assumptions, verify a calculation or chain, and convert the result into a decision.

Define the life-support boundary and minimum safe state

A closed-loop life-support system is a network of atmosphere, water, thermal, waste and monitoring functions. During an anomaly, the first task is not to restore nominal efficiency; it is to define the minimum safe state for the crew. That means identifying acceptable cabin atmosphere, protected water inventory, thermal limits, contamination boundaries and the time available before any limit is approached. The safe state becomes the anchor for troubleshooting.

Separate storage from regeneration capacity

A settlement can survive a temporary process outage only if stored reserves and alternate paths cover the repair time. A high nominal recovery rate does not remove the need for tanks, compressed gases, sorbent capacity or emergency consumables. Conversely, a large tank does not compensate for a process that cannot be restored before the reserve is

exhausted. Reliability analysis must connect inventory, failure detection, isolation, repair time and restart verification.

Treat sensor disagreement as an information problem

When two oxygen, carbon-dioxide or water-quality sensors disagree, selecting the convenient value is unsafe. Check sensor health, calibration status, location and response time, then seek an independent measurement or process indicator. The disagreement itself is operational evidence. Procedures should define when the system enters a conservative degraded mode because the true state is uncertain, even if no limit has yet been confirmed as exceeded.

Prevent cross-contamination during maintenance

Life-support maintenance can connect clean and dirty sides of a system through tools, hoses, gloves or temporary bypasses. Before opening hardware, define the contamination boundary and the post-maintenance acceptance test. Water quality, trace contaminants and microbial control require evidence after the repair, not only mechanical proof that the pump turns. Similar logic applies to cabin-air filters and condensate paths.

Manage crew workload as part of the failure

A degraded ECLSS mode can consume crew attention through manual sampling, valve operations, water rationing and repeated checks. That workload can become a common cause for mistakes elsewhere. The incident plan should assign roles, reduce nonessential tasks, preserve sleep and create clear handover records. A technically survivable system can still fail operationally if the crew cannot sustain the required manual workload.

Recover through evidence gates

Restart should proceed in stages: isolate the fault, verify the repair, test locally, reconnect to a protected buffer if possible, confirm stable trends and only then return the full loop to nominal service. Each gate needs measurable criteria. This prevents a repaired component from immediately contaminating or destabilizing the rest of the habitat. The goal is controlled recovery, not the fastest possible return to the original configuration.

Progressive mastery drills — eight linked checks

Drill 1 — Atmosphere control

Define which oxygen, carbon-dioxide and pressure measurements establish a minimum safe cabin state.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 2 — Water recovery

Separate recovered quantity, verified potable quantity and stored emergency reserve.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 3 — Waste and hygiene

Explain how waste handling can become a contamination path into clean water or living areas.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 4 — Dust control

Map a dust path from EVA suit to airlock to cabin and identify barriers that interrupt it.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 5 — Radiation shelter

Connect alert, crew travel time and shelter readiness into one survivability chain.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 6 — Medical autonomy

Identify what changes when evacuation to Earth is not an immediate option.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 7 — Common-cause failure

Give an example where two redundant components can fail because they share power, environment or maintenance error.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Drill 8 — 72-hour degraded mode

Build a shift-by-shift monitoring and conservation plan that the crew can actually sustain.

Expected reasoning. Show the physical meaning, units or evidence path, state at least one assumption, and explain what operational decision would change if the result or evidence were different.

Integrated exercise — Plan 72 hours without nominal water recovery

Assume a training habitat has a verified potable reserve and the main water-recovery processor must remain isolated for 72 hours. Build a response plan that separates drinking and food preparation, hygiene, medical uses, cleaning, contingency reserve, sampling and repair activities. Identify what evidence is required before recovered water can re-enter the potable inventory.

Reasoned solution. A strong answer establishes the initial verified inventory, protects a non-negotiable emergency fraction, reduces or suspends deferrable uses, tracks every withdrawal, prevents unverified recovered water from mixing with the clean tank, schedules repair and independent sampling, and defines acceptance criteria for chemistry and microbiological control before reconnection.

Primary-source bridge for this extension. [Official source 1](#) [Official source 2](#) [Official source 3](#). These links are evidence anchors already present in the French reference module; values and limits must still be checked against the source version applicable to the mission.

Sources and references

The references document operational ECLSS, the water-recovery milestone, and the preliminary dust limit. Safe-haven budgets are sizing exercises rather than NASA operational prescriptions.

Associated calculators

Apply this module with:

- [Mars habitat gas calculator](#)
- [Oxygen demand calculator](#)

- [NASA — Environmental Control and Life Support System](#) — Operational ISS life-support architecture.
- [NASA — ISS 98% water recovery milestone](#) — Demonstrated total water recovery milestone and prior 93–94% level.
- [NASA — Deep Space Habitation Systems](#) — Long-duration habitation and life-support context.
- [NASA — Martian dust exposure limits](#) — 2026 preliminary exposure requirement for Martian particles under 10 µm.
- [NASA NTRS — Safe Haven Configurations](#) — Primary or institutional source used for definitions, technology status, or module data.
- [NASA NTRS — Space Crop Considerations](#) — Primary or institutional source used for definitions, technology status, or module data.
- [NASA-STD-3001 Volume 2](#) — Primary or institutional source used for definitions, technology status, or module data.

First Man ECLSS closure dossier — survive the degraded loop, not only the nominal diagram

A life-support system is not a box labelled ‘air and water’. It is a set of coupled inventories, processors, sensors, valves, contamination barriers, power paths and crew actions. The training objective is to keep people safe when one part is uncertain, isolated or unavailable.

Close inventories before trusting percentages

The [NASA — Environmental Control and Life Support System](#) describes major life-support functions. A recovery percentage is useful only when attached to the underlying flows. Water accounting should distinguish gross crew demand, recovered stream, reject stream, unrecovered losses, verified potable storage and emergency reserve. A high recovery percentage cannot compensate for an empty or contaminated verified tank.

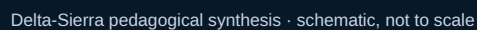
NASA has reported high ISS water-recovery performance; [NASA — ISS water recovery milestone](#) provides context. Mars operations add long resupply delays and different maintenance constraints, so the lesson is to understand the balance and evidence rather than copy one performance number into a future architecture.

Separate detection, isolation and recovery

An abnormal sensor reading should not trigger an undirected scramble. First confirm whether the signal is credible, then identify which branch may be affected, isolate it if the risk warrants, preserve a verified supply path and collect evidence. Repair is only one part of the response; return to service needs proof that the hazard is removed and that the system is stable after reconnection.

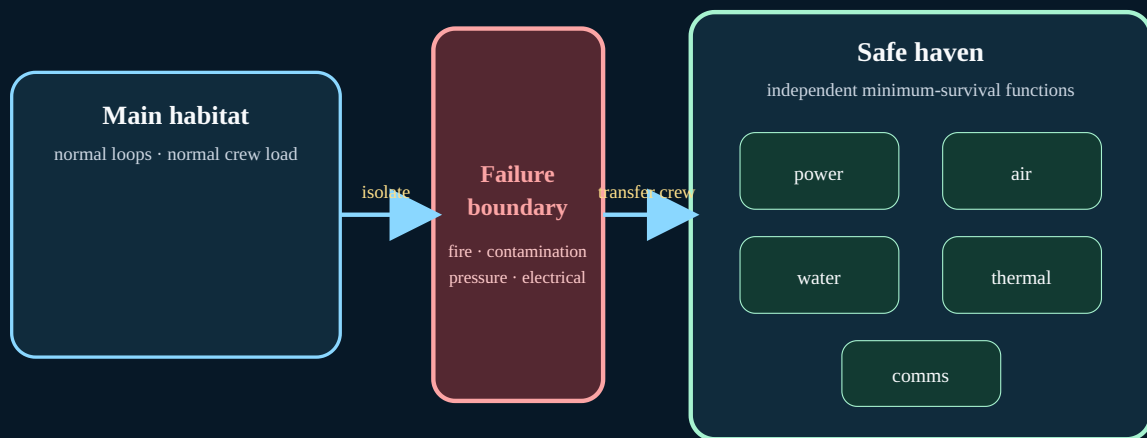
This is especially important for microbial or chemical contamination because quantity can remain normal while quality fails. A tank may be full yet unusable. Operational displays should therefore distinguish inventory state from quality state rather than collapsing both into one green icon.

Air, water, waste, sensors, storage and isolation paths.



Safe-haven independence map

Isolation boundary, crew transfer path and minimum survival functions are separated explicitly.



Independence test: the same initiating failure must not remove refuge power, atmosphere, water, heat rejection and communications.

Delta-Sierra pedagogical synthesis · schematic, not to scale

Main habitat, refuge, independent resources and failure boundaries. Pedagogical synthesis by Delta-Sierra from the primary sources cited in this course; schematic, not to scale.

Degraded mode needs an exit criterion

Teams often describe how to enter safe mode but not how to leave it. Return to service should require stable sensor trends, required samples or checks, restored redundancy where specified, and an explicit owner who accepts residual risk. If a bypass is left installed, that temporary configuration must be recorded so future operators do not assume the system is fully restored.

A long-duration Mars mission should also track recovery debt: maintenance deferred during the event, consumables used, reserve depleted, crew fatigue accumulated and redundant paths still unavailable. Mission capability is not fully restored until those debts are understood and accepted.

Three-failure ECLSS exercise — protect verified functions while diagnosis is incomplete

Failure A begins with a conductivity excursion in one water branch. The crew does not yet know whether the cause is contamination, sensor drift or a maintenance configuration error. The first objective is to preserve verified potable supply while preventing suspect water from mixing with trusted inventory. Isolate the branch, place affected storage in a clearly identified status, take confirmation samples and calculate verified-water endurance before deciding how aggressively to ration.

Failure B occurs six hours later when one carbon-dioxide removal train trips offline. The remaining train is available but crew workload is already elevated by the water investigation. The response now has two coupled limits: atmosphere-processing capacity and human attention. Nonessential maintenance and science are postponed; carbon-dioxide trend and crew symptoms are monitored; the team avoids creating a third failure by rushing maintenance without the correct isolation and cross-check.

Failure C is a temporary loss of one cooling loop that raises equipment temperature but does not immediately threaten the habitat. The correct priority is not automatically 'fix the newest alarm first'. The board compares time-to-limit for each function: verified water endurance, carbon-dioxide trend, thermal rise, repair duration and crew workload. The event with the shortest credible safe horizon receives priority while other systems are placed in stable degraded configurations.

Function	Evidence clock	Protected action	Return-to-service gate
Water	Verified stock / net deficit	Isolate suspect branch	Quality sample + stable loop
CO ₂ control	Trend to exposure threshold	Reduce load / restore train	Stable concentration with redundancy
Thermal	Time to equipment limit	Shed heat / reroute coolant	Temperature and flow stable
Crew	Person-hour saturation	Defer nonessential work	Backup coverage restored

Return-to-service review — proving that normal mode is actually normal

After the repairs, the crew should not close the event because alarms disappeared. It checks valve line-up, sensor plausibility, sample results, redundancy state, temporary jumpers or bypasses, consumables used and maintenance still deferred. If the water loop is restored but the backup pump remains unavailable, the function may be restored while redundancy is not. The mission state should reflect that distinction.

The final event record should also identify what the incident revealed about the design. Did one sensor create too much ambiguity? Were isolation points difficult to access? Did two systems compete for the same specialist? Was the safe-haven stock truly independent? These lessons become design inputs for the next configuration rather than disappearing into an operations log.

Review drills — move from explanation to operational judgement

1. **Isolation drill.** Write a three-step response to a suspect potable-water sample while preserving verified supply.
2. **Safe-haven drill.** List five functions that must remain independent enough for a refuge to be credible.
3. **Recovery-debt drill.** After a 24-hour emergency, identify at least four debts that can remain after the alarm clears.
4. **Sensor drill.** Explain why one normal pressure sensor cannot prove atmosphere quality.

Verified-water endurance during a recovery shortfall

$$t = V_{\text{verified}} / (N q_{\text{essential}} - q_{\text{recovery}})$$

1 — Concrete question	What operational question does this relation answer for verified-water endurance during a recovery shortfall?
2 — Intuition without symbols	When recovery no longer covers essential demand, verified storage supplies the remaining daily deficit until depletion.
3 — Quantities first	V_{verified} is verified usable water, N crew count, $q_{\text{essential}}$ essential demand per person per day, and q_{recovery} verified recovery per day.
4 — Formula	$t = V_{\text{verified}} / (N q_{\text{essential}} - q_{\text{recovery}})$
5 — Read aloud	Read the relation aloud term by term: $t = V_{\text{verified}} / (N q_{\text{essential}} - q_{\text{recovery}})$.
6 — Symbols and meaning	V_{verified} is verified usable water, N crew count, $q_{\text{essential}}$ essential demand per person per day, and q_{recovery} verified recovery per day.
7 — Pronunciation	Say subscripts, exponents, Greek letters, and operations explicitly so another person could reconstruct the relation without seeing the page.
8 — Units	Litres divided by litres/day gives days, provided the net deficit is positive.
9 — Convention	Every input must come from a measurement, a cited source, or an explicitly declared teaching assumption. Do not invent a missing mission value. Keep the same system boundary and time basis from start to finish.

10 — Why this operation	When recovery no longer covers essential demand, verified storage supplies the remaining daily deficit until depletion.
11 — Assumptions	This simplified relation does not replace qualification data, uncertainty analysis, failure modes, or the wider coupled-system model.
12 — Unit check	Litres divided by litres/day gives days, provided the net deficit is positive. Verify that units reduce to the unit of the requested quantity.
13 — Numerical case	Teaching example: $V_{\text{verified}} = 120 \text{ L}$, $Nq_{\text{essential}} = 72 \text{ L/day}$, and $q_{\text{recovery}} = 64 \text{ L/day}$ gives an 8 L/day deficit and $t = 120/8 = 15 \text{ days}$.
14 — Why the calculation works	When recovery no longer covers essential demand, verified storage supplies the remaining daily deficit until depletion.
15 — Algebra check	Recompute from the original inputs or invert the relation when possible; a second route should reproduce the same scale and unit.
16 — Mental estimate	Before accepting the exact result, estimate its order of magnitude and check that its direction matches the physical situation.
17 — Interpretation	The result is useful only as an operational statement about verified-water endurance during a recovery shortfall under the declared assumptions.
18 — What the result does not prove	This result alone does not prove hardware reliability, input-data quality, or whole-system safety outside the declared assumptions.
19 — Sensitivity	Vary the dominant input while holding the boundary conditions fixed, then explain whether the result rises, falls, or crosses a mission threshold.
20 — Guided and autonomous practice	----- Guided exercise. Verified recovery falls by 10%, from 64 to 57.6 L/day, while essential demand remains 72 L/day. Recompute endurance. Detailed guided correction — open after attempting Detailed correction. The new deficit is $72 - 57.6 = 14.4 \text{ L/day}$. Therefore $t = 120/14.4 = \text{about } 8.33 \text{ days}$. A 10% drop in recovered flow cuts endurance from 15 to 8.33 days because it acts on a small deficit in the denominator. Autonomous exercise. Build a second numerical scenario for “Verified-water endurance during a recovery shortfall” by changing at least two inputs in $t = V_{\text{verified}} / (Nq_{\text{essential}} - q_{\text{recovery}})$. Compute the result, check units and order of magnitude, then state whether the mission decision should change. Autonomous correction — specific criteria Autonomous correction. The answer must show substitution into $t = V_{\text{verified}} / (Nq_{\text{essential}} - q_{\text{recovery}})$, produce a value with its unit or an explicit logical result, compare it with the reference case, and justify the following decision: Set repair, rationing, and fallback thresholds before the protected vital reserve is consumed.
21 — Mission decision	Set repair, rationing, and fallback thresholds before the protected vital reserve is consumed.

Final ECLSS review — prove the crew remains safe while the diagnosis is wrong

- Are verified inventory and total inventory displayed separately?
- Can a suspect branch be isolated without losing every supply path?
- Does safe haven survive the same common-cause failure?
- Are sensor confirmation and quality sampling included in recovery?
- Is crew workload part of the degraded-mode model?
- Does return to service require evidence rather than disappearance of alarms?

The key stress test is uncertainty. For several hours, the team may not know whether the problem is sensor drift, contamination, configuration error or real process loss. A resilient life-support architecture preserves safe options while evidence is collected and keeps a clock on the resources that are actually verified.

Primary-source bridges used in this closure dossier

- [NASA — Environmental Control and Life Support System](#)
- [NASA — ISS water recovery milestone](#)
- [NASA NTRS — Safe Haven Configurations](#)
- [NASA-STD-3001 Volume 2](#)

Closure rule. An ECLSS recovery is complete only when the protected function, quality evidence, redundancy state and residual recovery debt are known.

FR ↔ EN competency matrix

#	French	English	Status
01	Autonomie d'un stock critique	Critical-stock endurance	PASS
02	Chaîne fonctionnelle de sûreté	Functional safety chain	PASS
03	Pression partielle dans un mélange	Partial pressure in a gas mixture	PASS
04	Bilan dynamique d'un inventaire	Dynamic inventory balance	PASS
05	Stœchiométrie de Sabatier	Sabatier stoichiometry	PASS
06	Couplage électrolyse–Sabatier	Electrolysis-Sabatier coupling	PASS
07	Besoin d'appoint avec récupération	Make-up demand with recovery	PASS
08	Effet du rendement de récupération	Recovery-efficiency leverage	PASS
09	Acceptation de l'eau produite	Produced-water acceptance	PASS
10	Masse d'un aliment humide	Wet-food mass from dry matter	PASS
11	Refuge autonome pendant trois jours	Three-day refuge water and energy	PASS
12	Autonomie d'un refuge	Refuge endurance	PASS
13	Charge totale de poussière	Total dust loading	PASS
14	Exposition moyenne pondérée	Time-weighted average exposure	PASS
15	Temps de retour en mode dégradé	Degraded-mode return time	PASS
16	Autonomie clinique locale	Local clinical autonomy	PASS
17	Risque de cause commune	Common-cause risk	PASS
18	Réserve vitale protégée	Protected vital-water reserve	PASS
19	Autonomie d'eau vérifiée en récupération dégradée	Verified-water endurance during a recovery shortfall	PASS