

Missions finales: construire une architecture Mars complète et résiliente

Édition française R77. Ce PDF conserve l'article pédagogique, les calculs, exercices, limites, décisions et figures disponibles du module.

Release source: R77-20260912.

Missions finales: construire une architecture Mars complète et résiliente

Comprendre le problème avant les équations

Question de départ — Missions finales: construire une architecture Mars complète et résiliente: comment « Dossier corrigé quantitatif de référence - scénario pédagogique complet » agit-il sur « Registre initial des hypothèses », et quel repère issu de « Fermer le budget d'eau avant de parler de confort » permet de vérifier la décision?

Intuition. Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

1

Dossier corrigé quantitatif de référence - scénario pédagogique complet

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.

2

Registre initial des hypothèses

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.

3

Fermer le budget d'eau avant de parler de confort

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.

Repère concret. L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

- Dossier corrigé quantitatif de référence - scénario pédagogique complet — Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.
- Registre initial des hypothèses — Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.
- Fermer le budget d'eau avant de parler de confort — Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture.



CARTE DE MAÎTRISE · MODULE 16

Quatre repères à maîtriser — Missions finales: construire une architecture Mars complète et résiliente

Dossier corrigé quantitatif de référence - scénario pédagogique complet

Définition

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Intuition ou cas concret

Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs.

Repère quantitatif

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Limite ou critère de vigilance

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Exercice guidé — Dossier corrigé quantitatif de référence - scénario pédagogique complet

Cas « Dossier corrigé quantitatif de référence - scénario pédagogique complet » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Corrigé raisonné — Dossier corrigé quantitatif de référence - scénario pédagogique complet

Point de départ

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Indice du cas

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Réserve à appliquer

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Conclusion

Il les reçoit s'il annonce ses hypothèses, définit les unités, ferme ses budgets, montre les interfaces et prend une décision cohérente avec les marges qu'il a lui-même calculées.

Registre initial des hypothèses

Définition

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Intuition ou cas concret

Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs.

Repère quantitatif

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Limite ou critère de vigilance

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Exercice guidé — Registre initial des hypothèses

Cas « Registre initial des hypothèses » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Corrigé raisonné — Registre initial des hypothèses

Point de départ

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Indice du cas

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Réserve à appliquer

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Conclusion

Il les reçoit s'il annonce ses hypothèses, définit les unités, ferme ses budgets, montre les interfaces et prend une décision cohérente avec les marges qu'il a lui-même calculées.

Fermer le budget d'eau avant de parler de confort

Définition

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Intuition ou cas concret

Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs.

Repère quantitatif

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Limite ou critère de vigilance

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Exercice guidé — Fermer le budget d'eau avant de parler de confort

Cas « Fermer le budget d'eau avant de parler de confort » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Corrigé raisonné — Fermer le budget d'eau avant de parler de confort

Point de départ

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Indice du cas

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Réserve à appliquer

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Conclusion

Il les reçoit s'il annonce ses hypothèses, définit les unités, ferme ses budgets, montre les interfaces et prend une décision cohérente avec les marges qu'il a lui-même calculées.

Oxygène et gaz: distinguer débit, stock et réserve d'urgence

Définition

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Intuition ou cas concret

Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs.

Repère quantitatif

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Limite ou critère de vigilance

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence

Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Corrigé raisonné — Oxygène et gaz: distinguer débit, stock et réserve d'urgence

Point de départ

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée.

Indice du cas

L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Réserve à appliquer

Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Conclusion

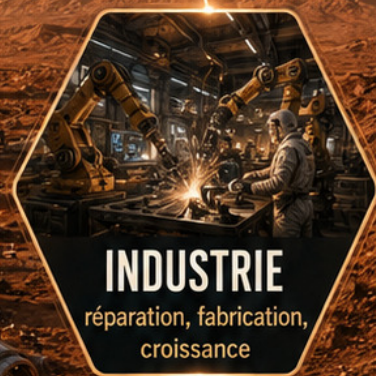
Il les reçoit s'il annonce ses hypothèses, définit les unités, ferme ses budgets, montre les interfaces et prend une décision cohérente avec les marges qu'il a lui-même calculées.

Télécharger ce cours en PDF

07 · Terre → Mars09 · Vaisseau11 · EDL12 · ECLSS14 · Fiabilité15 · Opérations16 · Missions finales

COLONIE MARTIENNE PERMANENTE

— Les 6 piliers d'une implantation durable —



Aucun pilier ne suffit seul :
la colonie échoue si l'un d'eux cède durablement.

DELTA-SIERRA • MARS



La mission finale ne juge pas un sous-système isolé: elle vérifie que transport, support-vie, énergie, habitat, industrie, équipage et gouvernance restent cohérents lorsqu'une panne ou un retard déforme le scénario initial.

Les quinze modules précédents apprennent à calculer, à lire une architecture et à reconnaître les limites d'un raisonnement trop simple. Le module 16 ne présente presque aucun nouveau concept. Il demande au contraire des relier. C'est le moment où une équation de propulsion rencontre un budget de masse, où un calcul de consommation d'eau rencontre un stock de secours, où une panne de communication rencontre une règle d'autorité locale, et où une belle architecture doit prouver qu'elle reste exploitable quand la réalité ne respecte plus le scénario nominal.

Une étude finale n'a pas besoin d'imiter un programme NASA ou SpaceX. Elle doit être explicitement présentée comme une architecture pédagogique Delta-Sierra: hypothèses datées, calculs reproductibles, marges visibles et frontière claire entre ce qui est démontré aujourd'hui et ce qui relève d'une extrapolation d'ingénierie.

1. Le cahier des charges: commencer par les fonctions, pas par le véhicule préféré

Chaque équipe reçoit un objectif de campagne: pré-déployer du fret, transporter un équipage, poser les éléments essentiels, vivre assez longtemps pour traverser une fenêtre de retour, puis laisser derrière elle une infrastructure plus robuste qu'à l'arrivée. Le premier travail consiste à transformer cet objectif en fonctions: énergie, air, eau, nourriture, thermique, communications, mobilité, maintenance, médical, refuge, stockage, production locale et retour.

Équipage de référence Choisir un effectif et expliquer pourquoi il est compatible avec habitat, médical, travail et secours.

Durée de campagne Choisir transit, séjour et fenêtre de retour, puis calculer les conséquences sur les consommables.

Fret prépositionné Identifier ce qui doit fonctionner avant l'arrivée humaine et ce qui peut attendre.

Retour Définir l'énergie, les ergols, les pièces et les décisions nécessaires pour conserver une option de retour crédible.

2. Construire l'architecture en chaînes fonctionnelles

Une bonne architecture se lit de gauche à droite: ressource d'entrée, transformation, stockage, distribution, usage, mesure, maintenance et mode dégradé. L'eau, par exemple, n'est pas seulement un réservoir. Il faut une source, une extraction, une purification, un stockage, une distribution, une récupération, des analyses de qualité et une stratégie si un contaminant interdit l'usage d'une boucle.

Pour chaque fonction vitale, la fiche finale doit indiquer: le moyen nominal, le moyen de secours, la durée pendant laquelle le secours tient, la manière de détecter la panne, la ressource commune susceptible de faire tomber les deux voies et l'action humaine ou automatique attendue. Ce tableau devient la colonne vertébrale de la revue de conception.

3. Fermer les budgets avant de discuter du décor

Une architecture qui ne ferme pas ses budgets n'est pas une architecture. Elle doit au minimum suivre masse, énergie, puissance de pointe, eau, oxygène, nourriture, volume habitable, stockage de données, capacité de communications, pièces de rechange et temps d'équipage. Les valeurs peuvent être pédagogiques, mais leur origine doit être expliquée.

Stock minimal protégé — séparer besoin nominal, réserve d'urgence et incertitude

1 — Question concrète

Quelle quantité faut-il protéger avant une période sans ravitaillement fiable ni production de remplacement garantie ?

2 — Intuition sans symboles

On couvre d'abord la consommation prévue pendant la période isolée, puis on ajoute une réserve d'urgence volontairement sanctuarisée et une marge d'incertitude séparée.

3 — Grandeurs

$S_{\min}$ est le stock minimal protégé ; q_{moy} le débit moyen vérifié ; t_{iso} la durée sans soutien ; S_{urg} la réserve d'urgence ; U la marge d'incertitude.

4 — Formule

$$S_{\min} = q_{\text{moy}} \times t_{\text{iso}} + S_{\text{urg}} + U$$

5 — Lecture

Le stock minimal égale la consommation moyenne multipliée par la durée isolée, plus la réserve d'urgence, plus la marge d'incertitude.

6 — Symboles et sens

Le produit débit-temps représente le besoin nominal ; les deux termes ajoutés représentent deux protections de nature différente.

7 — Prononciation

esse minimum égale q moyen fois té iso, plus esse urgence, plus U.

8 — Unités

Si q_{moy} est en unités/jour et t_{iso} en jours, leur produit est en unités ; S_{urg} , U et $S_{\min}$ utilisent la même unité de stock.

9 — Convention

Ne jamais compter deux fois la même protection. Si U provient d'une fraction d'incertitude, cette fraction s'applique au besoin nominal ; la réserve d'urgence reste distincte si elle protège une contingence différente.

10 — Pourquoi cette opération

Le débit multiplié par le temps donne la consommation nominale ; les additions protègent séparément l'urgence et l'incertitude.

11 — Hypothèses

Le débit moyen représente réellement l'intervalle, le stock est accessible et qualifié, et aucune dégradation non modélisée n'en rend une partie inutilisable.

12 — Contrôle d'unités

unités/jour $\times$ jours = unités ; les additions ne sont valides que si tous les termes sont exprimés dans cette même unité.

13 — Cas numérique

À 18 unités/jour pendant 45 jours, le besoin nominal vaut 810 unités. Une incertitude de 15 % ajoute 121,5 unités et une réserve d'urgence de 81 unités conduit à $S_{\min} = 1\,012,5$ unités.

14 — Pourquoi le calcul fonctionne

On construit d'abord la consommation nominale, puis on protège deux marges explicitement identifiables au lieu de les cacher dans un coefficient opaque.

15 — Contrôle algébrique

Si S_{dispo} est connu, $t_{\text{iso}} = (S_{\text{dispo}} - S_{\text{urg}} - U)/q_{\text{moy}}$, à condition que le numérateur soit positif et que U soit défini de façon cohérente.

16 — Estimation mentale

18 unités par jour sur environ 45 jours donnent un peu plus de 800 unités ; environ 200 unités de protections supplémentaires placent logiquement le total juste au-dessus de 1 000.

17 — Interprétation

Le critère protège 1 012,5 unités dans ce scénario. Passer sous ce seuil signifie que la marge approuvée est consommée, pas que la ressource tombe instantanément à zéro.

18 — Ce que le résultat ne prouve pas

Le calcul ne garantit ni consommation constante, ni accessibilité de tout le stock, ni conservation de sa qualité, ni retour du ravitaillement ou de la production à temps.

19 — Sensibilité

Une hausse du débit, une durée isolée plus longue ou une perte de stock qualifié augmente le besoin protégé ; si le stock disponible est inférieur aux protections seules, aucune durée positive n'est défendable.

20 — Exercices guidé et autonome

Exercice guidé. Une ressource est consommée à 12 unités/jour pendant 30 jours sans soutien. Protéger 60 unités d'urgence et 10 % d'incertitude sur le besoin nominal.

Correction guidée

Besoin nominal = $12 \times 30 = 360$; incertitude = 36 ; total protégé = $360 + 36 + 60 = 456$ unités.

Exercice autonome. Stock qualifié 860 unités, réserve d'urgence 80, incertitude fixe 100, consommation 18 unités/jour. Calculer la durée isolée maximale avant franchissement du seuil.

Correction autonome

Stock disponible pour consommation planifiée = $860 - 80 - 100 = 680$; durée = $680/18 \approx 37,8$ jours. Une campagne de 45 jours ne ferme donc pas ce critère.

21 — Décision mission

Utiliser le seuil comme gate : si l'inventaire qualifié vérifié passe dessous, mettre en HOLD les activités consommatrices et ouvrir une décision explicite de récupération ou de raccourcissement de campagne.

Si un équipage consomme une ressource à un taux moyen **q** pendant une durée **t**, le besoin de base est **q × t**. La vraie mission ajoute les pertes, la variabilité, les jours de refuge et le scénario de retard. L'objectif n'est pas de trouver un chiffre « exact » mais de montrer quelle hypothèse domine la masse et comment la conception change lorsque cette hypothèse bouge.

4. Mission finale A — le cargo doit rendre l'arrivée humaine moins risquée

Le cargo part en premier. Il transporte les éléments dont l'absence rendrait l'arrivée humaine inacceptable: énergie initiale, communications, moyens de déchargement, habitat ou refuge, réserves, pièces critiques et éventuellement équipements d'extraction locale. La mission doit définir ce qui est testé avant l'arrivée de l'équipage, quelles télémessures prouvent le bon fonctionnement et quel seuil provoquerait un report du départ humain.

Injectez ensuite une panne: un cargo manque la fenêtre, un panneau solaire est endommagé ou un rover de manutention reste immobilisé. L'équipe doit montrer si le site peut continuer à préparer l'arrivée avec moins de capacité ou s'il faut reconfigurer la campagne.

5. Mission finale B — le transit humain est un habitat en mouvement

Le vaisseau habité doit être évalué comme un habitat temporaire: air, eau, thermique, nourriture, sommeil, exercice, hygiène, médical, abri radiologique, maintenance et accès aux équipements. Le choix de propulsion ne suffit pas. Une réduction du temps de trajet peut déplacer de la masse vers la propulsion; une trajectoire plus lente peut augmenter les consommables et l'exposition. La bonne réponse est celle qui rend le système global le plus robuste pour le scénario choisi.

TRANSPORT TERRE-MARS

LA CHAÎNE COMPLÈTE D'UNE MISSION HABITÉE

1

PRÉ-DÉPLOYER LE CARGO

Les cargos sont envoyés en avance pour préparer l'arrivée de la mission.



2

LANCER L'ÉQUIPAGE

L'équipage décolle et rejoint le cargo en orbite terrestre.



3

TRANSITER AVEC SUPPORT-VIE

Le vaisseau voyage vers Mars avec ses systèmes vitaux opérationnels.



4

ATTERRIR / RÉCUPÉRER

Atterrissage sécurisé, déploiement et mise en service des habitats et équipements.



5

ASSURER LE RETOUR & VAGUE SUIVANTE

Retour de l'équipage et préparation de la prochaine mission.



UN CYCLE CONTINU POUR CONSTRUIRE
UNE PRÉSENCE HUMAINE DURABLE SUR MARS.

DELTA-SIERRA · MARS

6. Mission finale C — arrivée, EDL et mise en service du site

Le scénario doit relier la dispersion d'atterrissage aux opérations de surface. Deux véhicules séparés de plusieurs kilomètres peuvent être « tous deux posés avec succès » et pourtant rendre la campagne beaucoup plus difficile. Il faut donc définir les moyens de localisation, la mobilité disponible, la capacité de remorquage, les réserves d'énergie et le temps nécessaire pour mettre les fonctions vitales en service.

La mission finale doit également préciser ce qui se passe si l'équipage arrive alors qu'une partie du site n'est pas encore nominale. Existe-t-il un refuge indépendant? Combien de temps tient-il? Quelles tâches peuvent être reportées? Quelles opérations sont interdites tant qu'une vérification n'est pas terminée?

7. Mission finale D — transformer une base initiale en système durable

Une base qui survit cent jours n'est pas automatiquement une colonie. La campagne longue doit montrer comment la maintenance, les stocks, la production locale et la formation réduisent progressivement les dépendances. Une pièce produite localement n'est utile que si sa matière, sa géométrie et sa qualité sont contrôlées. Une ressource extraite n'est utile que si elle est purifiée, stockée et distribuée.

La soutenabilité se lit donc dans les boucles: recycler davantage, réparer plus de familles de pièces, fabriquer certains consommables, augmenter la capacité de refuge, documenter les procédures et transmettre les compétences à une équipe suivante.

8. Campagne longue: 500 sols sans scénario parfait

Le plan d'opérations doit couvrir un temps assez long pour faire apparaître les problèmes de vieillissement. Les filtres s'encrassent, les joints vieillissent, les batteries perdent de la capacité, les poussières s'accumulent, les pièces sont consommées et les humains se fatiguent. Le planning doit réserver du temps à l'inspection, à l'exercice, au soin, à la formation et au retour d'expérience.

On ne cherche pas à remplir chaque heure. Une architecture trop optimisée suppose souvent que rien d'imprévu n'arrive. La marge de temps est une ressource de résilience au même titre qu'un stock de pièces.

9. Pannes injectées: la mission n'est validée qu'après perturbation

- **Retard logistique:** le prochain cargo arrive plusieurs mois plus tard.
- **Énergie:** une tempête réduit fortement la production solaire.
- **ECLSS:** une chaîne d'oxygène devient indisponible pendant plusieurs jours.
- **Communications:** la Terre est momentanément indisponible ou trop lente pour la décision immédiate.
- **Mobilité:** un rover pressurisé est immobilisé loin du site.
- **Médical:** un membre d'équipage ne peut plus assurer sa fonction principale.

Pour chaque panne, le dossier final décrit la détection, l'autorité qui décide, les charges coupées, la durée disponible, le critère de retour à l'état nominal et la conséquence sur le reste de la campagne. Si une solution repose sur « on enverra une pièce depuis la Terre », elle doit intégrer la fenêtre de lancement et le temps réel avant disponibilité.

10. Les gates de décision: savoir dire « nous ne partons pas »

Gate 1 — départ du cargo: budgets fermés, interfaces figées, capacités de déploiement vérifiées.

Gate 2 — départ de l'équipage: fonctions critiques du site confirmées, réserves vérifiées, critères d'abandon explicites.

Gate 3 — engagement vers la surface: météo, EDL, navigation, communications et refuge compatibles avec l'arrivée.

Gate 4 — prolongation de campagne: stocks, santé, énergie, eau, maintenance et retour restent dans les limites acceptées.

Un bon dossier ne cherche pas à démontrer que la mission doit partir. Il cherche à rendre visible la condition qui impose de reporter ou d'abandonner. Cette capacité à dire « non » est un signe de maturité d'ingénierie.

11. Exercice quantitatif final — relier une marge à une décision

Supposons, uniquement pour l'exercice, qu'une réserve critique soit consommée à 18 unités par jour, que la campagne doive pouvoir tenir 45 jours sans apport extérieur et que l'équipe impose 25 % de marge. Le besoin de planification vaut:

Application — marge de consommable sur un cas chiffré

Le calcul 18 unités par jour sur 45 jours avec 25 % de protection est une application du dimensionnement de stock. Il ne constitue pas une deuxième loi : utiliser la mini-leçon canonique ci-dessus pour distinguer consommation nominale, réserve d'urgence et incertitude, puis reporter le résultat dans le gate de mission. Voir la mini-leçon canonique.

Si le stock mesuré après une panne tombe à 860 unités, la question n'est pas « peut-on encore survivre aujourd'hui? » mais « quelle décision faut-il prendre maintenant pour ne pas franchir une limite dans plusieurs semaines? ». L'équipe peut réduire une consommation, démarrer une production secondaire, interrompre une activité ou avancer un retour. La mission finale doit justifier ce choix avec des chiffres, pas avec une intuition.

Correction raisonnée

Le besoin avec marge est de 1 012,5 unités. Un stock de 860 unités laisse donc un déficit de 152,5 unités par rapport au critère de planification. À consommation inchangée, $860 / 18$ donne environ 47,8 jours d'autonomie brute, mais ce chiffre ne respecte plus la marge de 25 %. Pour conserver 45 jours avec cette marge, la consommation moyenne maximale devient $860 / (45 \times 1,25) \approx 15,3$ unités par jour, soit une réduction d'environ 15 %. Une autre réponse acceptable est de produire ou de récupérer au moins 152,5 unités avant l'échéance. La décision doit ensuite vérifier que l'économie choisie ne déplace pas le risque vers une fonction plus critique.

12. Dossier de soutenance: ce que l'équipe doit livrer

1. une page de mission et d'hypothèses;
2. une architecture fonctionnelle et ses interfaces;
3. les principaux budgets avec unités, marges et sources;
4. un calendrier cargo-équiperage-surface-retour;
5. les modes dégradés et stocks de secours;
6. au moins six pannes injectées;
7. une matrice de décisions et d'autorité;
8. les critères de départ, poursuite, repli et abandon;
9. un registre de ce qui est démontré, extrapolé ou prospectif;
10. une conclusion expliquant les trois plus grands risques résiduels.

13. Évaluer une architecture sans récompenser le spectacle

La note finale doit privilégier cohérence, traçabilité et capacité à reconnaître une limite. Une architecture moins spectaculaire mais dont les budgets, les secours et les décisions sont explicites vaut davantage qu'un concept visuellement impressionnant reposant sur des hypothèses cachées. Les points les plus importants sont la fermeture des fonctions vitales, la gestion des causes communes, la réparabilité, la discipline des marges et la clarté de la frontière entre fait et prospective.

14. La dernière compétence: transmettre le système à l'équipe suivante

Une mission humaine durable ne se termine pas au retour. Elle produit des données, des procédures, des pièces qualifiées, des erreurs connues et une base plus compréhensible pour ceux qui arrivent ensuite. La documentation finale doit donc expliquer non seulement ce qui a été construit, mais ce qui a changé pendant la campagne et pourquoi.

À ce stade, l'étudiant ne « connaît pas Mars » au sens encyclopédique. Il sait mieux faire quelque chose de plus utile: poser une hypothèse, la chiffrer, la relier aux autres systèmes, chercher ce qui peut la faire échouer, puis expliquer une décision de manière vérifiable.

Approfondissement du module 16: comprendre, calculer, vérifier et décider

Objectif du module — assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

1. Exigences et hypothèses de mission

Dans ce module, exigences et hypothèses de mission sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Masse utile livrée — distinguer manifeste brut et masse réellement disponible

1 — Question concrète

Quelle masse reste réellement disponible pour la mission après application d'un facteur de disponibilité explicite ?

2 — Intuition sans symboles

Le manifeste brut ne devient pas intégralement une ressource exploitable : on ne garde que la fraction réellement disponible sur la frontière définie.

3 — Grandeurs

M_livrée est la masse utilisable ; M_brute la masse nominale ; f_disponible la fraction effectivement disponible.

4 — Formule

$$M_{\text{livrée}} = M_{\text{brute}} \times f_{\text{disponible}}$$

5 — Lecture

La masse livrée utile égale la masse brute multipliée par la fraction disponible.

6 — Symboles et sens

M_livrée et M_brute sont des masses ; f_disponible est un nombre entre zéro et un défini pour la même frontière de mission.

7 — Prononciation

M livrée égale M brute fois effe disponible.

8 — Unités

kg × sans dimension = kg.

9 — Convention

Le facteur de disponibilité représente une seule correction déclarée. Il ne doit pas cacher une seconde marge de masse, une perte d'emballage ou une réserve d'atterrissage déjà comptée ailleurs.

10 — Pourquoi cette opération

La multiplication sélectionne la partie du manifeste brut réellement utilisable dans le budget aval.

11 — Hypothèses

Le manifeste brut et le facteur décrivent le même lot, au même état de revue et sans double comptage d'autres marges.

12 — Contrôle d'unités

Une fraction est sans unité ; la masse reste donc dans l'unité de M_{brute} .

13 — Cas numérique

Pour 1 800 kg bruts et une disponibilité de 0,92 : $M_{\text{livrée}} = 1\,800 \times 0,92 = 1\,656$ kg.

14 — Pourquoi le calcul fonctionne

On réduit le manifeste de 8 % ; la quantité disponible doit donc être légèrement inférieure à 1,8 tonne.

15 — Contrôle algébrique

$M_{\text{brute}} = M_{\text{livrée}}/f_{\text{disponible}}$ si la fraction est non nulle.

16 — Estimation mentale

92 % de 1 800 kg est proche de 1 660 kg ; 1 656 kg est cohérent.

17 — Interprétation

Le budget aval ne peut compter que 1 656 kg réellement disponibles dans ce cas.

18 — Ce que le résultat ne prouve pas

Ce calcul ne prédit ni pertes de lancement, ni dispersion d'atterrissage, ni dommage, ni emballage, ni aptitude fonctionnelle du matériel après arrivée.

19 — Sensibilité

À masse brute constante, passer de 0,92 à 0,80 abaisse directement la masse utilisable de 1 656 à 1 440 kg.

20 — Exercices guidé et autonome

Exercice guidé. Une livraison brute de 2 400 kg possède une disponibilité qualifiée de 0,88. Quelle masse budgéter en aval ?

Correction guidée

$2\,400 \times 0,88 = 2\,112$ kg utiles.

Exercice autonome. Il faut 1 900 kg utiles avec une disponibilité de 0,95. Quelle masse brute minimale planifier ?

Correction autonome

$1\,900/0,95 = 2\,000$ kg bruts.

21 — Décision mission

Fermer tous les budgets aval sur la masse utile livrée et conserver la masse brute comme donnée de transport séparée.

On injecte maintenant l'événement suivant: un cargo critique est retardé d'une fenêtre.

2. Budget de masse et réserves

Dans ce module, budget de masse et réserves sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Masse mission totale avec marge explicite

1 — Question concrète

Quelle masse totale faut-il annoncer lorsque les sous-systèmes sont sommés puis protégés par une marge de masse commune ?

2 — Intuition sans symboles

On additionne d'abord ce qui existe réellement dans le budget puis on rend la marge visible, au lieu de la disperser dans des sous-totaux impossibles à auditer.

3 — Grandeurs

M_i est la masse du sous-système i ; Σ additionne les masses ; m_{masse} est la marge fractionnaire ; M_{total} est le total margé.

4 — Formule

$$M_{\text{total}} = \Sigma M_i \times (1 + m_{\text{masse}})$$

5 — Lecture

La masse totale égale la somme des masses des sous-systèmes multipliée par un plus la marge de masse.

6 — Symboles et sens

Chaque M_i appartient à la même frontière de mission ; m_{masse} est sans dimension.

7 — Prononciation

M total égale sigma M i fois un plus m masse.

8 — Unités

kg $\times$ sans dimension = kg.

9 — Convention

La marge supérieure ne doit pas être réappliquée à une réserve identique déjà intégrée dans un sous-système.

10 — Pourquoi cette opération

La somme ferme la masse de base ; le facteur supérieur à un ajoute ensuite la réserve de croissance déclarée.

11 — Hypothèses

Toutes les masses sont sur une base compatible et la même protection n'est pas comptée deux fois.

12 — Contrôle d'unités

Une somme de kilogrammes reste en kilogrammes ; multiplier par un facteur sans dimension conserve l'unité.

13 — Cas numérique

Pour une somme de 10 500 kg et 15 % de marge : $M_{\text{total}} = 10\,500 \times 1,15 = 12\,075$ kg.

14 — Pourquoi le calcul fonctionne

La marge ajoute 1 575 kg aux 10 500 kg initiaux.

15 — Contrôle algébrique

La masse non margée se retrouve par $\Sigma M_i = M_{\text{total}} / (1 + m_{\text{masse}})$.

16 — Estimation mentale

15 % de 10,5 tonnes vaut environ 1,6 tonne ; un total proche de 12,1 tonnes est attendu.

17 — Interprétation

Le total margé est 12 075 kg et sépare clairement matériel prévu et réserve de croissance.

18 — Ce que le résultat ne prouve pas

Il ne démontre ni compatibilité de volume, ni centrage, ni capacité lanceur, ni performance EDL.

19 — Sensibilité

À somme fixe, une marge de 20 % porterait le même budget à 12 600 kg.

20 — Exercices guidé et autonome

Exercice guidé. La somme des sous-systèmes vaut 8 400 kg et la marge 12 %. Calculer le total.

Correction guidée

$$8\,400 \times 1,12 = 9\,408 \text{ kg.}$$

Exercice autonome. Un véhicule accepte 11 500 kg et la marge imposée est 15 %. Quelle somme de sous-systèmes ne faut-il pas dépasser ?

Correction autonome

$$11\,500/1,15 = 10\,000 \text{ kg de masse de base.}$$

21 — Décision mission

Afficher séparément masse de base et marge dans les gates lanceur/EDL afin de savoir si une dérive vient du matériel ou de la réserve protégée.

On injecte maintenant l'événement suivant: une source électrique devient indisponible pendant plusieurs sols.

3. Budget de puissance et énergie

Dans ce module, budget de puissance et énergie sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Budget énergétique quotidien — additionner puissance et durée de chaque usage

1 — Question concrète

Quelle énergie quotidienne totale résulte des différents équipements et de leurs temps de fonctionnement ?

2 — Intuition sans symboles

Chaque équipement consomme de l'énergie pendant le temps où il fonctionne. On calcule chaque contribution puis on les additionne.

3 — Grandeurs

E_{jour} est l'énergie totale ; P_i la puissance de la charge i ; t_i sa durée ; Σ indique la somme de toutes les contributions.

4 — Formule

$$E_{\text{jour}} = \sum (P_i \times t_i)$$

5 — Lecture

L'énergie du jour égale la somme, pour chaque charge, de sa puissance multipliée par sa durée.

6 — Symboles et sens

P_i et t_i doivent décrire le même état d'exploitation ; E_{jour} cumule les contributions.

7 — Prononciation

E jour égale sigma de P i fois té i.

8 — Unités

kW × h = kWh ; la somme reste en kWh.

9 — Convention

Toutes les durées appartiennent à la même journée comptable ; pertes et veille ne sont incluses que si les puissances déclarées les représentent.

10 — Pourquoi cette opération

Puissance fois durée donne l'énergie d'une charge ; sommer ferme le ledger énergétique.

11 — Hypothèses

Les profils sont représentatifs et aucune charge importante n'est oubliée ou comptée deux fois.

12 — Contrôle d'unités

Chaque terme produit des kWh ; additionner des kWh donne des kWh.

13 — Cas numérique

2 kW pendant 10 h donnent 20 kWh ; 4 kW pendant 6 h donnent 24 kWh ; 1 kW pendant 24 h donne 24 kWh ; total = 68 kWh.

14 — Pourquoi le calcul fonctionne

Le calcul conserve la contribution de chaque charge avant de former le total, ce qui rend l'audit possible.

15 — Contrôle algébrique

Si une seule durée est inconnue, elle se retrouve en retirant du total les autres énergies puis en divisant le reste par la puissance correspondante.

16 — Estimation mentale

20 + 24 + 24 vaut environ 70 kWh ; 68 kWh est cohérent.

17 — Interprétation

Le scénario demande 68 kWh sur la journée pour ces trois charges.

18 — Ce que le résultat ne prouve pas

Ce total ne dimensionne pas la puissance de pointe, les transitoires, l'onduleur ou le moment précis de charge/décharge du stockage.

19 — Sensibilité

Allonger la durée d'une charge forte augmente le budget plus vite que la même prolongation d'une petite charge.

20 — Exercices guidé et autonome

Exercice guidé. 3 kW pendant 8 h, 5 kW pendant 4 h et 0,5 kW pendant 24 h. Calculer l'énergie quotidienne.

Correction guidée

$$24 + 20 + 12 = 56 \text{ kWh.}$$

Exercice autonome. Le budget est limité à 80 kWh. Deux charges consomment déjà 50 kWh ; une charge de 5 kW reste à planifier. Combien d'heures au maximum ?

Correction autonome

Il reste 30 kWh ; $30/5 = 6$ h maximum.

21 — Décision mission

Fermer l'énergie avec ce ledger, puis exécuter séparément le gate puissance de pointe avant GO.

— « Budget de puissance et énergie ».

On injecte maintenant l'événement suivant: un capteur ECLSS dérive sans panne franche.

4. Boucles eau, oxygène et consommables

Dans ce module, boucles eau, oxygène et consommables sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Application — stock d'équipage avec marge

Cette variante multiplie consommation individuelle, effectif et durée avant d'appliquer une marge. Elle est conservée comme exercice de scénario, mais la règle de référence reste la mini-leçon de stock minimal protégé afin d'éviter deux méthodes concurrentes pour la même décision. Voir la mini-leçon canonique.

On injecte maintenant l'événement suivant: le rover de secours reste immobilisé loin de la base.

5. Chaîne cargo, déploiement et mise en service

Dans ce module, chaîne cargo, déploiement et mise en service sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Application cargo — masse réellement disponible

Le passage cargo réutilise exactement le principe de masse utile livrée. Il reste un cas d'application logistique et renvoie désormais à la mini-leçon canonique plutôt que de dupliquer la même formule. Voir la mini-leçon canonique.

On injecte maintenant l'événement suivant: une fuite lente augmente les besoins de gaz.

6. Transit humain et refuge

Dans ce module, transit humain et refuge sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Application — convertir un stock en horizon

Diviser un stock utile par un débit collectif est le raisonnement général des horizons de réserve. Les mini-leçons canoniques oxygène, nourriture et batterie portent désormais les hypothèses, unités, limites et exercices ; ce passage conserve seulement l'usage opérationnel dans le refuge. Voir la mini-leçon canonique.

On injecte maintenant l'événement suivant: une tempête impose l'annulation de plusieurs EVA.

7. EDL, dispersion et mobilité de secours

Dans ce module, edl, dispersion et mobilité de secours sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Application EDL — vérifier que le secours couvre dispersion et retour

La comparaison entre rayon de secours, dispersion, trajet retour et marge est un gate d'application du rayon protégé. Elle ne doit pas créer une deuxième mini-leçon concurrente : calculer d'abord le rayon canonique, puis vérifier ici que l'enveloppe EDL reste à l'intérieur. Voir la mini-leçon canonique.

On injecte maintenant l'événement suivant: un cargo critique est retardé d'une fenêtre. Dans le module 16, ce point doit être relu depuis la section « 7 — « EDL, dispersion et mobilité de secours ». EDL, dispersion et mobilité de secours »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

8. Campagne de 500 sols et maintenance

Dans ce module, campagne de 500 sols et maintenance sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Pannes attendues à partir de la durée de mission et du MTBF

1 — Question concrète

Combien de pannes moyennes un modèle simple suggère-t-il sur une durée d'exposition donnée ?

2 — Intuition sans symboles

Une mission qui dure plusieurs fois le temps moyen entre pannes doit s'attendre à plusieurs événements, sans savoir exactement quand ils surviendront.

3 — Grandeurs

N_{pannes} est le nombre moyen attendu ; t_{mission} la durée d'exposition ; MTBF le temps moyen entre pannes sur la même base.

4 — Formule

$$N_{\text{pannes}} \approx t_{\text{mission}} / \text{MTBF}$$

5 — Lecture

Le nombre moyen de pannes est approximativement la durée de mission divisée par le MTBF.

6 — Symboles et sens

t_{mission} et MTBF sont des durées compatibles ; N_{pannes} est un compte moyen sans dimension.

7 — Prononciation

N pannes environ égal à t mission divisé par M T B F.

8 — Unités

heures/heures = sans dimension.

9 — Convention

Le MTBF doit concerner le même équipement, le même régime et la même population que l'exposition analysée.

10 — Pourquoi cette opération

Le quotient indique combien d'intervalles moyens de panne tiennent dans la durée étudiée.

11 — Hypothèses

Le modèle suppose un taux moyen pertinent ; il ne représente pas automatiquement jeunesse, usure, causes communes ou réparations dépendantes.

12 — Contrôle d'unités

Deux temps exprimés dans la même unité s'annulent.

13 — Cas numérique

$t_{\text{mission}} = 7\,200\text{ h}$ et $\text{MTBF} = 2\,400\text{ h}$ donnent $N_{\text{pannes}} = 3,0$.

14 — Pourquoi le calcul fonctionne

La mission couvre trois intervalles moyens entre pannes.

15 — Contrôle algébrique

À nombre moyen fixé, $\text{MTBF} \approx t_{\text{mission}}/N_{\text{pannes}}$.

16 — Estimation mentale

7 200 est exactement trois fois 2 400 ; le résultat 3 est immédiat.

17 — Interprétation

Le chiffre sert de premier écran pour pièces de rechange et charge maintenance.

18 — Ce que le résultat ne prouve pas

Il ne fournit ni calendrier de pannes ni probabilité d'avoir exactement trois événements, et ne modélise pas les défaillances corrélées.

19 — Sensibilité

Une mission plus longue ou un MTBF plus court augmente le nombre moyen attendu.

20 — Exercices guidé et autonome

Exercice guidé. Durée 4 800 h, MTBF 1 600 h. Combien de pannes moyennes ?

Correction guidée

$4\,800/1\,600 = 3$ pannes moyennes.

Exercice autonome. On accepte au plus deux pannes moyennes sur 6 000 h. Quel MTBF minimal viser ?

Correction autonome

$MTBF = 6\,000/2 = 3\,000$ h au minimum dans ce modèle simplifié.

21 — Décision mission

Utiliser ce résultat pour pré-dimensionner spares et maintenance, puis appliquer un modèle de fiabilité adapté avant qualification.

— « Campagne de 500 sols et maintenance ».

On injecte maintenant l'événement suivant: une source électrique devient indisponible pendant plusieurs sols. Dans le module 16, ce point doit être relu depuis la section « 8 — « Campagne de 500 sols et maintenance ». Campagne de 500 sols et maintenance »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

9. Gates GO, HOLD et NO-GO

Dans ce module, gates go, hold et no-go sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Marge de capacité — mesurer la capacité protégée au-dessus du besoin

1 — Question concrète

Quelle marge relative reste-t-il entre la capacité réellement disponible et le besoin certifié ?

2 — Intuition sans symboles

On mesure d'abord l'excédent de capacité, puis on le rapporte au besoin afin de rendre comparables des systèmes de tailles différentes.

3 — Grandeurs

C_{dispo} est la capacité disponible ; C_{requis} le besoin ; m_{cap} la marge relative.

4 — Formule

$$m_cap = (C_dispo - C_requis) / C_requis$$

5 — Lecture

La marge de capacité égale la capacité disponible moins la capacité requise, le tout divisé par la capacité requise.

6 — Symboles et sens

Les deux capacités décrivent la même fonction et la même condition ; m_cap est sans dimension.

7 — Prononciation

m capacité égale C disponible moins C requise, divisé par C requise.

8 — Unités

même unité moins même unité, puis division par cette unité : sans dimension.

9 — Convention

Comparer des capacités sur une même base de température, duty-cycle, dégradation et niveau de qualification.

10 — Pourquoi cette opération

La différence donne le surplus absolu ; la division par le besoin transforme ce surplus en marge relative.

11 — Hypothèses

La capacité annoncée est réellement disponible dans les conditions mission et le besoin représente bien le cas de certification.

12 — Contrôle d'unités

Le numérateur et le dénominateur utilisent la même unité, qui s'annule.

13 — Cas numérique

$C_dispo = 125$ unités et $C_requis = 100$ donnent $(125 - 100) / 100 = 0,25 = 25 \%$.

14 — Pourquoi le calcul fonctionne

Le système possède 25 unités de surplus pour 100 unités nécessaires.

15 — Contrôle algébrique

$$C_dispo = C_requis \times (1 + m_cap).$$

16 — Estimation mentale

25 unités de surplus sur 100 correspondent naturellement à un quart, donc 25 %.

17 — Interprétation

La capacité disponible est 25 % au-dessus du besoin déclaré.

18 — Ce que le résultat ne prouve pas

Une marge positive ne prouve ni fiabilité, ni réponse dynamique, ni qualité du produit, ni survie à une panne.

19 — Sensibilité

Si le besoin passe de 100 à 115 à capacité fixe 125, la marge tombe à environ 8,7 %.

20 — Exercices guidé et autonome

Exercice guidé. Capacité 150, besoin 120. Calculer la marge.

Correction guidée

$$(150-120)/120 = 0,25 = 25 \%$$

Exercice autonome. Besoin 80 et marge minimale 20 %. Quelle capacité disponible faut-il garantir ?

Correction autonome

$$80 \times 1,20 = 96 \text{ unités.}$$

21 — Décision mission

Tracker la marge contre le besoin réellement certifié et déclencher HOLD si une dégradation consomme la réserve protégée.

On injecte maintenant l'événement suivant: un capteur ECLSS dérive sans panne franche.

10. Propagation de pannes entre sous-systèmes

Dans ce module, propagation de pannes entre sous-systèmes sert directement à assembler une mission cargo, un transit humain, l'arrivée sur Mars et une campagne de surface en un système dont les budgets et les secours restent cohérents.

Fiabilité d'un système en série — multiplier les probabilités de succès indépendantes

1 — Question concrète

Quelle fiabilité de premier ordre obtient-on lorsque plusieurs éléments sont tous nécessaires au succès ?

2 — Intuition sans symboles

Si chaque élément doit fonctionner, le système ne réussit que lorsque tous réussissent pendant le même intervalle.

3 — Grandeurs

R_i est la fiabilité de l'élément i ; Π indique leur produit ; $R_{\text{système}}$ est la fiabilité du chemin en série.

4 — Formule

$$R_{\text{système}} = \Pi R_i$$

5 — Lecture

La fiabilité du système égale le produit des fiabilités de tous les éléments requis.

6 — Symboles et sens

Chaque R_i est une probabilité comprise entre zéro et un sur le même intervalle.

7 — Prononciation

R système égale produit de R i.

8 — Unités

probabilité $\times$ probabilité reste sans dimension.

9 — Convention

La multiplication suppose ici des succès indépendants et un chemin pur en série sans redondance réparée.

10 — Pourquoi cette opération

Tous les éléments doivent réussir ; la probabilité jointe d'événements indépendants est leur produit.

11 — Hypothèses

Même intervalle de mission, tous les éléments requis, indépendance raisonnable ; pas de réparation, redondance active ou cause commune dans ce modèle simple.

12 — Contrôle d'unités

Le produit de nombres sans dimension reste sans dimension.

13 — Cas numérique

$0,98 \times 0,97 \times 0,99 \approx 0,941$, soit 94,1 %.

14 — Pourquoi le calcul fonctionne

Chaque facteur inférieur à un réduit légèrement le résultat ; trois éléments très fiables peuvent donc donner un système moins fiable que chacun pris séparément.

15 — Contrôle algébrique

Pour retrouver un facteur manquant, diviser $R_{\text{système}}$ par le produit des autres facteurs non nuls.

16 — Estimation mentale

$0,98 \times 0,97$ est proche de 0,95 ; multiplier encore par 0,99 doit rester proche de 0,94.

17 — Interprétation

Le modèle simplifié donne environ 94,1 % de succès du chemin en série sur l'intervalle.

18 — Ce que le résultat ne prouve pas

Il ne représente ni disponibilité, ni réparation, ni redondance, ni dépendances partagées, ni propagation de pannes.

19 — Sensibilité

Ajouter un élément nécessaire de fiabilité inférieure à un diminue toujours la fiabilité du pur chemin en série.

20 — Exercices guidé et autonome

Exercice guidé. Deux éléments indispensables ont des fiabilités 0,96 et 0,95. Calculer le chemin en série.

Correction guidée

$0,96 \times 0,95 = 0,912$, soit 91,2 %.

Exercice autonome. Trois éléments identiques doivent donner ensemble au moins 0,97. Quelle fiabilité individuelle minimale faut-il environ ?

Correction autonome

Il faut $R_i \geq \sqrt[3]{0,97} \approx 0,9899$, donc environ 99,0 % chacun dans ce modèle indépendant.

21 — Décision mission

Utiliser ce produit comme écran transparent ; dès que les dépendances ou redondances comptent, passer à un arbre de défaillances ou un modèle de blocs de fiabilité.

On injecte maintenant l'événement suivant: le rover de secours reste immobilisé loin de la base.

Exercices progressifs avec corrigés 1:1

Exercice 1: Exigences et hypothèses de mission

Le scénario comporte six personnes, 500 sols de surface, deux cargos précurseurs, un habitat principal, un refuge indépendant, deux rovers et une alimentation multi-source. Construire un registre de huit exigences avant de choisir une architecture. Pour chaque exigence, préciser: fonction protégée, grandeur mesurable, seuil, marge ou réserve, moyen de vérification et conséquence si la preuve manque. Classer chaque ligne en exigence dure (la mission ne part pas si elle n'est pas satisfaite) ou objectif de performance (on peut accepter une dégradation). Inclure obligatoirement énergie critique, eau, atmosphère, refuge, communication, mobilité de secours, maintenance et temps humain.

Un tableau de traçabilité et une décision GO/HOLD/NO-GO pour le départ humain. Aucun « cela devrait fonctionner » n'est accepté: une exigence doit être vérifiable.

On commence par séparer une exigence d'une solution. « Installer deux batteries » est une solution; « maintenir les charges vitales pendant l'interruption maximale crédible » est une exigence. Une ligne robuste pourrait être: Énergie critique — fournir 35 kW pendant 18 h après perte de la source principale — réserve de 20 % du stockage nominal non planifiable — vérification par essai de délestage et mesure de capacité — absence de preuve = HOLD.

Le même raisonnement s'applique à l'eau: l'exigence porte sur un horizon de continuité, pas sur la présence d'un réservoir. Pour l'atmosphère, la masse d'O₂ seule ne suffit pas; il faut aussi surveiller pression totale, CO₂, humidité et contaminants. Pour le refuge, l'exigence doit préciser combien de personnes, combien de temps et quelles fonctions restent indépendantes. Pour la mobilité, le critère doit intégrer l'aller-retour et la réserve, pas l'autonomie commerciale affichée. Pour la maintenance, on exige une capacité de diagnostic, de réparation ou de remplacement sur les fonctions vitales. Pour le temps humain, on limite la charge planifiée afin de conserver une réserve pour anomalies.

Une exigence est acceptable si un observateur indépendant peut dire PASS ou FAIL à partir d'une mesure, d'un essai ou d'un calcul. Si plusieurs exigences vitales n'ont pas encore de preuve, le verdict correct n'est pas NO-GO définitif mais HOLD: le système peut être prometteur, mais le départ humain reste interdit tant que les preuves ne sont pas fermées.

Exercice 2: Budget de masse et réserves

Chaque cargo précurseur a une masse brute pédagogique de 42 t. On suppose que la fraction réellement disponible au site après structure, emballage, réserves et pertes est $f = 0,82$. Calculer la masse utile disponible pour un cargo puis pour deux cargos. Le scénario exige ensuite 8 t de consommables et pièces réservées, qui ne doivent pas être comptées comme masse libre. Quelle masse reste réellement allouable aux autres fonctions? Faire le contrôle d'unité, l'ordre de grandeur et une sensibilité si f tombe à 0,75.

La relation est $M_{\text{utile}} = M_{\text{brute}} \times f$. M_{brute} est une masse en tonnes; f est une fraction sans unité; le résultat est donc une masse en tonnes. Pour un cargo: $42 \times 0,82 = 34,44$ t. Pour deux cargos: $2 \times 34,44 = 68,88$ t. L'ordre de grandeur mental est simple: 80 % de 84 t vaut environ 67 t; 68,88 t est donc plausible.

La réserve de 8 t n'est pas « disponible parce qu'elle a atterri ». Elle est affectée à une fonction de sécurité. La masse libre est donc $68,88 - 8 = 60,88$ t. Cette distinction évite une erreur classique des budgets système: compter deux fois une même marge, d'abord comme réserve puis comme ressource utilisable.

Si la fraction utile tombe à 0,75, les deux cargos fournissent $84 \times 0,75 = 63$ t. Après la réserve de 8 t, il reste 55 t. La perte de masse libre est $60,88 - 55 = 5,88$ t. Ce n'est pas un détail: 5,88 t peuvent représenter des pièces, du blindage, des consommables ou une marge EDL. La bonne décision n'est pas d'ignorer l'écart mais de rouvrir les allocations et vérifier quelles exigences deviennent non fermées.

Exercice 3: Budget de puissance, énergie et batterie

La puissance moyenne du scénario est 55 kW et la charge critique en mode dégradé est 35 kW. La batterie nominale vaut 900 kWh, mais 20 % restent en réserve non planifiée. Calculer: énergie consommée pendant un sol de 24,66 h au régime moyen; énergie planifiable de la batterie; autonomie à 35 kW; énergie consommée pendant une panne de 18 h; marge temporelle restante. Expliquer clairement la différence entre kW et kWh.

La puissance est un débit d'énergie; l'énergie est ce débit intégré sur une durée. La relation élémentaire est $E = P \times t$. Avec 55 kW pendant 24,66 h: $E = 55 \times 24,66 = 1\,356,3$ kWh, soit environ 1,36 MWh par sol. Le contrôle dimensionnel est kW $\times$ h = kWh.

On n'autorise pas 900 kWh comme capacité de mission si 20 % sont réservés. L'énergie planifiable vaut $900 \times (1 - 0,20) = 720$ kWh. À 35 kW constants, l'autonomie théorique est $720 / 35 = 20,57$ h. Pour une panne de 18 h, la consommation vaut $35 \times 18 = 630$ kWh. Il reste donc 90 kWh, soit $90 / 35 = 2,57$ h de marge temporelle.

Dire « la batterie tient » est trop vague. La formulation exploitable est: « avec les hypothèses annoncées, les charges critiques peuvent être tenues 18 h avec environ 2,6 h de marge ». Si la réparation plausible exige 24 h, le système ne ferme plus l'exigence: il faut réduire la charge critique, augmenter le stockage ou fournir une source alternative. L'erreur classique est de comparer 35 kW à 900 kWh sans introduire le temps.

Exercice 4: Boucles eau, oxygène et consommables

Pour six personnes et 500 sols, l'appoint net d'eau est supposé égal à 1,2 kg/personne/sol et l'appoint net d'O₂ à 0,9 kg/personne/sol. Calculer le besoin de campagne pour chacune des deux ressources. Calculer ensuite un tampon d'eau de 30 sols et l'O₂ requis pour trois sols de perte de production. Expliquer pourquoi « appoint net », « stock de campagne » et « réserve d'urgence » ne sont pas synonymes.

Pour une ressource consommée à débit constant, $m = q \times N \times t$. Ici q est le débit net par personne et par sol, N l'effectif et t la durée. Eau: $1,2 \times 6 \times 500 = 3\,600$ kg. O₂: $0,9 \times 6 \times 500 = 2\,700$ kg. Les unités kg/personne/sol $\times$ personnes $\times$ sols donnent bien des kg.

Le tampon d'eau de 30 sols vaut $1,2 \times 6 \times 30 = 216$ kg. Il répond à la question « combien doit être mobilisable pendant une interruption définie? », pas « combien sera consommé sur toute la campagne? Pour trois sols sans production principale d'O₂: $0,9 \times 6 \times 3 = 16,2$ kg. Si une réserve indépendante de 45 kg est réellement disponible pour cette fonction, il resterait arithmétiquement 28,8 kg après trois sols.

Le calcul O₂ ne prouve pas que l'atmosphère est habitable: CO₂, pression totale, gaz tampon, humidité et contaminants restent des contraintes séparées. De même, l'appoint net d'eau ne décrit pas les flux bruts de boisson, hygiène ou traitement. Le contrôle opérationnel porte sur les stocks réellement isolables et sur le débit net mesuré après anomalie.

Exercice 5: Chaîne cargo, déploiement et mise en service

Après l'atterrissage du second cargo, cinq tâches sont nécessaires: A inspection externe 8 h; B déploiement puissance 12 h après A; C pressurisation initiale 10 h après A; D test communications 6 h après B; E validation ECLSS 14 h après C. B et C peuvent être menées en parallèle par deux équipes. Calculer la durée minimale du chemin critique et expliquer ce qui se passe si C prend 6 h de retard.

On dessine d'abord les dépendances. A précède B et C. La branche puissance/communications dure $A + B + D = 8 + 12 + 6 = 26$ h. La branche pressurisation/ECLSS dure $A + C + E = 8 + 10 + 14 = 32$ h. Avec deux équipes réellement disponibles et des interfaces indépendantes, la durée minimale est donc le maximum des deux branches: 32 h. Additionner toutes les durées donnerait 50 h et ignorerait le parallélisme; annoncer 26 h ignorerait la branche la plus longue.

Si C prend 6 h de retard, la branche A-C-E passe à 38 h. Le chemin critique reste cette branche et la mise en service glisse de 6 h. La question suivante est opérationnelle: les consommables, l'énergie, les équipes et la fenêtre météo disposent-ils de 6 h de marge? Un retard de planning devient un risque système lorsqu'il consomme une réserve d'une autre fonction.

Un diagramme de tâches ne prouve pas que deux opérations peuvent réellement être parallèles. Il faut vérifier personnel, outils, accès, puissance et risques communs. Si B et C utilisent le même connecteur ou la même équipe, la supposée parallélisation disparaît.

Exercice 6: Transit humain et refuge indépendant

Le refuge doit accueillir six personnes pendant 72 h après isolement du volume principal. Pour l'exercice, utiliser 0,9 kg O₂/personne/sol et 2,5 kg d'eau/personne/jour en mode d'urgence. Calculer les masses minimales d'O₂ et d'eau pour trois jours. Ajouter 25 % de marge logistique et expliquer quelles autres fonctions doivent être vérifiées avant de déclarer le refuge « autonome ».

O₂ sans marge: $0,9 \times 6 \times 3 = 16,2$ kg. Avec 25 %: $16,2 \times 1,25 = 20,25$ kg. Eau: $2,5 \times 6 \times 3 = 45$ kg; avec 25 %: $45 \times 1,25 = 56,25$ kg. Le calcul est volontairement simple: débit $\times$ personnes $\times$ durée $\times$ (1 + marge).

Mais un refuge n'est pas autonome parce qu'il contient 20,25 kg d'O₂ et 56,25 kg d'eau. Il faut aussi vérifier l'élimination du CO₂, la circulation et le contrôle thermique, la pression, l'énergie, les communications, l'hygiène minimale, la gestion des déchets, le médical, le couchage et le risque incendie. Une marge sur deux consommables ne remplace pas l'indépendance fonctionnelle.

Si l'O₂ est suffisant mais que le scrubbing CO₂ ne tient que 30 h, l'autonomie du refuge est 30 h, pas 72 h. En ingénierie système, la chaîne est limitée par la fonction critique la plus courte. Le corrigé doit donc toujours rechercher le « maillon temporel » qui expire en premier.

Exercice 7: EDL, dispersion et mobilité de secours

Un rover a une autonomie totale de scénario de 60 km. On conserve 25 % de réserve pour terrain, détour et secours. Déduire un rayon opérationnel aller-retour sûr autour de la base. Un véhicule se pose à 18 km du site nominal. Quelle marge reste-t-il, et pourquoi cette réponse ne suffit-elle pas à autoriser immédiatement un secours?

On réserve d'abord 25 %: distance planifiable = $60 \times 0,75 = 45$ km. Pour un aller-retour symétrique, le rayon vaut $45 / 2 = 22,5$ km. Un point situé à 18 km est donc à l'intérieur de cette enveloppe avec une marge géométrique de $22,5 - 18 = 4,5$ km.

Le résultat ne dit pas « secours autorisé ». Il dit seulement que la distance horizontale nominale est compatible avec le modèle. Avant départ, on vérifie énergie réellement disponible, relief, adhérence, température, météo, état du deuxième rover, communications, capacité d'accueil et durée de survie du véhicule immobilisé. Un détour de 6 km ou une consommation dégradée peut consommer entièrement les 4,5 km de marge.

Sans la division par deux, on annoncerait 45 km et on oublierait le retour. Sans la réserve, on annoncerait 30 km. Ces deux erreurs sont typiques d'une autonomie publicitaire transformée trop vite en rayon opérationnel.

Exercice 8: Campagne de 500 sols, fiabilité et pièces de rechange

Quatre pompes identiques assurent une fonction auxiliaire. Pour l'exercice, chaque pompe a un MTBF pédagogique de 800 sols. Sur 500 sols, estimer le nombre moyen de défaillances attendu pour l'ensemble des quatre pompes avec $\lambda \approx t/\text{MTBF}$. Comparer ce résultat à un stock de trois unités de rechange et expliquer pourquoi l'espérance ne suffit pas à certifier le stock.

Pour une pompe, le nombre moyen d'événements sur 500 sols dans ce modèle de premier ordre est $500 / 800 = 0,625$. Pour quatre pompes exposées de façon comparable: $4 \times 0,625 = 2,5$ défaillances attendues. Un stock de trois rechanges semble donc, au niveau de l'espérance, légèrement supérieur au besoin moyen.

Mais « 2,5 défaillances attendues » ne signifie pas qu'il y en aura exactement deux ou trois. La distribution peut produire zéro événement ou davantage. Le modèle suppose en outre indépendance, taux constant et remplacement parfait; une contamination commune ou un défaut de lot peut invalider ces hypothèses. C'est pourquoi le stock ne se ferme pas par « trois > 2,5 ». Il faut regarder criticité, capacité de réparation, pièces communes, détection, cannibalisation, temps de remplacement et probabilité de queue.

Si les pompes sont réparables localement, trois unités complètes peuvent être conservatrices. Si elles sont non réparables et qu'une perte commune est crédible, le même stock peut être insuffisant. La bonne conclusion est donc conditionnelle au modèle de panne et à la maintenance, pas seulement à la moyenne.

Exercice 9: Gates GO, HOLD et NO-GO

À T-30 jours du départ humain, les essais donnent: batterie planifiable 720 kWh; charge critique 35 kW; exigence d'autonomie 18 h; tampon d'eau 216 kg; perte nette mesurée 1,4 kg/personne/sol au lieu de 1,2; rover de secours validé; refuge 72 h validé; communications secondaires non encore testées. Classer chaque point puis donner un verdict global GO/HOLD/NO-GO.

Énergie: besoin $35 \times 18 = 630$ kWh. Avec 720 kWh planifiables, la marge est 90 kWh: PASS sur le critère chiffré, sous réserve que la capacité soit réellement mesurée. Eau: à 1,4 kg/personne/sol, le tampon de 216 kg couvre $216 / (1,4 \times 6) = 25,7$ sols, pas 30. Si l'exigence dure est 30 sols, le point est FAIL tant que le débit net n'est pas réduit ou le stock augmenté.

Rover et refuge sont PASS si leurs essais couvrent les conditions prévues. Les communications secondaires non testées constituent une absence de preuve. Si elles sont requises comme voie de secours, le point est HOLD. Le verdict global est donc HOLD: aucune impossibilité fondamentale n'est démontrée, mais au moins une exigence de continuité eau n'est plus satisfaite et une redondance de communication n'est pas vérifiée.

Parce qu'on ne moyenne jamais un PASS énergétique avec un FAIL eau. Une exigence vitale dure est un gate, pas une note. Parce que les écarts sont potentiellement corrigeables avant départ. Le vocabulaire GO/HOLD/NO-GO sert précisément à distinguer « prêt », « pas encore prouvé » et « incompatible avec la mission ».

Exercice 10: Propagation de pannes entre sous-systèmes

Injecter simultanément deux anomalies: perte de la source principale pendant 18 h et dégradation de la récupération d'eau pendant 10 sols, faisant passer l'appoint net d'eau de 1,2 à 4,0 kg/personne/sol. Calculer l'énergie critique consommée et l'eau supplémentaire nécessaire. Puis décrire au moins quatre effets de propagation vers opérations, thermique, maintenance ou temps humain.

Énergie: $35 \text{ kW} \times 18 \text{ h} = 630$ kWh. Avec 720 kWh planifiables, il reste 90 kWh, soit environ 2,57 h de charge critique. Eau supplémentaire: l'écart de débit est $4,0 - 1,2 = 2,8$ kg/personne/sol. Sur six personnes et dix sols: $2,8 \times 6 \times 10 = 168$ kg à prélever sur un stock libre ou à produire autrement.

Les deux anomalies se couplent. Première propagation: la réparation de la boucle eau consomme du temps humain alors que l'équipage gère déjà le délestage électrique. Deuxième: certaines fonctions de traitement d'eau peuvent elles-mêmes être des charges électriques, ce qui impose de choisir quand les relancer. Troisième: moins de puissance peut dégrader le contrôle thermique ou imposer de reporter des opérations scientifiques. Quatrième: l'usage accru de stocks génère une dette logistique qui réduit la marge disponible pour une panne ultérieure.

Le système n'est pas évalué panne par panne dans des univers indépendants. On construit un nouvel état: énergie restante, stock d'eau restant, tâches différées, équipements indisponibles et temps de réparation. Le verdict reste HOLD tant que la trajectoire de récupération n'a pas démontré qu'aucun stock vital n'atteint son seuil avant le retour à un état stable.

Exercice 11: Perte de communications Terre-Mars pendant 48 h

Une interruption supprime le haut débit avec la Terre pendant 48 h. Le site produit 20 Go de données par jour, dont 2 Go/jour sont classés critiques. Calculer le stockage minimal pour ne perdre aucune donnée sur 48 h et le volume minimal prioritaire. Définir ensuite quelles décisions doivent rester locales et quelles informations seront envoyées en premier lors du rétablissement.

Sur deux jours, le volume total vaut $20 \times 2 = 40$ Go. Le volume critique vaut $2 \times 2 = 4$ Go. Un stockage local inférieur à 40 Go obligerait soit à supprimer des données, soit à réduire la production. En pratique on ajouterait une marge, des métadonnées, de la redondance et une politique d'écrasement; 40 Go n'est donc qu'un minimum pédagogique.

La partie la plus importante n'est pas le stockage. Les fonctions vitales ne doivent pas attendre une autorisation terrestre en temps réel. Isolement d'une fuite, passage en refuge, délestage, premiers soins selon procédures et protection d'un équipier relèvent de l'autorité locale prédéfinie. Les choix non urgents peuvent être journalisés et différés.

Au rétablissement, on ne vide pas 40 Go sans priorité. On envoie d'abord état équipage, état des fonctions vitales, anomalies, décisions prises, marges restantes et demandes d'expertise. Les données scientifiques ou vidéo volumineuses suivent ensuite. Le corrigé montre ainsi que DTN et autonomie sont des problèmes de gouvernance de l'information autant que de bande passante.

Exercice 12: Trade-off final entre deux architectures

Architecture A: batterie 900 kWh, réserve 20 %, charge critique 35 kW, masse ajoutée de stockage 0 t par rapport à la référence. Architecture B: batterie 1 200 kWh, réserve 20 %, charge critique abaissée à 32 kW, mais +1,8 t de masse. L'exigence dure est de tenir 24 h sans source principale. Calculer l'autonomie de chaque variante et déterminer si un score multicritère peut compenser l'échec d'une exigence dure.

Architecture A: énergie planifiable = $900 \times 0,8 = 720$ kWh. Autonomie = $720 / 35 = 20,57$ h. Elle échoue donc à l'exigence dure de 24 h. Architecture B: énergie planifiable = $1\,200 \times 0,8 = 960$ kWh. Autonomie = $960 / 32 = 30$ h. B possède 6 h de marge au-delà du seuil, au prix de 1,8 t supplémentaires.

Un score pondéré peut ensuite comparer masse, coût, maintenabilité, complexité ou marge, mais seulement entre solutions qui franchissent les gates obligatoires. On ne doit pas écrire « A gagne 9 points de masse et perd seulement 4 points d'autonomie, donc A est meilleure » si l'autonomie 24 h est une exigence de sécurité. Une exigence dure transforme l'espace de décision: A est éliminée ou doit être modifiée avant la comparaison finale.

B n'est pas automatiquement « la bonne architecture ». Ses 1,8 t peuvent rendre un autre budget impossible. La bonne démarche est donc: 1) vérifier les gates; 2) fermer les interfaces; 3) comparer les variantes encore admissibles; 4) documenter ce que la solution sacrifie et la marge restante. C'est cette chaîne de raisonnement, et non le choix du même chiffre que le corrigé, qui est évaluée.

Dossier solution de référence: mission intégrée sur 500 sols

Méthode de lecture: pour chaque phase ci-dessous, suivre cinq colonnes mentales: fonction recherchée, capacité nominale, capacité réellement disponible, mode dégradé, preuve permettant de revenir au nominal. Cette méthode évite de confondre présence d'un équipement et disponibilité d'une fonction.

1. Cargo précurseur

Le cargo est traité comme une condition d'ouverture de la mission humaine. Le dossier inventorie énergie initiale, communications, moyens de déchargement, pièces critiques, refuge et capacité de mise en service. Un équipement posé mais non testé ne compte pas comme capacité disponible. Pour « Cargo précurseur », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Cargo précurseur » sert à révéler les dépendances et chemins de propagation de panne.

Pour cargo précurseur, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Cargo précurseur », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Cargo précurseur », un nombre sans unité ou horizon temporel est incomplet. Pour « Cargo précurseur », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Cargo précurseur » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Une télémétrie unique n'est pas une preuve suffisante lorsqu'un biais commun est possible. Pour « Cargo précurseur », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Cargo précurseur » précise ce qui serait observé si l'état supposé était réel.

Pour « Cargo précurseur », retirez une capacité utile et recalculez l'horizon de décision. Dans « Cargo précurseur », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Cargo précurseur » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie.

Pour « Cargo précurseur », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Cargo précurseur », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé demande donc un bilan des conséquences croisées avant d'accepter une optimisation.

2. Validation avant départ humain

La décision de départ utilise uniquement les fonctions vérifiées au sol martien ou les capacités dont l'incertitude est explicitement acceptée. Les télémetries de puissance, de stockage, de communications et d'intégrité deviennent des preuves de disponibilité, pas des décorations de tableau de bord. Pour « Validation avant départ humain », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Validation avant départ humain » sert à révéler les dépendances et chemins de propagation de panne.

Pour validation avant départ humain, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Validation avant départ humain », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Validation avant départ humain », un nombre sans unité ou horizon temporel est incomplet. Pour « Validation avant départ humain », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Validation avant départ humain » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Validation avant départ humain », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Validation avant départ humain », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Validation avant départ humain » précise ce qui serait observé si l'état supposé était réel.

Pour « Validation avant départ humain », retirez une capacité utile et recalculez l'horizon de décision. Dans « Validation avant départ humain », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Validation avant départ humain » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie.

La faute la plus fréquente consiste à optimiser localement cette phase sans mesurer ce qu'elle impose aux autres. Dans « Validation avant départ humain », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Validation avant départ humain » demande donc un bilan des conséquences croisées avant d'accepter une optimisation.

3. Transit humain

Le véhicule de transit est budgété comme habitat autonome: air, eau, nourriture, thermique, énergie, sommeil, exercice, santé, abri radiatif, maintenance et communications. Chaque fonction reçoit une capacité nominale, une capacité de secours et une durée de survie. Pour « Transit humain », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Transit humain » sert à révéler les dépendances et chemins de propagation de panne.

Pour transit humain, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Transit humain », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Transit humain », un nombre sans unité ou horizon temporel est incomplet. Pour « Transit humain », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Transit humain » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Transit humain », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Transit humain », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Transit humain » précise ce qui serait observé si l'état supposé était réel.

Pour « Transit humain », retirez une capacité utile et recalculez l'horizon de décision. Dans « Transit humain », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Transit humain » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie.

Pour « Transit humain », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Transit humain », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Transit humain » demande donc un bilan des conséquences croisées avant d'accepter une optimisation.

4. Arrivée et EDL

La réussite de l'atterrissage ne se résume pas au contact avec le sol. Le dossier relie ellipse de dispersion, distance entre véhicules, mobilité, météo, réserve d'énergie, communications et accès au refuge. Un atterrissage techniquement réussi peut être opérationnellement mauvais. Pour « Arrivée et EDL », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Arrivée et EDL » sert à révéler les dépendances et chemins de propagation de panne.

Pour arrivée et edl, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Arrivée et EDL », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Arrivée et EDL », un nombre sans unité ou horizon temporel est incomplet. Pour « Arrivée et EDL », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Arrivée et EDL » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Arrivée et EDL », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Arrivée et EDL », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Arrivée et EDL » précise ce qui serait observé si l'état supposé était réel.

Pour « Arrivée et EDL », retirez une capacité utile et recalculez l'horizon de décision. Dans « Arrivée et EDL », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Arrivée et EDL » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie.

Pour « Arrivée et EDL », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Arrivée et EDL », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Arrivée et EDL » demande donc un bilan des conséquences croisées avant d'accepter une optimisation.

5. Mise en service de la base

Les premières heures et les premiers sols sont une séquence de commissioning. On vérifie alimentation, atmosphère, eau, capteurs, réseaux, sas, stockage, incendie et communications avant d'augmenter progressivement le niveau d'activité. Pour « Mise en service de la base », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Mise en service de la base » sert à révéler les dépendances et chemins de propagation de panne.

Pour mise en service de la base, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Mise en service de la base », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Mise en service de la base », un nombre sans unité ou horizon temporel est incomplet. Pour « Mise en service de la base », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Mise en service de la base » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Mise en service de la base », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Mise en service de la base », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Mise en service de la base » précise ce qui serait observé si l'état supposé était réel. Dans le module 16, ce point doit être relu depuis la section « 5 — « Mise en service de la base ». Mise en service de la base »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Mise en service de la base », retirez une capacité utile et recalculez l'horizon de décision. Dans « Mise en service de la base », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Mise en service de la base » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie. Dans le module 16, ce point doit être relu depuis la section « 5 — « Mise en service de la base ». Mise en service de la base »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Mise en service de la base », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Mise en service de la base », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Mise en service de la base » demande donc un bilan des conséquences croisées avant d'accepter une optimisation. Dans le module 16, ce point doit être relu depuis la section « 5 — « Mise en service de la base ». Mise en service de la base »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

6. Campagne de 500 sols

La longue durée fait apparaître usure, consommation de pièces, dérive de capteurs, changements de saison et accumulation de petites pertes. Le budget doit donc être recalculé à plusieurs jalons au lieu de supposer un état initial figé. Pour « Campagne de 500 sols », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Campagne de 500 sols » sert à révéler les dépendances et chemins de propagation de panne.

Pour campagne de 500 sols, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Campagne de 500 sols », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Campagne de 500 sols », un nombre sans unité ou horizon temporel est incomplet. Pour « Campagne de 500 sols », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Campagne de 500 sols » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Campagne de 500 sols », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Campagne de 500 sols », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Campagne de 500 sols » précise ce qui serait observé si l'état supposé était réel. Dans le module 16, ce point doit être relu depuis la section « 6 — « Campagne de

500 sols ». Campagne de 500 sols »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Campagne de 500 sols », retirez une capacité utile et recalculez l'horizon de décision. Dans « Campagne de 500 sols », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Campagne de 500 sols » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie. Dans le module 16, ce point doit être relu depuis la section « 6 — « Campagne de 500 sols ». Campagne de 500 sols »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Campagne de 500 sols », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Campagne de 500 sols », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Campagne de 500 sols » demande donc un bilan des conséquences croisées avant d'accepter une optimisation. Dans le module 16, ce point doit être relu depuis la section « 6 — « Campagne de 500 sols ». Campagne de 500 sols »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

7. Six pannes injectées

Chaque panne est suivie par une chronologie: détection, confirmation, isolement, changement de mode, ressources consommées, réparation, test et retour contrôlé. La correction examine aussi les causes communes et les erreurs de diagnostic possibles. Pour « Six pannes injectées », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Six pannes injectées » sert à révéler les dépendances et chemins de propagation de panne.

Pour six pannes injectées, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Six pannes injectées », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Six pannes injectées », un nombre sans unité ou horizon temporel est incomplet. Pour « Six pannes injectées », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Six pannes injectées » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Six pannes injectées », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Six pannes injectées », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Six pannes injectées » précise ce qui serait observé si l'état supposé était réel. Dans le module 16, ce point doit être relu depuis la section « 7 — « Six pannes injectées ». Six pannes injectées »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Six pannes injectées », retirez une capacité utile et recalculez l'horizon de décision. Dans « Six pannes injectées », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Six pannes injectées » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie. Dans le module 16, ce point doit être relu depuis la section « 7 — « Six pannes injectées ». Six pannes injectées »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Six pannes injectées », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Six pannes injectées », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Six pannes injectées » demande donc un bilan des conséquences croisées avant d'accepter une optimisation. Dans le module 16, ce point doit être relu depuis la section « 7 — « Six pannes injectées ». Six pannes injectées »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

8. Retour et héritage

Le retour n'est autorisé que si véhicule, consommables, santé équipage et chaîne de communication restent compatibles. La campagne doit aussi laisser une base mieux connue: journaux, pièces qualifiées, paramètres de fonctionnement et anomalies documentées. Pour « Retour et héritage », dressez d'abord les interfaces: ressources, commandes, données et dépendances. La cartographie de « Retour et héritage » sert à révéler les dépendances et chemins de propagation de panne.

Pour retour et héritage, le corrigé impose un tableau séparant besoin, capacité, marge et unité. Pour « Retour et héritage », retranchez de la capacité nominale indisponibilités, réserves et contraintes de simultanéité. Dans « Retour et héritage », un nombre sans unité ou horizon temporel est incomplet. Pour « Retour et héritage », une estimation à un chiffre significatif précède le calcul précis.

Le jalon « Retour et héritage » exige une preuve annoncée: mesure, test, inventaire, inspection ou démonstration. Pour « Retour et héritage », une télémétrie unique ne suffit pas si un biais commun est plausible. Pour « Retour et héritage », cherchez une confirmation indépendante ou une cohérence physique avec une autre grandeur. Le corrigé « Retour et héritage » précise ce qui serait observé si l'état supposé était réel. Dans le module 16, ce point doit être relu depuis la section « 8 — « Retour et héritage ». Retour et héritage »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Retour et héritage », retirez une capacité utile et recalculez l'horizon de décision. Dans « Retour et héritage », préservez fonctions vitales et options réversibles plutôt que le plan initial à tout prix. Le mode dégradé de « Retour et héritage » chiffre charges supprimées, stocks, durée, réparation et seuil de changement de stratégie. Dans le module 16, ce point doit être relu depuis la section « 8 — « Retour et héritage ». Retour et héritage »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Pour « Retour et héritage », refusez une optimisation locale dont les effets sur les autres fonctions ne sont pas chiffrés. Dans « Retour et héritage », une économie de masse doit être comparée à ses coûts de maintenance, secours, énergie et thermique. Le corrigé « Retour et héritage » demande donc un bilan des conséquences croisées avant d'accepter une optimisation. Dans le module 16, ce point doit être relu depuis la section « 8 — « Retour et héritage ». Retour et héritage »: la preuve demandée doit rester cohérente avec l'objectif « Missions finales: construire une architecture Mars complète et résiliente » et avec les marges réellement disponibles dans ce scénario.

Tableau maître des budgets et preuves

Budget	Question à fermer	Preuve attendue	Mode dégradé à étudier
Masse livrée	Quel besoin de masse livrée est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de masse livrée.	Recalculer masse livrée après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Puissance de pointe	Quel besoin de puissance de pointe est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de puissance de pointe.	Recalculer puissance de pointe après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Énergie quotidienne	Quel besoin de énergie quotidienne est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de énergie quotidienne.	Recalculer énergie quotidienne après retrait d'une capacité et annoncer le temps avant franchissement du seuil.

Budget	Question à fermer	Preuve attendue	Mode dégradé à étudier
Eau nette	Quel besoin de eau nette est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de eau nette.	Recalculer eau nette après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Oxygène et gaz	Quel besoin de oxygène et gaz est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de oxygène et gaz.	Recalculer oxygène et gaz après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Nourriture	Quel besoin de nourriture est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de nourriture.	Recalculer nourriture après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Pièces critiques	Quel besoin de pièces critiques est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de pièces critiques.	Recalculer pièces critiques après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Temps humain	Quel besoin de temps humain est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de temps humain.	Recalculer temps humain après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Mobilité	Quel besoin de mobilité est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de mobilité.	Recalculer mobilité après retrait d'une capacité et annoncer le temps avant franchissement du seuil.
Communications	Quel besoin de communications est simultané au scénario défavorable et quelle marge reste après indisponibilité?	Tableau d'hypothèses, unité, mesure ou test qui permet de confirmer la capacité de communications.	Recalculer communications après retrait d'une capacité et annoncer le temps avant franchissement du seuil.

Chronologie de six événements injectés

T0: l'anomalie est détectée et consignée. T+1: caractérisez « retard logistique » avec au moins deux indices qui ne partagent pas la même source d'erreur. T+2: redistribuez les charges ou les tâches pour empêcher la propagation de l'incident. T+3: mettez à jour le tableau de ressources du module 16 avec la capacité réellement restante. T+4: confrontez ce nouvel état au seuil de sécurité et au temps nécessaire pour atteindre une solution stable. T+5: la configuration nominale n'est restaurée qu'après démonstration de la fonction et enregistrement du retour d'expérience.

Événement 2: perte partielle de production électrique. T0: l'anomalie est détectée et consignée. T+1: confirmez « perte partielle de production électrique » avec une donnée indépendante avant de modifier la configuration. T+2: isolez la fonction touchée par « perte partielle de production électrique » et conservez en priorité les fonctions vitales. T+3: recalculez l'autonomie disponible dans l'état créé par « perte partielle de production électrique ». T+4: comparez cette autonomie au seuil de décision défini dans missions finales: construire une architecture mars complète et résiliente. T+5: le retour au nominal n'est autorisé qu'après un essai montrant que la cause de « perte partielle de production électrique » est maîtrisée.

Événement 3: dérive d'un capteur de fonction vitale. T0: l'anomalie est détectée et consignée. T+1: pour « dérive d'un capteur de fonction vitale », cherchez d'abord une seconde mesure qui ne dépende pas du même capteur ou de la même chaîne. T+2: basculez vers la ressource ou la procédure de secours pertinente

au module 16. T+3: établissez le nouveau bilan de temps, de stock et de capacité après cette bascule. T+4: décidez à partir de la marge restante, pas à partir du désir de poursuivre le plan initial. T+5: documentez le test de récupération de « dérive d'un capteur de fonction vitale » avant de réarmer la fonction.

Événement 4: immobilisation d'un moyen de mobilité. T0: l'anomalie est détectée et consignée. T+1: qualifiez « immobilisation d'un moyen de mobilité » en séparant symptôme, mesure et cause supposée. T+2: réduisez immédiatement les activités qui aggraveraient cette anomalie dans missions finales: construire une architecture mars complète et résiliente. T+3: vérifiez quelles redondances restent réellement disponibles après l'incident. T+4: appliquez le critère d'abandon ou de poursuite associé à la ressource devenue limitante. T+5: réintégrez la fonction seulement lorsque le contrôle contradictoire ne reproduit plus « immobilisation d'un moyen de mobilité ».

Événement 5: indisponibilité temporaire d'une compétence clé. T0: l'anomalie est détectée et consignée. T+1: ouvrez une fiche d'anomalie pour « indisponibilité temporaire d'une compétence clé » et confirmez l'écart par une observation distincte. T+2: placez l'équipage et les équipements dans la configuration sûre prévue pour ce type d'écart. T+3: chiffrez la conséquence de l'incident sur la durée, la puissance, les consommables ou la mobilité concernés. T+4: si la marge calculée franchit le seuil du module 16, déclenchez le scénario dégradé sans attendre. T+5: fermez l'anomalie uniquement après essai, lecture stable et validation croisée.

Événement 6: perte d'une capacité de communication ou de coordination. T0: l'anomalie est détectée et consignée. T+1: face à « perte d'une capacité de communication ou de coordination », interrompez l'interprétation intuitive et recherchez une preuve qui pourrait la contredire. T+2: sécurisez la fonction la plus difficile à remplacer dans missions finales: construire une architecture mars complète et résiliente. T+3: projetez l'état dégradé jusqu'au prochain point où une ressource, un délai ou une capacité devient critique. T+4: choisissez l'action qui préserve cette marge critique, même si elle sacrifie un objectif secondaire. T+5: avant reprise, refaites la mesure qui avait révélé « perte d'une capacité de communication ou de coordination » et comparez-la à une référence saine.

Grille de soutenance du dossier

- Hypothèses: 15 points.
- Budgets et unités: 20 points.
- Interfaces: 15 points.
- Modes dégradés: 15 points.
- Preuves et vérification: 10 points.
- Chronologie et opérations: 10 points.
- Analyse de sensibilité: 10 points.
- Clarté et traçabilité: 5 points.

Dossier corrigé quantitatif de référence - scénario pédagogique complet

Tout ce dossier est un scénario pédagogique construit pour apprendre à fermer une architecture. Les valeurs numériques ci-dessous ne décrivent ni un plan NASA, ni un plan SpaceX, ni une mission certifiée. Elles sont volontairement simples, arrondies et traçables afin que le lecteur puisse refaire les calculs. Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai. L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques nombres isolés.

Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. On suppose que les cargos ont déjà démontré l'alimentation minimale, la communication, un volume pressurisable, une réserve de consommables et une capacité de mobilité. Le départ de l'équipage n'est autorisé que si ces

fonctions ont été testées. Le corrigé travaille ensuite avec un habitat principal, un refuge indépendant, deux rovers capables de se secourir mutuellement, une production électrique multi-source et des stocks permettant de passer temporairement en mode dégradé.

1. Registre initial des hypothèses

Grandeur	Symbole	Hypothèse pédagogique	Pourquoi elle est nécessaire
Équipage	N	6 personnes	Dimensionne consommables, temps humain et capacité de refuge
Durée surface	t_s	500 sols	Transforme un débit quotidien en stock de campagne
Durée d'un sol	t_sol	24,66 h	Permet de convertir puissance moyenne et énergie par sol
Appoint net d'eau	q_eau	1,2 kg/personne/sol	Représente les pertes nettes après récupération dans ce scénario
Appoint net O2	q_O2	0,9 kg/personne/sol	Hypothèse de calcul d'un stock net; à remplacer par une valeur mission sourcée
Nourriture sèche	q_food	0,75 kg/personne/sol	Simplification pédagogique pour un budget de masse
Puissance moyenne	P_moy	55 kW	Somme pédagogique des charges moyennes actives
Charge critique	P_crit	35 kW	Charge conservée en mode dégradé
Stockage batterie nominal	E_bat	900 kWh	Capacité nominale du scénario
Réserve batterie non planifiée	r_bat	20 %	Empêche de considérer 100 % du stockage comme librement consommable
Autonomie rover	R_rover	60 km	Distance totale utilisable dans le scénario avant recharge
Réserve mobilité	r_rover	25 %	Réserve conservée pour détour, terrain et secours

2. Fermer le budget d'eau avant de parler de confort

Combien d'eau d'appoint faut-il importer ou produire localement si la boucle récupère la majorité de l'eau mais laisse une perte nette de 1,2 kg par personne et par sol? Le mot important est « net »: on ne multiplie pas la consommation brute de douche, d'hygiène et de boisson comme si toute l'eau disparaissait. On budgète ici uniquement ce qui doit réellement être remplacé après récupération, plus des tampons pour les interruptions.

Inventaire d'eau équipage — convertir une demande quotidienne en masse de campagne

1 — Question concrète

Quelle masse d'eau brute correspond à un débit individuel, un effectif et une durée donnés ?

2 — Intuition sans symboles

Chaque personne consomme une quantité par sol ; on multiplie par le nombre de personnes puis par le nombre de sols couverts.

3 — Grandeurs

m_{eau} est la demande brute ; q_{eau} la demande par personne et par sol ; N l'effectif ; t_s la durée.

4 — Formule

$$m_{\text{eau}} = q_{\text{eau}} \times N \times t_s$$

5 — Lecture

La masse d'eau égale la demande par personne et par sol multipliée par l'effectif puis par la durée.

6 — Symboles et sens

Le débit individuel, l'effectif et la durée décrivent la même campagne ; m_{eau} est une masse brute avant crédits de recyclage.

7 — Prononciation

m eau égale q eau fois enne fois té sols.

8 — Unités

$$\text{kg}/(\text{personne} \cdot \text{sol}) \times \text{personne} \times \text{sol} = \text{kg}.$$

9 — Convention

Fermer d'abord la demande brute ; récupération, pertes, stock inaccessible et réserve protégée sont des couches distinctes du budget boucle fermée.

10 — Pourquoi cette opération

L'effectif transforme la demande individuelle en demande équipage ; la durée cumule cette demande.

11 — Hypothèses

Le débit individuel est représentatif et la frontière de consommation reste la même pendant l'intervalle.

12 — Contrôle d'unités

Personnes et sols s'annulent, laissant des kilogrammes.

13 — Cas numérique

$3,2 \text{ kg}/(\text{personne} \cdot \text{sol}) \times 6 \text{ personnes} \times 30 \text{ sols} = 576 \text{ kg}$.

14 — Pourquoi le calcul fonctionne

La demande quotidienne équipage vaut 19,2 kg ; sur 30 sols, elle devient 576 kg.

15 — Contrôle algébrique

$t_s = m_{\text{eau}}/(q_{\text{eau}} \times N)$ si les autres grandeurs restent constantes.

16 — Estimation mentale

Environ 20 kg/sol pendant 30 sols donnent environ 600 kg ; 576 kg est cohérent.

17 — Interprétation

La demande brute de ce cas vaut 576 kg avant récupération et contingence.

18 — Ce que le résultat ne prouve pas

Elle ne donne pas la masse à importer ou produire : efficacité de récupération, fuites, accessibilité, qualité et besoins de procédé peuvent changer le make-up.

19 — Sensibilité

Chaque personne ou sol supplémentaire augmente linéairement la demande brute à débit individuel fixé.

20 — Exercices guidé et autonome

Exercice guidé. 2,8 kg/(personne·sol), 5 personnes, 40 sols. Calculer la demande brute.

Correction guidée

$2,8 \times 5 \times 40 = 560 \text{ kg}$.

Exercice autonome. Un stock brut de 720 kg doit couvrir 6 personnes pendant 50 sols. Quel débit individuel moyen maximal cela représente-t-il ?

Correction autonome

$720/(6 \times 50) = 2,4 \text{ kg}/(\text{personne} \cdot \text{sol})$.

21 — Décision mission

Fermer la demande brute puis appliquer séparément récupération, pertes et réserve afin que le make-up reste traçable.

$m_{\text{eau}} = 1,2 \times 6 \times 500 = 3\,600 \text{ kg}$. Le contrôle d'unité est direct: $\text{kg/personne/sol} \times \text{personnes} \times \text{sols} = \text{kg}$. Un ordre de grandeur mental donne environ $1 \times 6 \times 500 = 3\,000 \text{ kg}$; obtenir 36 000 kg ou 360 kg signifierait immédiatement une erreur de facteur dix.

Un tampon de 30 sols au même débit net vaut $1,2 \times 6 \times 30 = 216 \text{ kg}$. Dans le dossier de mission, ce tampon ne doit pas être confondu avec les 3 600 kg de besoin de campagne. Le besoin de campagne répond à « combien faut-il remplacer sur 500 sols? »; le tampon répond à « combien faut-il pouvoir mobiliser sans production nouvelle pendant une interruption définie? Ce sont deux questions différentes, et les additionner ou les comparer sans préciser le rôle du stock crée de faux raisonnements.

Si la production locale ou la récupération ne peut pas maintenir l'appoint net annoncé, la décision n'est pas immédiatement l'évacuation. On mesure d'abord la nouvelle perte nette, on recalcule le nombre de sols couverts par le stock mobilisable, puis on réduit les usages non vitaux et on répare. Le GO/HOLD dépend donc d'un horizon mesuré, pas d'une impression générale que « l'eau fonctionne encore ».

3. Oxygène et gaz: distinguer débit, stock et réserve d'urgence

Application — inventaire d'oxygène et horizon

La masse d'oxygène de campagne est un sous-calcul d'inventaire. Le pilotage mission se fait avec la mini-leçon canonique d'horizon O_2 , qui relie stock accessible, effectif et consommation jusqu'à une décision temporelle. Voir la mini-leçon canonique.

$m_{O_2} = 0,9 \times 6 \times 500 = 2\,700 \text{ kg}$ pour le scénario si cette valeur représentait réellement l'appoint net à fournir pendant toute la campagne. La valeur est volontairement pédagogique: elle sert à montrer la chaîne de calcul. Une étude réelle distinguerait consommation métabolique, récupération éventuelle, production, pertes de gaz, pressurisation, EVA, purge, réserve incendie et réserve de refuge.

Si la capacité principale de production est indisponible pendant trois sols et que la demande nette de scénario reste 0,9 kg/personne/sol, le stock de secours consommé est $0,9 \times 6 \times 3 = 16,2 \text{ kg}$. Si le refuge possède 45 kg de réserve utilisable consacrée à cette fonction, la marge arithmétique après trois sols est 28,8 kg. Mais le corrigé refuse d'appeler ces 28,8 kg une « marge de mission » tant que les autres usages du même stock ne sont pas vérifiés.

Le piège consiste à utiliser une masse d'oxygène comme si elle suffisait à décrire l'atmosphère habitable. La pression totale, les gaz tampons, le CO_2 , l'humidité, les contaminants et la capacité de circulation restent des contraintes séparées. Une réserve d' O_2 disponible n'est donc pas une preuve que l'habitat entier est exploitable.

4. Nourriture: un budget simple qui révèle immédiatement la masse logistique

Application — inventaire nourriture et horizon

Le cumul de nourriture sur la campagne reste utile comme vérification logistique, mais il est rattaché à la mini-leçon canonique d'horizon alimentaire afin que stock courant, réserve protégée et temps avant seuil soient traités dans un seul contrat pédagogique. Voir la mini-leçon canonique.

$m_{\text{food}} = 0,75 \times 6 \times 500 = 2\,250 \text{ kg}$. Ce chiffre ne couvre ici que la masse alimentaire sèche choisie pour l'exercice. Les emballages, pertes, diversité nutritionnelle, réserves supplémentaires, eau de préparation et logistique de stockage ne sont pas inclus. Le but est de montrer qu'un débit quotidien qui paraît petit devient plusieurs tonnes lorsqu'il est intégré sur 500 sols.

Si la durée augmente de 10 %, le besoin passe à 2 475 kg. Si, au contraire, une production locale remplace 20 % de la masse sèche après une phase de montée en puissance vérifiée, le besoin importé théorique devient 1 800 kg, mais ce gain ne peut être compté que si l'agriculture dispose déjà de son eau, de son énergie, de ses nutriments, de sa main-d'œuvre et de sa capacité de secours. Une économie de cargo qui crée quatre nouvelles dépendances non fermées n'est pas automatiquement un progrès.

5. Puissance et énergie: pourquoi 55 kW ne signifie pas 55 kWh

Énergie par sol martien — convertir puissance moyenne en énergie cumulée

1 — Question concrète

Quelle énergie correspond à une puissance moyenne maintenue pendant un sol martien complet ?

2 — Intuition sans symboles

La puissance est un débit d'énergie. La maintenir pendant toute la durée d'un sol accumule une énergie proportionnelle à cette durée.

3 — Grandeurs

E_{sol} est l'énergie d'un sol ; P_{moy} la puissance moyenne ; t_{sol} la durée du sol.

4 — Formule

$$E_{\text{sol}} = P_{\text{moy}} \times t_{\text{sol}}$$

5 — Lecture

L'énergie par sol égale la puissance moyenne multipliée par la durée du sol.

6 — Symboles et sens

P_{moy} doit représenter l'intervalle entier considéré ; t_{sol} est exprimé dans l'unité temporelle compatible.

7 — Prononciation

E sol égale P moyenne fois té sol.

8 — Unités

$$\text{kW} \times \text{h} = \text{kWh}.$$

9 — Convention

Pour un sol martien complet, utiliser environ 24,6597 h ; une charge intermittente doit être décrite par son propre profil et non cachée dans une moyenne mal définie.

10 — Pourquoi cette opération

Multiplier un débit d'énergie par le temps donne la quantité cumulée.

11 — Hypothèses

La puissance moyenne représente réellement l'intervalle et n'efface pas un régime opérationnel différent.

12 — Contrôle d'unités

Kilowatt multiplié par heure donne kilowattheure.

13 — Cas numérique

$5,0 \text{ kW} \times 24,6597 \text{ h} \approx 123,3 \text{ kWh}$ par sol.

14 — Pourquoi le calcul fonctionne

Chaque heure ajoute environ 5 kWh ; un peu moins de 25 h donne donc un peu moins de 125 kWh.

15 — Contrôle algébrique

$P_{\text{moy}} = E_{\text{sol}}/t_{\text{sol}}$.

16 — Estimation mentale

$5 \times 25 \approx 125 \text{ kWh}$, très proche de 123,3.

17 — Interprétation

Une charge moyenne continue de 5 kW représente environ 123,3 kWh par sol martien.

18 — Ce que le résultat ne prouve pas

L'énergie par sol ne révèle ni puissance de pointe, ni rampes, ni séquence charge/décharge, ni capacité d'onduleur.

19 — Sensibilité

À durée fixe, doubler la puissance moyenne double directement l'énergie par sol.

20 — Exercices guidé et autonome

Exercice guidé. Une charge moyenne de 8 kW fonctionne sur un sol complet. Calculer l'énergie.

Correction guidée

$$8 \times 24,6597 \approx 197,3 \text{ kWh/sol.}$$

Exercice autonome. Le budget énergétique autorise 246,6 kWh/sol pour une charge continue. Quelle puissance moyenne correspondante ?

Correction autonome

$$246,6/24,6597 \approx 10,0 \text{ kW.}$$

21 — Décision mission

Utiliser l'énergie par sol pour génération et stockage, avec un gate séparé pour puissance de pointe et transitoires.

$E_{\text{sol}} = 55 \times 24,66 = 1\,356,3 \text{ kWh}$ par sol, soit environ 1,36 MWh/sol. Le contrôle d'unité montre $\text{kW} \times \text{h} = \text{kWh}$. La puissance décrit un débit instantané d'énergie; l'énergie est l'accumulation de ce débit dans le temps. Confondre les deux conduit à des batteries, des câbles ou des sources totalement mal dimensionnés.

Avec 900 kWh nominaux et une réserve de 20 % non planifiée, on n'autorise que $900 \times 0,80 = 720 \text{ kWh}$ dans le scénario de secours. À 35 kW de charge critique constante, l'autonomie théorique est $720 / 35 = 20,57 \text{ h}$, soit environ 0,83 sol. Cela signifie qu'une architecture qui prétend « tenir un sol entier sur batterie » ne ferme pas ce besoin avec ces hypothèses. Soit il faut réduire la charge critique, augmenter le stockage, accepter une autre source de secours ou raccourcir le temps de transition.

Une perte totale de la source principale pendant 18 h consomme $35 \times 18 = 630 \text{ kWh}$ si la charge critique reste stable. Sur les 720 kWh autorisés, il reste 90 kWh, soit seulement 2,57 h de charge critique supplémentaire. Le verdict n'est donc pas « batterie suffisante » mais « batterie suffisante pour 18 h avec une marge temporelle d'environ 2,6 h dans ce scénario ». Cette formulation est beaucoup plus utile pour une règle GO/HOLD.

6. Mobilité de secours: transformer une autonomie commerciale en rayon opérationnel

Rayon de secours protégé — conserver le trajet retour avant de quitter l'habitat

1 — Question concrète

Quel rayon aller-retour simple peut être autorisé à partir d'une autonomie nominale et d'une réserve protégée ?

2 — Intuition sans symboles

Un rover de secours doit pouvoir aller jusqu'à la cible puis revenir. On protège d'abord une partie de l'autonomie annoncée, puis on partage le reste entre aller et retour.

3 — Grandeurs

R_sûr est le rayon planifié ; R_nom l'autonomie nominale ; f_utilisable la fraction autorisée après réserve.

4 — Formule

$$R_sûr = (R_nom \times f_utilisable) / 2$$

5 — Lecture

Le rayon sûr égale l'autonomie nominale multipliée par la fraction utilisable, puis divisée par deux.

6 — Symboles et sens

R_nom est une distance totale ; f_utilisable est sans dimension ; R_sûr est une distance aller simple.

7 — Prononciation

R sûr égale R nominal fois effe utilisable, divisé par deux.

8 — Unités

$$\text{km} \times \text{sans dimension} \div 2 = \text{km}.$$

9 — Convention

La géométrie est symétrique aller-retour. Terrain, détour, froid batterie, remorquage et charge de secours doivent réduire encore le rayon si nécessaire.

10 — Pourquoi cette opération

La réserve réduit la distance totale utilisable ; la division par deux protège un trajet aller et un trajet retour.

11 — Hypothèses

Même autonomie effective dans les deux sens, pas de recharge, pas de refuge alternatif et pas de pénalité terrain/météo dans ce modèle de premier ordre.

12 — Contrôle d'unités

La fraction ne change pas l'unité de distance et la division par deux conserve des kilomètres.

13 — Cas numérique

R_nom = 60 km et réserve 25 % donnent f_utilisable = 0,75 ; distance utilisable = 45 km ; R_sûr = 22,5 km.

14 — Pourquoi le calcul fonctionne

On protège 15 km sur les 60, puis on partage les 45 km restants entre les deux branches.

15 — Contrôle algébrique

Pour une cible à distance d , il faut au moins $R_{\text{nom}} \geq 2d/f_{\text{utilisable}}$ avant les pénalités supplémentaires.

16 — Estimation mentale

Trois quarts de 60 donnent 45 ; la moitié vaut 22,5.

17 — Interprétation

22,5 km est le rayon symétrique maximal du cas simplifié avant pénalités.

18 — Ce que le résultat ne prouve pas

Le résultat ne certifie ni route praticable, ni batterie chaude, ni remorquage, ni communications, ni disponibilité d'un refuge.

19 — Sensibilité

Augmenter la réserve réduit le rayon ; une route asymétrique ou un refuge à sens unique exige une géométrie différente.

20 — Exercices guidé et autonome

Exercice guidé. Autonomie nominale 80 km, réserve 30 %. Calculer le rayon simple.

Correction guidée

Fraction utilisable 0,70 ; distance utilisable 56 km ; rayon = 28 km.

Exercice autonome. Une victime est à 24 km. Le rover a 70 km nominaux, réserve 20 %, et le terrain ajoute 15 % à chaque branche. Le cas ferme-t-il proprement ?

Correction autonome

Distance utilisable = 56 km. Aller-retour terrain = $2 \times 24 \times 1,15 = 55,2$ km : seulement 0,8 km reste avant effets froid/remorquage. Verdict HOLD sans marge supplémentaire.

21 — Décision mission

Traiter le rayon comme gate de préservation d'option : si terrain et incertitude consomment la marge, réduire l'enveloppe ou ajouter une autre voie de secours.

$R_{\text{sûr}} = 60 \times 0,75 / 2 = 22,5$ km. La division par deux rappelle qu'un véhicule doit revenir ou qu'un véhicule de secours doit pouvoir effectuer un aller-retour; la réserve de 25 % absorbe détour, terrain, température, recherche ou dégradation. Un site scientifique à 18 km est donc dans l'enveloppe de ce modèle, mais il ne reste que 4,5 km de marge géométrique avant le seuil. Le terrain réel peut réduire cette marge bien avant le kilométrage théorique.

Si un rover s'immobilise à 18 km de la base, la décision de secours ne consiste pas à envoyer immédiatement le second rover. On confirme position, état de l'équipage, énergie et durée de survie du véhicule immobilisé; on vérifie météo et communications; on calcule la distance totale du véhicule de secours; on conserve sa propre réserve; puis on choisit entre dépannage, transfert d'équipage, attente ou abandon du matériel. Le but du rayon sûr est précisément de maintenir plusieurs options.

7. Temps humain: la ressource que les budgets de masse oublient

Application — capacité humaine disponible

Les personnes-heures disponibles constituent le dénominateur de la charge de maintenance. Ce passage devient un calcul d'application de la mini-leçon canonique d'utilisation maintenance, qui porte le ratio, les limites de compétence et la décision de marge. Voir la mini-leçon canonique.

$H_{dispo} = 6 \times 8 = 48$ heures-personnes par sol dans le scénario. Une réserve de 20 % pour anomalies, coordination, documentation et récupération représente 9,6 heures-personnes; il ne reste donc que 38,4 heures-personnes à planifier comme charge normale. Ce budget interdit de programmer simultanément maintenance lourde, grande EVA scientifique, inventaire cargo et exercice d'urgence comme si le temps humain était gratuit.

Lorsqu'une panne consomme 15 heures-personnes imprévues, le retard ne se mesure pas seulement en heures. Les tâches reportées peuvent elles-mêmes créer une dette: filtre non changé, échantillon non traité, pièce non inspectée ou sommeil réduit. Le corrigé demande donc de noter le travail reporté et le risque qu'il crée au lieu de simplement « rattraper plus tard ».

8. Tableau de fermeture des budgets

Budget	Besoin nominal du scénario	Réserve ou limite	Question de fermeture
Eau d'appoint	7,2 kg/sol pour 6 personnes	216 kg = 30 sols au débit net	Le stock est-il indépendant de la boucle en panne?
O2 net	5,4 kg/sol	16,2 kg pour 3 sols; exemple de réserve 45 kg	Le même stock sert-il à pressurisation ou EVA?
Nourriture sèche	4,5 kg/sol	2 250 kg sur 500 sols hors emballage	Quel stock reste après retard de mission?
Énergie moyenne	1 356,3 kWh/sol	720 kWh batterie planifiable	Quelle source prend le relais avant 20,6 h à 35 kW?
Charge critique	35 kW	630 kWh pour 18 h	Quelles charges sont réellement dans les 35 kW?
Mobilité	Rayon sûr 22,5 km	25 % de réserve kilométrique	Le terrain et la météo réduisent-ils ce rayon?
Temps humain	48 h-personnes/sol brutes	9,6 h-personnes de réserve	Quelles tâches sont abandonnées pendant une anomalie?

9. Six pannes injectées - corrigé chronologique

Panne 1 - Perte de la source principale pendant 18 h. T0: confirmer que la perte est réelle et isoler les charges non essentielles. T+15 min: passer à 35 kW critiques. Le besoin de 18 h vaut 630 kWh; le stockage planifiable vaut 720 kWh; la marge est 90 kWh, soit environ 2,6 h. HOLD sur les activités non vitales. NO-GO sur toute action qui pourrait prolonger l'indisponibilité au-delà de cette marge sans source alternative.

Panne 2 - Dégradation de la récupération d'eau pendant 10 sols. L'appoint net passe pédagogiquement de 1,2 à 4,0 kg/personne/sol. L'excès par rapport au nominal est $(4,0-1,2) \times 6 \times 10 = 168$ kg. On retire 168 kg du stock libre ou on compense par production. La règle opérationnelle doit annoncer le seuil de stock qui force l'arrêt d'usages non vitaux.

Données du cas

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence — Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Relation

L'appoint net passe pédagogiquement de 1,2 à 4,0 kg/personne/sol.

Raisonnement

Panne 2 - Dégradation de la récupération d'eau pendant 10 sols. L'appoint net passe pédagogiquement de 1,2 à 4,0 kg/personne/sol. L'excès par rapport au nominal est $(4,0-1,2) \times 6 \times 10 = 168$ kg. On retire 168 kg du stock libre ou on compense par production. La règle opérationnelle doit annoncer le seuil de stock qui force l'arrêt d'usages non vitaux.

Résultat

Panne 2 - Dégradation de la récupération d'eau pendant 10 sols.

Contrôle

La règle opérationnelle doit annoncer le seuil de stock qui force l'arrêt d'usages non vitaux.

Interprétation

On retire 168 kg du stock libre ou on compense par production.

Panne 3 - Production principale d'O2 indisponible trois sols. La demande nette du scénario est 16,2 kg. Une réserve de 45 kg laisse 28,8 kg après trois sols si aucun autre usage ne la consomme. Le corrigé exige une vérification indépendante de l'atmosphère et du CO2: posséder assez d'O2 ne prouve pas que l'air est sain.

Données du cas

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence — Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Relation

Le corrigé exige une vérification indépendante de l'atmosphère et du CO2: posséder assez d'O2 ne prouve pas que l'air est sain.

Raisonnement

Panne 3 - Production principale d'O2 indisponible trois sols. La demande nette du scénario est 16,2 kg. Une réserve de 45 kg laisse 28,8 kg après trois sols si aucun autre usage ne la consomme. Le corrigé exige une vérification indépendante de l'atmosphère et du CO2: posséder assez d'O2 ne prouve pas que l'air est sain.

Résultat

Panne 3 - Production principale d'O2 indisponible trois sols.

Interprétation

Une réserve de 45 kg laisse 28,8 kg après trois sols si aucun autre usage ne la consomme.

Panne 4 - Rover immobilisé à 18 km. Le rayon sûr calculé est 22,5 km. Le secours est géométriquement possible dans le modèle, mais la marge n'est que 4,5 km. On vérifie énergie réelle, trajet, météo, équipage et capacité du deuxième rover avant départ. Si un détour crédible dépasse la marge, HOLD puis stratégie alternative.

Données du cas

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence — Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Raisonnement

Panne 4 - Rover immobilisé à 18 km. Le rayon sûr calculé est 22,5 km. Le secours est géométriquement possible dans le modèle, mais la marge n'est que 4,5 km. On vérifie énergie réelle, trajet, météo, équipage et capacité du deuxième rover avant départ. Si un détour crédible dépasse la marge, HOLD puis stratégie alternative.

Résultat

Panne 4 - Rover immobilisé à 18 km.

Contrôle

Le secours est géométriquement possible dans le modèle, mais la marge n'est que 4,5 km.

Interprétation

Si un détour crédible dépasse la marge, HOLD puis stratégie alternative.

Panne 5 - Perte des communications haut débit pendant 48 h. La mission doit continuer avec procédures asynchrones et autonomie locale. Les fonctions vitales ne doivent pas dépendre d'une décision terrestre en temps réel. On conserve les journaux, on compresse les données essentielles et on définit quels événements exigent seulement notification versus autorisation préalable.

Données du cas

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence — Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Raisonnement

Panne 5 - Perte des communications haut débit pendant 48 h. La mission doit continuer avec procédures asynchrones et autonomie locale. Les fonctions vitales ne doivent pas dépendre d'une décision terrestre en temps réel. On conserve les journaux, on compresse les données essentielles et on définit quels événements exigent seulement notification versus autorisation préalable.

Résultat

Panne 5 - Perte des communications haut débit pendant 48 h.

Contrôle

On conserve les journaux, on compresse les données essentielles et on définit quels événements exigent seulement notification versus autorisation préalable.

Interprétation

Les fonctions vitales ne doivent pas dépendre d'une décision terrestre en temps réel.

Panne 6 - Isolement d'un tiers du volume habitable. L'événement ne détruit pas nécessairement le support-vie, mais il augmente densité humaine, charge sur les autres compartiments, bruit, circulation et contraintes de sommeil. On vérifie que le refuge, les couchages et les fonctions vitales restantes peuvent accueillir six personnes avant de déclarer le mode dégradé soutenable.

Données du cas

Exercice guidé — Oxygène et gaz: distinguer débit, stock et réserve d'urgence — Cas « Oxygène et gaz: distinguer débit, stock et réserve d'urgence » — Six personnes effectuent une campagne de surface de 500 sols après deux cargos précurseurs. Repère: L'objectif est de comprendre la méthode de fermeture des budgets et des marges, pas de donner l'illusion qu'une mission humaine vers Mars peut être validée par quelques... Réserve: Dans une étude réelle, chaque hypothèse devrait être remplacée par une donnée de conception sourcée, une exigence approuvée ou une mesure d'essai.

Raisonnement

Panne 6 - Isolement d'un tiers du volume habitable. L'événement ne détruit pas nécessairement le support-vie, mais il augmente densité humaine, charge sur les autres compartiments, bruit, circulation et contraintes de sommeil. On vérifie que le refuge, les couchages et les fonctions vitales restantes peuvent accueillir six personnes avant de déclarer le mode dégradé soutenable.

Résultat

Panne 6 - Isolement d'un tiers du volume habitable.

Contrôle

On vérifie que le refuge, les couchages et les fonctions vitales restantes peuvent accueillir six personnes avant de déclarer le mode dégradé soutenable.

Interprétation

L'événement ne détruit pas nécessairement le support-vie, mais il augmente densité humaine, charge sur les autres compartiments, bruit, circulation et contraintes de sommeil.

10. Matrice GO / HOLD / NO-GO

État	Signification	Exemple de critère dans ce scénario
GO	La fonction et sa marge sont démontrées; la prochaine phase peut commencer	Énergie critique disponible avec source ou stockage démontrant l'horizon exigé
HOLD	La mission reste sûre mais une incertitude ou une marge insuffisante interdit l'étape suivante	Stock d'eau encore suffisant mais perte nette non stabilisée après anomalie
NO-GO	Une fonction vitale, un secours ou une marge minimale n'est plus démontré	Aucune source électrique capable d'éviter l'épuisement avant réparation plausible
RETURN / SAFE MODE	On abandonne l'objectif nominal pour protéger l'équipage et conserver les options réversibles	Annulation EVA, refuge, rationnement, report science, préparation retour selon phase

Un étudiant ne reçoit pas les points parce qu'il choisit le même nombre que ce corrigé. Il les reçoit s'il annonce ses hypothèses, définit les unités, ferme ses budgets, montre les interfaces et prend une décision cohérente avec les marges qu'il a lui-même calculées. Une variante avec 45 kW critiques, 1 200 kWh de batterie ou une autre stratégie d'eau peut être meilleure ou pire; elle doit simplement démontrer sa cohérence avec les autres sous-systèmes.

Mini-projet intégrateur et dossier de référence

Produire le dossier solution d'une mission de six personnes sur 500 sols avec deux cargos précurseurs. Le dossier doit relier chronologie, budgets, interfaces, six pannes injectées, reconfiguration et critères de départ, d'atterrissage et de prolongation de campagne.

« Exercice 12: Trade-off final entre deux architectures » — hypothèses, budget, marges.

« Exercice 12: Trade-off final entre deux architectures » — interfaces et causes communes.

« Exercice 12: Trade-off final entre deux architectures » — calculs, limites, critères.

Verification de maîtrise du module 16

- « Exercice 12: Trade-off final entre deux architectures » — unités et ordre de grandeur.
- « Exercice 12: Trade-off final entre deux architectures » — cas dégradé.
- « Exercice 12: Trade-off final entre deux architectures » — marge décisionnelle.
- « Exercice 12: Trade-off final entre deux architectures » — mesure de contrôle.

Repères du passage: contrôle

Repères du passage: puissance

Repères du passage: exigence

Repères du passage: délestage

Repères du passage: humidité

Repères du passage: unité

Repères du passage: débit

Repères du passage: flux

Repères du passage: pressurisation

Repères du passage: masses

Repères du passage: contrôle thermique

Repères du passage: ingénierie système

Repères du passage: MTBF

Repères du passage: contamination

Repères du passage: redondance

Repères du passage: récupération

Repères du passage: bande passante

Repères du passage: maintenabilité

Repères du passage: disponibilité

Repères du passage: télémétrie

Repères du passage: optimisation

Repères du passage: sol martien

Repères du passage: phase

Repères du passage: ellipse

Repères du passage: chronologie

Repères du passage: NASA

Repères du passage: marge de mission

Sources et passerelles

- NASA — Human Spaceflight
- NASA — Space Technology Mission Directorate
- ESA — Human and Robotic Exploration
- Bible Mars — Transport Terre-Mars
- Bible Mars — ECLSS et habitat
- Bible Mars — Fiabilité et causes communes

Qualification d'ingénierie système — exigences, interfaces, V&V et preuve sur 500 sols

R76 apporte à la version française le dossier d'ingénierie système déjà présent en anglais. Une architecture martienne n'est pas fermée parce que ses sous-systèmes ont chacun un beau dossier : les exigences, interfaces, marges, risques, configurations, essais et procédures doivent raconter la même mission et la même version du système.

Exigences

Chaque exigence doit être nécessaire, mesurable, traçable vers un besoin de mission et associée à une méthode de vérification crédible.

Interfaces

Les échanges de puissance, chaleur, données, fluides, masse, temps et autorité entre sous-systèmes sont des objets d'ingénierie à part entière.

Vérification

La vérification demande si le système a été construit conformément aux exigences. Elle s'appuie sur analyse, inspection, démonstration ou essai avec critères explicites.

Validation

La validation demande si le système répond réellement au besoin opérationnel dans son contexte d'emploi, y compris avec équipage et scénarios dégradés.

1. La traçabilité part du besoin de mission et se termine par une preuve

Une exigence utile possède un parent, un propriétaire, une justification, une méthode de vérification et un état. Une phrase vague comme « le système doit être fiable » ne suffit pas. Il faut exprimer la fonction protégée, les conditions, le seuil attendu et la preuve qui permettra de dire PASS ou FAIL. La chaîne descend ensuite vers l'architecture et remonte vers les résultats d'essai.

2. Une matrice de vérification empêche « nous l'avons testé » de devenir une formule vide

La matrice relie chaque exigence à la méthode, au niveau d'essai, au moyen nécessaire, au critère d'acceptation, au responsable et au résultat. Elle expose immédiatement les exigences sans preuve, les tests qui ne couvrent aucune exigence et les dépendances à un moyen d'essai indisponible sur Mars.

3. Vérification et validation répondent à deux questions différentes

Un composant peut être parfaitement conforme à sa spécification et pourtant ne pas résoudre le problème opérationnel. La vérification demande « avons-nous construit correctement ? » ; la validation demande « avons-nous construit la bonne capacité pour l'usage réel ? ». Une boucle de support-vie vérifiée au banc doit encore être validée dans un scénario d'équipage, de maintenance, de bruit, de poussière et de panne réaliste.

4. Le contrôle d'interface est l'endroit où l'optimisme local rencontre la réalité du système

Un habitat, une centrale, un rover ou une unité ISRU peuvent chacun respecter leur propre budget et devenir incompatibles une fois connectés. Le registre d'interfaces doit porter unités, plages, tolérances, états dégradés, sens de responsabilité et configuration. Les interfaces logicielles et procédurales sont aussi critiques que les raccords physiques.

5. Les marges sont des réserves gérées, pas des pourcentages décoratifs

Masse, énergie, débit, stockage, volume, temps équipage et performance possèdent une valeur courante, une limite et une marge. Une marge empruntée pour sauver un sous-système ne peut pas disparaître du registre ; elle devient une décision de programme avec propriétaire et date de récupération prévue.

6. Les indicateurs de performance technique doivent révéler la tendance avant le dépassement

Attendre qu'une limite soit franchie est trop tard. Les paramètres critiques doivent être suivis avec tendance, incertitude et seuils d'action. Une capacité de récupération d'eau qui décline lentement, une dette maintenance qui croît ou une autonomie batterie qui se contracte sont des signaux de décision avant panne.

7. Qualification, acceptation et certification ne sont pas synonymes

La qualification démontre qu'un design représentatif supporte les environnements et marges prévus ; l'acceptation vérifie qu'un exemplaire livré est apte à l'emploi selon le plan défini ; la certification est une décision d'autorité dépendant du domaine et du cadre applicable. Les preuves doivent toujours être rattachées à la configuration qu'elles couvrent.

8. Les thread tests de bout en bout révèlent ce que les tests composants ne peuvent pas voir

1. **Perte communications.** Couper le lien Terre et vérifier horloge, état, autorité locale, procédures, file d'événements et reconnexion.

2. **Fuite cabine.** Injecter une indication, localiser, isoler, compter l'oxygène, basculer vers refuge et capturer la nouvelle configuration.
3. **Déficit énergétique.** Retirer une source majeure et vérifier délestage automatique, priorités manuelles, endurance batterie, thermique et séquence de reprise.
4. **Sauvetage rover.** Immobiliser un véhicule près du rayon protégé et suivre position, communications, consommables, véhicule secours, itinéraire et marge retour.
5. **Pièce critique.** Faire échouer un équipement remplaçable et démontrer diagnostic, accès, outillage, identité de pièce, configuration et retour en service.
6. **Relève équipage.** Donner le package libéré à une nouvelle équipe et lui demander de reproduire configuration, marges protégées, waivers, états dégradés et prochains gates sans mémoire orale.

9. Le change control évite qu'une réparation locale devienne la panne commune de demain

Tout changement accepté identifie les exigences, interfaces, dangers, procédures, modèles et preuves qu'il peut invalider. Une réparation locale, une mise à jour logicielle ou une pièce fabriquée sur Mars peut être urgente ; elle doit néanmoins laisser derrière elle une configuration exacte, un plan de retest et un chemin de rollback.

10. Un registre de risques expose les dépendances et les preuves

Deux redondances partageant le même logiciel, le même fluide, le même refroidissement ou la même erreur humaine ne sont pas indépendantes. Le registre doit associer cause, événement, conséquence, fonction protégée, mitigation, propriétaire et preuve. Une couleur verte obtenue par discussion ne retire pas un risque.

11. Campagne intégrée de vérification sur 500 sols

Gate	Condition injectée	Preuve exigée	Décision protégée
A — avant départ	un sous-système critique ne possède que la marge minimale acceptée	tendance, waiver, spare/recovery et absence d'emprunt caché	lancer, retarder ou dé-scoper
B — transit	perte communications pendant maintenance	horizon autonomie, autorité, procédures et réserves	continuer, différer ou passer en safe
C — premiers 30 sols	production énergie 18 % sous le plan	ledger énergie, thermique, cycles batterie et délestage	réduire charges ou consommer réserve
D — milieu campagne	panne récupération eau consommant l'unique spare	nouvel horizon eau, réparation et exposition à la panne suivante	nominal ou conservation
E — sauvetage	rover immobilisé près du rayon protégé avec communications dégradées	position, consommables, énergie secours, route et environnement	dispatch, shelter ou autre tactique
F — relève Sol 500	deux états dégradés acceptés doivent être transmis	baseline configuration, risques, waivers, marges, spares et anomalies	accepter ou refuser la relève

12. Dossier final — les artefacts doivent raconter la même architecture

La soutenance n'est close que si objectifs, arbre d'exigences, registre d'interfaces, budgets masse/énergie/thermique/données/consommables, risques et dangers, indicateurs de marge, matrice V&V, configuration, preuves de qualification/acceptation, concept opérations, logistique et dossier de relève sont cohérents entre eux. Toute contradiction est une finding, même lorsque chaque document est élégant pris séparément.

Passerelles d'ingénierie système

Ce dossier s'appuie sur la logique du NASA Systems Engineering Handbook : exigences traçables, interfaces contrôlées, vérification et validation distinctes, configuration maîtrisée et preuves liées à la version réelle du système.

Règle R76. La mission n'est pas « intégrée » tant que exigences, interfaces, marges, risques, V&V, configuration et opérations ne pointent pas vers la même architecture libérée.

Mission assurance et commandement intégré — protéger les options pendant 500 sols

Une mission longue n'est pas une collection de journées nominales. Le système doit rester gouvernable lorsque plusieurs fonctions se dégradent ensemble, lorsque les communications avec la Terre disparaissent temporairement, lorsque les réparations consomment les dernières pièces disponibles et lorsque l'équipage doit choisir entre restaurer une fonction aujourd'hui ou préserver le retour dans plusieurs mois. Cette partie aligne la version française sur les raisonnements d'intégration déjà exigés en anglais.

1. Séparer quatre horizons : survie, stabilisation, récupération et retour

Les équipes commettent facilement l'erreur d'utiliser un seul mot — autonomie — pour des réalités très différentes. L'horizon de survie répond à la question « combien de temps avant la perte d'une fonction vitale ? ». L'horizon de stabilisation demande combien de temps est disponible pour arrêter l'aggravation. L'horizon de récupération demande quand une capacité durable peut être restaurée. L'horizon de retour protège une option de départ ou de secours qui peut rester critique même si la base fonctionne encore.

Un même événement peut donc produire quatre horloges différentes. Une panne de traitement d'eau peut laisser plusieurs jours de réserve potable, quelques heures avant qu'un réservoir ne déborde ou qu'un autre système ne doive être arrêté, plusieurs sols avant qu'un spare puisse être installé, et des mois avant que l'impact sur le stock de retour ne devienne irréversible. Le commandement doit afficher ces horloges séparément.

2. Les dépendances transversales méritent leur propre registre

Les architectures sont souvent dessinées par métiers : énergie, ECLSS, communications, mobilité, médical, informatique. Les incidents réels traversent ces frontières. Une perte de puissance peut arrêter une pompe, dégrader le contrôle thermique, limiter les communications et immobiliser un outil de maintenance. Une fuite peut consommer de l'oxygène, du temps équipage, de l'énergie de ventilation et un filtre de réserve.

Le registre de dépendances documente les ressources partagées, les causes communes, les chemins de secours et les points uniques. Il doit être relu avant les campagnes de pannes, car une redondance dessinée sur deux boîtes séparées ne vaut rien si les deux dépendent du même bus, du même logiciel, du même refroidissement ou du même capteur.

3. Le temps équipage est un consommable, surtout en situation dégradée

Un plan nominal qui utilise déjà presque tout le temps disponible devient irréaliste dès la première anomalie. Diagnostic, inspection, déplacement en combinaison, mise en sécurité, recherche de pièces, documentation, consultation médicale, recharge et récupération humaine consomment des heures. La charge cognitive augmente en même temps que la durée de travail.

Le budget doit donc distinguer temps nominal, maintenance préventive, réserve d'anomalie et disponibilité de personnes réellement qualifiées. Deux membres présents ne sont pas deux techniciens interchangeables. Une architecture résiliente protège des marges de temps et des compétences croisées au lieu de supposer qu'un équipage pourra absorber indéfiniment la dette opérationnelle.

4. La capacité médicale est une chaîne de fonctions, pas une armoire

La présence de médicaments ou d'un échographe ne suffit pas. Une capacité clinique implique détection, diagnostic, décision, traitement, surveillance, environnement, énergie, stérilité, données, compétence et évacuation éventuelle. Chacune de ces fonctions possède son propre horizon de dégradation.

La revue doit demander ce qui arrive si le médecin est le patient, si la télémédecine est indisponible, si un consommable stérile est épuisé, si l'imagerie fonctionne mais que l'alimentation de secours ne permet pas son usage au moment critique. Le médical doit être exercé comme un système intégré.

5. Une perte de communications teste l'autorité déléguée

Avec Mars, le délai interdit déjà le pilotage temps réel depuis la Terre. Une perte complète de liaison pousse plus loin la même logique : qui peut arrêter une activité, reconfigurer un système, consommer une réserve protégée, modifier une procédure, engager un véhicule de secours ou déroger à un plan ? Si ces responsabilités ne sont pas définies avant l'incident, la mission possède une dépendance organisationnelle cachée.

Le plan autonome doit inclure une hiérarchie d'autorité, des seuils, des procédures locales et un journal des décisions. Lors du retour de la liaison, l'objectif n'est pas de « reprendre la main » comme si rien ne s'était passé, mais de réconcilier les configurations, événements et décisions prises localement.

6. Les spares et la cannibalisation constituent un portefeuille d'options

Compter les pièces ne suffit pas. Une pièce peut être présente mais inaccessible, non qualifiée, déjà réservée à une fonction plus critique ou inutilisable faute d'outillage. La cannibalisation transforme un équipement en donneur et déplace le risque plutôt qu'elle ne le supprime.

Le ledger doit classer chaque spare par fonction protégée, compatibilité, emplacement, temps d'accès, durée de remplacement, essais post-maintenance et conséquence de consommation. L'usage du dernier exemplaire doit déclencher automatiquement une réévaluation du risque de la mission.

7. La dette maintenance est une variable d'état

Reporter une action peut être une bonne décision pendant une urgence, mais ce report a un coût qui doit rester visible. Une inspection différée, un filtre utilisé au-delà de son intervalle, une vibration non investiguée ou un software patch temporaire augmentent la dette.

Chaque dette possède une échéance, un risque associé, un propriétaire et une condition de fermeture. Un système peut revenir au vert fonctionnel tout en restant rouge du point de vue de la dette de maintenance. La revue suivante doit voir cette différence.

8. Le véhicule de retour reste hors du trade space ordinaire

Une base qui consomme progressivement les marges de son véhicule de retour pour résoudre des problèmes locaux peut sembler plus productive tout en perdant son option de sortie. Propulseur, puissance, thermique, communications, consommables, logiciels et accès physique du retour doivent être protégés comme une branche parallèle de mission.

Tout emprunt à cette branche exige une autorité élevée, une analyse du nouveau scénario de retour et une preuve que la mission n'a pas transformé une difficulté locale en perte stratégique.

9. Le black-start doit restaurer la preuve avant la capacité discrétionnaire

Après une extinction majeure, redémarrer le maximum de charges n'est pas l'objectif. Il faut rétablir d'abord connaissance de l'état, horloge, communications locales, détection incendie/fuite, contrôle atmosphère minimal et mesures électriques. Ensuite seulement les charges non critiques reviennent dans un ordre maîtrisé.

Le test de black-start doit partir d'un système réellement privé de ses hypothèses habituelles : batteries partiellement déchargées, capteurs incertains, réseau informatique limité et équipage fatigué. Un plan qui n'a jamais été exécuté n'est qu'une intention.

10. La logistique se vérifie comme une récupération physique, pas comme un inventaire

Une pièce indiquée dans une base de données n'est pas disponible si elle est derrière une cargaison inaccessible, dans un conteneur non pressurisé pendant une tempête ou si personne ne sait quel outil ouvre son logement. Les exercices doivent chronométrer localisation, accès, transport, installation et essai.

Cette logique s'applique aussi à la nourriture, aux réactifs, aux combinaisons, aux batteries et au matériel médical. La mission protège des fonctions, pas des lignes de tableur.

11. La compétence équipage possède profondeur et date d'expiration

Une procédure critique ne peut reposer sur une seule personne. La matrice de compétences indique primaire, secondaire, niveau d'autonomie, dernière pratique et date de requalification. Les tâches rares nécessitent des répétitions espacées avant que la compétence ne s'érode.

La formation doit également tenir compte des scénarios où l'expert est indisponible, blessé ou engagé sur une autre urgence. La redondance humaine doit être testée, pas seulement déclarée.

12. Science et exploration doivent tenir dans la réalité maintenance

La science est un objectif de mission, mais elle doit rester ordonnançable autour des fonctions protégées. Une architecture qui n'atteint son programme scientifique qu'en consommant toute la marge de maintenance et de sommeil est structurellement en déficit.

Le planning utilise des niveaux de priorité, des conditions de déclenchement et des règles d'abandon. Une activité scientifique peut être différée sans être considérée comme un échec si la décision protège la mission et conserve la possibilité de la reprendre.

13. L'acceptation finale doit être adversariale

Une revue de fermeture ne demande pas « avez-vous un plan ? » mais « montrez-moi la preuve et la version du système qu'elle couvre ». Les reviewers choisissent des exigences au hasard, suivent leurs dépendances, demandent les preuves, injectent une panne, puis vérifient que les marges annoncées sont encore vraies après la reconfiguration.

Une architecture est prête quand elle résiste à cette contradiction sans dépendre de connaissances orales non documentées.

14. Campagne de douze situations couplées

1. **Énergie + thermique.** Une baisse de production solaire se combine à une boucle thermique partiellement dégradée.
2. **Eau + maintenance.** Le dernier spare d'une pompe est utilisé alors qu'une inspection préventive d'un second train est en retard.
3. **Communication + médical.** Une perte de liaison survient pendant un incident clinique qui aurait normalement utilisé un spécialiste terrestre.
4. **Rover + météo.** Un véhicule est immobilisé alors que la production énergétique du site diminue.
5. **Logiciel + configuration.** Un patch d'urgence corrige une panne locale mais modifie une interface partagée.
6. **Logistique + accès.** La pièce est présente mais située dans un conteneur dont le moyen de manutention principal est indisponible.
7. **Équipage + dette.** Deux personnes qualifiées sont absorbées par une réparation longue tandis qu'une seconde anomalie apparaît.
8. **Black-start + capteurs.** Le réseau revient avant certains capteurs de vérité et produit des états contradictoires.
9. **ISRU + retour.** L'augmentation de production locale propose d'utiliser une réserve énergétique protégée pour le retour.
10. **Incendie + communication.** Une alarme impose isolement de volume au moment où le lien extérieur disparaît.
11. **Relève + waivers.** La nouvelle équipe reçoit le système avec deux dérogations ouvertes et doit démontrer qu'elle en comprend les limites.
12. **Fin de campagne.** Une dernière panne survient lorsque la tentation est forte de consommer les marges restantes pour maximiser la science.

15. Dossier de relève — ce que l'équipe suivante doit pouvoir reproduire

La relève doit retrouver sans mémoire orale : configuration exacte, fonctions protégées, marges, dettes maintenance, risques ouverts, waivers, pièces consommées, versions logicielles, anomalies, changements locaux, critères de retour et prochains gates. Elle doit aussi pouvoir refaire les calculs critiques et identifier les hypothèses qui expirent avec le temps.

Le passage de commandement est donc une interface de sûreté. Une mission qui ne peut pas être héritée proprement n'est pas durable.

16. Matrice finale d'acceptation

Fonction protégée	État nominal	État dégradé accepté	Preuve	Gate
Atmosphère habitable	deux trains disponibles	un train + réserve explicitement chronométrée	test, tendance et stock	GO/HOLD
Énergie vitale	production + stockage avec marge	black-start et délestage prouvés	essai end-to-end	GO/HOLD
Eau	récupération nominale	stock + conservation + réparation	ledger horizon	GO/HOLD
Mobilité secours	deux moyens qualifiés	un moyen avec rayon réduit prouvé	essai trajet/énergie	GO/HOLD
Commandement autonome	liaison Terre disponible	procédures locales et autorité déléguée	exercice perte liaison	GO
Retour	branche protégée	aucun emprunt non approuvé	configuration et marges	NO-GO si compromis

Règle d'intégration R76

Le succès d'une campagne de 500 sols ne se mesure pas au nombre d'incidents évités mais à la capacité à détecter, ordonner, contenir, récupérer et transmettre les fonctions critiques tout en conservant les options de retour.

Control room de mission — états, autorité, configuration et résilience

Cette dernière extension rend explicites les notions qu'une revue de mission doit pouvoir retrouver sans les déduire entre les lignes. Elles ne rajoutent pas un catalogue d'équipements ; elles structurent la manière de savoir ce qui est encore vrai, ce qui est encore disponible et quelle option doit être protégée après une panne.

1. Une fonction protégée doit être nommée avant le matériel

« Maintenir une atmosphère respirable pendant une perte de boucle principale » est une fonction.
« Conserver le compresseur A » est une solution. En incident, le matériel peut changer ; la fonction protégée reste le repère qui permet de décider si une substitution, une réparation provisoire ou un délestage est acceptable.

2. Le temps avant perte de fonction ordonne les décisions

Chaque anomalie reçoit une horloge : temps avant hypoxie, avant perte thermique, avant batterie minimale, avant épuisement d'un stock ou avant fermeture d'une fenêtre de secours. Le contrôle room traite d'abord l'horloge la plus courte, sauf si une action irréversible détruit une fonction stratégique plus lointaine.

3. Un inventaire possède plusieurs états

Une ressource peut être à bord mais inaccessible, accessible mais non qualifiée, qualifiée mais déjà engagée, disponible mais non protégée. Le ledger distingue donc *présent*, *accessible*, *qualifié*, *disponible* et *protégé*. Cette distinction évite de compter deux fois une même pièce ou de promettre une capacité qui ne peut pas être utilisée au moment nécessaire.

4. Détection et fonction protégée doivent rester suffisamment indépendantes

Une panne ne doit pas rendre invisible sa propre détection. Si la même alimentation, le même réseau ou le même logiciel fait fonctionner l'équipement et son unique alarme, l'architecture possède une cause commune. Les fonctions vitales nécessitent des voies de preuve diversifiées ou au minimum un mode de vérification indépendant.

5. Les gates de récupération séparent fonction, redondance et marge

Après réparation, « ça remarche » n'est que le premier niveau. Il faut vérifier que la fonction est restaurée, que la redondance attendue est revenue, puis que les marges de mission et la configuration sont à nouveau compatibles avec la suite de campagne. La mission peut donc être fonctionnelle mais encore en HOLD.

6. Eau et nourriture doivent être traitées comme fonctions récupérables

Un stock alimentaire ou hydrique est une réserve ; la sécurité à long terme dépend aussi de la capacité à récupérer, produire, conserver, distribuer et surveiller. Les analyses doivent séparer stock protégé, consommation, pertes, capacité de récupération et temps nécessaire pour rétablir la fonction après panne.

7. La mobilité de surface appartient à l'architecture d'urgence

Les rovers ne servent pas seulement à l'exploration. Ils peuvent transporter un équipage vers un refuge, déplacer une pièce lourde, atteindre une source énergétique externe, secourir un EVA ou maintenir une liaison entre deux habitats. Rayon protégé, état de charge, équipage qualifié et disponibilité des moyens de récupération doivent donc figurer dans les gates d'urgence.

8. Les consommables ont une politique d'usage

La mission distingue consommation de routine, usage de contingence et réserve protégée. Cette politique évite qu'une suite de petites décisions raisonnables consomme progressivement le stock qui devait protéger un événement rare mais catastrophique. Toute ouverture d'une réserve protégée crée une nouvelle baseline.

9. La performance humaine de longue durée appartient au planning

Sommeil, charge cognitive, monotonie, conflits, récupération après EVA et cycles de travail influencent directement maintenance et sécurité. Le planning ne peut pas supposer une performance constante sur 500 sols. Les activités non critiques doivent pouvoir être déplacées lorsque la fatigue ou la charge d'anomalie augmente.

10. La fabrication locale inclut la qualification

Produire géométriquement une pièce ne prouve pas qu'elle est apte à une fonction critique. Matière, procédé, porosité, traitement, métrologie, nettoyage, documentation, essais et domaine d'emploi doivent être définis. Une pièce locale peut être autorisée pour une fonction non critique avant de l'être pour une barrière de pression ou une fonction médicale.

11. La stratégie de spares se construit par fonction protégée

La bonne question n'est pas « combien de pièces avons-nous ? » mais « quelles fonctions perdons-nous après la prochaine panne et quel chemin alternatif reste ? ». Les pièces polyvalentes, réparables ou fabricables localement peuvent protéger plusieurs fonctions ; les éléments rares sans substitution méritent une réserve plus forte.

12. Les probabilités non indépendantes ne se multiplient pas librement

Un registre de risque peut devenir trompeur si les probabilités de deux protections sont multipliées alors qu'elles partagent une cause. Logiciel commun, environnement, fournisseur, erreur procédure ou maintenance peuvent créer une corrélation forte. Lorsque l'indépendance n'est pas démontrée, la revue doit rester conservatrice.

13. Les pannes rares doivent être préparées sans épuiser l'exploitation courante

Former et exercer chaque jour tous les scénarios rares serait impossible. La mission choisit donc des scénarios à conséquence élevée, maintient des checklists, des kits et des compétences minimales, puis programme des répétitions espacées. Le coût de préparation est lui-même budgété dans le temps équipage.

14. Le handover est une interface de sûreté

Une relève mal préparée recrée des erreurs déjà comprises. Les décisions locales, limitations temporaires, réparations non standard, pièces substituées et hypothèses de calcul doivent être visibles dans un package unique. L'équipe entrante reformule les risques majeurs et refait plusieurs calculs critiques avant transfert d'autorité.

15. Une réussite locale ne doit pas détruire le retour

Une campagne peut battre ses objectifs scientifiques et industriels tout en devenant stratégiquement fragile si elle consomme les moyens de retour. Les critères de succès incluent donc explicitement l'intégrité de la branche retour ou la décision assumée de changer l'architecture de mission selon une autorité définie.

16. L'incident intégré de 72 heures

Le scénario final combine baisse de production électrique, panne d'un train de récupération d'eau, indisponibilité temporaire du lien Terre, équipier diminué et rover immobilisé. Les premières heures visent la survie et la stabilisation ; la première journée restaure la connaissance d'état et les marges ; les jours suivants ferment la réparation et la configuration.

La réussite n'est pas d'éviter toute perte de performance. Elle consiste à conserver les fonctions vitales, ne pas consommer une réserve protégée sans autorité, garder un chemin vers le retour, documenter chaque changement et rendre à la relève une architecture dont l'état peut être reproduit.

17. Questions de la revue finale

- Quelles fonctions sont réellement protégées et pour combien de temps ?
- Quelles redondances partagent encore une cause commune ?
- Quelle dette maintenance est ouverte et quand devient-elle dangereuse ?
- Quels stocks sont seulement présents et lesquels sont réellement accessibles et qualifiés ?
- Quelle panne rendrait son propre diagnostic difficile ?
- Quel changement récent a invalidé une ancienne preuve ?
- Quelles décisions l'équipage peut-il prendre sans Terre ?
- Quel événement ferait passer la mission de GO à HOLD puis à NO-GO ?
- La branche retour reste-t-elle protégée après la dernière reconfiguration ?
- Une équipe nouvelle pourrait-elle reproduire ces réponses avec le package actuel ?

Conclusion opérationnelle

La fermeture du module 16 n'est pas un exercice de volume. Elle exige que FR et EN permettent de prendre les mêmes décisions : protéger des fonctions, gérer plusieurs horloges, distinguer inventaire et disponibilité, suivre la configuration, démontrer V&V, préserver le retour et transmettre la mission à une autre équipe.

R76 · PARITÉ QUANTITATIVE FR↔EN

Huit fermetures quantitatives qui manquaient explicitement au français

Le compteur de formules n'est pas une preuve de parité. Ces huit mini-leçons ajoutent les compétences opérationnelles présentes en anglais mais encore implicites ou absentes en français : appoint d'eau, endurance batterie, énergie critique, horizons oxygène et nourriture, charge de maintenance, couverture de rechanges et autonomie de commandement.

Appoint d'eau de campagne — convertir une perte nette vérifiée en masse à fournir

1 — Question concrète

Quelle masse d'eau d'appoint faut-il prévoir pour un équipage lorsque la perte nette quotidienne par personne est déjà caractérisée ?

2 — Intuition sans symboles

Chaque personne perd chaque sol une petite quantité d'eau qui n'est pas récupérée. On additionne cette perte pour tout l'équipage puis sur toute la durée de la campagne.

3 — Grandeurs

M_{appoint} est la masse d'appoint sur la campagne ; q_{net} la perte nette vérifiée par personne et par sol ; N l'effectif ; t la durée en sols.

4 — Formule

$$M_{\text{appoint}} = q_{\text{net}} \times N \times t$$

5 — Lecture

La masse d'appoint égale la perte nette par personne et par sol multipliée par l'effectif puis par la durée.

6 — Symboles et sens

M_{appoint} est la masse à fournir ; q_{net} un débit massique net individuel ; N un nombre de personnes ; t une durée.

7 — Prononciation

M_{appoint} égale q_{net} fois N fois t .

8 — Unités

$$\text{kg}/(\text{personne} \cdot \text{sol}) \times \text{personne} \times \text{sol} = \text{kg}.$$

9 — Convention

Le débit net doit correspondre au même état d'exploitation et à la même frontière de qualité. Eau potable, hygiène et eau de procédé ne se mélangent pas implicitement.

10 — Pourquoi cette opération

L'effectif transforme la perte individuelle en perte d'équipage ; la durée cumule ensuite cette perte quotidienne sur toute la campagne.

11 — Hypothèses

Le débit net est supposé constant sur l'intervalle. Fuites accidentelles, démarrage, maintenance et réserve d'urgence sont traités séparément.

12 — Contrôle d'unités

Les personnes et les sols s'annulent, il reste une masse en kilogrammes.

13 — Cas numérique

Avec 1,2 kg/(personne·sol), 6 personnes et 500 sols : besoin quotidien = $1,2 \times 6 = 7,2$ kg/sol ;
masse d'appoint = $7,2 \times 500 = 3\,600$ kg.

14 — Pourquoi le calcul fonctionne

On passe d'abord d'une perte individuelle à une perte collective, puis d'un débit collectif à une masse cumulée.

15 — Contrôle algébrique

Si la masse disponible est connue, l'horizon constant devient $t = M_{\text{disponible}} / (q_{\text{net}} \times N)$.

16 — Estimation mentale

Environ 7 kg par sol pendant environ 500 sols donnent environ 3 500 kg ; 3 600 kg est donc cohérent.

17 — Interprétation

Le scénario pédagogique exige 3,6 tonnes d'appoint net sur 500 sols avant d'ajouter les réserves protégées et les pertes exceptionnelles.

18 — Ce que le résultat ne prouve pas

Il ne démontre ni la capacité de récupération de l'ECLSS, ni la qualité de l'eau, ni sa distribution, son stockage ou sa disponibilité réelle.

19 — Sensibilité

Si la perte nette double en mode dégradé, la consommation de campagne double immédiatement ; une baisse vers zéro n'annule pas les exigences de qualité et de redondance.

20 — Exercices guidé et autonome

Exercice guidé. Pour 4 personnes, 1,5 kg/(personne·sol) et 30 sols, calculer l'appoint.

Correction guidée

$1,5 \times 4 = 6 \text{ kg/sol}$; $6 \times 30 = 180 \text{ kg}$. La réserve d'urgence reste séparée.

Exercice autonome. Six personnes disposent de 600 kg accessibles avec une perte nette de 2 kg/(personne·sol). Calculer l'horizon et citer deux raisons pour lesquelles ce n'est pas un temps de survie garanti.

Correction autonome

Débit équipage = 12 kg/sol ; horizon = $600/12 = 50 \text{ sols}$. La qualité, la distribution, l'énergie, la maintenance et l'accessibilité peuvent réduire l'horizon réellement exploitable.

21 — Décision mission

Utiliser cette masse pour fermer l'inventaire nominal, puis protéger une réserve distincte et vérifier la fonction de récupération ; une quantité totale sans qualité ni accessibilité ne ferme pas la mission.

Endurance batterie sur charge critique — convertir l'énergie réellement utilisable en temps de survie électrique

1 — Question concrète

Combien de temps une batterie nominale peut-elle soutenir une charge critique après réserve protégée et pertes de conversion ?

2 — Intuition sans symboles

Une partie de l'énergie stockée doit rester intouchable et une autre partie se perd à la conversion. Le temps disponible est l'énergie réellement livrable divisée par la vitesse à laquelle la charge la consomme.

3 — Grandeurs

E_{nom} est l'énergie nominale ; $r_{\text{réserve}}$ la fraction protégée ; η le rendement de livraison ; P_{crit} la puissance critique ; t_{bat} l'endurance.

4 — Formule

$$t_{\text{bat}} = E_{\text{nom}} \times (1 - r_{\text{réserve}}) \times \eta / P_{\text{crit}}$$

5 — Lecture

L'endurance égale l'énergie nominale multipliée par la part non réservée puis par le rendement, le tout divisé par la puissance critique.

6 — Symboles et sens

t_{bat} est une durée ; E_{nom} une énergie ; $r_{réserve}$ et η sont sans dimension ; P_{crit} est une puissance.

7 — Prononciation

té batterie égale E nominal fois un moins erre réserve fois éta, divisé par P critique.

8 — Unités

kWh $\times$ sans dimension $\times$ sans dimension $\div$ kW = h.

9 — Convention

Réserve et rendement sont saisis comme fractions : 20 % = 0,20 et 92 % = 0,92.

10 — Pourquoi cette opération

On retire d'abord la part protégée, puis on applique les pertes de livraison ; l'énergie utilisable divisée par une puissance donne une durée.

11 — Hypothèses

Charge critique constante, capacité nominale pertinente et absence de déclassement supplémentaire dû au froid, au vieillissement ou à la limite de puissance au-delà de ceux déjà représentés.

12 — Contrôle d'unités

Une énergie en kWh divisée par une puissance en kW donne des heures.

13 — Cas numérique

900 kWh nominaux, réserve 20 %, rendement 92 % : énergie livrable = $900 \times 0,80 \times 0,92 = 662,4$ kWh. Pour 35 kW, endurance = $662,4/35 = 18,93$ h.

14 — Pourquoi le calcul fonctionne

La multiplication construit l'énergie réellement dépensable ; la division mesure combien d'heures cette énergie peut alimenter le débit de puissance critique.

15 — Contrôle algébrique

Pour une endurance cible, $E_{nom} = t_{bat} \times P_{crit} / [(1-r_{réserve}) \times \eta]$.

16 — Estimation mentale

Environ 660 kWh à environ 35 kW donnent un peu moins de 20 h, cohérent avec 18,9 h.

17 — Interprétation

Dans ce cas, la charge critique peut être tenue environ 18,9 h avant d'atteindre la frontière de réserve protégée.

18 — Ce que le résultat ne prouve pas

Il ne prouve pas que la batterie peut fournir 35 kW en continu à la température réelle ni que toutes les charges réellement critiques sont incluses.

19 — Sensibilité

À 45 kW, la même énergie livrable ne tient plus qu'environ 14,72 h ; toute croissance de charge consomme rapidement le temps de réparation.

20 — Exercices guidé et autonome

Exercice guidé. Avec 1 200 kWh, 25 % de réserve, 90 % de rendement et 40 kW critiques, calculer l'endurance.

Correction guidée

Énergie livrable = $1\,200 \times 0,75 \times 0,90 = 810$ kWh ; endurance = $810/40 = 20,25$ h.

Exercice autonome. Une réparation demande 16 h et l'on veut 2 h de marge. Avec 900 kWh, 20 % de réserve et 92 % de rendement, quelle charge constante maximale est admissible ?

Correction autonome

Durée exigée = 18 h ; énergie livrable = 662,4 kWh ; puissance maximale = $662,4/18 = 36,8$ kW. Au-delà, il faut délester, accélérer la réparation ou fournir une autre source.

21 — Décision mission

Comparer l'endurance démontrée au temps crédible de réparation avec marge. Si la réparation dépasse l'endurance, l'état est HOLD/NO-GO, pas GO optimiste.

Énergie d'une charge critique — transformer une durée de protection en réserve livrée

1 — Question concrète

Quelle énergie faut-il livrer pour maintenir une fonction électrique protégée pendant une durée imposée ?

2 — Intuition sans symboles

Une charge puissante consomme davantage d'énergie et une protection plus longue demande davantage de réserve. La mission doit convertir la durée d'urgence en énergie avant de dimensionner le stockage.

3 — Grandeurs

P_{crit} est la puissance de la charge protégée ; $t_{support}$ la durée de soutien ; E_{req} l'énergie à livrer à la charge.

4 — Formule

$$E_{req} = P_{crit} \times t_{support}$$

5 — Lecture

L'énergie requise égale la puissance critique multipliée par la durée de soutien.

6 — Symboles et sens

E_{req} est une énergie, P_{crit} une puissance et $t_{support}$ une durée.

7 — Prononciation

E requis égale P critique fois té support.

8 — Unités

$$kW \times h = kWh.$$

9 — Convention

La formule porte sur l'énergie effectivement livrée à la charge ; le dimensionnement du stockage doit ensuite intégrer rendement, vieillissement, température et réserve protégée.

10 — Pourquoi cette opération

La puissance est un débit d'énergie ; la multiplier par la durée donne l'énergie cumulée.

11 — Hypothèses

La puissance critique est supposée représentative et constante sur l'intervalle ; les transitoires et pertes amont sont traités séparément.

12 — Contrôle d'unités

Kilowatt multiplié par heure donne kilowattheure.

13 — Cas numérique

Pour 4,0 kW pendant 18 h : $E_{req} = 4,0 \times 18 = 72$ kWh livrés.

14 — Pourquoi le calcul fonctionne

Chaque heure ajoute 4 kWh au besoin ; dix-huit heures en ajoutent donc dix-huit fois autant.

15 — Contrôle algébrique

La durée couverte vaut $t_{\text{support}} = E_{\text{req}}/P_{\text{crit}}$ et la puissance admissible $P_{\text{crit}} = E_{\text{req}}/t_{\text{support}}$.

16 — Estimation mentale

4 kW pendant environ 20 h donneraient environ 80 kWh ; 72 kWh pour 18 h est plausible.

17 — Interprétation

Le profil critique réclame 72 kWh réellement livrés pendant 18 h, indépendamment de l'énergie consacrée aux usages non vitaux.

18 — Ce que le résultat ne prouve pas

Il ne dimensionne pas à lui seul une batterie ou un générateur et ne prouve pas la tenue thermique, la puissance de pointe ou l'accessibilité de l'énergie.

19 — Sensibilité

Allonger la durée de soutien de 25 % augmente exactement de 25 % l'énergie livrée nécessaire si la puissance reste constante.

20 — Exercices guidé et autonome

Exercice guidé. Une charge critique de 6 kW doit tenir 12 h. Calculer l'énergie livrée.

Correction guidée

$$6 \times 12 = 72 \text{ kWh.}$$

Exercice autonome. Un stockage ne peut livrer que 96 kWh au profil critique. Quelle puissance constante maximale peut-on soutenir pendant 16 h ?

Correction autonome

$P = 96/16 = 6 \text{ kW}$. Les pertes et réserves doivent être intégrées avant de traduire ce résultat en capacité nominale de batterie.

21 — Décision mission

Fermer séparément l'énergie des charges vitales afin qu'aucun usage discrétionnaire ne puisse consommer implicitement la réserve de survie.

Horizon de réserve d'oxygène — convertir une masse accessible en temps avant perte de fonction

1 — Question concrète

Combien de temps une réserve d'oxygène qualifiée et accessible peut-elle soutenir l'équipage à un débit de planification donné ?

2 — Intuition sans symboles

La réserve disponible est consommée plus vite lorsque l'équipage est plus nombreux ou lorsque la consommation individuelle augmente. Diviser la réserve par la consommation totale donne l'horizon d'inventaire.

3 — Grandeurs

M_O2_utile est la masse d'oxygène qualifiée accessible ; N_équipage l'effectif ; q_O2 la consommation de planification par personne et par jour ; t_O2 l'horizon.

4 — Formule

$$t_{O2} = M_{O2_utile} / (N_{\text{équipage}} \times q_{O2})$$

5 — Lecture

L'horizon oxygène égale la masse utile divisée par l'effectif multiplié par la consommation individuelle.

6 — Symboles et sens

t_O2 est une durée ; M_O2_utile une masse ; N_équipage un nombre de personnes ; q_O2 un débit massique individuel.

7 — Prononciation

té O deux égale M O deux utile divisé par enne équipage fois q O deux.

8 — Unités

$$\text{kg} \div [\text{personnes} \times \text{kg}/(\text{personne} \cdot \text{jour})] = \text{jour}.$$

9 — Convention

La masse comptée doit être réellement accessible, compatible avec la pression et la stratégie incendie ; le débit utilisé est une valeur de planification déclarée.

10 — Pourquoi cette opération

L'effectif transforme le débit individuel en consommation collective ; la réserve divisée par ce débit donne le temps avant épuisement.

11 — Hypothèses

Le débit moyen est tenu constant et l'intégrité de la chaîne de distribution est supposée disponible pendant l'intervalle.

12 — Contrôle d'unités

Les kilogrammes et personnes s'annulent correctement, il reste une durée en jours.

13 — Cas numérique

36 kg accessibles, 6 personnes et 0,84 kg/(personne·jour) donnent $t_{O_2} = 36/(6 \times 0,84) \approx 7,14$ jours.

14 — Pourquoi le calcul fonctionne

La consommation collective vaut 5,04 kg/jour ; 36 kg divisés par ce débit couvrent un peu plus de sept jours.

15 — Contrôle algébrique

La masse nécessaire pour un horizon cible vaut $M_{O_2\text{ utile}} = t_{O_2} \times N_{\text{équipage}} \times q_{O_2}$.

16 — Estimation mentale

Environ 5 kg/jour consommés dans une réserve de 35–36 kg donnent environ une semaine.

17 — Interprétation

La réserve soutient environ 7,1 jours au débit retenu ; cette horloge doit être comparée à celles du CO₂, de la pression et de l'énergie.

18 — Ce que le résultat ne prouve pas

Il ne prouve ni la disponibilité du matériel de distribution, ni la qualité de l'atmosphère, ni le bon fonctionnement de l'élimination du CO₂.

19 — Sensibilité

Ajouter deux personnes au même stock réduit l'horizon de 25 % si le débit individuel reste identique.

20 — Exercices guidé et autonome

Exercice guidé. 24 kg d'oxygène servent 4 personnes à 0,8 kg/(personne·jour). Calculer l'horizon.

Correction guidée

Consommation collective = 3,2 kg/j ; horizon = $24/3,2 = 7,5$ jours.

Exercice autonome. Quelle masse accessible faut-il garantir pour 6 personnes pendant 10 jours à 0,84 kg/(personne·jour) ?

Correction autonome

$M = 10 \times 6 \times 0,84 = 50,4$ kg, avant marge et réserves supplémentaires.

21 — Décision mission

Placer l'horizon oxygène sur le même tableau temps-avant-perte que CO₂, pression et énergie ; l'horloge la plus courte commande l'action.

Horizon alimentaire avec réserve protégée — distinguer stock courant et dernier recours

1 — Question concrète

Pendant combien de temps le stock alimentaire courant couvre-t-il l'équipage si une masse d'urgence reste volontairement protégée ?

2 — Intuition sans symboles

Tout le stock présent n'est pas forcément disponible pour la consommation normale. On retire d'abord la réserve sanctuarisée, puis on compare le stock courant au rythme de consommation de l'équipage.

3 — Grandeurs

M_{food} est le stock comestible total ; $M_{\text{réserve}}$ la masse protégée ; $N_{\text{équipage}}$ l'effectif ; q_{food} la consommation par personne et par jour ; t_{food} l'horizon courant.

4 — Formule

$$t_{\text{food}} = (M_{\text{food}} - M_{\text{réserve}}) / (N_{\text{équipage}} \times q_{\text{food}})$$

5 — Lecture

L'horizon alimentaire égale le stock total moins la réserve, divisé par la consommation collective quotidienne.

6 — Symboles et sens

Les deux masses sont en kilogrammes ; q_{food} est un débit massique individuel ; t_{food} est une durée.

7 — Prononciation

t_{food} égale M_{food} moins $M_{\text{réserve}}$, divisé par $N_{\text{équipage}}$ fois q_{food} .

8 — Unités

$$\text{kg} \div [\text{personnes} \times \text{kg}/(\text{personne} \cdot \text{jour})] = \text{jour}.$$

9 — Convention

La réserve n'est libérée que par une règle explicite de commandement ; masse alimentaire ne signifie pas automatiquement nutrition, compatibilité menu ou absence de pertes.

10 — Pourquoi cette opération

La soustraction protège l'urgence ; la division transforme le stock consommable restant en durée au débit collectif.

11 — Hypothèses

Consommation moyenne constante, stock réellement comestible et accessible, absence de pertes non prévues.

12 — Contrôle d'unités

Le numérateur est une masse et le dénominateur une masse par jour : le quotient donne des jours.

13 — Cas numérique

420 kg au total, 60 kg protégés, 6 personnes et 0,80 kg/(personne-jour) : $t_{\text{food}} = 360/4,8 = 75$ jours.

14 — Pourquoi le calcul fonctionne

Après retrait de la réserve, l'équipage consomme 4,8 kg par jour dans un stock courant de 360 kg.

15 — Contrôle algébrique

Le stock total nécessaire pour un horizon donné vaut $M_{\text{food}} = M_{\text{réserve}} + t_{\text{food}} \times N_{\text{équipage}} \times q_{\text{food}}$.

16 — Estimation mentale

360 kg à environ 5 kg/jour donnent un peu plus de 70 jours ; 75 jours est cohérent.

17 — Interprétation

Le stock courant couvre 75 jours tout en laissant 60 kg hors consommation ordinaire.

18 — Ce que le résultat ne prouve pas

Il ne garantit ni la valeur nutritionnelle, ni l'acceptabilité, ni la durée de conservation, ni l'intégrité des emballages.

19 — Sensibilité

Une hausse de 10 % de la consommation réduit l'horizon d'environ 75 à 68,2 jours.

20 — Exercices guidé et autonome

Exercice guidé. 300 kg dont 40 kg protégés servent 5 personnes consommant 0,8 kg/jour. Calculer l'horizon courant.

Correction guidée

Stock courant = 260 kg ; consommation collective = 4 kg/j ; horizon = 65 jours.

Exercice autonome. Quel stock total faut-il pour 6 personnes, 90 jours, 0,75 kg/(personne-jour) et une réserve protégée de 80 kg ?

Correction autonome

Besoin courant = $6 \times 90 \times 0,75 = 405$ kg ; stock total = $405 + 80 = 485$ kg.

21 — Décision mission

La libération de la réserve alimentaire est une décision de commandement liée à un plan de récupération, jamais une marge cachée dans le calendrier.

Utilisation de la capacité maintenance — mesurer la marge de travail qualifié réellement disponible

1 — Question concrète

La capacité de travail qualifiée peut-elle absorber la maintenance prévue sans saturer l'équipage ?

2 — Intuition sans symboles

Une mission peut disposer de nombreuses heures humaines tout en manquer de personnes qualifiées pour les tâches critiques. Il faut comparer le travail réellement requis au volume de travail qualifié réellement disponible.

3 — Grandeurs

H_requis est le nombre d'heures-personnes de maintenance nécessaires sur la période ; H_qualifié les heures-personnes qualifiées disponibles après repos et autres tâches protégées ; U_maint l'utilisation.

4 — Formule

$$U_{\text{maint}} = H_{\text{requis}} / H_{\text{qualifié}}$$

5 — Lecture

L'utilisation maintenance égale les heures requises divisées par les heures qualifiées disponibles.

6 — Symboles et sens

H_requis et H_qualifié sont des heures-personnes sur le même intervalle ; U_maint est sans dimension.

7 — Prononciation

U maintenance égale H requis divisé par H qualifié.

8 — Unités

heure-personne / heure-personne = sans dimension.

9 — Convention

Des heures ne sont substituables que si les compétences, habilitations et contraintes de fatigue permettent réellement la tâche.

10 — Pourquoi cette opération

Le quotient mesure la fraction de la capacité qualifiée déjà engagée par la charge de maintenance.

11 — Hypothèses

Même période de référence, qualification connue, temps de repos et autres tâches protégées déjà retirés de la capacité.

12 — Contrôle d'unités

Les mêmes unités d'heures-personnes s'annulent.

13 — Cas numérique

96 h/semaine requises et 120 h/semaine qualifiées donnent $U_{\text{maint}} = 96/120 = 0,80 = 80 \%$.

14 — Pourquoi le calcul fonctionne

Il reste 20 % de capacité, soit 24 h/semaine, pour absorber les aléas sans reporter immédiatement une autre tâche.

15 — Contrôle algébrique

La capacité qualifiée minimale pour une utilisation cible vaut $H_{\text{qualifié}} = H_{\text{requis}}/U_{\text{cible}}$.

16 — Estimation mentale

100 h de travail pour 120 h disponibles représentent un peu plus de quatre cinquièmes, donc environ 80 %.

17 — Interprétation

À 80 %, la maintenance n'est pas encore saturée mais la marge pour une panne supplémentaire est limitée.

18 — Ce que le résultat ne prouve pas

Il ne prouve pas que les compétences sont interchangeable, que les tâches peuvent être parallélisées ni que la fatigue restera acceptable.

19 — Sensibilité

Une panne ajoutant 18 h porte la charge à $114/120 = 95 \%$, laissant très peu de marge.

20 — Exercices guidé et autonome

Exercice guidé. 72 h sont requises pour 96 h qualifiées disponibles. Calculer l'utilisation.

Correction guidée

$72/96 = 0,75 = 75 \%$; il reste 24 h de marge qualifiée.

Exercice autonome. Pour 110 h requises, quelle capacité faut-il pour maintenir l'utilisation au plus à 85 % ?

Correction autonome

$H_{\text{qualifié}} = 110/0,85 \approx 129,4$ h. Il faut donc au moins environ 130 h qualifiées sur la période.

21 — Décision mission

Protéger une marge de maintenance qualifiée suffisante pour qu'une panne n'oblige pas à différer une autre tâche de sûreté.

Couverture de pièces critiques — compter uniquement les rechanges réellement utilisables

1 — Question concrète

Les pièces de rechange qualifiées, compatibles et accessibles couvrent-elles le scénario de panne défini ?

2 — Intuition sans symboles

Un stock sur une étagère n'est une réserve que si la pièce fonctionne, correspond à la bonne configuration et peut être récupérée à temps. La couverture compare ce stock utile au besoin du scénario.

3 — Grandeurs

$N_{\text{serviceable}}$ est le nombre de rechanges utilisables ; N_{requis} le nombre exigé par le scénario ; C_{spare} le ratio de couverture.

4 — Formule

$C_{\text{spare}} = N_{\text{serviceable}} / N_{\text{requis}}$

5 — Lecture

La couverture de rechange égale le nombre de pièces utilisables divisé par le nombre exigé.

6 — Symboles et sens

Les deux nombres sont des comptes de pièces sur la même configuration ; le ratio est sans dimension.

7 — Prononciation

C spare égale N serviceable divisé par N requis.

8 — Unités

pièces / pièces = sans dimension.

9 — Convention

Ne compter que les pièces qualifiées, accessibles et compatibles ; un ratio supérieur à un ne protège pas d'un défaut de cause commune.

10 — Pourquoi cette opération

Le rapport indique combien de fois le stock utile couvre le besoin du cas de contingence.

11 — Hypothèses

Scénario de panne défini, inventaire à jour, compatibilité et état de service connus.

12 — Contrôle d'unités

Les comptes de pièces s'annulent ; la couverture est un nombre pur.

13 — Cas numérique

3 rechanges utilisables pour un cas exigeant 2 unités donnent $C_{\text{spare}} = 3/2 = 1,5$.

14 — Pourquoi le calcul fonctionne

Le scénario consomme deux unités ; trois unités disponibles représentent une fois et demie ce besoin.

15 — Contrôle algébrique

Le nombre minimum de rechanges pour une couverture cible vaut $N_{\text{serviceable}} = C_{\text{spare}} \times N_{\text{requis}}$, arrondi au nombre entier supérieur.

16 — Estimation mentale

Trois pièces pour deux nécessaires donnent naturellement une couverture de 1,5.

17 — Interprétation

Le stock utile couvre 1,5 fois le besoin défini, à condition que les trois unités restent réellement utilisables.

18 — Ce que le résultat ne prouve pas

Il ne couvre pas les défauts de cause commune, une mauvaise configuration, un stockage inaccessible ou un outillage absent.

19 — Sensibilité

La mise en quarantaine d'une seule des trois pièces ramène la couverture de 1,5 à 1,0.

20 — Exercices guidé et autonome

Exercice guidé. Quatre pièces utilisables sont disponibles pour un cas en exigeant trois.

Correction guidée

$C = 4/3 \approx 1,33$. Il faut ensuite vérifier compatibilité, numéro de série et temps de récupération.

Exercice autonome. Un scénario exige deux pièces. Quatre sont en stock, mais une est en quarantaine et une autre est inaccessible pendant l'incident. Calculer la couverture utile.

Correction autonome

Seules deux pièces sont réellement serviceables et accessibles ; $C = 2/2 = 1,0$. Le stock physique de quatre ne doit pas être utilisé comme numérateur.

21 — Décision mission

La matrice d'acceptation ne compte que les rechanges serviceables, récupérables et compatibles avec la configuration réellement déployée.

Fenêtre d'autonomie de commandement — laisser la contrainte la plus courte fixer la limite

1 — Question concrète

Pendant combien de temps l'équipage peut-il poursuivre localement une mission sûre lors d'une perte de communications ?

2 — Intuition sans symboles

Plusieurs limites peuvent expirer à des moments différents : autorité procédurale, ressources protégées ou qualité de navigation. L'autonomie sûre s'arrête dès que la première limite est atteinte.

3 — Grandeurs

t_{proc} est l'horizon des procédures et autorités ; $t_{\text{ressource}}$ l'horizon des ressources protégées ; t_{nav} l'horizon de navigation/estimation d'état ; t_{auto} leur minimum.

4 — Formule

$t_{\text{auto}} = \min(t_{\text{proc}}, t_{\text{ressource}}, t_{\text{nav}})$

5 — Lecture

La fenêtre d'autonomie est le minimum des horizons procédure, ressource et navigation.

6 — Symboles et sens

Tous les horizons sont des durées définies pour le même état mission ; le minimum est la première contrainte à expirer.

7 — Prononciation

té auto égale minimum de té procédure, té ressource et té navigation.

8 — Unités

minimum d'heures, heures et heures = heures.

9 — Convention

Les trois horizons doivent être calculés pour le même état mission et la même politique d'autonomie ; perdre la liaison peut dégrader progressivement connaissance et coordination.

10 — Pourquoi cette opération

Une action locale n'est sûre que tant que toutes les contraintes restent valides ; la durée admissible est donc l'horizon le plus court.

11 — Hypothèses

Procédures pré-autorisées, ressources et navigation caractérisées ; aucune nouvelle contrainte plus courte n'apparaît pendant l'intervalle.

12 — Contrôle d'unités

Comparer des durées homogènes conserve une durée.

13 — Cas numérique

18 h de procédure, 30 h de ressources et 12 h de navigation donnent $t_{\text{auto}} = \min(18, 30, 12) = 12$ h.

14 — Pourquoi le calcul fonctionne

À 12 h, la navigation atteint sa limite alors que les deux autres horizons ne sont pas encore épuisés ; continuer au-delà violerait donc une contrainte validée.

15 — Contrôle algébrique

La fenêtre calculée doit être inférieure ou égale à chacun des horizons composants.

16 — Estimation mentale

Parmi 18, 30 et 12 heures, la limite évidente est 12 heures ; aucun calcul complexe n'est nécessaire.

17 — Interprétation

La navigation/estimation d'état limite ici l'autonomie à 12 h malgré une réserve de ressources beaucoup plus longue.

18 — Ce que le résultat ne prouve pas

Il ne prouve pas que les procédures restent adaptées à un état qui évolue, ni que la perte de communication n'ajoute pas une nouvelle contrainte.

19 — Sensibilité

Allonger un horizon non limitant de 30 à 40 h ne change rien tant que la limite de 12 h reste la plus courte.

20 — Exercices guidé et autonome

Exercice guidé. Les horizons valent 10 h, 14 h et 16 h. Déterminer la fenêtre autonome.

Correction guidée

Le minimum est 10 h ; la procédure/autorité est donc la première contrainte.

Exercice autonome. Après mise à jour de navigation, les horizons sont 18 h, 20 h et 24 h. Quelle contrainte devient limitante et quelle fenêtre annoncer ?

Correction autonome

La procédure/autorité à 18 h devient la limite. La fenêtre autonome annoncée est 18 h, avec déclencheur HOLD avant son expiration.

21 — Décision mission

Préautoriser les actions seulement à l'intérieur du plus petit horizon validé et définir un déclencheur HOLD avant son expiration.