

Fiabilité et résilience: prévoir la panne et organiser le retour

Comprendre le problème avant les équations

Question de départ — Fiabilité et résilience: prévoir la panne et organiser le retour: comment « Fiabilité, disponibilité et résilience répondent à des questions différentes » agit-il sur « Lire un MTBF sans lui faire dire l'avenir », et quel repère issu de « La disponibilité montre le rôle de la réparation » permet de vérifier la décision?

Intuition. La fiabilité décrit la probabilité qu'un élément accomplisse sa fonction pendant une durée donnée sous des conditions définies. La disponibilité inclut aussi la capacité à revenir au service après panne.

1

Fiabilité, disponibilité et résilience répondent à des questions différentes

La fiabilité décrit la probabilité qu'un élément accomplisse sa fonction pendant une durée donnée sous des conditions définies.

2

Lire un MTBF sans lui faire dire l'avenir

MTBF signifie Mean Time Between Failures.

3

La disponibilité montre le rôle de la réparation

Un modèle simple utilise $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$.

Repère concret. La disponibilité demande s'il est prêt quand on en a besoin, donc elle dépend aussi de la réparation.

- Fiabilité, disponibilité et résilience répondent à des questions différentes — La fiabilité décrit la probabilité qu'un élément accomplisse sa fonction pendant une durée donnée sous des conditions définies.
- Lire un MTBF sans lui faire dire l'avenir — MTBF signifie Mean Time Between Failures.
- La disponibilité montre le rôle de la réparation — Un modèle simple utilise $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$.

FIABILITÉ D'UNE COLONIE MARTIENNE

Ce qui empêche une petite panne de devenir une grande crise

-  **REDONDANCE**
prévoir une seconde voie
-  **MAINTENANCE**
surveiller, entretenir, anticiper
-  **PIÈCES DE RECHANGE**
tenir un stock critique
-  **FORMATION CROISÉE**
plusieurs personnes savent agir
-  **DOCUMENTATION**
transmettre le savoir et les procédures

 Une colonie échoue rarement d'un seul coup : elle échoue quand plusieurs marges de sécurité disparaissent en même temps.

DELTA - SIERRA • MARS

FIABILITÉ D'UNE COLONIE MARTIENNE

Ce qui empêche une petite panne de devenir une grande crise

-  **REDONDANCE**
prévoir une seconde voie
-  **MAINTENANCE**
surveiller, entretenir, anticiper
-  **PIÈCES DE RECHANGE**
tenir un stock critique
-  **FORMATION CROISÉE**
plusieurs personnes savent agir
-  **DOCUMENTATION**
transmettre le savoir et les procédures

 Une colonie échoue rarement d'un seul coup : elle échoue quand plusieurs marges de sécurité disparaissent en même temps.

DELTA - SIERRA • MARS

La résilience ne consiste pas à promettre zéro panne: elle combine détection, isolement, mode dégradé, réparation et retour maîtrisé au service.



Visualisation conceptuelle d'un retour d'EVA. Conserver la combinaison dans le sas pendant les premières étapes de nettoyage limite l'introduction de **poussière** dans le volume habitable et constitue une barrière supplémentaire contre les erreurs de procédure ou d'étanchéité.



La résilience d'une source critique combine redondance, stockage, modes dégradés et capacité à isoler une panne.

Une mission martienne ne peut pas promettre qu'aucun équipement ne tombera en panne. Elle doit plutôt montrer qu'une panne crédible sera détectée, comprise suffisamment vite, isolée, supportée par un [mode dégradé](#) et réparée avec les ressources disponibles. Ce module distingue fiabilité, disponibilité, [redondance](#), [maintenabilité](#) et résilience, puis les relie à des méthodes de preuve.

RAMPE ZÉRO PRÉREQUIS · MODULE 14

Comprendre avant de décider

Une mission longue ne peut pas supposer que tout fonctionnera. Elle doit continuer à assurer les fonctions vitales lorsqu'un composant, un capteur ou une chaîne entière se dégrade.

Progression du module — défaillance; redondance; mode dégradé; résilience.

défaillance

Définition. Une défaillance est la perte ou la dégradation d'une fonction par rapport au comportement exigé. Elle peut être totale, partielle, intermittente ou latente.

Exemple. Une pompe peut cesser complètement, fournir un [débit](#) insuffisant ou produire des mesures incohérentes avant la panne totale.

Piège. Une anomalie détectée n'est pas toujours une défaillance confirmée; le diagnostic doit distinguer capteur, commande et fonction physique.

Contrôle mental. Distinguez perte complète, performance dégradée et mesure erronée: ces trois états n'entraînent pas le même diagnostic ni le même secours.

Exercice guidé — défaillance

Situation à reconnaître. Une défaillance est la perte ou la dégradation d'une fonction par rapport au comportement exigé. Elle peut être totale, partielle, intermittente ou latente.

Vérification demandée. Distinguez perte complète, performance dégradée et mesure erronée: ces trois états n'entraînent pas le même diagnostic ni le même secours.

Erreur à écarter. Une anomalie détectée n'est pas toujours une défaillance confirmée; le diagnostic doit distinguer capteur, commande et fonction physique.

Corrigé raisonné

Sens précis

Une défaillance est la perte ou la dégradation d'une fonction par rapport au comportement exigé. Elle peut être totale, partielle, intermittente ou latente.

Test du cas

Distinguez perte complète, performance dégradée et mesure erronée: ces trois états n'entraînent pas le même diagnostic ni le même secours.

Piège exclu

Une anomalie détectée n'est pas toujours une défaillance confirmée; le diagnostic doit distinguer capteur, commande et fonction physique.

Conséquence opérationnelle

Dans le cas ce point, l'équipe doit retenir le point suivant: Une anomalie détectée n'est pas toujours une défaillance confirmée; le diagnostic doit distinguer capteur, commande et fonction physique.. Toute violation de cette limite impose de requalifier l'état du système avant de poursuivre.

Quantification

défaillance: relation qualitative ici; aucune unité intrinsèque.

Vérification

défaillance: confronter conclusion, contrôle et piège de la carte.

redondance

Définition. La redondance ajoute plusieurs moyens capables d'assurer une fonction afin qu'une perte ne supprime pas immédiatement le service.

Exemple. Deux pompes indépendantes peuvent permettre de continuer à faire circuler un fluide après la panne de l'une.

Piège. Deux équipements identiques partageant la même alimentation ou le même logiciel peuvent tomber ensemble: la redondance doit traiter les causes communes.

Contrôle mental. Deux équipements identiques ne sont pas réellement redondants s'ils partagent la même alimentation, le même logiciel ou la même cause de défaillance.

Exercice guidé — redondance

Situation à reconnaître. La redondance ajoute plusieurs moyens capables d'assurer une fonction afin qu'une perte ne supprime pas immédiatement le service.

Vérification demandée. Deux équipements identiques ne sont pas réellement redondants s'ils partagent la même alimentation, le même logiciel ou la même cause de défaillance.

Erreur à écarter. Deux équipements identiques partageant la même alimentation ou le même logiciel peuvent tomber ensemble: la redondance doit traiter les causes communes.

Corrigé raisonné

Sens précis

La redondance ajoute plusieurs moyens capables d'assurer une fonction afin qu'une perte ne supprime pas immédiatement le service.

Test du cas

Deux équipements identiques ne sont pas réellement redondants s'ils partagent la même alimentation, le même logiciel ou la même cause de défaillance.

Piège exclu

Deux équipements identiques partageant la même alimentation ou le même logiciel peuvent tomber ensemble: la redondance doit traiter les causes communes.

Conséquence opérationnelle

Le garde-fou associé à ce point est concret: Deux équipements identiques partageant la même alimentation ou le même logiciel peuvent tomber ensemble: la redondance doit traiter les causes communes.. Si ce risque apparaît, la valeur calculée ne doit pas être utilisée seule pour valider la configuration.

mode dégradé

Définition. Un mode dégradé maintient une partie des fonctions avec performances réduites afin de préserver sécurité et capacité de [récupération](#).

Exemple. Après perte d'une boucle de refroidissement, l'équipage peut couper des charges non essentielles pour rester sous la capacité thermique restante.

Piège. Un mode dégradé doit être défini avant la panne; improviser sous pression augmente le risque de surcharge cachée.

Contrôle mental. Supprimez une capacité nominale et vérifiez que les fonctions vitales restantes ont encore des ressources, une durée et des critères de sortie explicitement connus.

Exercice guidé — mode dégradé

Situation à reconnaître. Un mode dégradé maintient une partie des fonctions avec performances réduites afin de préserver sécurité et capacité de récupération.

Vérification demandée. Supprimez une capacité nominale et vérifiez que les fonctions vitales restantes ont encore des ressources, une durée et des critères de sortie explicitement connus.

Erreur à écarter. Un mode dégradé doit être défini avant la panne; improviser sous pression augmente le risque de surcharge cachée.

Corrigé raisonné

Sens précis

Un mode dégradé maintient une partie des fonctions avec performances réduites afin de préserver sécurité et capacité de récupération.

Test du cas

Supprimez une capacité nominale et vérifiez que les fonctions vitales restantes ont encore des ressources, une durée et des critères de sortie explicitement connus.

Piège exclu

Un mode dégradé doit être défini avant la panne; improviser sous pression augmente le risque de surcharge cachée.

Conséquence opérationnelle

Dans le cas ce point, l'équipe doit retenir le point suivant: Un mode dégradé doit être défini avant la panne; improviser sous pression augmente le risque de surcharge cachée.. Toute violation de cette limite impose de requalifier l'état du système avant de poursuivre.

Quantification

mode dégradé: relation qualitative ici; aucune unité intrinsèque.

Vérification

mode dégradé: confronter conclusion, contrôle et piège de la carte.

résilience

Définition. La résilience est la capacité d'un système à absorber une perturbation, continuer une mission acceptable, se reconfigurer et restaurer progressivement ses fonctions.

Exemple. Une architecture résiliente combine détection, isolation, réserve, procédures et moyens de réparation.

Piège. Résilience ne signifie pas invulnérabilité: elle dépend des scénarios et des ressources réellement disponibles.

Contrôle mental. Après la panne, demandez non seulement si le système survit mais s'il peut diagnostiquer, se reconfigurer et retrouver un état durable sans consommer toutes ses réserves.

Exercice guidé — résilience

Situation à reconnaître. La résilience est la capacité d'un système à absorber une perturbation, continuer une mission acceptable, se reconfigurer et restaurer progressivement ses fonctions.

Vérification demandée. Après la panne, demandez non seulement si le système survit mais s'il peut diagnostiquer, se reconfigurer et retrouver un état durable sans consommer toutes ses réserves.

Erreur à écarter. Résilience ne signifie pas invulnérabilité: elle dépend des scénarios et des ressources réellement disponibles.

Corrigé raisonné

Sens précis

La résilience est la capacité d'un système à absorber une perturbation, continuer une mission acceptable, se reconfigurer et restaurer progressivement ses fonctions.

Test du cas

Après la panne, demandez non seulement si le système survit mais s'il peut diagnostiquer, se reconfigurer et retrouver un état durable sans consommer toutes ses réserves.

Piège exclu

Résilience ne signifie pas invulnérabilité: elle dépend des scénarios et des ressources réellement disponibles.

Conséquence opérationnelle

Dans le cas ce point, l'équipe doit retenir le point suivant: Résilience ne signifie pas invulnérabilité: elle dépend des scénarios et des ressources réellement disponibles.. Toute violation de cette limite impose de requalifier l'état du système avant de poursuivre.

Mini-leçons quantitatives canoniques

Ce bloc constitue la référence quantitative du module; les valeurs d'exercice sont pédagogiques et ne doivent pas être confondues avec des données de mission.

Fiabilité sous taux de défaillance constant

$$R = \exp(-\lambda \times t)$$

1 — Question concrète

Que permet de calculer « $R = \exp(-\lambda \times t)$ » dans « Fiabilité sous taux de défaillance constant » ?

2 — Intuition sans symboles

Quand un risque instantané reste constant, la probabilité de survivre décroît progressivement avec le temps.

3 — Grandeurs

R: probabilité de survie sans défaillance; λ : taux de défaillance constant; t: durée

4 — Formule

$$R = \exp(-\lambda \times t)$$

5 — Lecture

Lire « $R = \exp(-\lambda \times t)$ » en nommant chaque opération et chaque indice.

6 — Symboles et sens

R: probabilité de survie sans défaillance; λ : taux de défaillance constant; t: durée

7 — Prononciation

Dire explicitement les indices, puissances, lettres grecques et parenthèses afin de reconstruire la relation sans voir la page.

8 — Unités

R sans dimension; λ en 1/h; t en h

9 — Convention

Conserver le même repère, la même base de temps, la même frontière de système et la même convention de signe pendant toute la substitution.

10 — Pourquoi cette opération

La loi exponentielle traduit une évolution proportionnelle à l'état restant et non une diminution linéaire par pas constant.

11 — Hypothèses

Le paramètre de taux est supposé constant sur l'intervalle et les événements sont modélisés selon l'hypothèse annoncée.

12 — Contrôle d'unités

R sans dimension; λ en 1/h; t en h Vérifier que la simplification dimensionnelle conduit bien à l'unité de la grandeur recherchée.

13 — Cas numérique

Avec $\lambda = 0,0005$ 1/h et $t = 1\,000$ h, $R = \exp(-0,5) \approx 0,6065$.

14 — Pourquoi le calcul fonctionne

La loi exponentielle traduit une évolution proportionnelle à l'état restant et non une diminution linéaire par pas constant.

15 — Contrôle indépendant

Le logarithme naturel du résultat permet de revenir au produit taux $\times$ durée.

16 — Estimation mentale

Un petit produit taux $\times$ durée implique un résultat proche de un; un produit grand l'éloigne rapidement de un.

17 — Interprétation

Cette probabilité décrit le modèle choisi, pas l'avenir certain d'un composant particulier.

18 — Ce que le résultat ne prouve pas

Le calcul ne prouve ni que les entrées sont justes ni que le modèle reste valide hors du scénario déclaré; ces deux questions doivent être vérifiées séparément.

19 — Sensibilité

L'effet du temps et du taux se cumule dans leur produit, puis l'exponentielle amplifie la différence.

20 — Exercices guidé et autonome

Exercice guidé. $\lambda = 0,0002$ 1/h et $t = 500$ h.

Correction guidée détaillée — ouvrir après essai

$\lambda = 0,0002$ 1/h et $t = 500$ h. $R = \exp(-0,10) \approx 0,9048$.

Exercice autonome. $\lambda = 0,001$ 1/h et $t = 200$ h.

Correction autonome — ouvrir après essai

$\lambda = 0,001$ 1/h et $t = 200$ h. $R = \exp(-0,20) \approx 0,8187$.

21 — Décision mission

Utiliser cette loi seulement si l'hypothèse de taux approximativement constant est défendable sur la phase étudiée.

Disponibilité intrinsèque

$$A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

1 — Question concrète

Que permet de calculer « $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$ » dans « Disponibilité intrinsèque » ?

2 — Intuition sans symboles

La disponibilité augmente quand les périodes de service sont longues et les réparations courtes.

3 — Grandeurs

A: disponibilité; MTBF: temps moyen entre défaillances; MTTR: temps moyen de réparation

4 — Formule

$$A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

5 — Lecture

Lire « $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$ » en nommant chaque opération et chaque indice.

6 — Symboles et sens

A: disponibilité; MTBF: temps moyen entre défaillances; MTTR: temps moyen de réparation

7 — Prononciation

Dire explicitement les indices, puissances, lettres grecques et parenthèses afin de reconstruire la relation sans voir la page.

8 — Unités

A sans dimension; MTBF et MTTR dans la même unité de temps

9 — Convention

Conserver le même repère, la même base de temps, la même frontière de système et la même convention de signe pendant toute la substitution.

10 — Pourquoi cette opération

La division compare une quantité à une référence homogène et produit un indicateur de proportion.

11 — Hypothèses

Les deux quantités doivent appartenir au même périmètre et à la même période.

12 — Contrôle d'unités

A sans dimension; MTBF et MTTR dans la même unité de temps Vérifier que la simplification dimensionnelle conduit bien à l'unité de la grandeur recherchée.

13 — Cas numérique

Avec $\text{MTBF} = 1\,000$ h et $\text{MTTR} = 10$ h, $A = 1\,000 / 1\,010 \approx 0,9901$, soit 99,01 %.

14 — Pourquoi le calcul fonctionne

La division compare une quantité à une référence homogène et produit un indicateur de proportion.

15 — Contrôle indépendant

Multiplier le résultat par le dénominateur doit restituer le numérateur.

16 — Estimation mentale

Avant calcul, comparer mentalement le numérateur au dénominateur pour savoir si le résultat doit être inférieur, proche ou supérieur à un.

17 — Interprétation

La formule montre directement pourquoi la maintenabilité peut compenser partiellement une fréquence de panne donnée.

18 — Ce que le résultat ne prouve pas

Le calcul ne prouve ni que les entrées sont justes ni que le modèle reste valide hors du scénario déclaré; ces deux questions doivent être vérifiées séparément.

19 — Sensibilité

Le résultat augmente si le numérateur augmente et diminue si le dénominateur augmente, toutes choses égales par ailleurs.

20 — Exercices guidé et autonome

Exercice guidé. MTBF = 500 h et MTTR = 5 h.

Correction guidée détaillée — ouvrir après essai

MTBF = 500 h et MTTR = 5 h. $A = 500/505 \approx 0,9901 = 99,01 \%$.

Exercice autonome. MTBF = 800 h et MTTR = 20 h.

Correction autonome — ouvrir après essai

MTBF = 800 h et MTTR = 20 h. $A = 800/820 \approx 0,9756 = 97,56 \%$.

21 — Décision mission

Comparer l'intrinsèque à l'opérationnel en ajoutant séparément les délais logistiques et administratifs.

Fiabilité d'une chaîne en série

$R_{\text{series}} = R_1 \times R_2 \times R_3$

1 — Question concrète

Que permet de calculer « $R_{\text{series}} = R_1 \times R_2 \times R_3$ » dans « Fiabilité d'une chaîne en série » ?

2 — Intuition sans symboles

Dans une chaîne où chaque élément est indispensable, il faut que tous survivent pour que la fonction survive.

3 — Grandeurs

R_{series} : fiabilité de la chaîne; R_1 : fiabilité du premier élément; R_2 : fiabilité du deuxième; R_3 : fiabilité du troisième

4 — Formule

$R_{\text{series}} = R_1 \times R_2 \times R_3$

5 — Lecture

Lire « $R_{\text{series}} = R_1 \times R_2 \times R_3$ » en nommant chaque opération et chaque indice.

6 — Symboles et sens

R_{series} : fiabilité de la chaîne; R_1 : fiabilité du premier élément; R_2 : fiabilité du deuxième; R_3 : fiabilité du troisième

7 — Prononciation

Dire explicitement les indices, puissances, lettres grecques et parenthèses afin de reconstruire la relation sans voir la page.

8 — Unités

toutes les fiabilités sans dimension

9 — Convention

Conserver le même repère, la même base de temps, la même frontière de système et la même convention de signe pendant toute la substitution.

10 — Pourquoi cette opération

La multiplication transforme un taux ou une grandeur spécifique en quantité totale sur l'intervalle ou la population considérée.

11 — Hypothèses

Les facteurs doivent décrire le même scénario et leurs unités doivent être compatibles.

12 — Contrôle d'unités

toutes les fiabilités sans dimension Vérifier que la simplification dimensionnelle conduit bien à l'unité de la grandeur recherchée.

13 — Cas numérique

Avec $R_1 = 0,99$, $R_2 = 0,98$ et $R_3 = 0,97$, $R_{\text{series}} = 0,99 \times 0,98 \times 0,97 \approx 0,9411$.

14 — Pourquoi le calcul fonctionne

La multiplication transforme un taux ou une grandeur spécifique en quantité totale sur l'intervalle ou la population considérée.

15 — Contrôle indépendant

Diviser le résultat par un facteur non nul doit retrouver l'autre facteur.

16 — Estimation mentale

Estimer séparément l'ordre de grandeur de chaque facteur permet de prévoir celui du produit.

17 — Interprétation

Même de très bons composants peuvent former une chaîne nettement moins fiable si tous sont obligatoires.

18 — Ce que le résultat ne prouve pas

Le calcul ne prouve ni que les entrées sont justes ni que le modèle reste valide hors du scénario déclaré; ces deux questions doivent être vérifiées séparément.

19 — Sensibilité

À facteurs indépendants, une variation relative d'un facteur se transmet directement au produit.

20 — Exercices guidé et autonome

Exercice guidé. $R_1 = 0,995$, $R_2 = 0,990$, $R_3 = 0,985$.

Correction guidée détaillée — ouvrir après essai

$R_1 = 0,995$, $R_2 = 0,990$, $R_3 = 0,985$. $R_{\text{series}} \approx 0,9703$.

Exercice autonome. $R_1 = R_2 = R_3 = 0,95$.

Correction autonome — ouvrir après essai

$R_1 = R_2 = R_3 = 0,95$. $R_{\text{series}} = 0,95^3 \approx 0,8574$.

21 — Décision mission

Identifier les éléments réellement en série avant de multiplier des probabilités.

Redondance de deux unités indépendantes

$$R_{\text{parallel}} = 1 - (1 - R_{\text{unit}})^2$$

1 — Question concrète

Que permet de calculer « $R_{\text{parallel}} = 1 - (1 - R_{\text{unit}})^2$ » dans « Redondance de deux unités indépendantes » ?

2 — Intuition sans symboles

Deux unités indépendantes permettent à la fonction de survivre tant qu'au moins une reste disponible.

3 — Grandeurs

R_{parallel} : fiabilité de la fonction redondante; R_{unit} : fiabilité d'une unité identique

4 — Formule

$$R_{\text{parallel}} = 1 - (1 - R_{\text{unit}})^2$$

5 — Lecture

Lire « $R_{\text{parallel}} = 1 - (1 - R_{\text{unit}})^2$ » en nommant chaque opération et chaque indice.

6 — Symboles et sens

R_{parallel} : fiabilité de la fonction redondante; R_{unit} : fiabilité d'une unité identique

7 — Prononciation

Dire explicitement les indices, puissances, lettres grecques et parenthèses afin de reconstruire la relation sans voir la page.

8 — Unités

fiabilités sans dimension

9 — Convention

Conserver le même repère, la même base de temps, la même frontière de système et la même convention de signe pendant toute la substitution.

10 — Pourquoi cette opération

La relation met en équation le mécanisme quantitatif décrit par la mini-leçon et permet de vérifier le raisonnement par substitution numérique.

11 — Hypothèses

Les entrées doivent provenir du même scénario, avec unités, signes et conventions explicitement alignés.

12 — Contrôle d'unités

fiabilités sans dimension Vérifier que la simplification dimensionnelle conduit bien à l'unité de la grandeur recherchée.

13 — Cas numérique

Avec $R_{\text{unit}} = 0,90$, $R_{\text{parallel}} = 1 - 0,10^2 = 0,99$.

14 — Pourquoi le calcul fonctionne

La relation met en équation le mécanisme quantitatif décrit par la mini-leçon et permet de vérifier le raisonnement par substitution numérique.

15 — Contrôle indépendant

Recalculer par la relation inverse ou par une seconde méthode doit retrouver le même ordre de grandeur.

16 — Estimation mentale

Un ordre de grandeur estimé avant la calculatrice permet de détecter les erreurs de facteur, de signe ou d'unité.

17 — Interprétation

Le gain disparaît si une cause commune peut rendre les deux unités indisponibles simultanément.

18 — Ce que le résultat ne prouve pas

Le calcul ne prouve ni que les entrées sont justes ni que le modèle reste valide hors du scénario déclaré; ces deux questions doivent être vérifiées séparément.

19 — Sensibilité

Faire varier une entrée à la fois permet d'identifier la variable qui pilote le plus la décision.

20 — Exercices guidé et autonome

Exercice guidé. $R_{\text{unit}} = 0,95$.

Correction guidée détaillée — ouvrir après essai

$R_{\text{unit}} = 0,95$. $R_{\text{parallel}} = 1 - 0,05^2 = 0,9975$.

Exercice autonome. $R_{\text{unit}} = 0,80$.

Correction autonome — ouvrir après essai

$R_{\text{unit}} = 0,80$. $R_{\text{parallel}} = 1 - 0,20^2 = 0,96$.

21 — Décision mission

Valider l'indépendance physique, fonctionnelle et procédurale avant de créditer le gain de redondance.

Capacité restante après perte

$C_{\text{remaining}} = C_{\text{nominal}} - C_{\text{lost}}$

1 — Question concrète

Que permet de calculer « $C_{\text{remaining}} = C_{\text{nominal}} - C_{\text{lost}}$ » dans « Capacité restante après perte » ?

2 — Intuition sans symboles

La résilience opérationnelle se mesure souvent par le service qui reste après une panne, pas seulement par le fait que la panne existe.

3 — Grandeurs

C_remaining: capacité encore utilisable; C_nominal: capacité nominale; C_lost: capacité perdue ou indisponible

4 — Formule

$$C_{\text{remaining}} = C_{\text{nominal}} - C_{\text{lost}}$$

5 — Lecture

Lire « $C_{\text{remaining}} = C_{\text{nominal}} - C_{\text{lost}}$ » en nommant chaque opération et chaque indice.

6 — Symboles et sens

C_remaining: capacité encore utilisable; C_nominal: capacité nominale; C_lost: capacité perdue ou indisponible

7 — Prononciation

Dire explicitement les indices, puissances, lettres grecques et parenthèses afin de reconstruire la relation sans voir la page.

8 — Unités

les trois capacités dans la même unité opérationnelle

9 — Convention

Conserver le même repère, la même base de temps, la même frontière de système et la même convention de signe pendant toute la substitution.

10 — Pourquoi cette opération

La soustraction isole la marge ou la variation entre deux grandeurs exprimées sur la même base.

11 — Hypothèses

Les deux termes doivent utiliser le même repère, la même unité et la même frontière de système.

12 — Contrôle d'unités

les trois capacités dans la même unité opérationnelle Vérifier que la simplification dimensionnelle conduit bien à l'unité de la grandeur recherchée.

13 — Cas numérique

Avec $C_{\text{nominal}} = 12$ unités/h et $C_{\text{lost}} = 4$ unités/h, $C_{\text{remaining}} = 8$ unités/h.

14 — Pourquoi le calcul fonctionne

La soustraction isole la marge ou la variation entre deux grandeurs exprimées sur la même base.

15 — Contrôle indépendant

Ajouter la différence au terme retiré doit restituer le terme initial.

16 — Estimation mentale

Comparer les deux termes suffit à prévoir le signe et l'ordre de grandeur de la différence.

17 — Interprétation

Cette marge doit être comparée au besoin minimal du mode dégradé.

18 — Ce que le résultat ne prouve pas

Le calcul ne prouve ni que les entrées sont justes ni que le modèle reste valide hors du scénario déclaré; ces deux questions doivent être vérifiées séparément.

19 — Sensibilité

Une hausse du premier terme augmente le résultat; une hausse du second le diminue à pente unitaire.

20 — Exercices guidé et autonome

Exercice guidé. $C_{\text{nominal}} = 20$ kW et $C_{\text{lost}} = 6$ kW.

Correction guidée détaillée — ouvrir après essai

$C_{\text{nominal}} = 20$ kW et $C_{\text{lost}} = 6$ kW. $C_{\text{remaining}} = 20 - 6 = 14$ kW.

Exercice autonome. $C_{\text{nominal}} = 50$ L/h et $C_{\text{lost}} = 15$ L/h.

Correction autonome — ouvrir après essai

$C_{\text{nominal}} = 50$ L/h et $C_{\text{lost}} = 15$ L/h. $C_{\text{remaining}} = 50 - 15 = 35$ L/h.

21 — Décision mission

Basculer en mode sûr si la capacité restante ne couvre plus la fonction vitale minimale.

Progression

1. Définir les notions.
2. Identifier les informations nécessaires.
3. Appliquer un critère simple.
4. Introduire une panne ou une information fausse.
5. Décider sous contrainte avec justification.

Gate zéro prérequis

- Je sais expliquer les rôles et les critères.
- Je sais distinguer observation et interprétation.
- Je peux calculer une **marge** simple.
- Je sais annoncer la limite qui ferait interrompre ou modifier une décision concernant « Comprendre avant de décider ».

1. Fiabilité, disponibilité et résilience répondent à des questions différentes

La **fiabilité** décrit la **probabilité** qu'un élément accomplisse sa fonction pendant une durée donnée sous des conditions définies. La **disponibilité** inclut aussi la capacité à revenir au service après panne. La **résilience** ajoute l'idée de conserver une mission acceptable malgré perturbation, dégradation et récupération. Un système peut être peu fiable mais rapidement réparable, ou très fiable mais catastrophique lorsqu'il échoue.

La fiabilité décrit la probabilité qu'un élément accomplisse sa fonction pendant une durée et dans des conditions données. La disponibilité demande s'il est prêt quand on en a besoin, donc elle dépend aussi de la réparation. La résilience va plus loin: peut-on préserver une fonction essentielle, se reconfigurer puis revenir vers un état durable après l'événement? Un système peut être très fiable mais peu résilient si une panne rare est irréparable. À l'inverse, un équipement qui tombe plus souvent en panne peut offrir un excellent service si la détection est rapide, les pièces accessibles et le mode dégradé acceptable. Ces trois mots doivent donc rester séparés dans les exigences et les calculs.

2. Lire un MTBF sans lui faire dire l'avenir

MTBF signifie Mean Time Between Failures. Il décrit une statistique de population sous un modèle et un domaine d'utilisation. Ce n'est pas la date de mort d'une pièce. Dans un modèle exponentiel, un taux constant λ donne $R(t)=e^{-\lambda t}$. Cette hypothèse ignore le rodage et l'usure; elle doit donc être utilisée avec prudence.

Le MTBF, mean time between failures, est une statistique de population ou de modèle, pas une date de décès d'un composant particulier. Sous une hypothèse **exponentielle** simplifiée à taux de panne constant λ , la fiabilité vaut $R(t)=e^{-\lambda t}$ et $MTBF=1/\lambda$. Un MTBF de 10 000 h ne signifie pas que l'équipement fonctionnera 10 000 h puis cassera. Il signifie que le modèle attribue un certain taux d'événements sur une population. Pour Mars, l'hypothèse de taux constant peut être mauvaise en présence d'usure, radiation, poussière ou cycles thermiques. Le chiffre doit toujours être accompagné du domaine d'essai et de l'incertitude.

3. La disponibilité montre le rôle de la réparation

Un modèle simple utilise $A = MTBF/(MTBF+MTTR)$. **MTTR** est le temps moyen de réparation. Avec 1 000 h de MTBF et 10 h de MTTR, $A \approx 1\,000/1\,010 \approx 0,990$. Si le MTTR tombe à 2 h, la disponibilité augmente sans modifier le taux de panne.

Exercice A — disponibilité

Calculez A pour MTBF = 500 h et MTTR = 5 h.

$A = 500/(500+5) = 500/505 \approx 0,9901$, soit environ 99,01 %. Le chiffre n'inclut les délais logistiques que si la définition de MTTR les inclut.

Données du cas

Exercice A — disponibilité — Calculez A pour MTBF = 500 h et MTTR = 5 h.

Relation

$A = 500/(500+5) = 500/505 \approx 0,9901$, soit environ 99,01 %.

Raisonnement

$A = 500/(500+5) = 500/505 \approx 0,9901$, soit environ 99,01 %. Le chiffre n'inclut les délais logistiques que si la définition de MTTR les inclut.

Résultat

$A = 500/(500+5) = 500/505 \approx 0,9901$, soit environ 99,01 %.

Interprétation

Le chiffre n'inclut les délais logistiques que si la définition de MTTR les inclut.

Une approximation courante de disponibilité intrinsèque est $A = \text{MTBF}/(\text{MTBF} + \text{MTTR})$. Si MTBF = 1 000 h et MTTR = 10 h, $A \approx 1\,000/1\,010 = 0,990$, soit 99,0 %. Réduire le MTTR à 2 h donne environ 99,8 % sans changer la fréquence de panne. Le calcul montre pourquoi accès, diagnostic, outillage et test après réparation peuvent être aussi importants qu'une amélioration de fiabilité composant. Mais cette formule suppose notamment des réparations possibles et ne représente pas automatiquement logistique de rechanges, attente d'EVA, causes communes ou files de maintenance. Il faut savoir ce que l'indicateur exclut.

4. FMEA et FMECA parcourent les modes de défaillance

Une FMEA demande: comment ce composant ou cette fonction peut-il échouer, quel est l'effet local, quel est l'effet système et comment détecter la panne? La FMECA ajoute une appréciation de criticité. L'intérêt est de rendre visibles les pannes simples, les points critiques et les besoins de détection ou de maintenance.

Une FMEA parcourt les fonctions ou composants et demande: comment cela peut-il échouer, quel effet local puis système, comment le détecter et quelle action limite la conséquence? La FMECA ajoute une notion de criticité. La valeur n'est pas dans le tableau lui-même mais dans la découverte d'interfaces cachées et de modes non couverts. Une ligne 'capteur faux' doit par exemple préciser si la panne est détectée, si le logiciel peut croire la mesure et quel actionneur sera commandé. Pour un habitat martien, la FMEA doit aussi inclure maintenance, logiciel, erreur humaine et défaillances après réparation, sinon elle décrit seulement le matériel neuf.

5. L'arbre de défaillance raisonne depuis l'événement redouté

Un Fault Tree Analysis part d'un événement comme « perte de pressurisation » et remonte vers les combinaisons possibles. Des portes logiques ET/OU aident à représenter les chemins. L'arbre ne remplace pas l'ingénierie physique: deux événements peuvent être corrélés même si le schéma les dessine séparément.

L'arbre de défaillance part d'un événement redouté et remonte vers les combinaisons de causes. Une porte OR signifie qu'une cause parmi plusieurs suffit; une porte AND exige une combinaison. Ce raisonnement est particulièrement utile pour les causes communes. Deux pompes peuvent sembler redondantes, mais si la perte de leur alimentation unique suffit à perdre le débit, l'arbre révèle que la branche commune domine. Les probabilités peuvent être ajoutées lorsque les hypothèses d'indépendance sont crédibles, mais l'intérêt premier reste logique: montrer quelles combinaisons rendent la fonction indisponible et où une séparation physique, électrique ou logicielle change réellement le résultat.

6. La redondance n'est utile que si les causes sont séparées

Deux pompes sur le même bus, deux ordinateurs avec le même bug ou deux capteurs affectés par la même contamination peuvent échouer ensemble. La revue doit chercher alimentation, refroidissement, logiciel, connecteurs, calibration, environnement et procédure communs.

Exercice B — vraie ou fausse indépendance



L'éloignement limite certaines conséquences mais ajoute câbles, conversion, maintenance et dépendances de distribution: la résilience se juge sur toute la chaîne.

Deux calculateurs identiques utilisent deux alimentations séparées mais le même logiciel. Citez une **cause commune** encore présente.

Un défaut logiciel ou une erreur commune de **configuration** peut affecter simultanément les deux calculateurs malgré les alimentations séparées.

Données du cas

Exercice B — vraie ou fausse indépendance — L'éloignement limite certaines conséquences mais ajoute câbles, conversion, maintenance et dépendances de distribution: la résilience se juge sur toute la chaîne. Deux calculateurs identiques utilisent deux alimentations séparées mais le même logiciel. Citez une cause commune encore présente.

Raisonnement

Un défaut logiciel ou une erreur commune de configuration peut affecter simultanément les deux calculateurs malgré les alimentations séparées.

Résultat

Un défaut logiciel ou une erreur commune de configuration peut affecter simultanément les deux calculateurs malgré les alimentations séparées.

Interprétation

Un défaut logiciel ou une erreur commune de configuration peut affecter simultanément les deux calculateurs malgré les alimentations séparées.

La redondance ne vaut que si les voies possèdent assez d'indépendance. Deux calculateurs dans le même boîtier peuvent partager alimentation, **température**, connecteur, logiciel et erreur de configuration. Une panne commune peut donc supprimer les deux. La diversité peut porter sur le matériel, le logiciel, le principe de mesure ou la localisation. Elle a cependant un coût de validation et de maintenance. La question de revue n'est pas « combien d'unités ? » mais 'quelles causes peuvent encore les perdre ensemble?'. Pour une colonie, il faut aussi considérer la capacité de réparation: deux unités non réparables peuvent être moins résilientes qu'une unité robuste soutenue par des modules remplaçables et un bypass.

7. FDIR: détecter, isoler, récupérer

Détection: reconnaître une incohérence. Isolation: estimer la cause ou au moins la zone fautive. Récupération: choisir un état sûr ou une reconfiguration. Le temps disponible change selon la panne. Une fuite lente peut permettre un diagnostic long; un défaut de contrôle d'attitude peut exiger une réaction automatique rapide.

FDIR signifie Fault Detection, Isolation and Recovery: détecter qu'un comportement sort du domaine attendu, isoler la cause ou au moins la zone fautive, puis récupérer une fonction sûre. Chaque étape peut échouer. Une alarme trop sensible crée des faux positifs; une isolation trop agressive peut couper le seul équipement sain; une récupération automatique peut réintroduire la panne. Les preuves doivent donc être graduées. Un premier seuil peut demander confirmation par une mesure indépendante, un second basculer en mode dégradé, puis une vérification autoriser le retour. L'objectif n'est pas d'automatiser toute décision mais de garantir que l'état reste compréhensible et contrôlable pendant l'anomalie.

8. Safe mode ne signifie pas tout éteindre

Un mode de sauvegarde conserve les fonctions qui empêchent l'état de se dégrader: énergie, thermique, attitude, communications et parfois [support-vie](#). Il doit être stable assez longtemps pour analyser. S'il consomme une ressource plus vite qu'on ne peut intervenir, il n'est pas réellement sûr.

Un safe mode est une configuration stable conçue pour préserver des ressources et éviter l'escalade. Il ne signifie pas 'tout éteindre'. Un vaisseau doit continuer à produire de l'énergie, contrôler certaines températures, maintenir une attitude compatible avec panneaux et communications et protéger l'équipage. Le safe mode doit donc avoir ses propres exigences de [puissance](#), capteurs, actionneurs et durée. S'il dépend d'un composant qui vient justement de tomber en panne, il n'est pas un vrai refuge. La validation injecte des fautes et vérifie que le système atteint ce mode avec les ressources réellement restantes, puis qu'il existe une voie de diagnostic et de récupération.

9. La maintenabilité se conçoit dans la géométrie

Une pièce accessible, testable, isolable et munie de connecteurs remplaçables peut réduire énormément le temps de restauration. À l'inverse, un composant « redondant » derrière des éléments qu'il faut démonter pendant deux jours peut transformer une petite panne en indisponibilité majeure.

La maintenabilité se dessine avant la panne. Temps d'accès, masse d'un panneau, connecteurs, volumes de travail, outils, points de test, isolation électrique et nécessité d'une EVA peuvent dominer le MTTR. Une pièce facilement remplaçable sur banc peut devenir impraticable lorsqu'elle est installée derrière deux conduites. Le design doit donc simuler l'intervention avec l'outillage et les gants prévus, puis inclure le temps de remise en configuration et de vérification. Sur Mars, une réparation locale peut aussi créer une nouvelle configuration qui doit être tracée. La résilience dépend autant de la capacité à prouver le retour en service que du geste mécanique lui-même.

10. Scénario: deux pannes indépendantes deviennent une panne commune par procédure

Une première panne conduit l'équipage à reconfigurer deux services sur un même bus de secours. Une seconde panne du bus supprime alors les deux services. Le couplage n'existait pas au départ; il a été créé par la récupération. Les analyses de résilience doivent donc examiner les configurations dégradées, pas seulement l'architecture nominale.

Deux pannes indépendantes peuvent devenir une panne commune par la procédure. Si l'équipe utilise le même mauvais fichier de configuration pour remplacer deux contrôleurs, la duplication matérielle n'aide plus. De même, une [checklist](#) ambiguë peut conduire deux opérateurs à isoler la même mauvaise vanne. La fiabilité humaine et organisationnelle doit donc être intégrée aux analyses. Les procédures critiques exigent des critères observables, des confirmations indépendantes lorsque l'action est irréversible et une gestion de version. Le retour d'expérience doit modifier le document contrôlé sans effacer l'historique, afin qu'une erreur corrigée ne réapparaisse quelques mois plus tard sur un autre système.

Étude guidée — deux architectures de pompe

Architecture A possède deux pompes identiques en parallèle; architecture B une pompe active, un bypass à 60 % de débit et trois modules facilement remplaçables. À première vue, A semble plus redondante. Mais si les deux pompes A partagent un seul contrôleur et une seule alimentation, une cause commune peut supprimer les deux. B peut au contraire conserver 60 % du service pendant huit heures, assez pour remplacer un module en deux heures et le tester avant remise en ligne.

Le calcul de disponibilité ne suffit pas à lui seul. Il faut dérouler la séquence: temps de détection, stabilisation, accès, réparation, essai et reprise. Un MTTR annoncé de 30 minutes sur banc peut devenir quatre heures dans l'habitat si l'accès exige [dépressurisation](#) d'une zone ou déplacement d'équipements.

L'exercice final demande quel changement apporte le plus de résilience: troisième pompe identique, seconde alimentation, bypass manuel, diagnostic indépendant ou meilleure accessibilité. La réponse dépend de la cause dominante révélée par l'arbre de défaillance, pas du nombre brut de composants.

11. Mini-projet: construire un dossier de résilience

1. Choisissez une fonction vitale.
2. Définissez son événement redouté.
3. Listez cinq modes de panne.
4. Identifiez les causes communes.
5. Décrivez détection, mode dégradé et réparation.
6. Calculez un indicateur simple de disponibilité.
7. Ajoutez une seconde panne pendant le mode dégradé.

Le dossier est bon si l'on comprend ce qui reste possible après la première panne et comment le service revient.

12. Atelier mission — comparer redondance et réparabilité

Considérons deux architectures pédagogiques. L'architecture A possède deux pompes identiques non réparables, chacune capable de fournir tout le débit. L'architecture B possède une seule pompe en service mais trois modules facilement remplaçables et un bypass manuel. Laquelle est « plus fiable »? La question est incomplète. Il faut connaître taux de panne, causes communes, temps de remplacement, stock, durée acceptable sans circulation et capacité du bypass.

Si le remplacement d'un module prend 2 h et que le mode bypass maintient 60 % du débit pendant 8 h, B peut avoir une excellente résilience même avec moins de redondance instantanée. À l'inverse, si les deux pompes A partagent le même contrôleur, leur duplication ne protège pas d'une panne commune. La résilience se juge sur la séquence complète de l'événement.

Un bon dossier décrit aussi le **temps de détection**, le **temps de stabilisation**, le **temps de réparation** et le **temps de vérification**. Additionner seulement le temps passé à tourner une clé sous-estime le MTTR opérationnel.

13. Limites des probabilités et importance de la preuve physique

Des probabilités très précises peuvent donner une impression scientifique même lorsque leurs entrées sont fragiles. Les données terrestres ne représentent pas toujours poussière, radiation, faible gravité, longues périodes sans maintenance spécialisée ou configurations martiennes. Les modèles probabilistes doivent donc être accompagnés d'essais, inspection, compréhension physique des mécanismes de panne et retour d'expérience.

Un chiffre de fiabilité est utile s'il change une décision: ajouter une indépendance, rendre une pièce accessible, augmenter un stock, modifier un intervalle d'inspection ou créer un mode dégradé. S'il n'a aucune conséquence de conception ou d'exploitation, il risque de devenir un indicateur décoratif.

Sources et références

Calculateurs associés

Mettre en pratique ce module avec:

- [Calculateur de disponibilité et rechanges](#)

- [NASA SMA — Reliability and Maintainability](#)
- [NASA GSFC-HDBK-8004 — FMECA](#)
- [NASA-STD-8729.1 — Reliability and Maintainability](#)

Complément primaire vérifié: [NASA Systems Engineering Handbook](#)

Studio d'ingénierie — comparer deux architectures de disponibilité

Pour une loi exponentielle simple, la fiabilité sans réparation pendant une durée t s'écrit $R(t)=\exp(-t/MTBF)$. Avec $MTBF = 1\,500\text{ h}$ et $t = 500\text{ h}$, $R \approx \exp(-1/3) \approx 0,716$. Deux chaînes réellement indépendantes en parallèle donneraient alors une probabilité théorique d'en conserver au moins une de $1-(1-R)^2 \approx 0,919$. Ce calcul pédagogique montre à la fois le gain de redondance et l'importance de l'hypothèse d'indépendance.

Le piège final est une cause commune: les deux chaînes redondantes partagent la même alimentation. L'élève doit expliquer pourquoi deux équipements identiques ne forment plus une vraie redondance si une seule panne peut les supprimer ensemble. Il doit proposer un changement architectural — séparation électrique, diversité ou [refuge](#) fonctionnel — et définir l'essai qui démontrera que la cause commune a réellement été rompue.

Matrice de parité FR ↔ EN

FR	EN
Fiabilité sous taux de défaillance constant	Reliability with a constant failure rate
Disponibilité intrinsèque	Intrinsic availability
Fiabilité d'une chaîne en série	Reliability of a series chain
Redondance de deux unités indépendantes	Two-unit independent redundancy
Capacité restante après perte	Remaining capacity after a loss

Termes de la progression. [défaillance](#)