

## Résilience aux défaillances multiples: reconfiguration et retour au service

 Systèmes de fiabilité, maintenance et résilience d'une implantation martienne.

Illustration système premium — la résilience dépend de la redondance, de la maintenance, des pièces de rechange, de la polyvalence et d'une reconfiguration maîtrisée.

Raisonner lorsque deux ou trois pannes se combinent, épuisent les redondances et imposent de reconstruire progressivement un service sûr.

## Comprendre le problème avant les équations

Question de départ — Résilience aux défaillances multiples: reconfiguration et retour au service: comment « Panne primaire et effets secondaires » agit-il sur « Fonctions critiques et dépendances », et quel repère issu de « Détection et confiance dans les capteurs » permet de vérifier la décision?

**Intuition.** Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.



### Panne primaire et effets secondaires

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.



### Fonctions critiques et dépendances

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.



### Détection et confiance dans les capteurs

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

**Repère concret.** Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».

- Panne primaire et effets secondaires — Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des...
- Fonctions critiques et dépendances — Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des...
- Détection et confiance dans les capteurs — Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des...

## CARTE DE MAÎTRISE · MODULE 57

### Quatre repères à maîtriser — Résilience aux défaillances multiples: reconfiguration et retour au service

#### Panne primaire et effets secondaires

##### Définition

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

##### Intuition ou cas concret

Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer

**Repère quantitatif**

d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».

**Limite ou critère de vigilance**

Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Exercice guidé — Panne primaire et effets secondaires**

Cas « Panne primaire et effets secondaires » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au...

Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Corrigé raisonné — Panne primaire et effets secondaires****Point de départ**

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

**Indice du cas**

Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».

**Réserve à appliquer**

Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Conclusion**

Livable: données, unités, résultat, marge, décision.

## Fonctions critiques et dépendances

### Définition

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

### Intuition ou cas concret

Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

### Repère quantitatif

Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».

### Limite ou critère de vigilance

Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

### Exercice guidé — Fonctions critiques et dépendances

Cas « Fonctions critiques et dépendances » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au...

Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

### Corrigé raisonné — Fonctions critiques et dépendances

|                            |                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Point de départ</b>     | Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges. |
| <b>Indice du cas</b>       | Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».                                                                           |
| <b>Réserve à appliquer</b> | Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».                                                                |
| <b>Conclusion</b>          | Livable: données, unités, résultat, marge, décision.                                                                                                                                        |

## Détection et confiance dans les capteurs

|                                       |                                                                                                                                                                                                                                                |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Définition</b>                     | Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.                                                    |
| <b>Intuition ou cas concret</b>       | Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges. |
| <b>Repère quantitatif</b>             | Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».                                                                                                                              |
| <b>Limite ou critère de vigilance</b> | Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».                                                                                                                   |

### Exercice guidé — Détection et confiance dans les capteurs

Cas « Détection et confiance dans les capteurs » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au...

Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

## Corrigé raisonné — Détection et confiance dans les capteurs

|                            |                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Point de départ</b>     | Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges. |
| <b>Indice du cas</b>       | Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».                                                                           |
| <b>Réserve à appliquer</b> | Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».                                                                |
| <b>Conclusion</b>          | Livrible: données, unités, résultat, marge, décision.                                                                                                                                       |

## États nominal, dégradé et survie

|                                       |                                                                                                                                                                                                                                                |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Définition</b>                     | Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.                                                    |
| <b>Intuition ou cas concret</b>       | Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges. |
| <b>Repère quantitatif</b>             | Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».                                                                                                                              |
| <b>Limite ou critère de vigilance</b> | Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».                                                                                                                   |

### Exercice guidé — États nominal, dégradé et survie

Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au...

Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut

90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

#### Corrigé raisonné — États nominal, dégradé et survie

|                            |                                                                                                                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Point de départ</b>     | Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges. |
| <b>Indice du cas</b>       | Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ».                                                                           |
| <b>Réserve à appliquer</b> | Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».                                                                |
| <b>Conclusion</b>          | Livrable: données, unités, résultat, marge, décision.                                                                                                                                       |

Ce module s'appuie sur modules 00 à 52 selon le sujet, mais il reste lisible isolément: les symboles déterminants pour résilience aux défaillances multiples: reconfiguration et retour au service sont explicités au premier calcul.

## Objectifs de maîtrise

- Savoir reconnaître un cas réel de « La seconde panne change la nature du problème » à partir d'indices observables.
- Présenter les données et unités nécessaires à l'analyse de « Causes communes ».
- Tester la sensibilité du résultat à une hypothèse de « Cascades entre systèmes ».
- Formuler le critère qui autorise, retarde ou interdit la décision liée à « Configuration minimale sûre ».

## 1. La seconde panne change la nature du problème

Une architecture peut tolérer une panne simple et devenir extrêmement fragile face à une seconde. Deux pompes redondantes ne protègent pas si elles partagent alimentation, refroidissement ou logiciel. La **résilience** commence donc par la carte des dépendances communes et par la capacité à maintenir une fonction minimale même lorsque la configuration nominale n'est plus disponible.

## 2. Causes communes

Les causes communes comprennent **incendie**, inondation, **contamination**, erreur logicielle, mauvais lot de pièces, surtension ou erreur humaine. Elles peuvent neutraliser plusieurs redondances simultanément. Séparer physiquement, diversifier les technologies ou les versions et isoler les stocks réduit ce risque, mais chaque mesure a un coût. Le choix doit être lié à la criticité de la fonction.

## 3. Cascades entre systèmes

Une panne énergie peut arrêter pompes et refroidissement; la hausse thermique peut ensuite dégrader batteries ou électronique; la perte de communication complique le diagnostic. La cascade n'est pas une liste de pannes indépendantes: c'est une chaîne causale. Les procédures doivent reconnaître les signaux précoces et couper certaines charges avant que la propagation ne rende la **récupération** impossible.

## 4. Configuration minimale sûre

En crise, l'objectif n'est pas de restaurer immédiatement toute la colonie. On cherche d'abord un **état** stable: volume refuge, atmosphère contrôlée, eau minimale, **puissance** critique, communication et capacité médicale. Les fonctions industrielles ou scientifiques restent arrêtées jusqu'à ce que les réserves et la **marge** énergétique permettent leur retour.

## 5. Reconfiguration

La reconfiguration utilise les chemins alternatifs prévus: basculer un bus, raccorder une pompe de secours, isoler un compartiment, transférer l'équipage ou déplacer une charge vers un autre contrôleur. Ces actions doivent être testées avant la crise. Une connexion d'urgence jamais essayée peut être mécaniquement inaccessible ou incompatible au moment où elle devient vitale.

## 6. Diagnostic sous incertitude

Après plusieurs pannes, certains capteurs peuvent eux-mêmes être faux. Le diagnostic croise mesures indépendantes, [observation](#) locale et comportement du [système](#). On évite de multiplier les changements simultanés car cela masque la causalité. Une bonne [procédure](#) restaure d'abord la capacité d'observer puis modifie une variable à la fois lorsque le temps le permet.

## Approfondissement du module 57: comprendre, calculer, vérifier et décider

Objectif du module — raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

### 1. Panne primaire et effets secondaires

Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$\text{Facteur\_propagation} = \text{N\_effets\_secondaires} / \text{N\_pannes\_primaires}$

### **Question de départ**

Dans «1. Panne primaire et effets secondaires», comment chiffrer Facteur\_propagation en prenant N\_pannes\_primaires comme base de comparaison de N\_effets\_secondaires?

### **Lecture à voix haute**

Lecture guidée: «Facteur indice propagation égale N indice effets indice secondaires divisé par N indice pannes indice primaires».

### **Symboles, prononciation et sens**

Facteur\_propagation («Facteur propagation»): nombre moyen d'effets secondaires par panne primaire; N\_effets\_secondaires («N effets secondaires»): nombre de effets secondaires; N\_pannes\_primaires («N pannes primaires»): nombre de pannes primaires

### **Unités**

Facteur propagation → sans dimension; N effets secondaires → compte; N pannes primaires → compte.

### **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

### **Pourquoi cette opération**

Le calcul n'additionne pas N\_effets\_secondaires et N\_pannes\_primaires; il met N\_effets\_secondaires à l'échelle de N\_pannes\_primaires. Cette comparaison multiplicative conduit au quotient  $\text{Facteur\_propagation} = (\text{N\_effets\_secondaires}) / (\text{N\_pannes\_primaires})$ .

### **Substitution et calcul**

L'application de «Facteur\_propagation = N\_effets\_secondaires / N\_pannes\_primaires» consiste à évaluer séparément N\_effets\_secondaires et N\_pannes\_primaires à partir des entrées sourcées, puis à diviser le premier résultat par le second.

### **Saisie sur calculatrice**

Calculatrice: préparer le haut  $N_{\text{effets\_secondaires}}$ , préparer le bas  $N_{\text{pannes\_primaires}}$ , puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

### **Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de  $N_{\text{effets\_secondaires}}$  divisée par grandeur de  $N_{\text{pannes\_primaires}}$ . Le résultat grossier sert de borne de plausibilité pour  $\text{Facteur\_propagation}$ .

### **Contrôle indépendant**

Contrôle croisé: utiliser la multiplication  $\text{Facteur\_propagation} \cdot N_{\text{pannes\_primaires}}$  plutôt qu'une seconde division. Le résultat doit être compatible avec  $N_{\text{effets\_secondaires}}$ .

### **Interprétation physique ou opérationnelle**

Le résultat associé à « $\text{Facteur\_propagation} = N_{\text{effets\_secondaires}} / N_{\text{pannes\_primaires}}$ » doit être replacé dans «1. Panne primaire et effets secondaires». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative:  $\text{Facteur\_propagation}$  exprime  $N_{\text{effets\_secondaires}}$  relativement à  $N_{\text{pannes\_primaires}}$ .

### **Variation / sensibilité**

Si  $N_{\text{effets\_secondaires}}$  est multiplié par 1,1,  $\text{Facteur\_propagation}$  l'est aussi; si  $N_{\text{pannes\_primaires}}$  est multiplié par 1,1, le résultat est divisé par 1,1.

### **Limite / hypothèse**

Le modèle de ratio suppose que  $N_{\text{effets\_secondaires}}$  et  $N_{\text{pannes\_primaires}}$  sont comparables et que  $N_{\text{pannes\_primaires}}$  ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

Termes: MTBF · MTTR

On injecte maintenant l'événement suivant: perte d'énergie suivie d'une dégradation ECLSS.

## 2. Fonctions critiques et dépendances

Dans ce module, fonctions critiques et dépendances sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$A_{\text{série}} = \prod A_i$$

### Question de départ

Dans «2. Fonctions critiques et dépendances», quel produit obtient-on en appliquant successivement tous les facteurs de  $A_{\text{série}} = \prod A_i$ ?

### Lecture à voix haute

Lecture guidée: «A indice série égale pi majuscule A indice i».

### Symboles, prononciation et sens

$A_{\text{série}}$  («a série»): disponibilité globale d'une chaîne de fonctions toutes nécessaires;  $\prod$  («pi majuscule»): opérateur produit;  $A_i$  («a indice i»): disponibilité du composant ou de la fonction i, comprise entre 0 et 1.

### Unités

$A_{\text{série}}$  et chaque  $A_i$  sont sans dimension, compris entre 0 et 1.

### Origine et statut des valeurs

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées.

### Pourquoi cette opération

Dans un modèle simple de composants indépendants montés en série fonctionnelle, la chaîne n'est disponible que si tous les éléments nécessaires le sont simultanément. On multiplie donc leurs disponibilités.

### Substitution et calcul

Procédure symbolique: lister les facteurs i réellement applicables, calculer chacun puis former leur produit  $\prod$ . Ne pas ajouter de facteur fictif pour compléter la relation.

### Saisie sur calculatrice

Calculer les facteurs séparément puis les multiplier successivement; conserver les facteurs affichés pour identifier immédiatement celui qui dégradé produit.

**Estimation mentale**

Pour des facteurs compris entre 0 et 1, le produit ne peut dépasser le plus petit facteur et décroît quand on ajoute une contrainte supplémentaire.

**Contrôle indépendant**

Le produit ne peut pas dépasser le plus petit  $A_i$ . Avec deux composants à 0,90 et 0,80,  $A_{\text{série}} = 0,72$ ; obtenir 0,90 ou davantage révélerait une erreur.

**Interprétation physique ou opérationnelle**

Le résultat associé à « $A_{\text{série}} = \prod A_i$ » doit être replacé dans «2. Fonctions critiques et dépendances». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

**Traduction en français courant**

En français courant: A série est obtenu en multipliant successivement tous les facteurs concernés; chacun peut dégrader ou renforcer le résultat selon sa valeur.

**Variation / sensibilité**

Sensibilité: le produit dépend de tous les facteurs; pour des facteurs positifs, une variation relative d'un facteur se transmet directement au produit si les autres restent constants.

**Limite / hypothèse**

Limites: la multiplication directe suppose que la structure probabiliste ou fonctionnelle du modèle autorise ce produit. Des causes communes ou dépendances entre facteurs peuvent invalider une interprétation naïve.

On injecte maintenant l'événement suivant: rover immobilisé avec communications intermittentes.

**3. Détection et confiance dans les capteurs**

Dans ce module, détection et confiance dans les capteurs sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$z_{\text{écart}} = |x_1 - x_2| / u_{\text{combinée}}$$

### Question de départ

Dans «3. Détection et confiance dans les capteurs», comment chiffrer  $z_{\text{écart}}$  en prenant  $u_{\text{combinée}}$  comme base de comparaison de  $|x_1 - x_2|$ ?

### Lecture à voix haute

Lecture guidée: «z indice écart égale |x indice 1 - x indice 2| divisé par u indice combinée».

### Symboles, prononciation et sens

$z_{\text{écart}}$  («z écart»): écart normalisé en nombre d'incertitudes combinées;  $x_1$  («x un») et  $x_2$  («x deux»): deux estimations de la même grandeur;  $u_{\text{combinée}}$  («u combinée»): incertitude-type combinée exprimée dans la même unité que  $x_1$  et  $x_2$ .

### Unités

$x_1$ ,  $x_2$  et  $u_{\text{combinée}}$  doivent avoir la même unité physique. Leur différence divisée par une incertitude de même unité donne  $z_{\text{écart}}$  sans dimension.

### Origine et statut des valeurs

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées.

### Pourquoi cette opération

Le numérateur mesure l'écart entre les deux valeurs; le dénominateur exprime l'échelle d'incertitude attendue. Le quotient indique combien d'incertitudes combinées séparent les valeurs.

### Substitution et calcul

L'application de « $z_{\text{écart}} = |x_1 - x_2| / u_{\text{combinée}}$ » consiste à évaluer séparément  $|x_1 - x_2|$  et  $u_{\text{combinée}}$  à partir des entrées sourcées, puis à diviser le premier résultat par le second.

### Saisie sur calculatrice

Calculatrice: préparer le haut  $|x_1 - x_2|$ , préparer le bas  $u_{\text{combinée}}$ , puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

**Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de  $|x_1 - x_2|$  divisée par grandeur de  $u_{\text{combinée}}$ . Le résultat grossier sert de borne de plausibilité pour  $z_{\text{écart}}$ .

**Contrôle indépendant**

Contrôle inverse:  $z_{\text{écart}} \times u_{\text{combinée}}$  doit redonner  $|x_1 - x_2|$ .

**Interprétation physique ou opérationnelle**

Le résultat associé à « $z_{\text{écart}} = |x_1 - x_2| / u_{\text{combinée}}$ » doit être remplacé dans «3. Détection et confiance dans les capteurs». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

**Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative:  $z_{\text{écart}}$  exprime  $|x_1 - x_2|$  relativement à  $u_{\text{combinée}}$ .

**Variation / sensibilité**

Si  $|x_1 - x_2|$  est multiplié par 1,1,  $z_{\text{écart}}$  l'est aussi; si  $u_{\text{combinée}}$  est multiplié par 1,1, le résultat est divisé par 1,1.

**Limite / hypothèse**

$u_{\text{combinée}}$  doit être strictement positive et calculée avec un modèle d'incertitude compatible avec la corrélation éventuelle entre  $x_1$  et  $x_2$ .

— « Détection et confiance dans les capteurs ».

On injecte maintenant l'événement suivant: incident médical combiné à un retard logistique.

**4. États nominal, dégradé et survie**

Dans ce module, états nominal, dégradé et survie sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$\text{Marge\_fonction} = \text{Capacité\_restante} - \text{Besoin\_min}$

### **Question de départ**

Que vaut Marge\_fonction après le retrait défini par

«Marge\_fonction = Capacité\_restante - Besoin\_min» au passage «4. États nominal, dégradé et survie»?

### **Lecture à voix haute**

Lecture guidée: «Marge indice fonction égale Capacité indice restante - Besoin indice min».

### **Symboles, prononciation et sens**

Marge\_fonction: capacité disponible au-delà du minimum nécessaire; Capacité\_restante: capacité encore disponible après les pannes ou reconfigurations; Besoin\_min: capacité minimale requise pour maintenir la fonction.

### **Unités**

Marge\_fonction, Capacité\_restante et Besoin\_min doivent être exprimés dans la même unité de capacité propre à la fonction (W, kg/h, L/h, etc.).

### **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

### **Pourquoi cette opération**

On soustrait le minimum nécessaire de la capacité restante. Une marge positive signifie que la fonction reste soutenable; une marge négative signale un déficit.

### **Substitution et calcul**

Écrire les valeurs avec leurs unités, effectuer les conversions nécessaires, puis soustraire le second terme du premier comme le prescrit la relation.

### **Saisie sur calculatrice**

La saisie suit la phrase mathématique: valeur de gauche, moins, valeur retranchée; une parenthèse éventuelle est résolue avant la différence finale.

### **Estimation mentale**

Avant le calcul fin, arrondir les deux entrées et estimer leur séparation; le résultat exact doit rester cohérent avec cette différence grossière.

### **Contrôle indépendant**

Contrôle inverse: `Marge_fonction + Besoin_min` doit redonner `Capacité_restante`.

### **Interprétation physique ou opérationnelle**

Le résultat associé à «`Marge_fonction = Capacité_restante - Besoin_min`» doit être replacé dans «4. États nominal, dégradé et survie». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Sans notation, `Marge_fonction` mesure ici la marge ou l'écart restant lorsque la seconde quantité est retirée de la première.

### **Variation / sensibilité**

Faire varier séparément les deux entrées de  $\pm 10\%$  montre que leur influence sur `Marge_fonction` est opposée.

### **Limite / hypothèse**

Les entrées doivent partager unité, date ou fenêtre temporelle et frontière de système. Un mélange de périmètres rendrait l'écart trompeur.

On injecte maintenant l'événement suivant: capteurs contradictoires pendant une panne.

## **5. Priorisation des charges**

Dans ce module, priorisation des charges sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$f\_charge\_servie = P\_servie / P\_critique$$

### **Question de départ**

Dans «5. Priorisation des charges», comment chiffrer `f_charge_servie` en prenant `P_critique` comme base de comparaison de `P_servie`?

## **Lecture à voix haute**

Lecture guidée: «f indice charge indice servie égale P indice servie divisé par P indice critique».

## **Symboles, prononciation et sens**

f\_charge\_servie: fraction de la puissance critique réellement alimentée; P\_servie: puissance critique effectivement servie; P\_critique: puissance totale demandée par les charges classées critiques.

## **Unités**

P\_servie et P\_critique dans la même unité de puissance; f\_charge\_servie sans dimension entre 0 et 1 lorsque la puissance servie ne dépasse pas le besoin critique.

## **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées.

## **Pourquoi cette opération**

Le quotient mesure la part de la demande critique encore alimentée.

## **Substitution et calcul**

L'application de «f\_charge\_servie = P\_servie / P\_critique» consiste à évaluer séparément P\_servie et P\_critique à partir des entrées sourcées, puis à diviser le premier résultat par le second.

## **Saisie sur calculatrice**

Calculatrice: préparer le haut P\_servie, préparer le bas P\_critique, puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

## **Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de P\_servie divisée par grandeur de P\_critique. Le résultat grossier sert de borne de plausibilité pour f\_charge\_servie.

## **Contrôle indépendant**

f\_charge\_servie × P\_critique doit redonner P\_servie.

### **Interprétation physique ou opérationnelle**

Le résultat associé à « $f_{\text{charge\_servie}} = P_{\text{servie}} / P_{\text{critique}}$ » doit être remplacé dans «5. Priorisation des charges». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative:  $f_{\text{charge\_servie}}$  exprime  $P_{\text{servie}}$  relativement à  $P_{\text{critique}}$ .

### **Variation / sensibilité**

Si  $P_{\text{servie}}$  est multiplié par 1,1,  $f_{\text{charge\_servie}}$  l'est aussi; si  $P_{\text{critique}}$  est multiplié par 1,1, le résultat est divisé par 1,1.

### **Limite / hypothèse**

Le modèle de ratio suppose que  $P_{\text{servie}}$  et  $P_{\text{critique}}$  sont comparables et que  $P_{\text{critique}}$  ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

On injecte maintenant l'événement suivant: réparation réussie mais test de retour au service échoué.

## **6. Reconfiguration et diversité**

Dans ce module, reconfiguration et diversité sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$A_{\text{redondant}} = 1 - \prod (1 - A_i)$$

### **Question de départ**

Que vaut  $A_{\text{redondant}}$  après le retrait défini par « $A_{\text{redondant}} = 1 - \prod (1 - A_i)$ » au passage «6. Reconfiguration et diversité»?

### **Lecture à voix haute**

Lecture guidée: «A indice redondant égale 1 - pi majuscule (1 - A indice i)».

## **Symboles, prononciation et sens**

$A_{\text{redondant}}$  («A redondant»): disponibilité du système redondant;  
 $A_i$  («A indice i»): disponibilité du composant i;  $\Pi$  («pi majuscule»): produit de tous les facteurs indexés. Chaque  $1-A_i$  est l'indisponibilité du composant i.

## **Unités**

Toutes les disponibilités et indisponibilités sont des fractions sans dimension comprises entre 0 et 1. Le produit  $\Pi(1-A_i)$ , puis 1 moins ce produit, restent sans dimension.

## **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

## **Pourquoi cette opération**

Pour chaque composant i,  $1-A_i$  est sa probabilité ou fraction d'indisponibilité. Sous l'hypothèse d'indépendance,  $\Pi(1-A_i)$  est l'indisponibilité simultanée de tous les composants redondants. La disponibilité d'au moins un composant vaut donc  $1-\Pi(1-A_i)$ .

## **Substitution et calcul**

Écrire les valeurs avec leurs unités, effectuer les conversions nécessaires, puis soustraire le second terme du premier comme le prescrit la relation.

## **Saisie sur calculatrice**

La saisie suit la phrase mathématique: valeur de gauche, moins, valeur retranchée; une parenthèse éventuelle est résolue avant la différence finale.

## **Estimation mentale**

Avant le calcul fin, arrondir les deux entrées et estimer leur séparation; le résultat exact doit rester cohérent avec cette différence grossière.

## **Contrôle indépendant**

Contrôle indépendant – calculer d'abord  $U=\Pi(1-A_i)$ , puis vérifier  $A_{\text{redondant}}+U=1$ . Avec deux composants identiques de disponibilité A, la formule doit donner  $1-(1-A)^2$ .

### **Interprétation physique ou opérationnelle**

Le résultat associé à « $A_{\text{redondant}} = 1 - \prod(1 - A_i)$ » doit être remplacé dans «6. Reconfiguration et diversité». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Sans notation,  $A_{\text{redondant}}$  mesure ici la marge ou l'écart restant lorsque la seconde quantité est retirée de la première.

### **Variation / sensibilité**

Augmenter n'importe quel  $A_i$  réduit le produit des indisponibilités et augmente  $A_{\text{redondant}}$ . L'effet n'est pas une simple différence linéaire; il dépend du produit des autres indisponibilités.

### **Limite / hypothèse**

Cette forme suppose que les indisponibilités des branches redondantes sont indépendantes. Les défaillances de cause commune, ressources partagées et dépendances de maintenance peuvent rendre le produit  $\prod(1-A_i)$  trop optimiste.

On injecte maintenant l'événement suivant: deux redondances partagent une cause commune.

## **7. Récupération progressive**

Dans ce module, récupération progressive sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$f_{\text{restauré}} = N_{\text{fonctions\_restaurées}} / N_{\text{fonctions\_critiques}}$$

### **Question de départ**

Dans «7. Récupération progressive», comment chiffrer  $f_{\text{restauré}}$  en prenant  $N_{\text{fonctions\_critiques}}$  comme base de comparaison de  $N_{\text{fonctions\_restaurées}}$ ?

### **Lecture à voix haute**

Lecture guidée: « $f$  indice restauré égale  $N$  indice fonctions indice restaurées divisé par  $N$  indice fonctions indice critiques».

## **Symboles, prononciation et sens**

f\_restauré («f restauré»): fraction «restauré» comprise entre 0 et 1; N\_fonctions\_restaurées («N fonctions restaurées»): nombre de fonctions restaurées; N\_fonctions\_critiques («N fonctions critiques»): nombre de fonctions critiques

## **Unités**

f restauré → sans dimension [0;1]; N fonctions restaurées → compte; N fonctions critiques → compte.

## **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

## **Pourquoi cette opération**

Le calcul n'additionne pas N\_fonctions\_restaurées et N\_fonctions\_critiques; il met N\_fonctions\_restaurées à l'échelle de N\_fonctions\_critiques. Cette comparaison multiplicative conduit au quotient  $f_{\text{restauré}} = \frac{N_{\text{fonctions\_restaurées}}}{N_{\text{fonctions\_critiques}}}$ .

## **Substitution et calcul**

L'application de « $f_{\text{restauré}} = \frac{N_{\text{fonctions\_restaurées}}}{N_{\text{fonctions\_critiques}}}$ » consiste à évaluer séparément N\_fonctions\_restaurées et N\_fonctions\_critiques à partir des entrées sourcées, puis à diviser le premier résultat par le second.

## **Saisie sur calculatrice**

Calculatrice: préparer le haut N\_fonctions\_restaurées, préparer le bas N\_fonctions\_critiques, puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

## **Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de N\_fonctions\_restaurées divisée par grandeur de N\_fonctions\_critiques. Le résultat grossier sert de borne de plausibilité pour f\_restauré.

### **Contrôle indépendant**

Contrôle croisé: utiliser la multiplication  $f_{\text{restauré}} \cdot N_{\text{fonctions\_critiques}}$  plutôt qu'une seconde division. Le résultat doit être compatible avec  $N_{\text{fonctions\_restaurées}}$ .

### **Interprétation physique ou opérationnelle**

Le résultat associé à « $f_{\text{restauré}} = N_{\text{fonctions\_restaurées}} / N_{\text{fonctions\_critiques}}$ » doit être replacé dans «7. Récupération progressive». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative:  $f_{\text{restauré}}$  exprime  $N_{\text{fonctions\_restaurées}}$  relativement à  $N_{\text{fonctions\_critiques}}$ .

### **Variation / sensibilité**

Si  $N_{\text{fonctions\_restaurées}}$  est multiplié par 1,1,  $f_{\text{restauré}}$  l'est aussi; si  $N_{\text{fonctions\_critiques}}$  est multiplié par 1,1, le résultat est divisé par 1,1.

### **Limite / hypothèse**

Le modèle de ratio suppose que  $N_{\text{fonctions\_restaurées}}$  et  $N_{\text{fonctions\_critiques}}$  sont comparables et que  $N_{\text{fonctions\_critiques}}$  ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

On injecte maintenant l'événement suivant: perte d'énergie suivie d'une dégradation ECLSS.

## **8. Critères de transition mesurables**

Dans ce module, critères de transition mesurables sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$f_{\text{transition}} = N_{\text{critères\_OK}} / N_{\text{critères\_requis}}$$

### **Question de départ**

Dans «8. Critères de transition mesurables», comment chiffrer  $f_{\text{transition}}$  en prenant  $N_{\text{critères\_requis}}$  comme base de comparaison de  $N_{\text{critères\_OK}}$ ?

## **Lecture à voix haute**

Lecture guidée: «f indice transition égale N indice critères indice OK divisé par N indice critères indice requis».

## **Symboles, prononciation et sens**

f\_transition («f transition»): fraction «transition» comprise entre 0 et 1; N\_critères\_OK («N critères OK»): nombre de critères OK; N\_critères\_requis («N critères requis»): nombre de critères requis

## **Unités**

f transition → sans dimension [0;1]; N critères OK → compte; N critères requis → compte.

## **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

## **Pourquoi cette opération**

Le calcul n'additionne pas N\_critères\_OK et N\_critères\_requis; il met N\_critères\_OK à l'échelle de N\_critères\_requis. Cette comparaison multiplicative conduit au quotient  $f\_transition = (N\_critères\_OK) / (N\_critères\_requis)$ .

## **Substitution et calcul**

L'application de «f\_transition = N\_critères\_OK / N\_critères\_requis» consiste à évaluer séparément N\_critères\_OK et N\_critères\_requis à partir des entrées sourcées, puis à diviser le premier résultat par le second.

## **Saisie sur calculatrice**

Calculatrice: préparer le haut N\_critères\_OK, préparer le bas N\_critères\_requis, puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

## **Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de N\_critères\_OK divisée par grandeur de N\_critères\_requis. Le résultat grossier sert de borne de plausibilité pour f\_transition.

### **Contrôle indépendant**

Contrôle croisé: utiliser la multiplication  $f_{\text{transition}} \cdot N_{\text{critères\_requis}}$  plutôt qu'une seconde division. Le résultat doit être compatible avec  $N_{\text{critères\_OK}}$ .

### **Interprétation physique ou opérationnelle**

Le résultat associé à « $f_{\text{transition}} = N_{\text{critères\_OK}} / N_{\text{critères\_requis}}$ » doit être replacé dans «8. Critères de transition mesurables». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative:  $f_{\text{transition}}$  exprime  $N_{\text{critères\_OK}}$  relativement à  $N_{\text{critères\_requis}}$ .

### **Variation / sensibilité**

Si  $N_{\text{critères\_OK}}$  est multiplié par 1,1,  $f_{\text{transition}}$  l'est aussi; si  $N_{\text{critères\_requis}}$  est multiplié par 1,1, le résultat est divisé par 1,1.

### **Limite / hypothèse**

Le modèle de ratio suppose que  $N_{\text{critères\_OK}}$  et  $N_{\text{critères\_requis}}$  sont comparables et que  $N_{\text{critères\_requis}}$  ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

— « Critères de transition mesurables ».

On injecte maintenant l'événement suivant: rover immobilisé avec communications intermittentes.

## **9. Ressources consommées pendant la crise**

Dans ce module, ressources consommées pendant la crise sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$\text{Autonomie} = \text{Stock} / \text{Débit\_mode}$

### **Question de départ**

Dans «9. Ressources consommées pendant la crise», comment chiffrer Autonomie en prenant Débit\_mode comme base de comparaison de Stock?

### **Lecture à voix haute**

Lecture guidée: «Autonomie égale Stock divisé par Débit indice mode».

### **Symboles, prononciation et sens**

Autonomie: durée pendant laquelle le stock peut soutenir le débit du mode de crise; Stock: quantité disponible de la ressource; Débit\_mode: débit du stock correspondant dans le mode considéré dans le mode considéré.

### **Unités**

Stock et Débit\_mode doivent porter la même grandeur: kg avec kg/h, L avec L/h, kWh avec kWh/h ou kW après cohérence énergétique. Leur quotient donne une durée.

### **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

### **Pourquoi cette opération**

Une quantité divisée par une consommation par unité de temps donne le temps avant épuisement.

### **Substitution et calcul**

L'application de «Autonomie = Stock / Débit\_mode» consiste à évaluer séparément Stock et Débit\_mode à partir des entrées sourcées, puis à diviser le premier résultat par le second.

### **Saisie sur calculatrice**

Calculatrice: préparer le haut Stock, préparer le bas Débit\_mode, puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

**Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de Stock divisée par grandeur de Débit\_mode. Le résultat grossier sert de borne de plausibilité pour Autonomie.

**Contrôle indépendant**

Autonomie×Débit\_mode doit redonner Stock.

**Interprétation physique ou opérationnelle**

Le résultat associé à «Autonomie = Stock / Débit\_mode» doit être remplacé dans «9. Ressources consommées pendant la crise». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

**Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative: Autonomie exprime Stock relativement à Débit\_mode.

**Variation / sensibilité**

Si Stock est multiplié par 1,1, Autonomie l'est aussi; si Débit\_mode est multiplié par 1,1, le résultat est divisé par 1,1.

**Limite / hypothèse**

Le modèle de ratio suppose que Stock et Débit\_mode sont comparables et que Débit\_mode ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

On injecte maintenant l'événement suivant: incident médical combiné à un retard logistique.

**10. Post-mortem et prévention de récurrence**

Dans ce module, post-mortem et prévention de récurrence sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au service sans perdre la traçabilité des fonctions et des marges.

$$\text{Taux\_récurrence} = \text{N\_incidents\_similaires} / \text{N\_incidents}$$

**Question de départ**

Dans «10. Post-mortem et prévention de récurrence», comment chiffrer Taux\_récurrence en prenant N\_incidents comme base de comparaison de N\_incidents\_similaires?

## **Lecture à voix haute**

Lecture guidée: «Taux indice récidive égale N indice incidents indice similaires divisé par N indice incidents».

## **Symboles, prononciation et sens**

Taux\_récidive («Taux récidive»): proportion «Taux récidive» rapportée au total correspondant; N\_incidents\_similaires («N incidents similaires»): nombre de incidents similaires; N\_incidents («N incidents»): nombre de incidents

## **Unités**

Taux\_récidive est sans dimension; N\_incidents\_similaires et N\_incidents sont des comptes. Le dénominateur doit être non nul et les deux comptes porter sur le même périmètre d'incidents.

## **Origine et statut des valeurs**

Les données numériques ne sont pas interchangeables: une mesure, une constante reconnue, une donnée de mission et une hypothèse d'exercice doivent rester distinguées. Dans ce cas précis, les entrées proviennent de: les disponibilités, probabilités de panne et temps de récupération.

## **Pourquoi cette opération**

Le calcul n'additionne pas N\_incidents\_similaires et N\_incidents; il met N\_incidents\_similaires à l'échelle de N\_incidents. Cette comparaison multiplicative conduit au quotient  $\text{Taux\_récidive} = (\text{N\_incidents\_similaires}) / (\text{N\_incidents})$ .

## **Substitution et calcul**

L'application de «Taux\_récidive = N\_incidents\_similaires / N\_incidents» consiste à évaluer séparément N\_incidents\_similaires et N\_incidents à partir des entrées sourcées, puis à diviser le premier résultat par le second.

## **Saisie sur calculatrice**

Calculatrice: préparer le haut N\_incidents\_similaires, préparer le bas N\_incidents, puis exécuter une seule division entre ces deux valeurs déjà vérifiées.

## **Estimation mentale**

Arrondir seulement pour l'estimation: grandeur de N\_incidents\_similaires divisée par grandeur de N\_incidents. Le résultat grossier sert de borne de plausibilité pour Taux\_récidive.

### **Contrôle indépendant**

Contrôle croisé: utiliser la multiplication

Taux\_récidive·N\_incidents plutôt qu'une seconde division. Le résultat doit être compatible avec N\_incidents\_similaires.

### **Interprétation physique ou opérationnelle**

Le résultat associé à «Taux\_récidive = N\_incidents\_similaires / N\_incidents» doit être replacé dans «10. Post-mortem et prévention de récidive». Unité, frontière d'analyse et hypothèses sont indispensables pour éviter qu'un nombre correct soit interprété de travers.

### **Traduction en français courant**

Le quotient transforme les deux quantités en une comparaison relative: Taux\_récidive exprime N\_incidents\_similaires relativement à N\_incidents.

### **Variation / sensibilité**

Si N\_incidents\_similaires est multiplié par 1,1, Taux\_récidive l'est aussi; si N\_incidents est multiplié par 1,1, le résultat est divisé par 1,1.

### **Limite / hypothèse**

Le modèle de ratio suppose que N\_incidents\_similaires et N\_incidents sont comparables et que N\_incidents ne s'annule pas. Les unités seules ne suffisent pas si les frontières diffèrent.

On injecte maintenant l'événement suivant: capteurs contradictoires pendant une panne.

## **Exercices progressifs avec corrigés 1:1**

### **Exercice 1: Panne primaire et effets secondaires**

Analysez panne primaire et effets secondaires. Relation à tester: «  $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$  ». Cas dégradé: rover immobilisé avec communications intermittentes. Livrable: données, unités, résultat, marge, décision.

**Données du cas**

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Raisonnement**

Corrigé — Exercice 1: Panne primaire et effets secondaires

**Résultat**

Corrigé — Exercice 1: Panne primaire et effets secondaires

**Exercice 2: Fonctions critiques et dépendances**

Analysez fonctions critiques et dépendances. Relation à tester: « Autonomie = Stock / Débit\_mode ». Cas dégradé: incident médical combiné à un retard logistique. Livrable: données, unités, résultat, marge, décision.

**Corrigé — Exercice 2: Fonctions critiques et dépendances****Données du cas**

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Raisonnement**

Corrigé — Exercice 2: Fonctions critiques et dépendances

**Résultat**

Corrigé — Exercice 2: Fonctions critiques et dépendances

### Exercice 3: Détection et confiance dans les capteurs

Analysez détection et confiance dans les capteurs. Relation à tester: «  $\text{Marge\_fonction} = \text{Capacité\_restante} - \text{Besoin\_min}$  ». Cas dégradé: capteurs contradictoires pendant une panne. Livrable: données, unités, résultat, marge, décision.

#### Corrigé — Exercice 3: Détection et confiance dans les capteurs

##### Données du cas

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

##### Raisonnement

Corrigé — Exercice 3: Détection et confiance dans les capteurs

##### Résultat

Corrigé — Exercice 3: Détection et confiance dans les capteurs

### Exercice 4: États nominal, dégradé et survie

Analysez états nominal, dégradé et survie. Relation à tester: «  $\text{Temps\_recup} = \Sigma(t_{\text{isolement}} + t_{\text{réparation}} + t_{\text{test}})$  ». Cas dégradé: réparation réussie mais test de retour au service échoué. Livrable: données, unités, résultat, marge, décision.

#### Corrigé — Exercice 4: États nominal, dégradé et survie

##### Données du cas

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne

**Raisonnement**

**Résultat**

primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

Corrigé — Exercice 4: États nominal, dégradé et survie

Corrigé — Exercice 4: États nominal, dégradé et survie

## Exercice 5: Priorisation des charges

Relation à tester: «  $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$  ». Cas dégradé: deux redondances partagent une cause commune. Livrable: données, unités, résultat, marge, décision.

### Corrigé — Exercice 5: Priorisation des charges

**Données du cas**

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Raisonnement**

Corrigé — Exercice 5: Priorisation des charges

**Résultat**

Corrigé — Exercice 5: Priorisation des charges

## Exercice 6: Reconfiguration et diversité

Relation à tester: «  $\text{Autonomie} = \text{Stock} / \text{Débit\_mode}$  ». Cas dégradé: perte d'énergie suivie d'une dégradation ECLSS. Livrable: données, unités, résultat, marge, décision.

### Corrigé — Exercice 6: Reconfiguration et diversité

**Données du cas**

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Raisonnement**

Corrigé — Exercice 6: Reconfiguration et diversité

**Résultat**

Corrigé — Exercice 6: Reconfiguration et diversité

**Exercice 7: Récupération progressive**

Relation à tester: «  $\text{Marge\_fonction} = \text{Capacité\_restante} - \text{Besoin\_min}$  ». Cas dégradé: rover immobilisé avec communications intermittentes. Livrable: données, unités, résultat, marge, décision.

**Corrigé — Exercice 7: Récupération progressive****Données du cas**

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

**Raisonnement**

Corrigé — Exercice 7: Récupération progressive

**Résultat**

Corrigé — Exercice 7: Récupération progressive

## Exercice 8: Critères de transition mesurables

Analysez critères de transition mesurables. Relation à tester: « Temps\_récup =  $\Sigma(t_{\text{isolement}} + t_{\text{réparation}} + t_{\text{test}})$  ». Cas dégradé: incident médical combiné à un retard logistique. Livrable: données, unités, résultat, marge, décision.

### Corrigé — Exercice 8: Critères de transition mesurables

#### Données du cas

Exercice guidé — États nominal, dégradé et survie — Cas « États nominal, dégradé et survie » — Dans ce module, panne primaire et effets secondaires sert directement à raisonner sur les cascades de défaillances, passer d'un état nominal à un état dégradé puis revenir au... Repère: Avec MTBF 900 h et MTTR 100 h, la disponibilité pédagogique vaut 90 % — « Panne primaire et effets secondaires ». Réserve: Cette moyenne ne décrit pas la gravité d'une panne unique ni les causes communes — « Panne primaire et effets secondaires ».

#### Raisonnement

Corrigé — Exercice 8: Critères de transition mesurables

#### Résultat

Corrigé — Exercice 8: Critères de transition mesurables

## Mini-projet intégrateur et dossier de référence

Traiter trois scénarios multi-pannes complets. Pour chacun: chronologie, fonctions perdues, état choisi, ressources restantes, décisions, reconfiguration, critères de récupération et post-mortem.

« Exercice 8: Critères de transition mesurables » — hypothèses, budget, marges.

« Exercice 8: Critères de transition mesurables » — interfaces et causes communes.

« Exercice 8: Critères de transition mesurables » — calculs, limites, critères.

Repères du passage: [inventaire](#)

Repères du passage: [sous-système](#) · [masse](#)

## Verification de maîtrise du module 57

- « Exercice 8: Critères de transition mesurables » — unités et ordre de grandeur.
- « Exercice 8: Critères de transition mesurables » — cas dégradé.
- « Exercice 8: Critères de transition mesurables » — marge décisionnelle.
- « Exercice 8: Critères de transition mesurables » — mesure de contrôle.
- Termes de contrôle: [Vérification](#)

Repères du passage: [contrôle](#)

Repères du passage: [disponibilité](#) · [substitution](#)

[moyenne](#) · [ordre de grandeur](#) · [validation](#)

Repères du passage: [Mode dégradé](#) · [ECLSS](#)

Repères du passage: [autonomie](#)

Repères du passage: [cause commune](#)

Repères du passage: [chronologie](#)

**Termes.** [moyenne](#) · [ordre de grandeur](#) · [validation](#)

## 7. Ressources de récupération

Réparer exige énergie, personnes, outils, pièces, temps et parfois atmosphère sûre. La planification de résilience réserve donc ces ressources. Utiliser toute la batterie pour maintenir une charge non essentielle peut supprimer la capacité de redémarrer une pompe critique quelques heures plus tard.

## 8. Retour progressif au nominal

Lorsque la cause est maîtrisée, les charges reviennent par étapes. Chaque étape possède un critère de stabilité. On surveille tension, [température](#), [pression](#), [débit](#) et consommation avant d'ajouter la fonction suivante. Le retour au nominal trop rapide peut recréer la cascade ou vider les réserves juste après la première récupération.

## Approfondissement: scénarios au-delà de N+1

Le classique N+1 protège contre la perte d'un élément, pas nécessairement contre une panne de zone ou de ressource commune. Les exercices doivent donc inclure des scénarios comme « un générateur perdu + une boucle de refroidissement limitée + un technicien indisponible ».

L'objectif est de révéler les dépendances que le calcul de [redondance](#) simple ne voit pas.

## Approfondissement: dette de configuration après crise

Les contournements accumulés pendant une crise créent une configuration atypique: câbles temporaires, protections désactivées, pièces empruntées ailleurs. Cette dette doit être inventoriée et résorbée. Sinon la colonie peut revenir à une apparence nominale tout en ayant perdu plusieurs barrières invisibles.

### 9. Exemple calculé: énergie de récupération

Le [refuge](#) consomme 22 kW et la capacité disponible après panne est de 35 kW. Il reste donc 13 kW pour récupération. Une pompe de remise en service exige 9 kW pendant trois heures: elle est compatible, mais seulement 4 kW restent pour les autres charges temporaires. Si un [atelier](#) de 8 kW est démarré en même temps, la limite est dépassée. La séquence de récupération doit donc être planifiée énergétiquement.

### Étude de cas calculée: combien de temps une batterie peut-elle combler un déficit critique?

**HYPOTHÈSE PÉDAGOGIQUE** — La charge critique vaut 42 kW. Après une panne multiple, le générateur survivant fournit 30 kW. La batterie possède 18 kWh nominaux mais 20 % doivent rester en réserve.

On note  $P_c$  la charge critique et  $P_g$  la puissance disponible, en kW;  $\Delta P$  le déficit, en kW;  $E_n$  l'énergie nominale, en kWh;  $r$  la réserve, sans unité;  $E_u$  l'énergie utilisable;  $t$  le temps de pontage.

$\Delta P = P_c - P_g = 42 - 30 = 12$  kW.  $E_u = 18 \times (1 - 0,20) = 14,4$  kWh.  $t = E_u \div \Delta P = 14,4 \div 12 = 1,2$  h = 72 min.

La batterie ne « résout » pas la multipanne: elle achète 72 minutes dans ce scénario simplifié pour délester, reconfigurer, réparer ou atteindre une configuration minimale sûre.

## 10. Exercice

Une colonie perd un des deux convertisseurs principaux puis détecte une fuite sur une boucle d'eau. Construire les trois premières actions, la configuration minimale sûre et l'ordre de retour des fonctions non vitales.

## 11. Solution raisonnée

La priorité est d'empêcher la cascade: stabiliser le réseau électrique, isoler la fuite, préserver eau et refuge, puis vérifier les capteurs. Les charges industrielles restent arrêtées. Une fois les réserves connues et la boucle stabilisée, les fonctions sont réintroduites par ordre de criticité avec contrôle de marge. Le diagnostic de la cause commune vient avant le redémarrage du second équipement si elle pourrait aussi l'endommager.

## 12. Mini-projet

Construire un exercice multi-pannes de six heures impliquant énergie, ECLSS, [mobilité](#) et communication. Définir événements injectés, informations disponibles, décisions attendues, critères de réussite et données à conserver pour le débriefing.

Visualisation conceptuelle : la résilience est démontrée lorsque la colonie préserve les fonctions critiques, diagnostique l'incertitude, se reconfigure puis revient en service sans provoquer une nouvelle panne.

### **Résilience multipannes : survivre à la seconde défaillance plutôt qu'à la première seulement**

La redondance n'est pas une garantie si plusieurs équipements partagent alimentation, refroidissement, logiciel, environnement, maintenance ou erreur de conception. Après une anomalie, l'équipe doit reconstruire les dépendances réelles et séparer observations, hypothèses et actions.

## **La cause commune change la valeur d'une redondance**

Deux voies prétendument indépendantes peuvent être perdues ensemble par un facteur partagé. Le modèle pédagogique ci-dessous sépare une part de défaillance commune et une part indépendante.

## **La récupération avance par portes de preuve**

On restaure d'abord la fonction critique minimale, on observe les mesures attendues puis on réintroduit progressivement les branches et les charges. Chaque étape possède un critère de succès et un critère d'abandon.

## **La saturation humaine peut devenir la prochaine cause commune**

Plusieurs alarmes peuvent exiger les mêmes spécialistes. Les plans de résilience doivent prévoir doublures, passations écrites et limites au nombre d'actions manuelles simultanées suivies par une seule personne.

## **La dette de configuration survit à la crise**

Cavaliers temporaires, contournements logiciels, capteurs isolés et réseaux croisés doivent être consignés en temps réel. Le retour à la normale n'est pas terminé tant que l'état physique et la documentation ne coïncident pas.

### **Probabilité pédagogique de perte de deux voies avec cause commune**

$$P_{\text{perte}} \approx \beta p + (1-\beta)^2 p^2$$

$p$  représente ici une probabilité marginale de défaillance d'une voie et  $\beta$  la fraction attribuée à une cause commune dans ce modèle simplifié. Le terme indépendant doit être cohérent avec l'hypothèse retenue ; cette formule sert à montrer que même un petit  $\beta$  peut dominer le bénéfice de redondance.

► Exercice — trois alarmes ne prouvent pas trois pannes indépendantes

Pour relier cet atelier aux références déjà utilisées par le module, consulter [NASA — Systems Engineering Handbook](#) et [NASA — Reliability and Maintainability Standard](#).

---

#### Sources primaires et passerelles

- [NASA — Systems Engineering Handbook](#)
- [NASA — Reliability and Maintainability Standard](#)
- [NASA JSC — Spaceflight Operations](#)