STRMTG

SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

Journée d'échanges Tramways 17 mai 2018

Allocation des niveaux de sécurité avec la norme EN 61508

Utilisation de la norme NF EN 61508

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

La norme **NF EN 61508** fournit une approche générique de toutes les activités liées au cycle de vie de sécurité des systèmes électriques et/ou électroniques et/ou électroniques programmables qui sont utilisés pour réaliser des fonctions de sécurité.

La norme rappelle également que **le secteur d'application doit être approprié et notamment ses pratiques reconnues.**

La norme **NF EN 50126-1** met en évidence les spécificités du domaine ferroviaire. Elle est applicable à la spécification et à la démonstration des exigences de FDMS pour toute application ferroviaire et à tout niveau d'une telle application.

La norme NF EN 50126-1 est LA norme de référence appliquée dans le domaine des transports guidés (citée dans l'arrêté du 23/03/2003 relatif à la composition des dossiers de sécurité en TGU).

Elle est complétée d'un groupe de normes connexes :

- **NF EN 50128** Logiciels pour systèmes de commande et de protection ferroviaire ;
- **NF EN 50129** Systèmes électroniques de sécurité pour la signalisation

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

NF EN 61 508 (janvier 2011) Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

- Partie 1 = Exigences générales
- Partie 2 = Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
- Partie 3 = Exigences concernant les logiciels
- Partie 4 = Définitions et abréviations
- **Partie 5 = Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité**
- Partie 6 = Ligne directrice pour l'application de la CEI 61508-2 et de la CEI 61508 -3
- Partie 7 = Présentation de techniques et mesures

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

Partie 5 - Annexe E
Méthode du graphe de risque

Paramètres utilisés :

- conséquence de l'événement dangereux (C)

- la fréquence et la durée d'exposition au danger (F)

- la possibilité d'éviter l'événement dangereux (P)

- la probabilité de l'occurrence non souhaitée (W) => probabilité que l'événement dangereux se produise en l'absence de systèmes relatifs à la sécurité (mais en présence de dispositifs externes de réduction de risque)

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

Graphe de risque
Schéma général

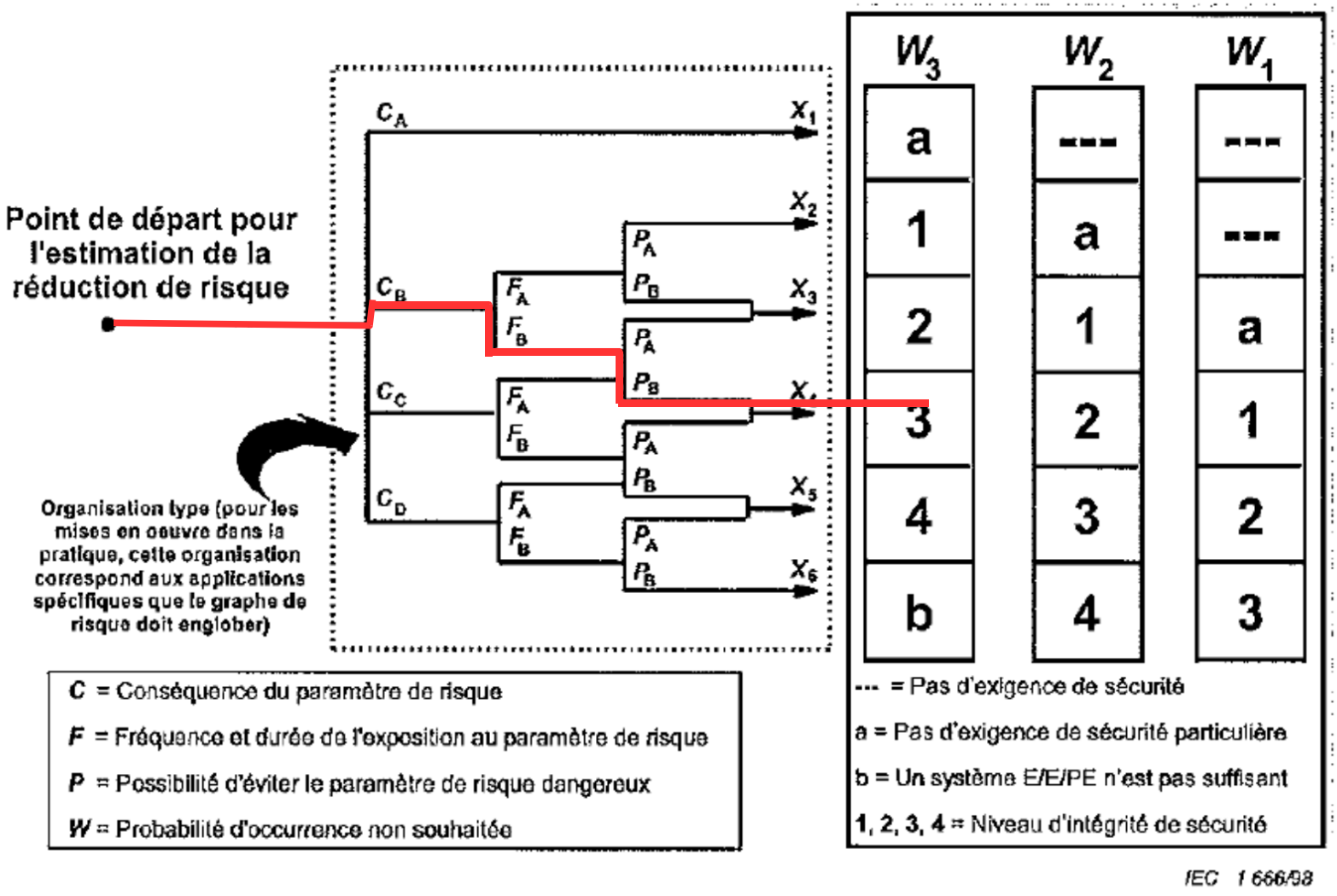


Figure E.1 – Graphe de risque – schéma général

« Absence de commande FU par manipulateur »
Exemple d'approche NF EN 50126-1

Niveau de gravité = Critique ou catastrophique selon collision tiers ou entre rames

Fréquence d'un événement dangereux => pour que le risque soit acceptable, la fréquence de l'événement dangereux doit être improbable

=> $P \leq 10^{-9}/h$

=> mais possibilité d'activation FS par le conducteur

=> $P \leq 10^{-7}/h$

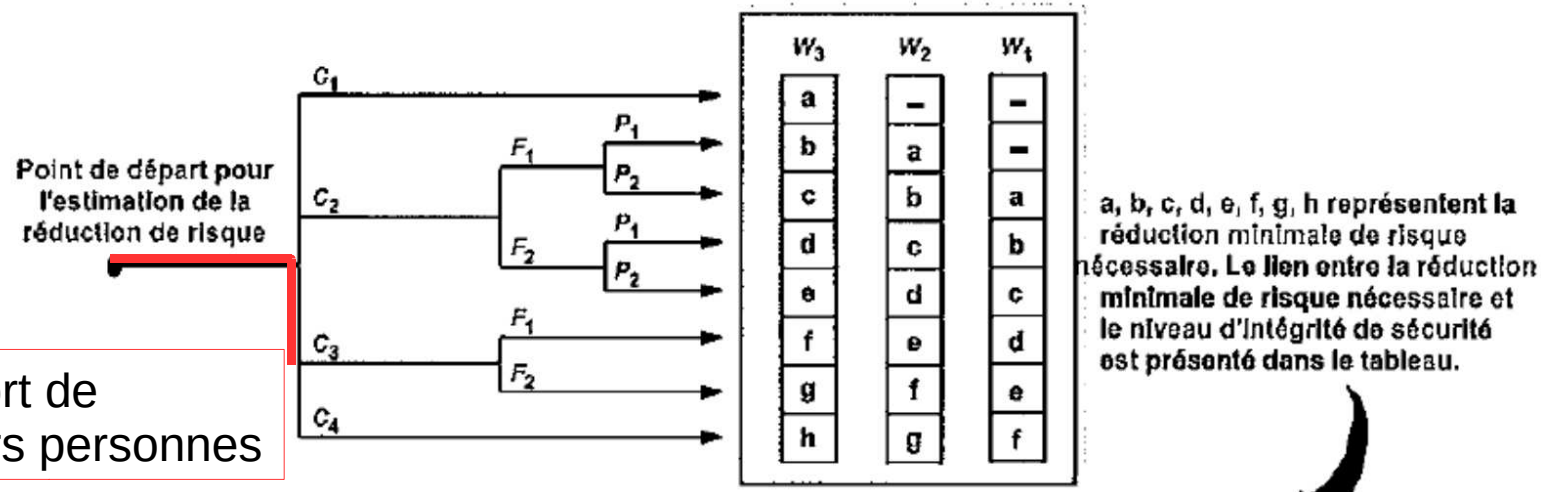
=> SIL 3

		Gravité			
		Catastrophique	**Critique**	**Marginal**	**Insignifiant**
Occurrence	Probable $10^{-5}/h<P\leq10^{-3}/h$	Inacceptable	Inacceptable	Inacceptable	acceptable
	Rare $10^{-7}/h<P\leq10^{-5}/h$	Inacceptable	Inacceptable	Acceptable	Acceptable
	Improbable $10^{-9}/h<P\leq10^{-7}/h$	Inacceptable	acceptable	acceptable	Acceptable
	Ext. improbable $P\leq10^{-9}/h$	acceptable	acceptable	acceptable	Acceptable

Zone de risque inacceptable

« Absence de commande FU par manipulateur » - Graphe **exemple** de la 61508

C3 : Mort de plusieurs personnes



C = Conséquence du paramètre de risque

F = Fréquence et durée de l'exposition au paramètre de risque

P = Possibilité d'éviter le paramètre de risque dangereux

W = Probabilité d'occurrence non souhaitée

a, b, c ... h = Estimation de la réduction de risque nécessairepour les SRS

Réduction minimale de risque nécessaire	Niveau d'intégrité de sécurité
-	Pas d'exigence de sécurité
a	Pas d'exigence de sécurité spéciale
b, c	1
d	2
e, f	3
g	4
h	Un système E/E/PE n'est pas suffisant

IEC 1 667/98

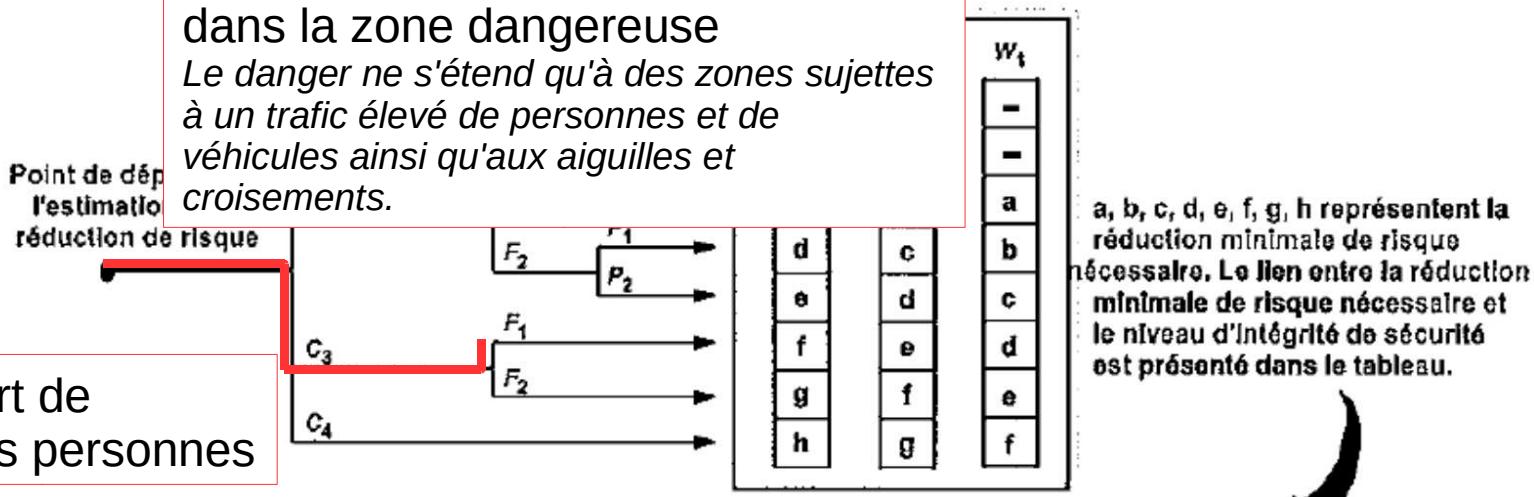
Figure E.2 – Graphe de risque – exemple (illustre seulement les principes généraux)

« Absence de commande FU par manipulateur » - Graphe **exemple** de la 61508

F1 : Exposition rare à fréquente dans la zone dangereuse

Le danger ne s'étend qu'à des zones sujettes à un trafic élevé de personnes et de véhicules ainsi qu'aux aiguilles et croisements.

C3 : Mort de plusieurs personnes



C = Conséquence du paramètre de risque

F = Fréquence et durée de l'exposition au paramètre de risque

P = Possibilité d'éviter le paramètre de risque dangereux

W = Probabilité d'occurrence non souhaitée

a, b, c ... h = Estimation de la réduction de risque nécessairepour les SRS

Réduction minimale de risque nécessaire	Niveau d'intégrité de sécurité
-	Pas d'exigence de sécurité
a	Pas d'exigence de sécurité spéciale
b, c	1
d	2
e, f	3
g	4
h	Un système E/E/PE n'est pas suffisant

IEC 1 667/98

Figure E.2 – Graphe de risque – exemple (illustre seulement les principes généraux)

« Absence de commande FU par manipulateur » - Graphe **exemple** de la 61508

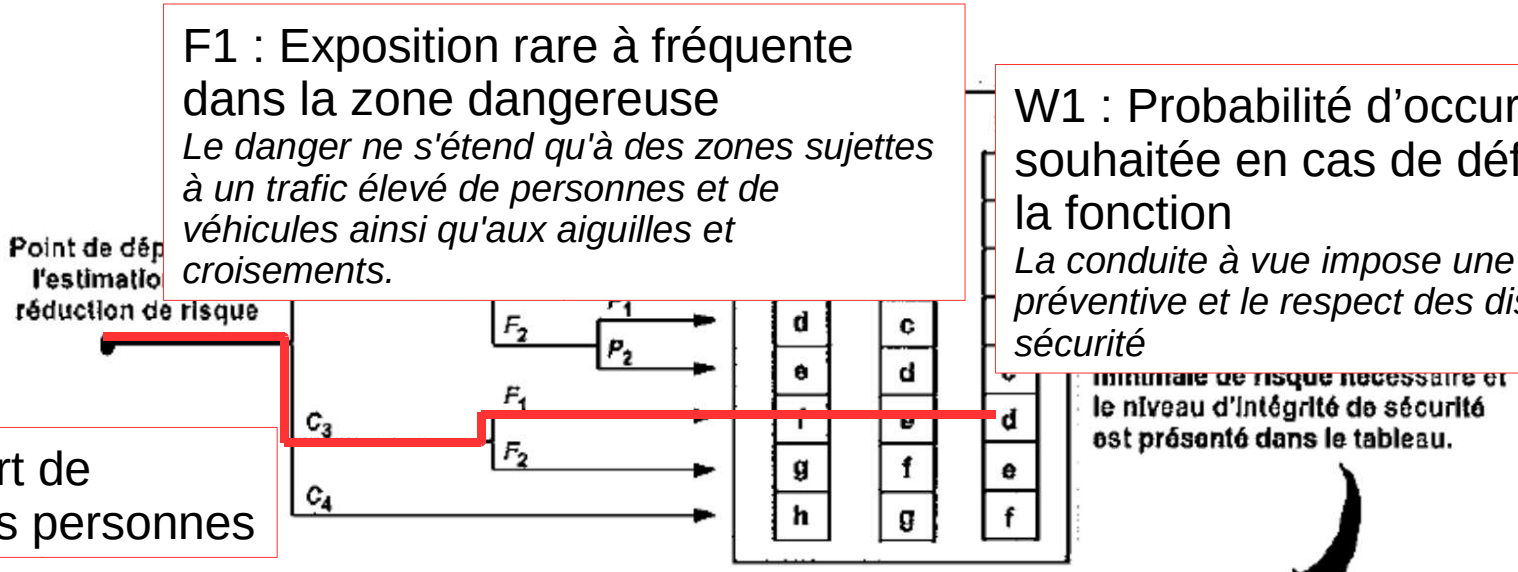
F1 : Exposition rare à fréquente dans la zone dangereuse

Le danger ne s'étend qu'à des zones sujettes à un trafic élevé de personnes et de véhicules ainsi qu'aux aiguilles et croisements.

W1 : Probabilité d'occurrence non souhaitée en cas de défaillance de la fonction

La conduite à vue impose une conduite préventive et le respect des distances de sécurité

C3 : Mort de plusieurs personnes



C = Conséquence du paramètre de risque

F = Fréquence et durée de l'exposition au paramètre de risque

P = Possibilité d'éviter le paramètre de risque dangereux

W = Probabilité d'occurrence non souhaitée

a, b, c ... h = Estimation de la réduction de risque nécessairepour les SRS

Réduction minimale de risque nécessaire	Niveau d'intégrité de sécurité
-	Pas d'exigence de sécurité
a	Pas d'exigence de sécurité spéciale
b, c	1
d	2
e, f	3
g	4
h	Un système E/E/PE n'est pas suffisant

IEC 1 667/98

Figure E.2 – Graphe de risque – exemple (illustre seulement les principes généraux)

« Absence de commande FU par manipulateur » - Graphe **exemple** de la 61508

F1 : Exposition rare à fréquente dans la zone dangereuse

Le danger ne s'étend qu'à des zones sujettes à un trafic élevé de personnes et de véhicules ainsi qu'aux aiguilles et croisements.

W1 : Probabilité d'occurrence non souhaitée en cas de défaillance de la fonction

La conduite à vue impose une conduite préventive et le respect des distances de sécurité

C3 : Mort de plusieurs personnes

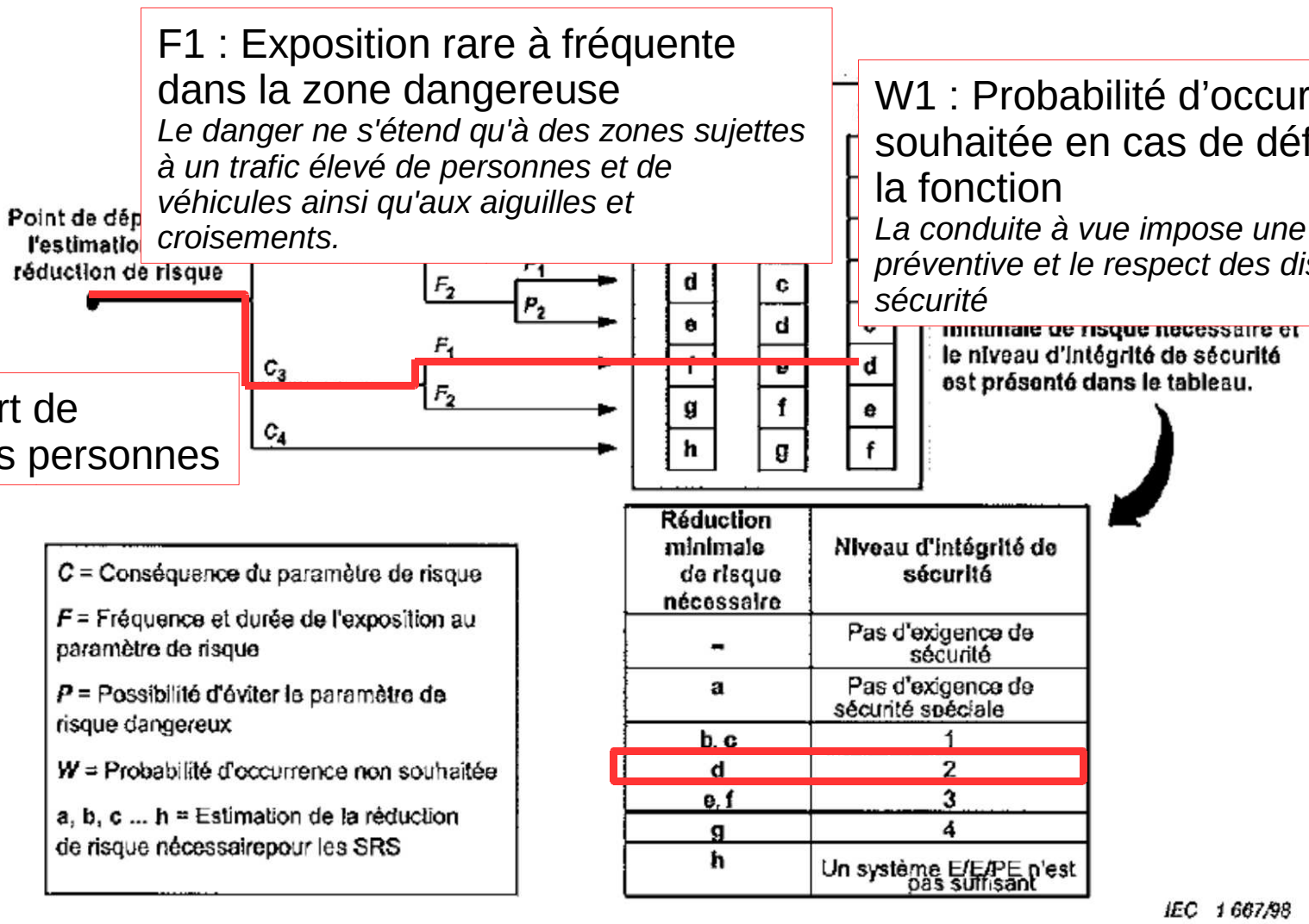
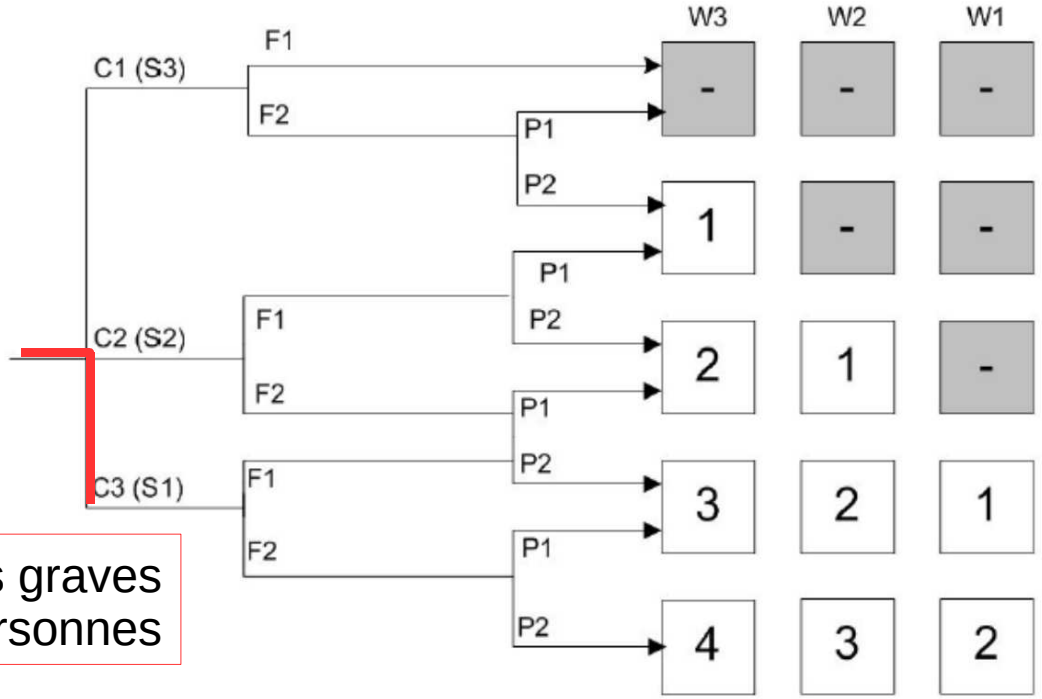


Figure E.2 – Graphe de risque – exemple (illustre seulement les principes généraux)

« Absence de commande FU par manipulateur »

Exemple EN 61508 avec proposition d'étalonnage



C3 : Mort ou blessures graves pour plusieurs personnes

4 : SIL4 est équivalent à un THR inférieur à 10^{-8} ($THR < 10^{-8}$) ;

3 : SIL3 est équivalent à un THR inférieur à 10^{-7} ($10^{-8} \leq THR < 10^{-7}$) ;

2 : SIL2 est équivalent à un THR inférieur à 10^{-6} ($10^{-7} \leq THR < 10^{-6}$) ;

1 : SIL1 est équivalent à un THR inférieur à 10^{-5} ($10^{-6} \leq THR < 10^{-5}$).

-: Aucune exigence spécifique en matière de sécurité

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

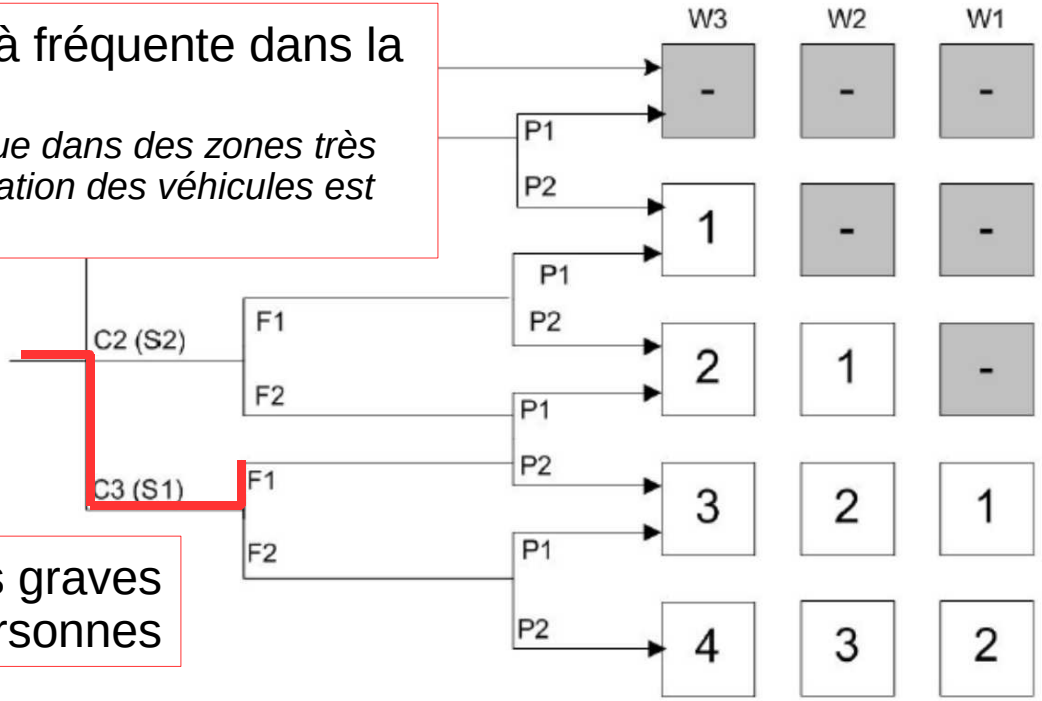
« Absence de commande FU par manipulateur »

Exemple EN 61508 avec proposition d'étalonnage

F1 : Exposition rare à fréquente dans la zone dangereuse

Le danger n'est présent que dans des zones très fréquentées et/ou la circulation des véhicules est importante

C3 : Mort ou blessures graves pour plusieurs personnes



4 : SIL4 est équivalent à un THR inférieur à 10^{-8} ($THR < 10^{-8}$) ;

3 : SIL3 est équivalent à un THR inférieur à 10^{-7} ($10^{-8} \leq THR < 10^{-7}$) ;

2 : SIL2 est équivalent à un THR inférieur à 10^{-6} ($10^{-7} \leq THR < 10^{-6}$) ;

1 : SIL1 est équivalent à un THR inférieur à 10^{-5} ($10^{-6} \leq THR < 10^{-5}$).

-: Aucune exigence spécifique en matière de sécurité

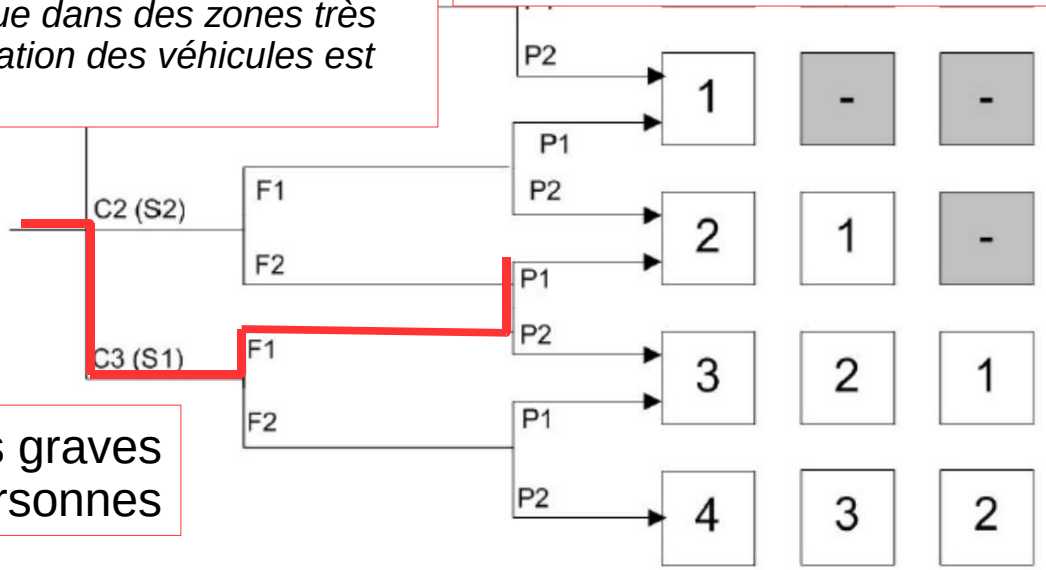
STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

« Absence de commande FU par manipulateur »

Exemple EN 61508 avec proposition d'étalonnage

F1 : Exposition rare à fréquente dans la zone dangereuse
Le danger n'est présent que dans des zones très fréquentées et/ou la circulation des véhicules est importante

P1 : Possibilité d'éviter les dangers
Le conducteur peut taper le FS



C3 : Mort ou blessures graves pour plusieurs personnes

4 : SIL4 est équivalent à un THR inférieur à 10^{-8} (THR < 10^{-8}) ;

3 : SIL3 est équivalent à un THR inférieur à 10^{-7} (10^{-8} ≤ THR < 10^{-7}) ;

2 : SIL2 est équivalent à un THR inférieur à 10^{-6} (10^{-7} ≤ THR < 10^{-6}) ;

1 : SIL1 est équivalent à un THR inférieur à 10^{-5} (10^{-6} ≤ THR < 10^{-5}).

-: Aucune exigence spécifique en matière de sécurité

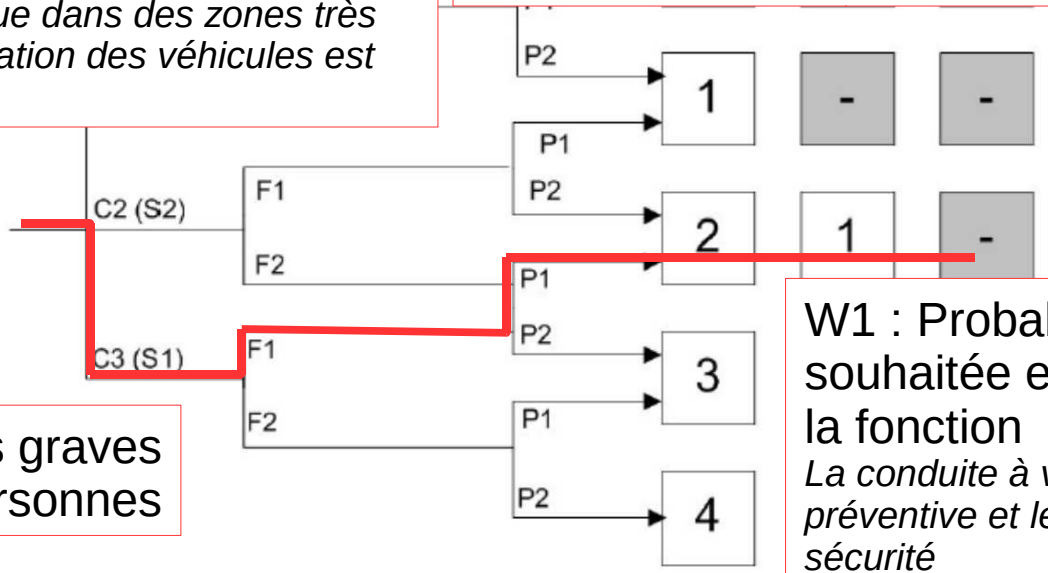
STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

« Absence de commande FU par manipulateur »

Exemple EN 61508 avec proposition d'étalonnage

F1 : Exposition rare à fréquente dans la zone dangereuse
Le danger n'est présent que dans des zones très fréquentées et/ou la circulation des véhicules est importante

P1 : Possibilité d'éviter les dangers
Le conducteur peut taper le FS



C3 : Mort ou blessures graves pour plusieurs personnes

W1 : Probabilité d'occurrence non souhaitée en cas de défaillance de la fonction
La conduite à vue impose une conduite préventive et le respect des distances de sécurité

4 : SIL4 est équivalent à un THR inférieur à 10^{-8} (THR < 10^{-8}) ;

3 : SIL3 est équivalent à un THR inférieur à 10^{-7} (10^{-8} ≤ THR < 10^{-7}) ;

2 : SIL2 est équivalent à un THR inférieur à 10^{-6} (10^{-7} ≤ THR < 10^{-6}) ;

1 : SIL1 est équivalent à un THR inférieur à 10^{-5} (10^{-6} ≤ THR < 10^{-5}).

-: Aucune exigence spécifique en matière de sécurité

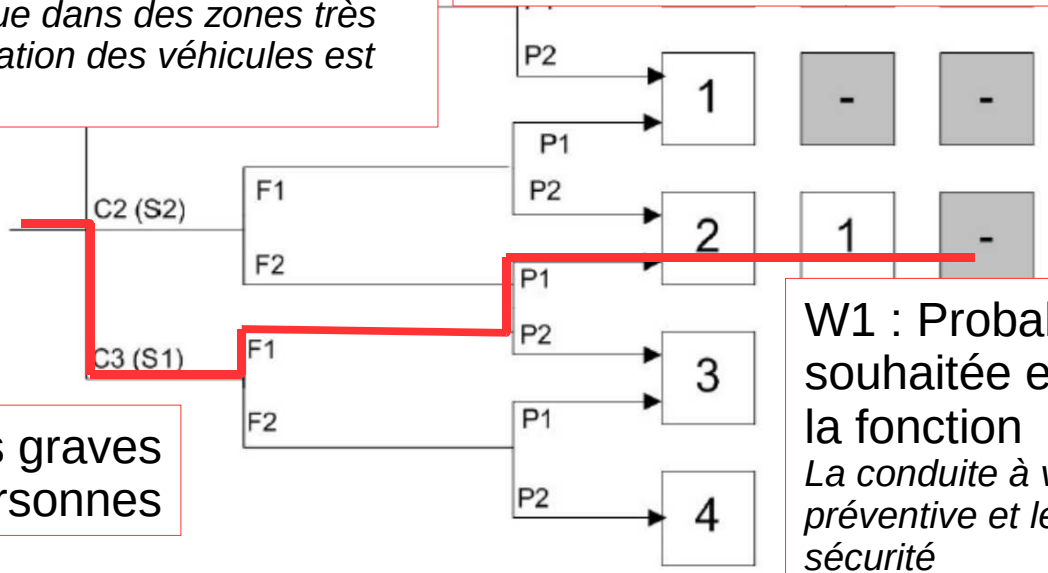
STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

« Absence de commande FU par manipulateur »

Exemple EN 61508 avec proposition d'étalonnage

F1 : Exposition rare à fréquente dans la zone dangereuse
Le danger n'est présent que dans des zones très fréquentées et/ou la circulation des véhicules est importante

P1 : Possibilité d'éviter les dangers
Le conducteur peut taper le FS



C3 : Mort ou blessures graves pour plusieurs personnes

W1 : Probabilité d'occurrence non souhaitée en cas de défaillance de la fonction
La conduite à vue impose une conduite préventive et le respect des distances de sécurité

4 : SIL4 est équivalent à un THR inférieur à 10^{-8} (THR < 10^{-8}) ;

3 : SIL3 est équivalent à un THR inférieur à 10^{-7} (10^{-8} ≤ THR < 10^{-7}) ;

2 : SIL2 est équivalent à un THR inférieur à 10^{-6} (10^{-7} ≤ THR < 10^{-6}) ;

1 : SIL1 est équivalent à un THR inférieur à 10^{-5} (10^{-6} ≤ THR < 10^{-5}).

-: Aucune exigence spécifique en matière de sécurité

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

Synthèse

Pour un même danger « Absence de commande FU par manipulateur »

Trois résultats différents selon les approches EN 50126 et EN 61508
=> SIL3, SIL 2 et pas de SIL

=> Forte réticence du STRMTG à utiliser la norme EN 61508 pour **l'allocation des niveaux de sécurité** alors qu'une norme sectorielle existe citée dans la réglementation des TGU

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

Merci de votre attention