Qualification d'une télétransmission

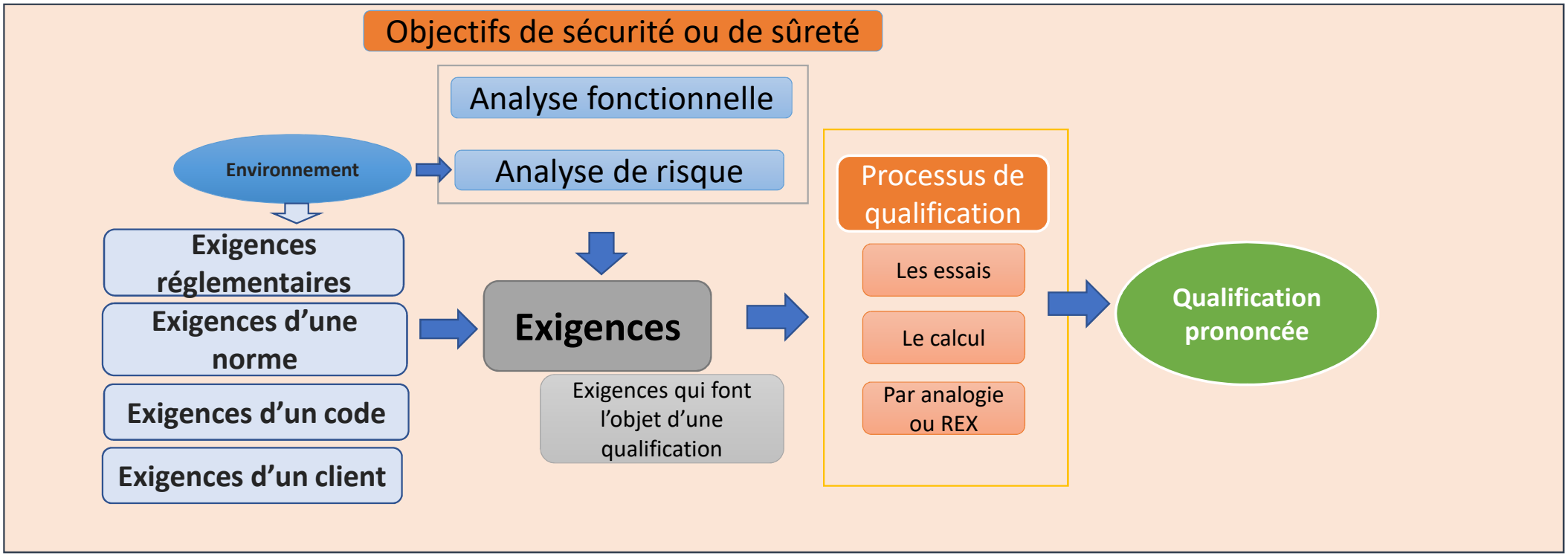
Alain JANVIER

Le 21 mars 2016

Définition

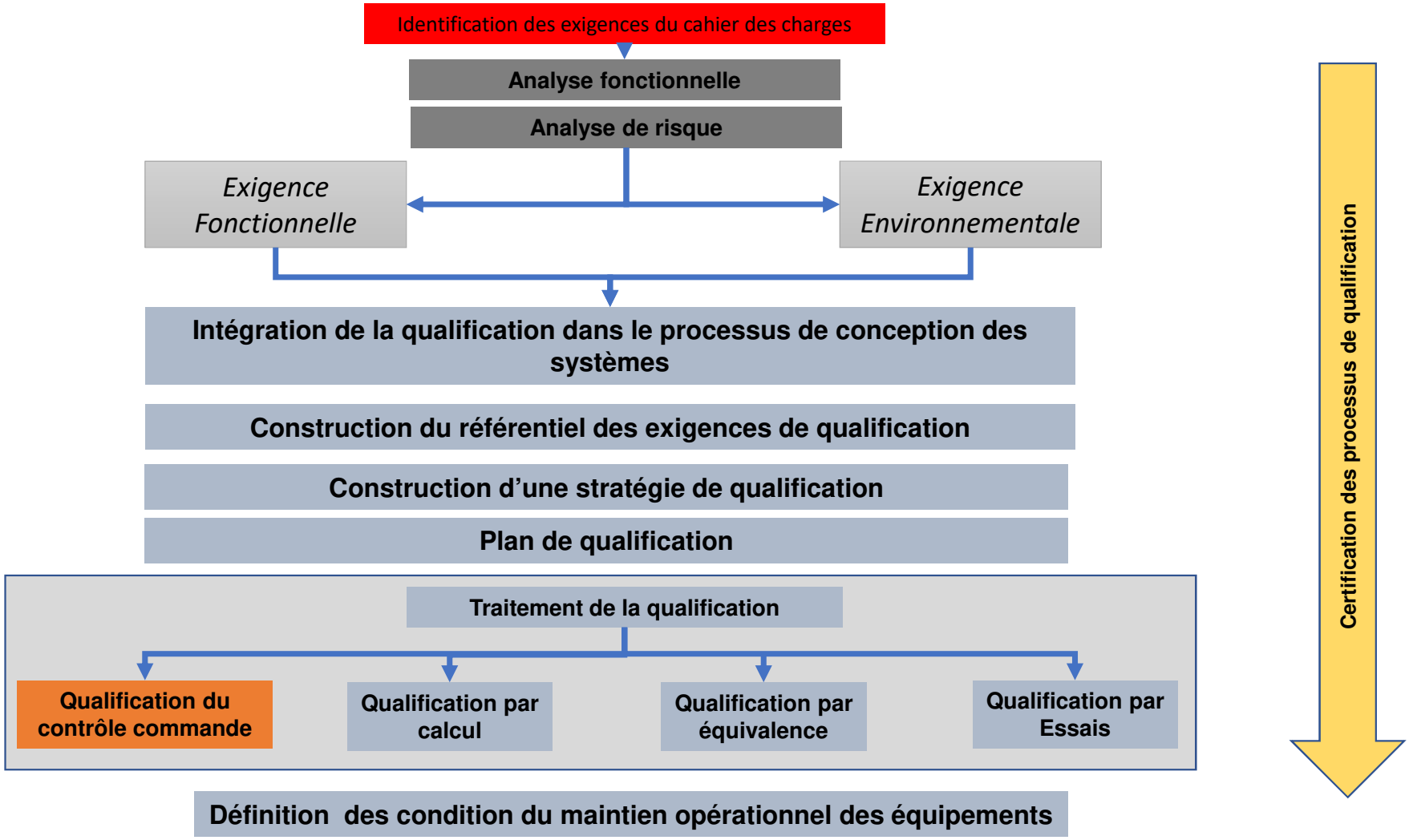
Qualification d'un équipement: (AFCEN)

La qualification d'un modèle est **la constatation** de la conformité d'un modèle à l'ensemble des exigences prescrites dans une norme ou une spécification technique, et suivant laquelle on reconnaît son aptitude à rendre le service requis dans toutes les conditions d'environnement où il peut se trouver.

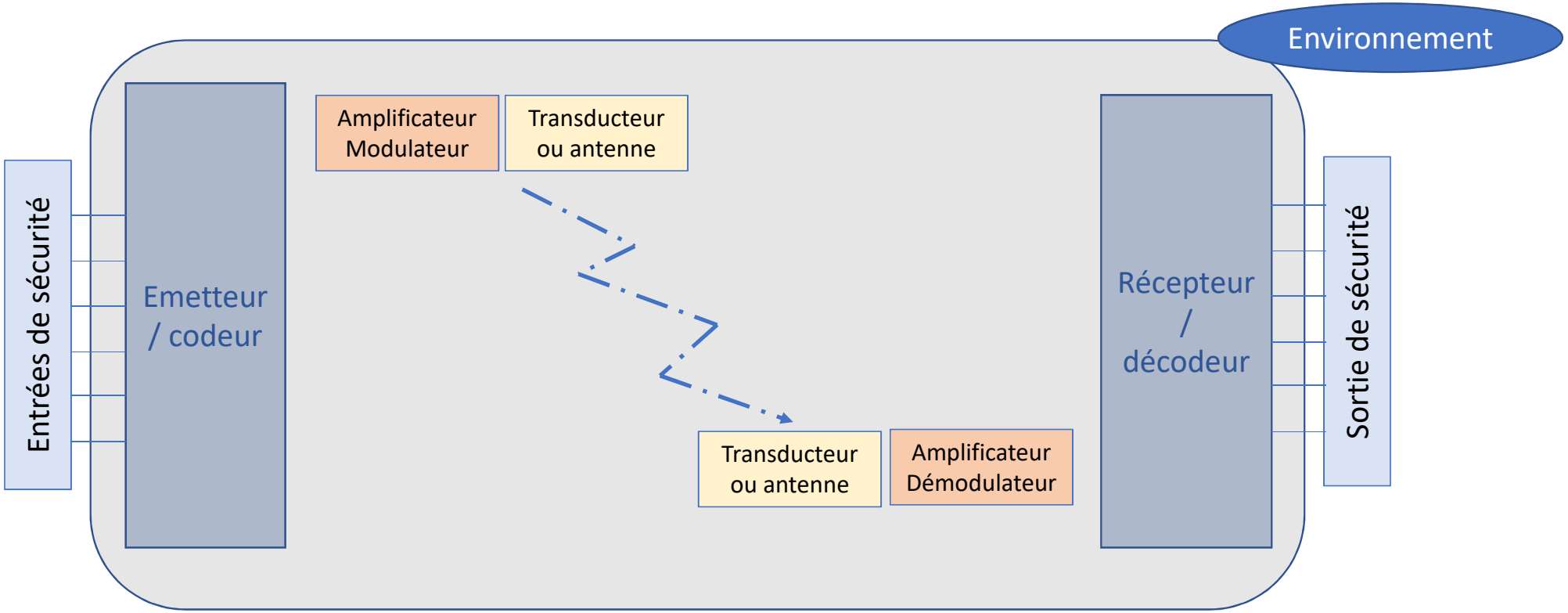


Son but est d'apporter la démonstration documentée que le matériel et les instructions sont aptes à remplir sa ou ses fonction(s) de sécurité ou de sûreté dans les conditions spécifiées.

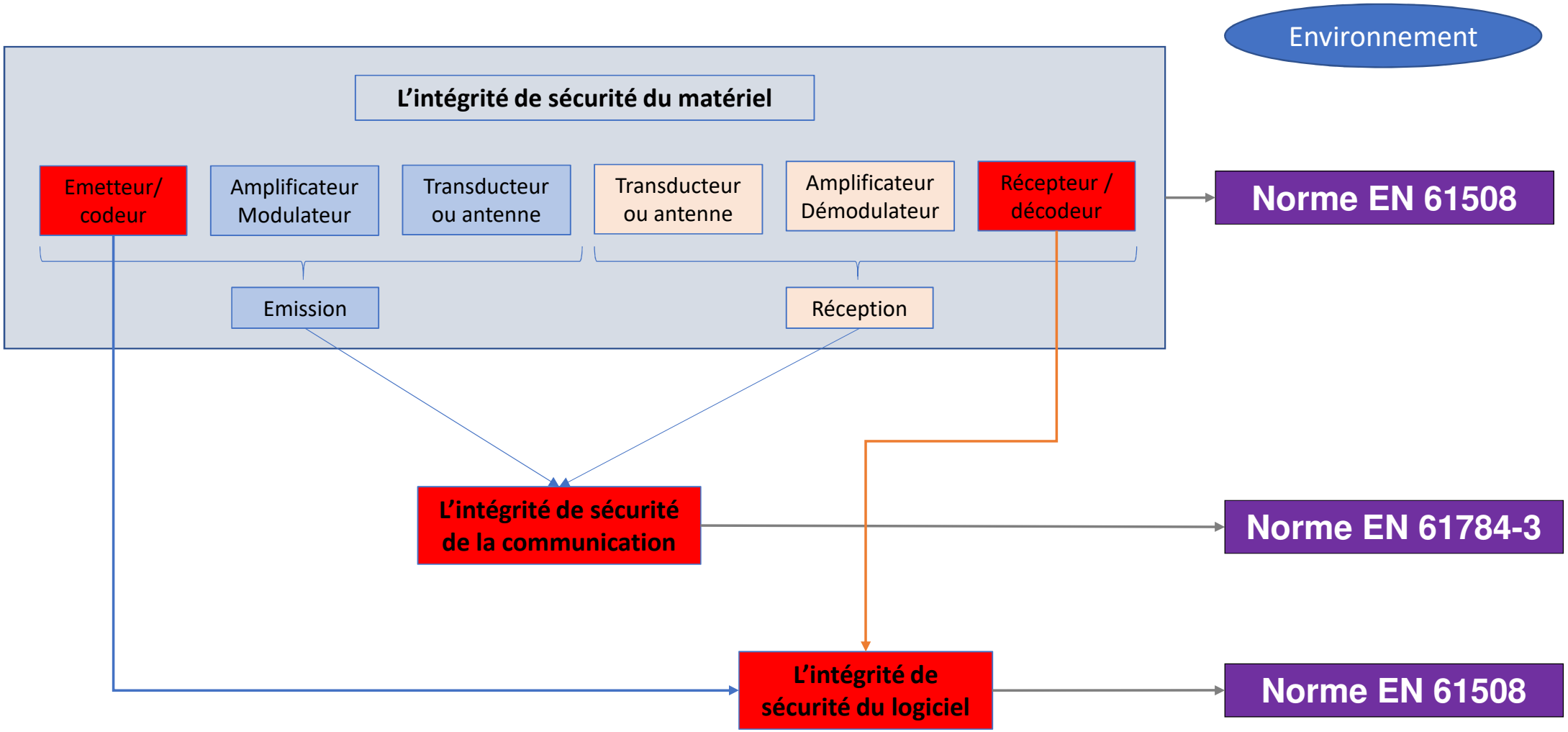
Démarche de qualification



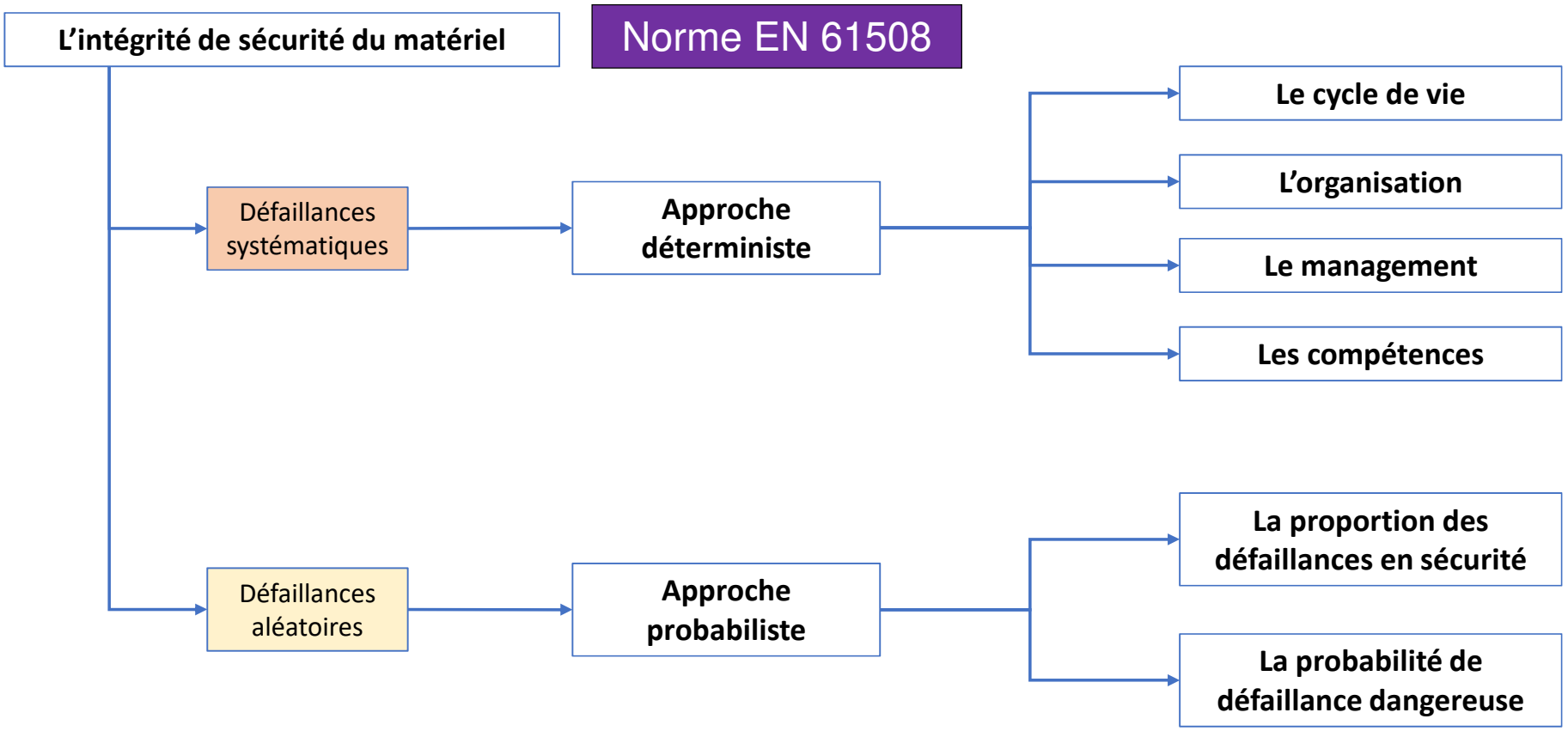
Qualification d'une télétransmission



Qualification d'une télétransmission



Qualification de la partie matériel



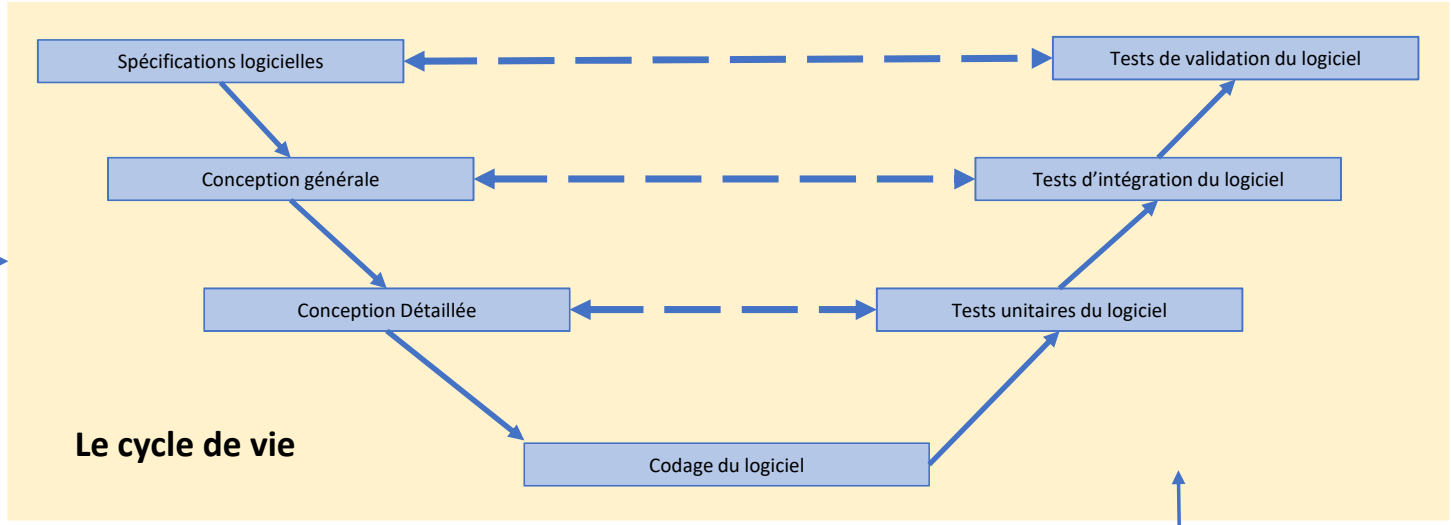
Qualification de la partie logiciel

L'intégrité de sécurité du logiciel

Norme EN 61508

Défaillances systématiques

Approche déterministe



L'organisation

Des phases du cycle de vie

Le management

Les compétences

Requises pour chaque phase du cycle de vie

Qualification de la partie logiciel

L'intégrité de sécurité du logiciel

Points importants de qualification

- **L'identification** des fonctions de sécurité traitées par le logiciel (spécifications)
- La définition des phases de construction du logiciel (organisation, compétences, documentation associée)
- La définition des phases de vérification du logiciel (organisation, compétences, documentation associée et indépendance / construction)
- La définition des phases de validation du logiciel (organisation, compétences, documentation associée et indépendance / construction)
- La cohérence entre les phases (management)
- **L'analyse des risques résiduels liés à la couverture des phases de vérification et de validation** (tests, analyses, examens, relectures, …)

Qualification de la partie communication

L'intégrité de sécurité de la communication*

Norme EN 61784-3

Approche déterministe

La résistance face aux menaces identifiées

- La corruption des messages
- La répétition de message non prévue
- La séquence incorrect des messages
- La perte de messages
- Le retard inacceptable sur la transmission de messages
- L'insertion de messages
- La mascarade
- L'erreur d'adressage

Assuré par le logiciel

LE LOGICIEL

Supporté par le logiciel

Protocole de communication

Approche probabiliste

La probabilité de défaillance dangereuse du canal de communication

- Le calcul du taux d'erreurs résiduelles

*Canal noir

Qualification de la partie communication

L'intégrité de sécurité de la communication – Approche déterministe

La norme EN 61784-3 préconise des solutions techniques pour le traitement des menaces :

Erreurs de communication	Mesures de sécurité							
	Numéro de séquence (voir 5.4.2)	Horodatage (voir 5.4.3)	Délai (voir 5.4.4)	Authentification de connexion (voir 5.4.5)	Message en retour (voir 5.4.6)	Assurance d'intégrité des données (voir 5.4.7)	Redondance avec contre-vérification (voir 5.4.8)	Différents systèmes d'assurance d'intégrité des données (voir 5.4.9)
Corruption (voir 5.3.2)					X[d]	X	Uniquement pour un bus série [c]	
Répétition non prévue (voir 5.3.3)	X	X					X	
Séquence incorrecte (voir 5.3.4)	X	X					X	
Perte (voir 5.3.5)	X				X		X	
Retard inacceptable (voir 5.3.6)		X	X[b]					
Insertion (voir 5.3.7)	X[e]	X[e]		X[a]	X		X	
Déguisement (voir 5.3.8)				X	X[d]			X
Adressage (voir 5.3.9)				X				

Qualification de la partie communication

L'intégrité de sécurité de la communication – Approche probabiliste

La norme EN 61784-3 préconise que le canal de communication ne consomme pas plus de 1 % de la probabilité de défaillance dangereuse totale de la fonction de sécurité

Applicable pour les fonctions de sécurité jusqu'au niveau SIL	Probabilité d'une défaillance dangereuse par heure pour le système de communication de sécurité fonctionnelle	Taux d'erreurs résiduelles maximal admissible pour le système de communication de sécurité fonctionnelle
4	$< 10^{-10}$ / h	$\Lambda < 10^{-10}$ / h
3	$< 10^{-9}$ / h	$\Lambda < 10^{-9}$ / h
2	$< 10^{-8}$ / h	$\Lambda < 10^{-8}$ / h
1	$< 10^{-7}$ /h	$\Lambda < 10^{-7}$ / h
NOTE Les valeurs données dans ce tableau sont basées sur l'hypothèse selon laquelle la contribution du système de communication de sécurité fonctionnelle au nombre total de défaillances de la fonction de sécurité ne dépasse pas 1%.		

Par exemple, pour un niveau d'intégrité de sécurité SIL3 recherché, le taux d'erreurs résiduelles maximal du canal de communication doit être : $\Lambda < 1.10^{-9}$

Qualification de la partie communication

L'intégrité de sécurité de la communication – Approche probabiliste

Calcul du taux d'erreurs résiduelles par heure du canal de communication :

$$\lambda_{SC}(Pe) = R_{SC}(Pe) \times v \quad (1)$$

$$\lambda_{SCL}(Pe) = \lambda_{SC}(Pe) \times m \quad (2)$$

Eléments de l'équation	Définition
λ_{SC} (Pe)	Taux d'erreurs résiduelles par heure du canal de communication de sécurité par rapport à la probabilité d'erreurs sur les éléments binaires (voir 3.1.36)
λ_{SCL} (Pe)	Taux d'erreurs résiduelles par heure de la couche de communication de sécurité en fonction de la probabilité d'erreurs sur les éléments binaires (voir 3.1.36)
Pe	Probabilité d'erreurs sur les éléments binaires (voir Article B.3) **/ Préconisation : Pe = 10^{-2}**
R_{SC} (Pe)	Probabilité d'erreurs résiduelles du canal de communication de sécurité en fonction de la probabilité d'erreurs sur les éléments binaires (voir 3.1.35)
v	Fréquence d'échantillonnage maximale des SPDU par heure
m	Nombre maximal de connexions logiques autorisé dans une seule fonction de sécurité (voir la Figure 9 et la Figure 10)

Merci de votre attention