# Concevoir en fonction du risque

# 1. Définition d’une analyse des risques

Analyse ayant pour objet d’identifier et d’évaluer des risques (*) liés à l’utilisation d’un système.

(*) risques des personnes et des biens confiés

## 2. Pourquoi faire une analyse des risques

- Parce que exigée par la loi:

Pour les risques des personnes, la direction machine n° 2006/42/CE (révisée et applicable depuis le 1er janvier 2010) précise que :

1. La sécurité est obligatoire et doit être intégrée à la conception. Le fabricant doit donc concevoir à partir de l'analyse des risques.
2. Le respect des exigences essentielles est impératif, même si elles sont à appliquer avec discernement en tenant compte des contraintes économiques
3. Les obligations du fabricant concernent les emplois prévus mais aussi les mauvais usages raisonnablement prévisibles. Elles ne concernent pas les usages fantaisistes.
4. Le fabricant doit faire la preuve de la conformité de sa machine aux exigences essentielles au travers de la constitution d'un dossier technique qui est obligatoire

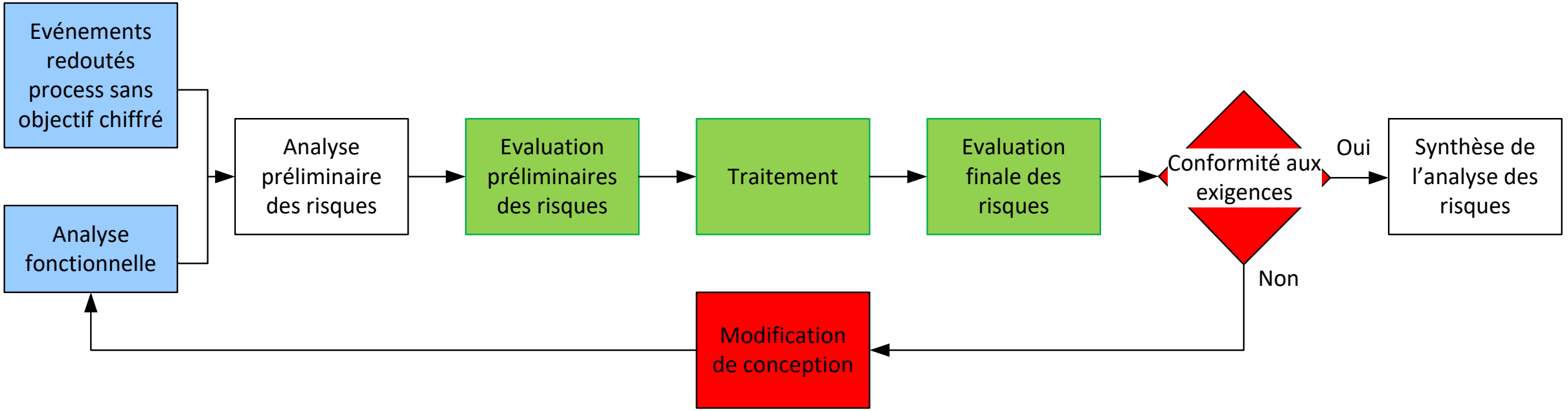
- Pour assurer aux exploitants un usage sécurisé de leur machine sans dégradation de leur outils de production (risques des biens confiés) CRT 018

# 3. Risques des biens confiés

Deux approches sont possibles:

- Cas 1 : L’approche qualitative.
- Cas 2 : L’approche quantitative.

# 3.1 Cas 1 –L'approche qualitative - Démarche générale



## a. Données d’entrées

- L’analyse fonctionnelle en cours de rédaction mais suffisamment avancée pour définir les fonctions principales de l’application (déroulé opératoire), fonctions qui feront l’objet de l’APR

- Les évènements redoutés « process » du client
  - Note EDF D30591140056664

## b. Analyse préliminaire des risques APR

➢ Définition

L'APR permet :

- ➢ D'identifier systématiquement l'ensemble des évènements redoutés potentiels de la machine, susceptibles de compromettre les événements redoutés process
- ➢ De mettre en évidence les causes et les scénarii générateurs de ces évènements redoutés,

➢ Méthode

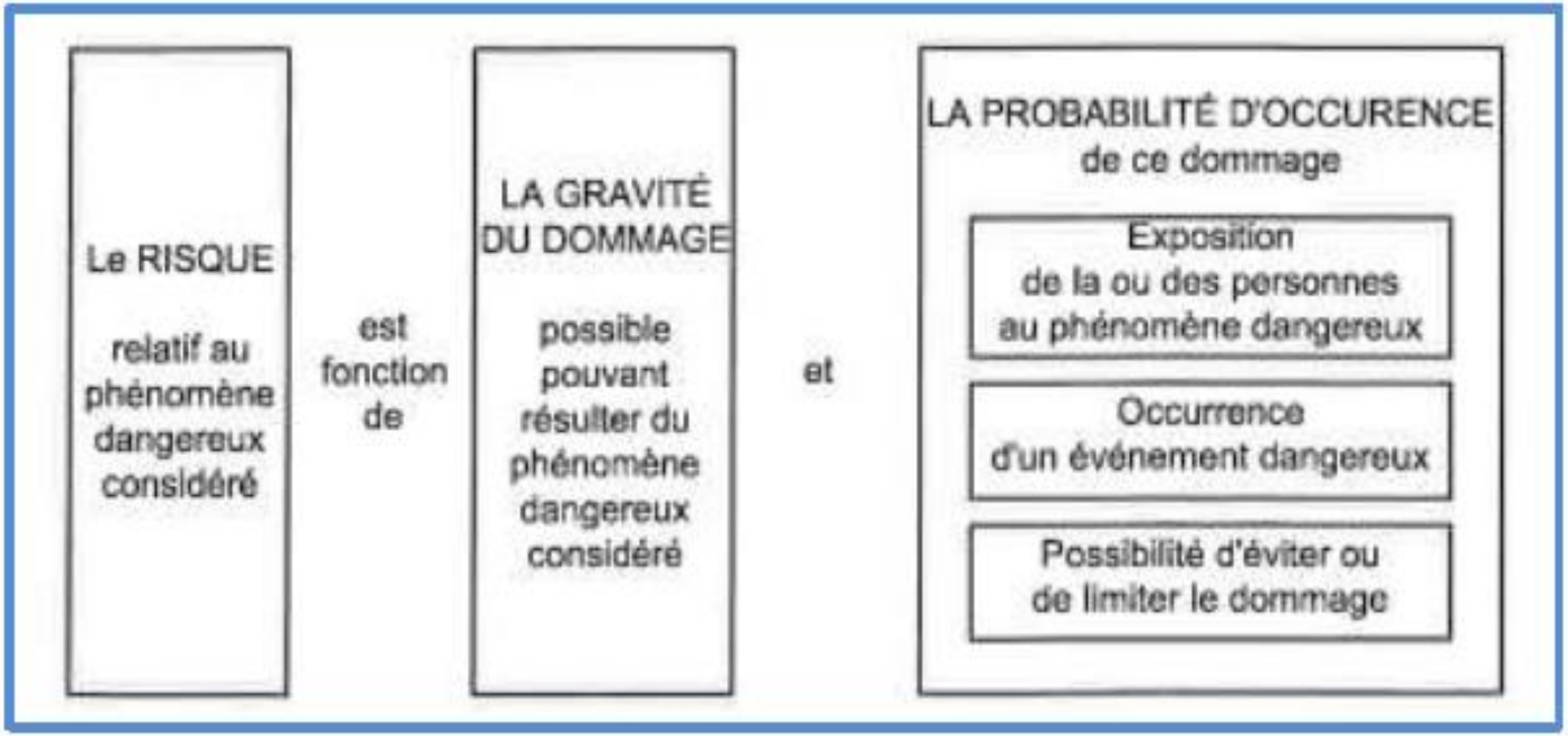
Etape 1 : identification des fonctions à réaliser par la machine (analyse fonctionnelle)

Etape 2 : identification des événements redoutés machine selon les modes de défaillances des fonctions suivants :

- Pas de fonction : non activation de la fonction demandée
- Perte de la fonction : fonction arrêtée en cours d'exécution
- Non-arrêt de la fonction : défaillance d'arrêt à un moment prescrit
- Fonction dégradée : performances nominales non tenues
- Fonction intempestive: Fonctionnement prématuré

## c. Evaluation préliminaire des risques

Pour chaque situation dangereuse, une évaluation du risque est effectuée selon le principe ci-dessous :



## c. Evaluation préliminaire des risques

En général, la cotation de la gravité s'effectue selon quatre classes de gravité : de G1 (mineure) à G4 (catastrophique)

| Niveau | Gravité | Conséquence d'une défaillance |
|---|---|---|
| G1 | Mineure | - Sans effet sur les personnes et les biens<br>- Panne simple, mineure : défaillance fonctionnelle négligeable, les performances sont maintenues |
| G2 | Majeure | - Blessures ou maladies légères<br>- Indisponibilité avec réparation sans perte d'exploitation significative : panne d'une fonction non essentielle et fonctionnement possible après réparation (interruption courte de la mission) |
| G3 | Sérieuse | - Blessures ou maladies incapacitantes<br>- Indisponibilité avec réparation et perte significative d'exploitation : dégradation irréversible d'une fonction essentielle, le temps d'intervention est pénalisant. |
| G4 | Catastrophique | - Mort d'hommes<br>- Situation accidentelle avec dommages graves sur le système (destruction de biens confiés)<br>- Impact environnemental |

## c. Evaluation préliminaire des risques

En général, la cotation de la probabilité d'occurrence s'effectue selon les quatre classes suivantes définies de P1 (très faible) à P4 (forte)

| Classe | Probabilité d'occurrence (description) | Fréquence or Probabilité | |
|---|---|---|---|
| | | Fréquence | Probabilité |
| **P1** | Très improbable ou impossible | Jamais sur la durée de vie de l'appareil | $P < 10^{-9}/h$ |
| **P2** | Rare | Pas plus d'une fois sur la durée de vie de l'appareil | Entre $10^{-6}$ et $10^{-9}/h$ |
| **P3** | Probable | Pas plus d'une fois sur le temps de fonctionnement annuel | Entre $10^{-3}$ et $10^{-6}/h$ |
| **P4** | Très probable | Plus d'une fois sur le temps de fonctionnement annuel | $P > 10^{-3}/h$ |

## c. Evaluation préliminaire des risques

La criticité du risque est le caractère critique de l'événement apprécié à l'aide du couple gravité/probabilité d'occurrence selon la matrice de criticité ci-dessous :

| **Gravité** (Santé et Sécurité) | | | | | |
|---|---|---|---|---|---|
| | **G4** | **3** | **3** | **3** | **3** |
| | **G3** | **2** | **3** | **3** | **3** |
| | **G2** | **2** | **2** | **2** | **3** |
| | **G1** | **1** | **1** | **1** | **1** |
| | | **P1** | **P2** | **P3** | **P4** |
| | | **Probabilité d'occurrence** | | | |

Avec les niveaux de criticité suivants

| Niveaux de criticité | Catégorie |
|---|---|
| 1 | Acceptable |
| 2 | Tolérable |
| 3 | Inacceptable |

## d. Réduction des risques

Les recommandations / mesures de réduction du risque ont pour objectif de :

- Donner des recommandations pour limiter la gravité du risque. Il s'agit de la désignation des dispositions à prendre, en conception et en exploitation, permettant d'atténuer la gravité du risque.
- Diminuer l'occurrence du risque en :
  - Réduisant la fréquence et/ou la durée d'exposition au phénomène dangereux ;
  - Réduisant la probabilité d'occurrence des évènements dangereux possibles ;
  - Mettant en place des moyens pour éviter le risque.

## e. Evaluation finale des risques/conformité aux exigences

Une évaluation de la criticité du risque résiduel, c'est-à-dire après la prise en compte des mesures de réduction du risque est effectuée afin de vérifier que les barrières proposées sont suffisantes pour satisfaire le niveau de risque « Acceptable ».

Si après réduction le risque reste au niveau « Tolérable » ou « Inacceptable » les actions suivantes doivent être engagées dans cet ordre :

Action 1: revoir la conception afin de trouver une parade de réduction

Action 2 : identifier avec l'exploitant de la machine des moyens additionnels de réduction du risque (interverrouillage avec une autre machines, consignes d'exploitation…)

Action 3 : si aucune mesure de réduction n'est possible le risque doit être considéré comme résiduel.

## f. Synthèse

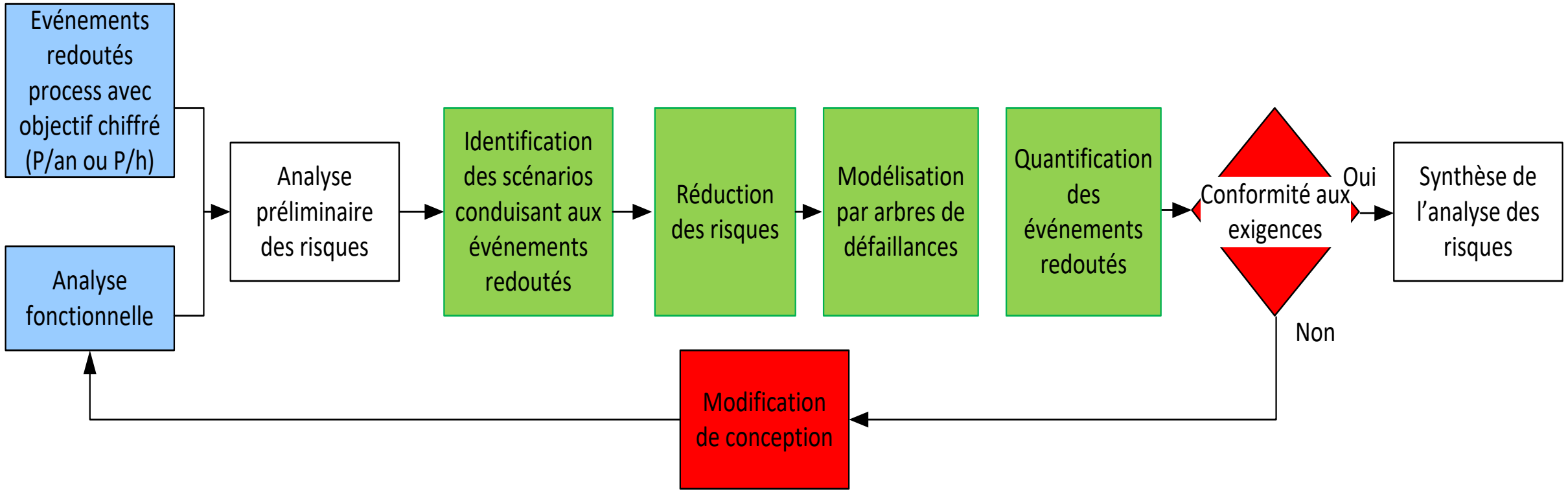
La synthèse de l'analyse des risques doit identifier clairement :

- Les risques résiduels. Ces risques seront également rappelés dans la notice d'instruction,

- Les parades exportées à l'exploitation c'est-à-dire les parades de réduction des risques qui sont de la responsabilité de l'exploitant,

- La liste des fonctions de sécurités qui devront être mises en œuvre durant la conception de la machine pou réduire/éliminer les risques identifiés.

## 3.2 Cas 2 – L'approche quantitative - Démarche générale



## a. Données d'entrées

➢ L'analyse fonctionnelle en cours de rédaction mais suffisamment avancée pour définir les fonctions principales de l'application (déroulé opératoire), fonctions qui feront l'objet de l'APR

➢Les évènements redoutés du client avec un objectif chiffré en terme de probabilité d'occurrence du type probabilité par heures de fonctionnement ou par an.

- **Exemple : chute de la charge avec une probabilité d'occurrence inférieure à 10-7/ an**

## b. Analyse préliminaire des risques/ Indentification des scénarios/ réduction des risques

Démarche identique au cas 1. Le but étant d'identifier les scenarios de défaillances qui conduiront aux évènements redoutés et de définir les parades de réduction.

## c. Modélisation par arbres de défaillances

Il s'agit de modéliser l'ensemble des composants mécanique et électrique qui interviennent dans le scénarios de défaillances et les parades de réduction identifiés

## d. Quantification des événements redoutés

Il s'agit de calculer la probabilité d'occurrence de l'événement ainsi modélisé à partir de la durée de mission de la machine et des données de fiabilité de tous les composants impliqués dans le scénario

- **Exemple**

## e. Conformité/Synthèse

Il s'agit de comparer le résultats du calcul de probabilité avec l'objectif fixé. Des modifications de conception sont à envisager tant que l'objectif n'est pas atteint

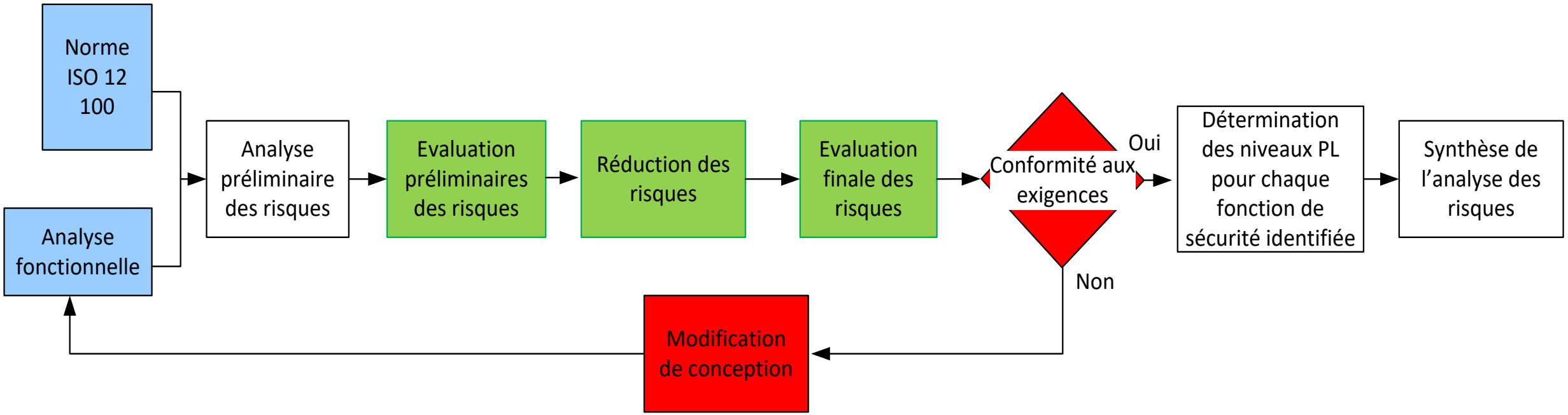
- **Exemple**

La synthèse confirme que l'objectif est atteint et précise l'ensemble des conditions requises (données de fiaibilité des composants)

- **Exemple**

# 4 Analyse des risques des personnes

## 4.1 Démarche générale



## 4.2 Données d'entrées

- L'analyse fonctionnelle en cours de rédaction mais suffisamment avancée pour définir les fonctions principales de l'application (déroulé opératoire), fonctions qui feront l'objet de l'APR
- Les normes ISO 12100 & ISO 14121

Les normes EN ISO 12100 et EN ISO 14121 fournissent une explication élémentaire des principes selon lesquels et des méthodes avec lesquelles l'appréciation du risque, l'analyse des risques et la réduction des risques doivent être réalisées.

La norme EN ISO 14121-1:2007 remplace la norme précédente EN 1050. L'EN ISO 12100, constituée de deux parties, remplace l'EN 292.

Ensemble, ces deux normes consistent un recueil des dangers, facteurs de risque et principes de conception à prendre en compte.

## 4.3 Analyse préliminaire des risques APR

➢**Idem risque biens confiés**

## 4.4 Evaluation préliminaire des risques

➢**Idem risque biens confiés**

| Classe | Gravité | Conséquence d'une défaillance |
|---|---|---|
| G1 | Mineure | Sans effet sur la santé et la sécurité des personnes. |
| G2 | Majeure | Impact mineur sur la santé et la sécurité des personnes : blessures ou maladie légères. |
| G3 | Sérieuse | Impact majeur sur la santé et la sécurité des personnes : blessures ou maladie sérieuse. |
| G4 | Catastrophique | Impact sérieux sur la santé et la sécurité des personnes : mort |

## 4.5 Réduction des risques

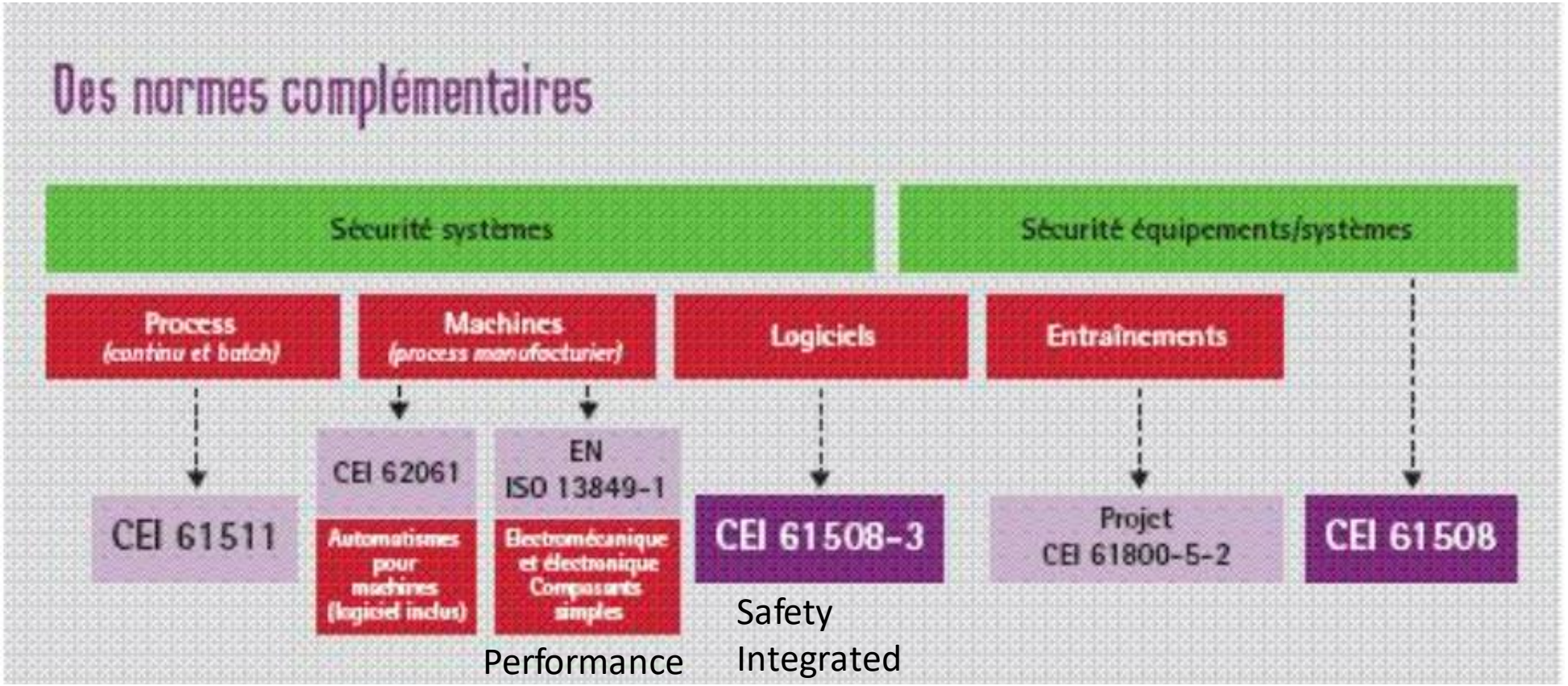
➢**Idem risque biens confiés**

## 4.6 Evaluation finale des risques/ conformité aux exigences

➢**Idem risque biens confiés**

.

## 4.7 Normes de sécurité




Les normes de sécurité ISO 13849 et CEI 61508 traitent du risques des personnes. La norme ISO 13849 prend en compte les aspects mécanique, électrique et hydraulique alors que la norme CEI 61508 se focalise sur les aspect électronique et logiciel.

## 4.7 Détermination des niveaux Pl

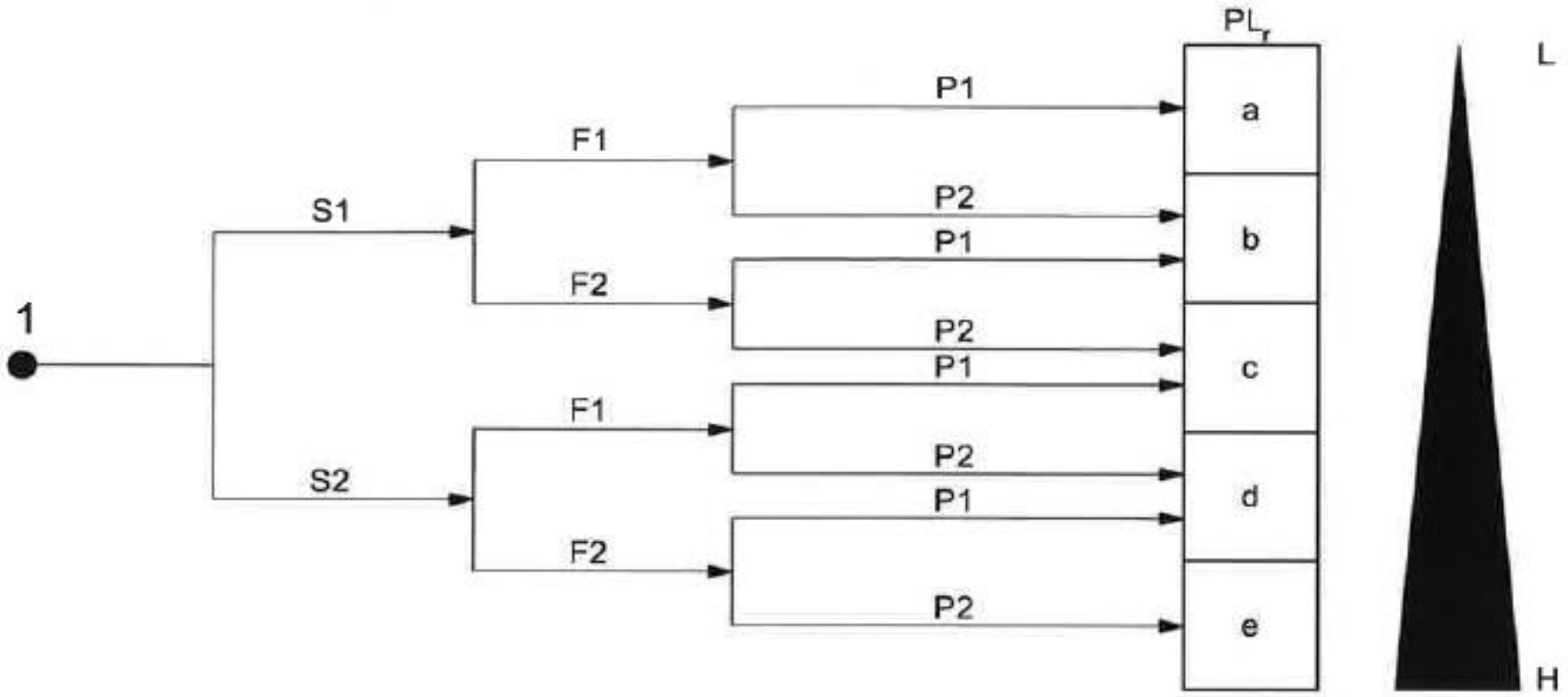
La détermination du niveau de PL sera effectuée pour l'ensemble des fonctions de sécurité identifiées pour réduire les risques des personnes.

D'après la norme NF EN ISO 13849-1, les paramètres de risque sont :

- S Gravité de la blessure :
  - S1 blessure légère (normalement réversible)
  - S2 blessure grave (normalement irréversible, y compris le décès)
- F fréquence et/ou durée d'exposition au phénomène dangereux
  - F1 rare à assez fréquente et/ou courte durée d'exposition
  - F2 fréquente à continue et/ou longue durée d'exposition
- P possibilité d'éviter le phénomène dangereux ou de limiter le dommage
  - P1 possible sous certaines conditions
  - P2 rarement possible

## 4.7. Détermination des niveaux Pl

Le niveau de PL est défini selon le graphique ci-dessous issu de l'annexe A de l'ISO13849-1 :



## 4.8 Synthèse

La synthèse de l’analyse des risques doit identifier clairement :

- Les risques résiduels. Ces risques seront également rappelés dans la notice d’instruction,

- Les parades exportées à l’exploitation c’est-à-dire les parades de réduction des risques qui sont de la responsabilité de l’exploitant,

- La liste des fonctions de sécurités qui devront être mises en œuvre durant la conception de la machine pou réduire/éliminer les risques identifiés avec leur niveau Pl associé.

# 5. Analyse des modes de défaillances de leurs effets et de leur criticité (AMDEC)

## 5.1. Définition

L'AMDEC est une analyse matérielle. Sur la base d'une décomposition matérielle et fonctionnelle qui définissent les composants ou groupes de composants, est réalisée une analyse de modes de défaillance et une évaluation de leurs effets et de leur criticité.

Elle complète l'APR.

## 5.2. Données d'entrée

L'arborescence matérielle basée sur les nomenclatures électriques et mécaniques :

=> 5.3. Données de sorties

L'AMDEC définit la liste des composants critiques

# 6. Analyse des risques approche menace

## 6.1. Méthodologie générale

L'approche menace consiste à analyser le moyen de manutention sous trois angles :

1) l'impact sur la machine d'agressions externes (une agression externe résulte d'une modification des caractéristiques des milieux extérieurs, en dehors des limites considérées comme définissant l'environnement normal. Exemple : erreurs humaines, jets de liquide, etc.)

2) la capacité de la machine à agresser des éléments de son environnement (Charge, opérateurs, autres moyens en interface, pièces tournantes non cartérisées…)

3) les menaces internes causées par la présence au sein de la machine d'éléments potentiellement dangereux (c'est-à-dire dont une défaillance est susceptible d'agresser d'autres éléments du moyen, exemple une marche frein serré pouvant déclencher un incendie).

## 6.2 Types de menaces étudiés

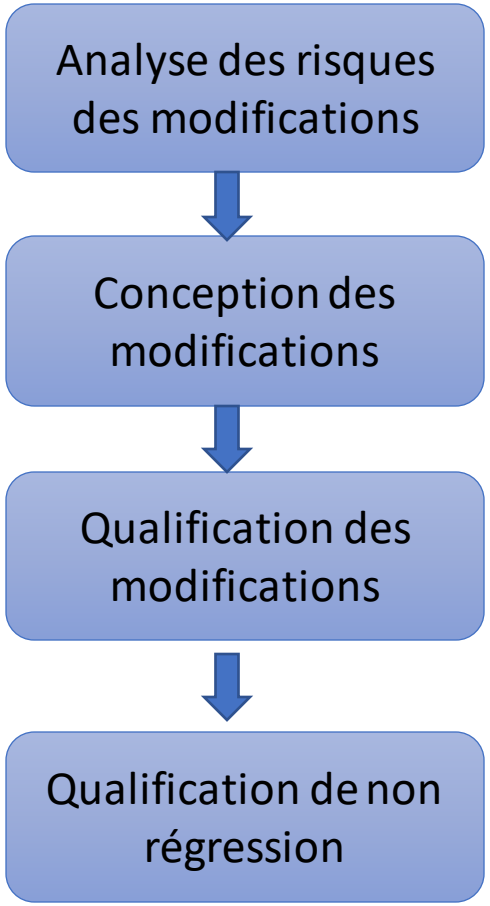
L'approche menace est établie à partir d'une liste générique de dangers définie à partir des conditions environnementales du cahier des charge (température, humidité, CEM etc..), du Rex REEL et des directives en analyses des risques, tel qu'une perte d'alimentation électrique, surtension, variation de fréquence etc…

Exemple :

# 7. Cas des modifications

## 7.1.Analyse de non régression

L'analyse de non régression se déroulent en 4 étapes




Les modifications envisagées introduisent – elles de nouveaux risques ?

Où sont localisées les modifications ?

Quels sont les critères de réception des modifications ?

Comment garantir que ce qui n'est pas modifié n'a pas été impacté par les modifications ?