SECURITE DES PATIENTS

Sécurité des prestations
Gestion des évènements indésirables associées aux soins

Pr Maxime K. DRABO
Dr NANA W. Félicité

Identification et traitement des RAS

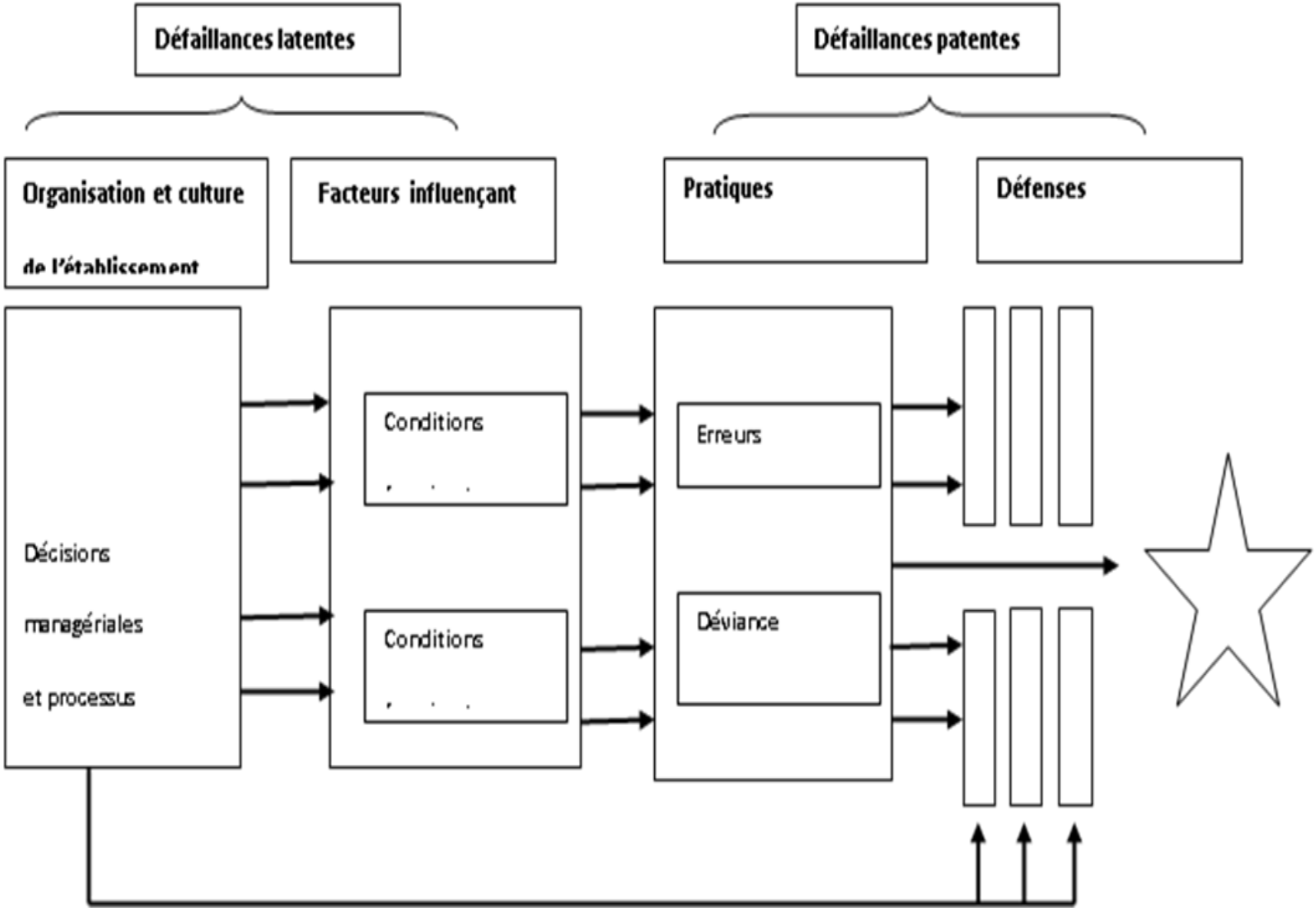
Typologie des défaillances

Typologie des défaillance modèle selon J. Reason

- de deux types distincts de défaillances :

- **les défaillances patentes ou erreurs actives:** est l'erreur de l'acteur de première ligne qui va être en lien direct avec l'accident (erreur de diagnostic).
- **les défaillances latentes:** caractéristique du système qui a contribué à la survenue de l'accident (surcharge de travail, fatigue, stress).

Typologie des défaillance modèle selon J. Reason



Typologie des défaillance
Source des défaillances

La compréhension de la survenue des accidents impose la prise en compte des différentes sources de défaillance.

- **Les défaillances techniques**
- **les erreurs humaines**
- **Les défaillances des systèmes liées à la notion de déviance**
- **Les défaillances des systèmes liées a l'organisation**

Défaillances techniques

- Les équipements peuvent connaître des défaillances se traduisant soit par:
- une interruption de fonctionnement (panne informatique entraînant une non-disponibilité des données patient, panne électrique, panne d'un dispositif médical),
- des fonctionnements anormaux (résultat erroné

fourni par un automate, dysfonctionnement du thermostat d'une couveuse, modification du débit d'une seringue électrique, etc.).

erreurs humaines

- La défaillance des systèmes complexes conduit à s'intéresser au rôle de l'erreur humaine.
- La littérature montre l’importance de l’erreur humaine. Ainsi, l’analyse des accidents impute 65 à 80 % des causes immédiates aux opérateurs de première ligne dans l’industrie et les transports publics (Woods et al., 1994 ; Hollnagel, 1993).
- Plusieurs notions sont à prendre en compte pour améliorer la sécurité des systèmes.

erreurs humaines

- La défaillance des systèmes complexes conduit à s'intéresser au rôle de l'erreur humaine.
- La littérature montre l’importance de l’erreur humaine. Ainsi, l’analyse des accidents impute 65 à 80 % des causes immédiates aux opérateurs de première ligne dans l’industrie et les transports publics (Woods et al., 1994 ; Hollnagel, 1993).
- Plusieurs notions sont à prendre en compte pour améliorer la sécurité des systèmes.

erreurs humaines

- **L'impossibilité de supprimer l'erreur du fonctionnement humain**
- L’erreur est inséparable de l’intelligence humaine (Reason, 1993).
- **La compréhension des différents mécanismes d'erreurs**

Reason en propose une classification en trois catégories :

  – les **erreurs de routine** correspondent au fonctionnement fondé sur les habitudes.

erreurs humaines

Il s'agit de défaillances dans la surveillance de l'exécution.

L'action se déroule sans contrôle conscient, dans le cadre de problèmes familiers.

Le sujet n'a pas pris conscience qu'il y avait un problème. Ce sont les erreurs les plus fréquentes ;

- les erreurs **d'activation de connaissance**

Le sujet est face à une difficulté qu'il ne peut pas résoudre de façon routinière. Il a conscience d'avoir un problème et cherche une solution.

erreurs humaines

L’erreur va résulter d’une mauvaise solution qui résulte elle même de l’activation d’une mauvaise règle.

Cette erreur n’est pas contradictoire avec l’idée que le sujet possède par ailleurs la connaissance de la bonne solution ; mais il n’a pas su l’activer, la recouvrir en mémoire, ou pas pu, faute de temps, s’en servir ; une autre solution moins valide mais immédiatement disponible -s’est imposée à sa logique d’action ;

erreurs humaines

- les erreurs de **possession de connaissance.**

Le sujet est ignorant de la solution du problème qu'il a à régler. Il mobilise toute sa cognition, lentement, pas à pas, pour produire une nouvelle solution. L'erreur peut alors revêtir différentes formes : bonne solution hors délais, mauvaise solution, etc.

Les défaillances des systèmes liées à la notion de déviance

- Des études récentes relatives à la sécurité montrent que tout système comporte une déviance volontaire par rapport aux normes, instructions et directives.
- Pour Vaughan, la déviance s'installe chez les opérateurs par extension progressive en raison, d'une part d'un contrôle de plus en plus approximatif du fait de l'absence d'incident et d'accident, et d'autre part de la tolérance de la hiérarchie

Les défaillances des systèmes liées à la notion de déviance

La déviance a les caractéristiques suivantes :

- elle est vue d'abord comme une source de bénéfice et non comme un risque ;
- elle permet, dans certains cas, une performance plus grande pour le système, pour le professionnel ou pour le patient ;
- elle est tolérée par la hiérarchie qui, parfois, la sollicite ;
- elle peut passer inaperçue lorsqu'elle est installée car l'ensemble des professionnels de l'hopital ou du secteur s'y est habitué

Les défaillances des systèmes liées à la notion de déviance

- La déviance est à distinguer de l'erreur.
- La déviance existe dans tout système et à chaque niveau (management, encadrement, opérateurs).
- La déviance est facteur potentiel de performance mais aussi de risque.
- La déviance est à reconnaître et à traiter en considérant le fait qu'elle correspond à un mécanisme d'adaptation du système.

Les défaillances des systèmes liées a l'organisation

- Dans toute organisation humaine, on constate des défaillances. Ces dernières peuvent porter atteinte à la sécurité.

Plusieurs circonstances peuvent favoriser ces défaillances :

- la survenue de dysfonctionnement dans un ou plusieurs processus particuliers ;
- la saturation de la capacité de l'établissement liée à une augmentation du flux d'activité ;

Les défaillances des systèmes liées a l’organisation

- l'inadaptation entre les besoins évolutifs à satisfaire et l'organisation en place ;
- l'interaction imprévue de plusieurs processus liée à des circonstances particulières d'occurrence rare. La complexité croissante des systèmes et l'augmentation du nombre d'intervenants diminue la visibilité des actions et de leurs effets.

Maitrise du risque

Maitrise du risque

- « l'erreur n'est pas évitable mais elle est relativement prévisible en fonction des enjeux de la situation, des conditions de travail, des compétences »Reason
- . Un système sûr n'est pas un système dans lequel il ne se commet pas d'erreurs, mais un système qui se protège par une suite de défenses en profondeur contre le développement « d'histoires d'accidents » à partir des erreurs commises.
- Aucune de ces défenses ne peut garantir la sécurité, mais leur empilement finit par conférer une fiabilité acceptable au système.

Maitrise du risque

La maitrise des risques combine :

- Une approche réactive qui s'intéresse a posteriori aux événements indésirables survenus ou avérés. Elle vise à limiter leur nombre ou à réduire leur conséquences par la mise en place d'actions correctives.
- Une approche préventive ou anticipative qui identifie a priori les événements redoutés ou événements indésirables par une analyse du système et de ses dangers. Elle comprend l'identification des situations dangereuses et des vulnérabilités de l'établissement puis la mise en place d'action préventive et le suivi de leur efficacité

Maitrise du risque: Identification du risque

La première étape dans la connaissance des risques est de les repérer. L'identification des risques se réalise grâce à plusieurs approches complémentaires.

- **Une identification a priori:** peut s'effectuer avant de débuter une nouvelle activité. Cela permet de gérer les risques prévisibles d'une activité afin de ne pas exposer inutilement les personnes à un risque.

Cette démarche utilise des méthodes spécifiques. Bon nombre sont communes à la démarche qualité et à la gestion des risques. Elles reposent en grande partie sur l'analyse fonctionnelle des processus indispensables pour anticiper sur les risques de forte gravité qui sont par nature exceptionnels.

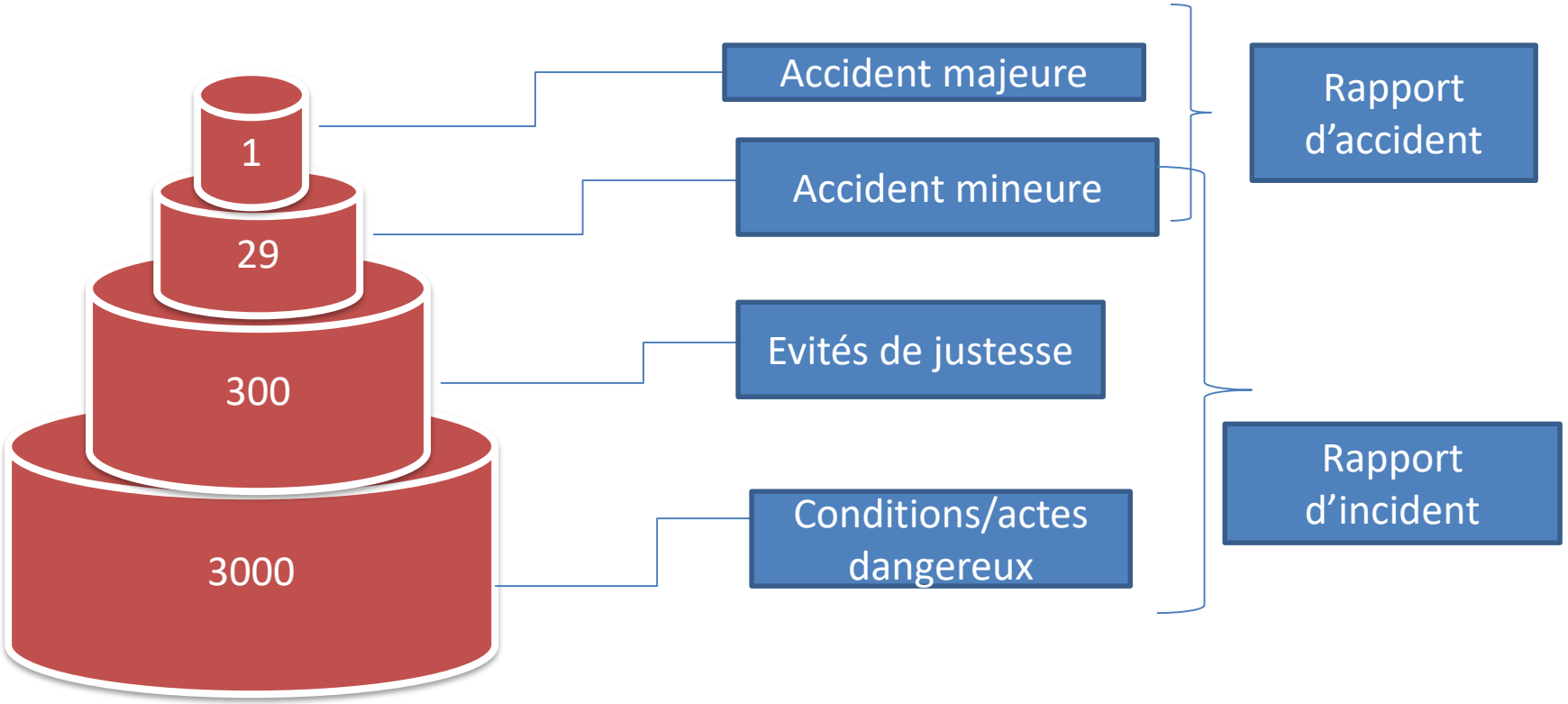
Maitrise du risque: Identification du risque

- **Une identification a posteriori: Il** s'agit de prendre en compte des événements qui témoignent de l'existence de risque. En l'absence de démarche de gestion des risques, les événements se produisent sans que l'institution en tire un enseignement. les anomalies et incidents sont corrélés aux accidents. L'accident ne survient jamais de manière isolée sans anomalie ou incident dans le système

Plusieurs types d'événements sont donc à considérer: - Les accidents et catastrophes

- Les presque accidents (« near miss »), les précurseurs et les événements sentinelles
- incidents et aux dysfonctionnements

Loi Heinrich



Maitrise du risque: Identification du risque

Plusieurs méthodes d'identification des risques a posteriori sont possibles :

- la notification des événements indésirables. On peut choisir de notifier :
  - tous les événements indésirables
  - des événements en fonction de certains critères (gravité, etc.)
  - d'une liste d'événements prédéterminés (événements sentinelles, vigilances)
  - les enquêtes, par exemple: enquête sur dossier du patient, analyses de mortalité /morbidité

Maitrise du risque: Identification du risque

- les informations disponibles dans l'ensemble de la vie de l' établissement:
  - ✓ risques identifiés par les professionnels et communiqués à l'administration,
  - ✓ risques identifiés par les différentes instances (CHSCT, comités de vigilances)
  - ✓ réclamations et plaintes exprimées par les patients ou leurs familles,
  - ✓ risques identifiés par la démarche qualité,
  - ✓ audits organisationnels.

Maitrise du risque: Analyse des risques

L’analyse des risques permet d’approfondir la connaissance des risques identifiés.

- **Détermination de la fréquence et de la gravité**

Elle permet de caractériser les risques à partir des deux déterminants essentiels que sont la fréquence et la gravité.

Cette première approche permet notamment la hiérarchisation des risques en vue de prioriser leur traitement

Fréquence et gravité sont des grandeurs estimées qui peuvent être établies avec une certaine subjectivité.

Maitrise du risque: Analyse des risques

➢ Identification des causes racines

Cette analyse est essentielle si l'on souhaite agir sur le risque. Elle s'applique notamment à la démarche a posteriori.

Les événements sont analysés afin d'identifier leur cause. Il s'agit à la fois de causes proximales et de causes racines. Cette analyse est le préalable au traitement des risques qui passera par une action sur les causes.

L'ensemble de ces analyses doit être conduit selon un protocole formalisé afin que l'enquête soit systématique, exhaustive, efficace, et ne se limite pas à une explication superficielle accompagnée d'une mise en cause individuelle.

Maitrise du risque: Analyse des risques

➢ Identification des causes racines

Cette analyse est essentielle si l'on souhaite agir sur le risque. Elle s'applique notamment à la démarche a posteriori.

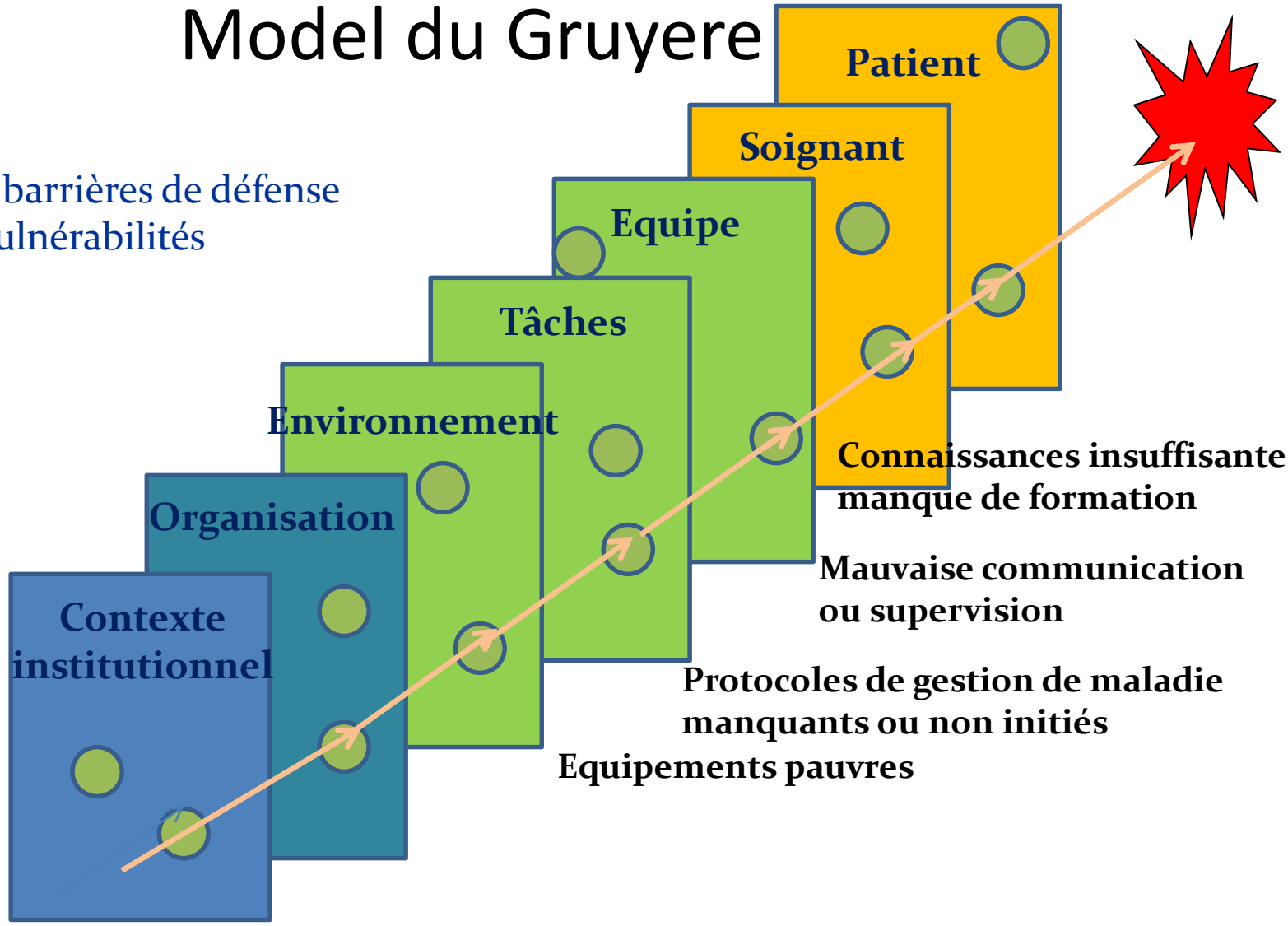
Les événements sont analysés afin d'identifier leur cause. Il s'agit à la fois de causes proximales et de causes racines. Cette analyse est le préalable au traitement des risques qui passera par une action sur les causes.

L'ensemble de ces analyses doit être conduit selon un protocole formalisé afin que l'enquête soit systématique, exhaustive, efficace, et ne se limite pas à une explication superficielle accompagnée d'une mise en cause individuelle.

Methodes d’analyse du risque

Model du Gruyere

Plaques: barrières de défense
Trous : vulnérabilités



TRAITEMENT DES RISQUES

Traitement des risques

- Le traitement des risques repose sur une combinaison de trois mécanismes : la prévention ; la récupération et l'atténuation ou protection.
- Le pré-requis commun à leur utilisation est la connaissance du risque.
- Ces mécanismes doivent être envisagés de façon globale et cohérente dans une stratégie d'ensemble
- Le traitement des risques consiste soit à ne pas s'exposer au risque soit à mettre en place des défenses en profondeur intervenant si possible avant la réalisation du risque ou à défaut après pour en limiter les conséquences.

Traitement des risques

❖ **Prévention et récupération:** visent à réduire la fréquence du risque.

Leur objectif est d'éviter la survenue d'un événement redouté. La prévention n'a pas d'effet sur la gravité lorsque le risque se réalise.

Plusieurs notions sont à distinguer :

- **la suppression du risque :** la prévention peut être obtenue soit par la suppression du risque, soit par la suppression de l'activité, soit par la modification du procédé en éliminant les étapes porteuses de risque

Traitement des risques

- **la prévention** (en dehors de la suppression et de la récupération) : elle a pour objectif d'éviter que ne se produisent les défaillances
- **la récupération** correspond au dépistage et au traitement d'une défaillance entre le moment où elle se produit et la réalisation de l’événement redouté auquel elle aurait pu conduire.

Traitement des risques

Plusieurs stratégies sont possibles.

- La suppression du risque à sa source:
  - la suppression de l'activité
  - ne pas s'engager dans une activité qui apparaît comme trop risquée pour l'organisation (évitement).
  - une modification du processus : on modifie le procédé utilisé ou l'enchaînement des différentes étapes du processus pour faire disparaître le risque en ne s'exposant pas au danger.

Traitement des risques

- **Les actions de prévention sans suppression du risque:**

  Elles reposent sur la construction de défenses en profondeur (ou barrières) contre le risque. Les défenses permettent soit d'empêcher la défaillance soit de l'identifier et de la récupérer avant que le risque se réalise. Il peut s'agir :

  - de modification du processus.
  - d'actions sur la compétence des équipes sur un processus insuffisamment maîtrisé
  - de mettre en place une ségrégation du risque.

  Le terme ségrégation correspond à l'action de séparer, de mettre à part.

Traitement des risques

Deux types de ségrégation sont possibles :

- **Ségrégation par duplication**

Lorsqu'un matériel précis, un dispositif ou encore un effectif de personnes est indispensable à une activité dont l'organisation ne peut pas se passer, il peut être nécessaire de dupliquer les ressources.

Grâce à cette duplication, une défaillance affectant l'élément indispensable est récupérée par la mise en œuvre du dispositif de secours (aspirateur, sauvegarde informatique)

La limite de la est qu'elle entraîne nécessairement un surcoût.

Traitement des risques

- **Ségrégation par séparation**

La séparation s'applique lorsqu'une entité physique génère du fait de son existence en une seule et même entité des risques trop graves pour que l'unicité de cette entité soit maintenue. Il faut donc séparer l'entité en plusieurs sous-entités. La ségrégation par séparation prévient la réalisation d'un événement de grande ampleur.

Répartir un stock important de produits inflammables dans plusieurs sites est une ségrégation par séparation. Une explosion d'un des lieux de stockage a une gravité beaucoup moins importante que si le stockage est réalisé en un lieu unique.

Traitement des risques

❖ **Protection (ou atténuation)**

La protection permet de réduire les conséquences d'un risque qui s'est réalisé. Elle repose sur des actions dont la mise en œuvre atténue les conséquences d’un risque qu’il est impossible d’éviter.

Cela suppose cependant d'identifier a priori ce risque. La fréquence d’apparition du risque n’est pas modifiée mais sa gravité est diminuée.

Traitement des risques

La situation est anticipée, les procédures à mettre en œuvre sont prédéterminées, les ressources requises sont en place, le personnel est formé à réagir. Les actions adaptées sont mises en œuvre lorsque la situation survient.

Défenses en profondeur

- sont des mécanismes intégrés au système qui permettent de limiter la production ou la propagation des défaillances.
- Elles sont mises en place dans le cadre des savoir- faire des professionnels.
- La démarche de gestion des risques renforce ces défenses de façon explicite. On distingue:
- Les défenses matérielles sont par exemple les détrompeurs , les alarmes, les contrôles, les redondances.
- Les défenses immatérielles sont par exemple la réglementation, la formation, les procédures.

Défenses en profondeur

- Un système de sécurité performant est en général « multi-défendu » par plusieurs cycles de prévention et de récupération. Il s'agit de mesures de prévention ou de récupération ciblées sur une hiérarchie d'événements redoutés.
- Les actions de récupération d'un niveau correspondent souvent à la prévention du niveau suivant.
- Lorsque le système est sûr, les niveaux de prévention et de récupération correspondent davantage à des défenses organisationnelles qu'à des défenses techniques

- **Merci**
- **Question?**