



# Evolution des méthodes d'analyse de la Fiabilité Humaine



# Evolution dans la philosophie HRA

De

**l'erreur humaine**

**1ère  
Génération**

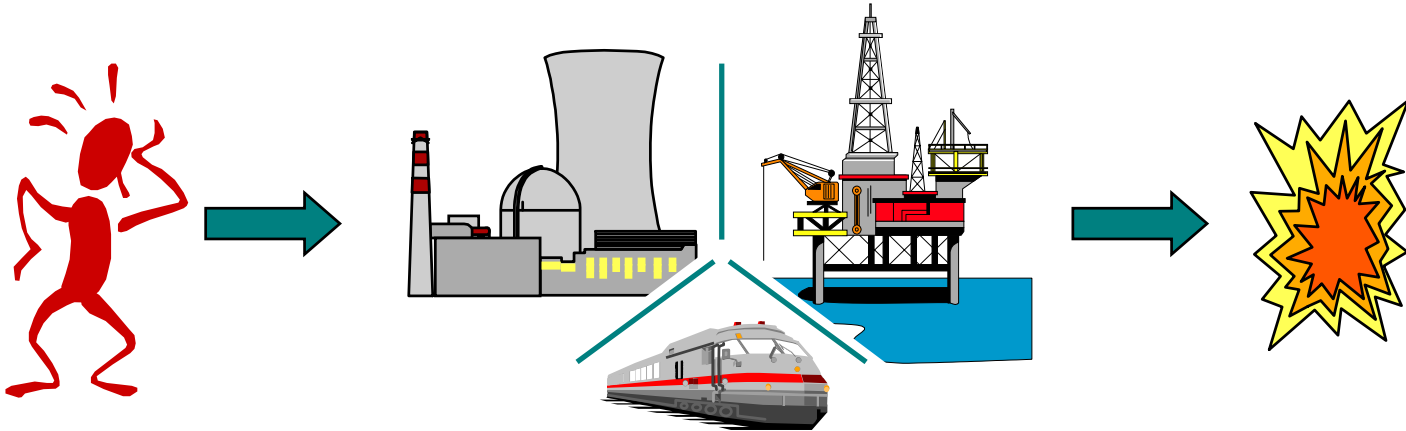
au

**dysfonctionnement d'un système**

**2ème  
Génération**

**comme base pour expliquer l'échec**

# Modèle d'accident simple



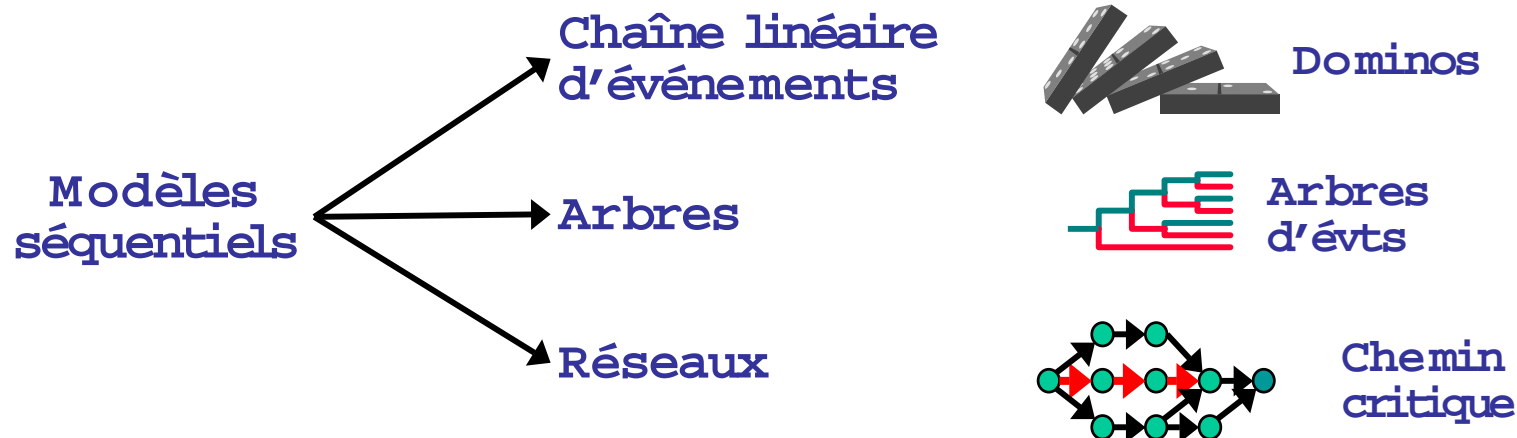
Erreur/Violation

Conséquence  
inattendue/indésirée



# Modèles séquentiels d'analyse et de gestion des risques

↳ Méthodes HRA de 1ère génération (60's)



Principe de l'analyse de risques

Recherche des causes spécifiques reconnaissables et des liens cause-effet bien définis.

Objectif du management de la sécurité

Elimination ou confinement des causes identifiées.



# Quelques méthodes marquantes de 1ère Génération

## ◆ THERP

- la toute première méthode HRA (1964)

## ◆ SLIM

- l'utilisation systématique de jugements d'experts



# THERP : principes

## Technique for Human Error Rate Prediction

Description des défaillances de système (missions FH) (AMDEC)



Décomposition des tâches en enchaînement d'actions élémentaires  
(arbre d'événements)



Evaluation des probabilités d'échec de chaque action  
en fonction de son type et de son contexte (PSFs)



Application éventuelle d'un modèle de dépendance  
(probabilités conditionnelles)

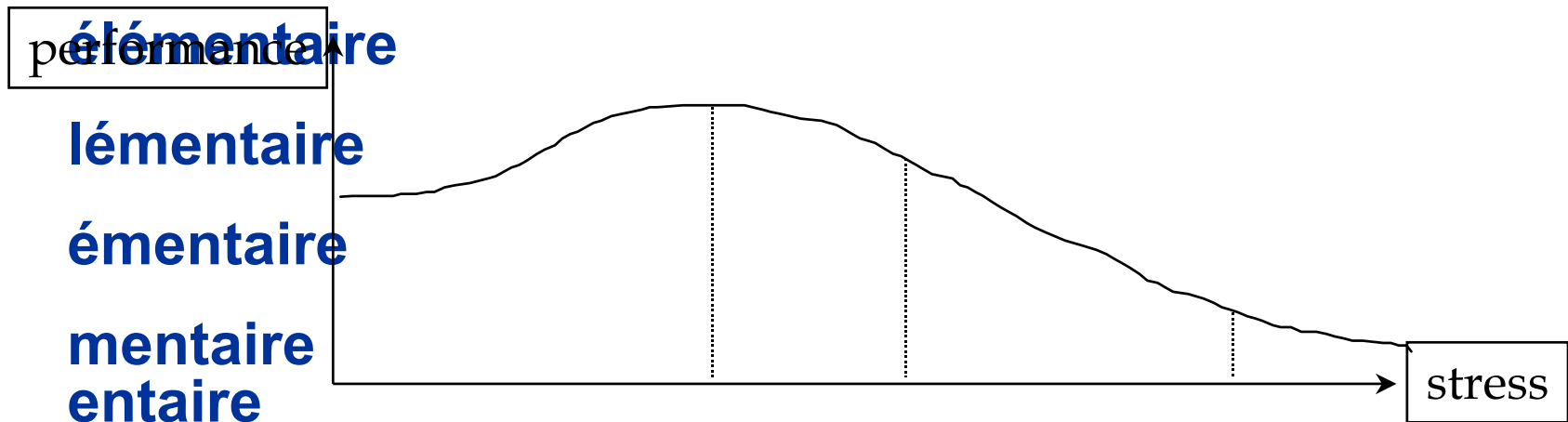


Combinaison des probabilités élémentaires



# THERP : exemple de PSF

- ◆ L'influence du stress dans l'évaluation de la probabilité d'échec d'une action  
probabilité d'échec d'une action élémentaire



élémentaire  
élémentaire  
élémentaire  
élémentaire  
élémentaire  
fonction du niveau de stress  
u de stress

$ur = 2 * P0$

erreur = P0

2 à 5 \* P0



# L'Erreur Humaine est-elle un objet d'analyse pertinent pour appréhender la Fiabilité Humaine ?

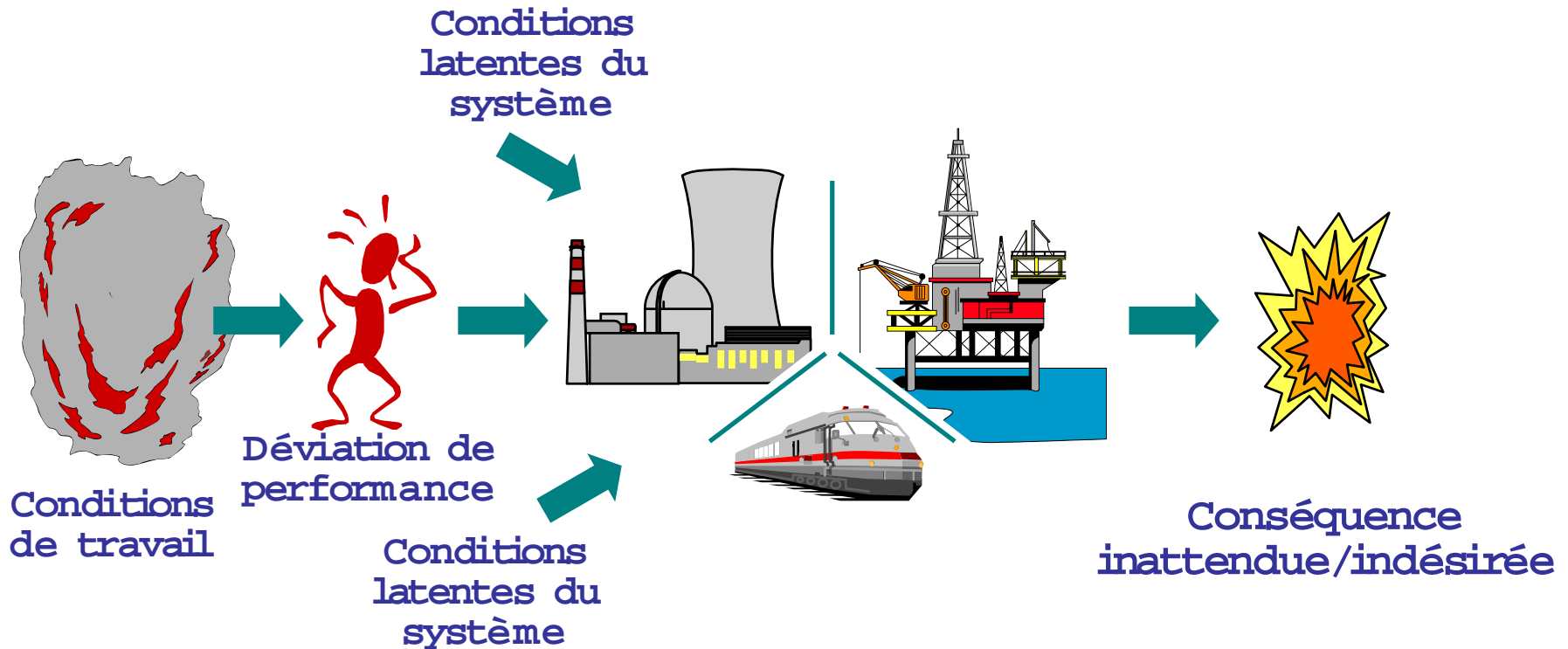


# Erreurs et conséquences sur la sécurité



Les effets de l'erreur dépendent des propriétés du système et du contexte dans lequel elle se produit

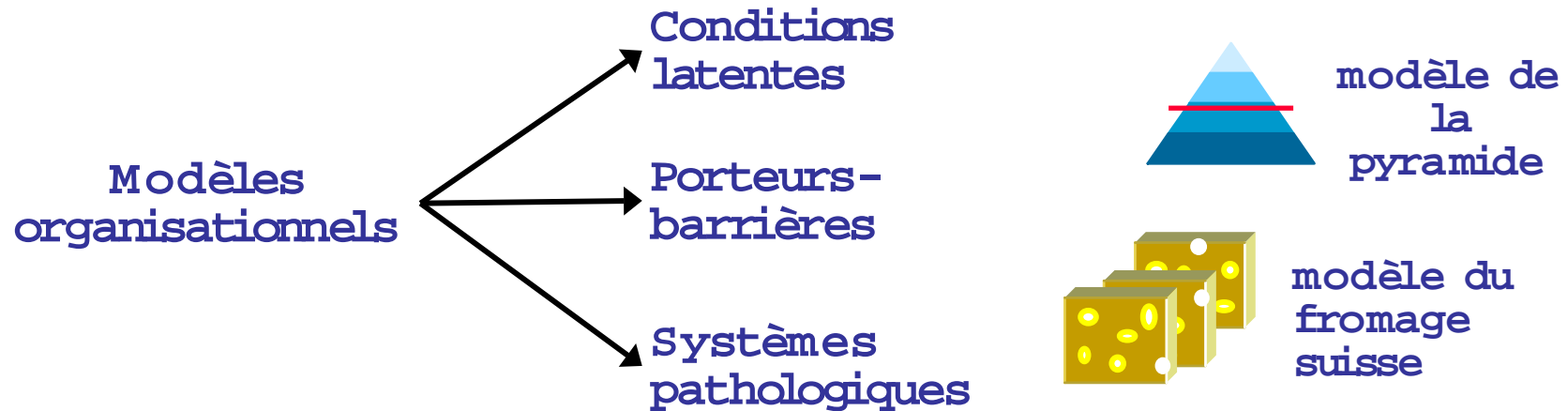
# Modèle d'accident intermédiaire





# Modèles organisationnels d'analyse et de gestion des risques

↳ Méthodes HRA de 1ère génération élaborées (90's)



Principe de l'analyse de risques

Recherche des "porteurs" et des conditions latentes; définition d'indicateurs de la santé générale du système

Objectif du management de la sécurité

Renforcer les barrières de défense



# PAWOF: une méthode HRA basée sur un modèle d'accident organisationnel

Proactive Assessment of Organizational and Workplace Factors

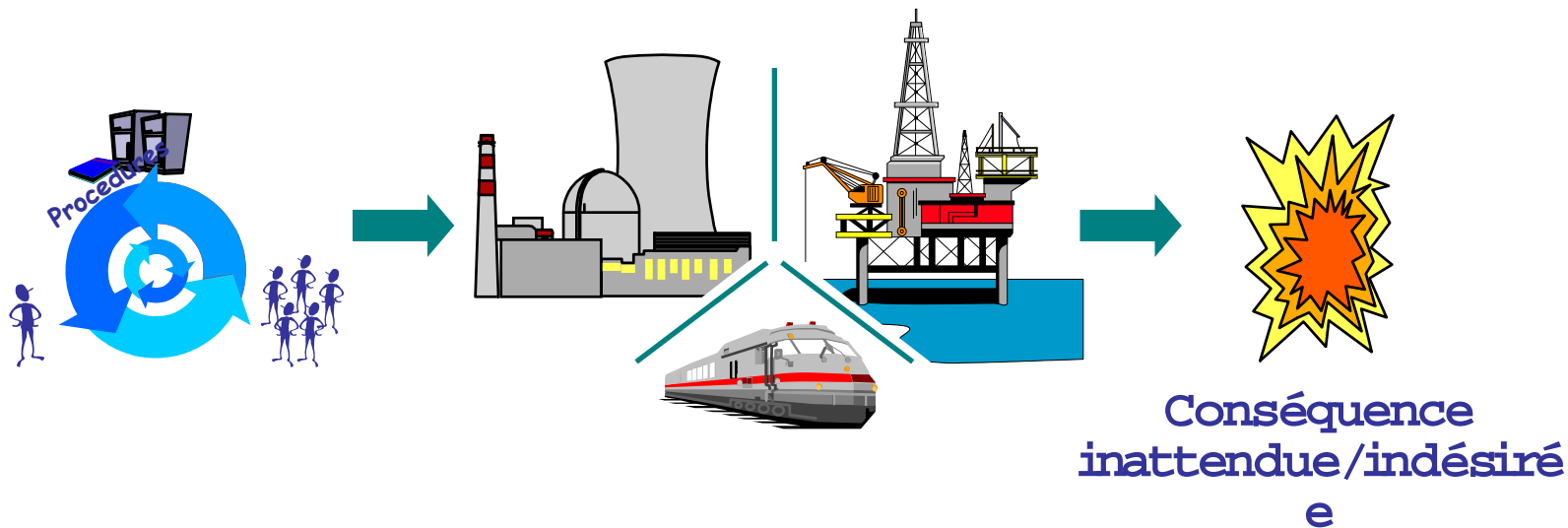
- ◆ **Principe: questionnaire sur des indicateurs permettant de suivre l'évolution de la «santé» de l'organisation (conditions latentes)**
- ◆ **Grands thèmes passés en revue pour l'organisation:**
  - **Attitude du management de haut niveau vis-à-vis de la performance humaine (combien de fois le directeur du site 'descend-il' dans la centrale/SdC/... ?)**
  - **Culture juste favorisant la remontée des problèmes**
  - **Culture d'apprentissage**
  - **Conscience de la qualité de la performance humaine**
  - **Anticipation des problèmes**
  - **Flexibilité**
  - **Visibilité sur la marge restant (dégradation des barrières, ...)**



# Principales limites des méthodes organisationnelles

- ◆ Le lien des indicateurs de la santé organisationnelle à la sécurité est implicite
- ◆ Elles se concentrent toujours sur une déviation de performance i.e. sur une erreur, par rapport à une « droit chemin »

# Modèle d'accident actuel



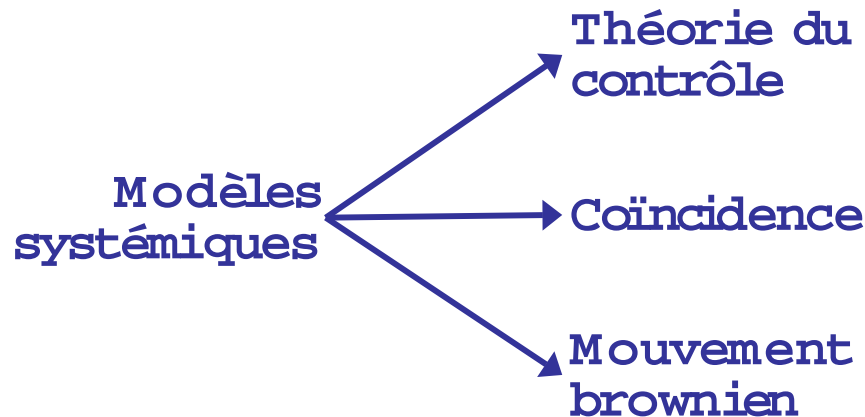
Les accidents résultent de coïncidences d'événements, plutôt que de séquences de défaillances

Les événements qui se combinent en accident peuvent relever tant de la variabilité "normale" de la performance que de défaillances propres



# Modèles systémiques d'analyse et de gestion des risques

↳ Méthodes HRA de 2ème génération



Principe de l'analyse de risque

Recherche des dépendances inhabituelles, et des "conditions communes" (modes communs)

Objectif du management de la sécurité

Surveillance et contrôle des conséquences de la variabilité de la performance



# Quelques exemples de méthodes HRA de 2ème génération

- ◆ **MERMOS**
- ◆ **ATHEANA**
- ◆ **PHERA**
- ◆ ...





# Modélisation fonctionnelle du système

- ◆ **Systeme de conduite/contrôle...qui inclut *a minima* équipe + procédures + interface**
- ◆ **Modélisation des fonctions nécessaires et suffisantes pour que ce système assume ses missions liées à la sécurité avec succès**
- ◆ **Recherche systématique des modes de défaillance de ces fonctions**
- ◆ **Pour chacun d'entre eux, recherche des coïncidences susceptibles de les expliquer**  
(raisonnement du point de vue des acteurs dans la situations: quelles bonnes raisons pourraient-ils avoir pour s'engager dans une conduite/un contrôle menant à l'échec <- définit par rapport à une référence externe, non présente dans la situation)



# Les méthodes HRA de 2<sup>ème</sup> génération

## Vers la recherche de « coïncidences » d'événements

### MERMOS dans le nucléaire

#### ◆ Mission FH: non arrêt de l'IS

##### Exemples de « coïncidences »

- La dégradation de l'inventaire en eau étant lente, l'équipe considère que celui-ci est correct tant que le Niveau Cuve n'a pas effectivement atteint le seuil précisé dans les procédures
  - Augmentation rapide de la pression dans l'enceinte
  - L'Ingénieur Sûreté n'est pas présent en salle de commande, ou bien suit la stratégie du reste de l'équipe
  - Le Superviseur suit la stratégie des opérateurs
- 
- L'Opérateur Réacteur arrête accidentellement les pompes d'IS (erreur sur un test, ...)
  - L'information sur le Niveau Cuve dont dispose l'opérateur est erronée (capteur défaillant, problème de contrôle commande, ...)
  - Le Superviseur et l'Ingénieur Sûreté disposent de la même information que l'Opérateur Réacteur sur le Niveau Cuve

### PHERA dans l'ATM

#### ◆ Mission FH: détection de conflits potentiels avec MTCD

- Problème non affiché sur l'écran MTCD du contrôleur (non considéré comme conflit par le système, défaillance d'interface, ...)
  - Le contrôleur se fie le plus souvent au système MTCD pour détecter les conflits potentiels
  - Le problème n'est pas affiché non plus sur l'écran PTCD de l'autre contrôleur
- 
- Distractions dans la salle de contrôle
  - Conflit atténué par erreur par le contrôleur
  - Pas de communication entre les deux contrôleurs
- 
- La fenêtre MTCD n'est pas affichée sur l'écran radar des deux contrôleurs
  - Les contrôleurs ne sont pas familiers avec le nouveau système
  - Haute densité de trafic



# Une évolution selon deux axes

- ◆ **De l'individu au système**
  - individu
  - équipe
  - organisation
  - système socio-technique
  
- ◆ **De l'Erreur Humaine à la Variabilité de la Performance**
  - erreur humaine
  - dysfonctionnement organisationnel
  - variabilité de la performance



# Conclusion

## Evolution de l'analyse des "aspects FH" et de la gestion des risques



## Conditions de succès Evolution culturelle & structurelle