UNIVERSITÉ DE TECHNOLOGIE DE COMPIÈGNE

UTC

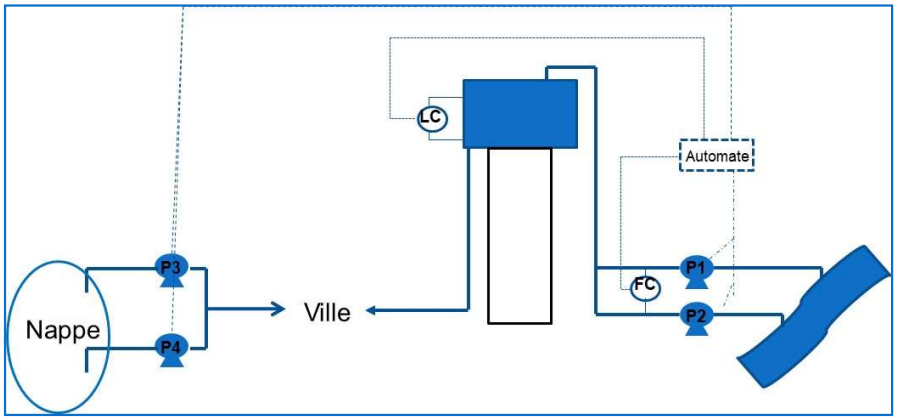
Maitrise des Risques

Cours 9 : la méthode AMDEC et des applications

UV TS01

Resp : christophe.proust@utc.fr

Pour compléter d'autres méthodes…



Mot guide	Dérive	Causes possibles	Conséquences	Moyens de détection	Actions correctives	Remarques
TROP de	Trop de niveau	Trop de débit entrant • dérive de la pompe P1 qui accélère • démarrage intempestif de P2 • défaillance débitmètre FC qui sous estime le débit	Augmentation jusqu'à débordement du château d'eau (différence de vitesse de remplissage selon les causes)	LC	Instruction à l'automate d'arrêter l'alimentation électrique momentané de P1	Mettre en place un capteur niveau spécifique avec alarme + procédures par superviseur
		Mauvaise régulation du niveau par LC (niveau trop bas)	Idem + déclenchement pompes P3&P4 ? (trop de débit en ville?)	(LC???) -	?? -	Idem
		Pas assez de débit sortant • défaillance en aval (tuyauterie bouchée, …)	Débordement du …. + pas assez de débit en ville	LC	Arrêt momentané de P1	Idem

La méthode AMDEC

Une méthode ciblée sur les défaillances des appareils/composants

Analyse des Modes de Défaillance et de leurs Effets (et Criticité) AMDE(C)

Approche par le mode de défaillance : Démarrage ou arrêt intempestif, refus de …

- Identifier les défaillances
- Déterminer les causes & conséquences
- Evaluer la gravité
- Proposer des actions correctives

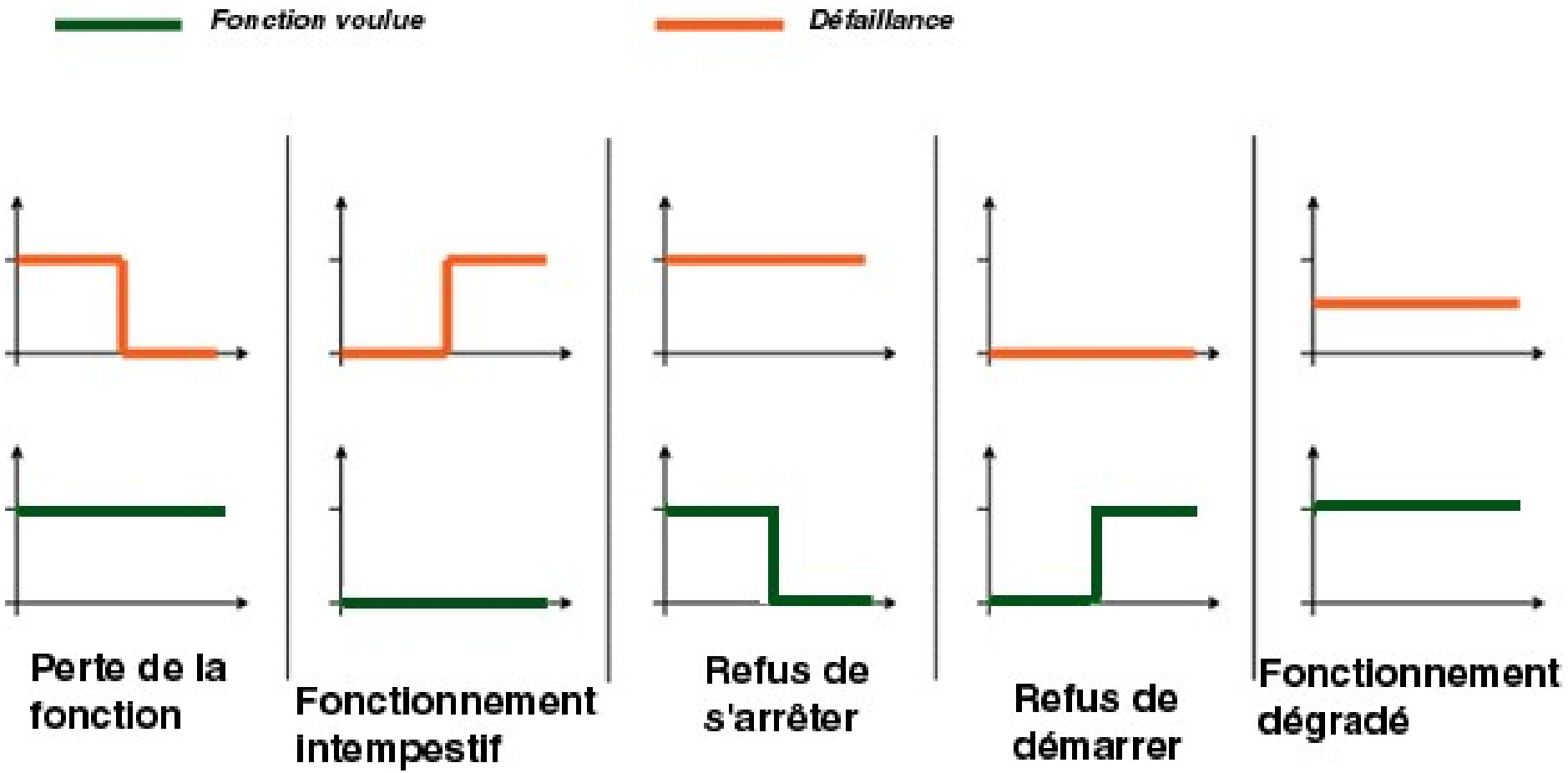
Historique

- **1949 armée américaine :** MIL-P-1629 « Procédures pour l'Analyse des Modes de Défaillance, de leurs effets et de leur Criticité »
- **Années 60** aux USA usage dans le secteur aéronautique
- **Années 70** essor en Europe dans les industries automobile, chimique, nucléaire
- **Années 80** généralisation aux sous traitants
- **Actuellement**
  - Industries à risque : nucléaire, spatial, …
  - Qualité

Les choix préliminaires

- Types d'approche
  - Qualitative
  - Semi-quantitative
  - Quantitative
- Positionnement de l'analyse
  - Fonctionnelle
  - Matérielle
- Niveau de décomposition le plus bas
  - Systèmes / sous systèmes
  - Appareils
  - Composants

Les modes de défaillance « génériques »



A ne pas confondre avec les causes

Exemples de modes de défaillance (extrait de la norme CEI 60812)

1	Défaillance structurelle (rupture)	19	Ne s'arrête pas
2	Blocage physique ou coincement	20	Ne démarre pas
3	Vibrations	21	Ne commute pas
4	Ne reste pas en position	22	Fonctionnement prématuré
5	Ne s'ouvre pas	23	Fonctionnement après le délai prévu (retard)
6	Ne se ferme pas	24	Entrée erronée (augmentation)
7	Défaillance en position ouverte	25	Entrée erronée (diminution)
8	Défaillance en position fermée	26	Sortie erronée (augmentation)
9	Fuite interne	27	Sortie erronée (diminution)
10	Fuite externe	28	Perte de l'entrée
11	Dépasse la limite supérieure tolérée	29	Perte de la sortie
12	Dépasse la limite inférieure tolérée	30	Court-circuit (électrique)
13	Fonctionnement intempestif (inopportun)	31	Court-ouvert (électrique)
14	Fonctionnement intermittent (discontinu)	32	Fuite (électrique)
15	Fonctionnement irrégulier	33	Autres conditions de défaillance exceptionnelles suivant les caractéristiques du système, les conditions de fonctionnement et les contraintes opérationnelles
16	Indication erronée		
17	Ecoulement réduit		
18	Mise en marche erronée		

Mode de défaillance vs Causes

Mode de défaillance	Causes
Comment ? (*selon quelle modalité*)	**Pourquoi ?**
Refus de s'ouvrir	Blocage mécanique Erreur humaine *(défaut de commande pour vanne pilotée)*

ation

Déroulement de l'analyse

1. Définition de l'élément à étudier
2. Définition de sa (ses) fonction (s)/ état(s)
3. Recherche des modes de défaillance
4. Définition des critères de gravité
5. Recherche des causes
6. Détermination des conséquences
7. Evaluation de la gravité
8. Recherche des moyens de détection
9. Recherche des actions correctrices

Tableau d'analyse

Exemple de tableau

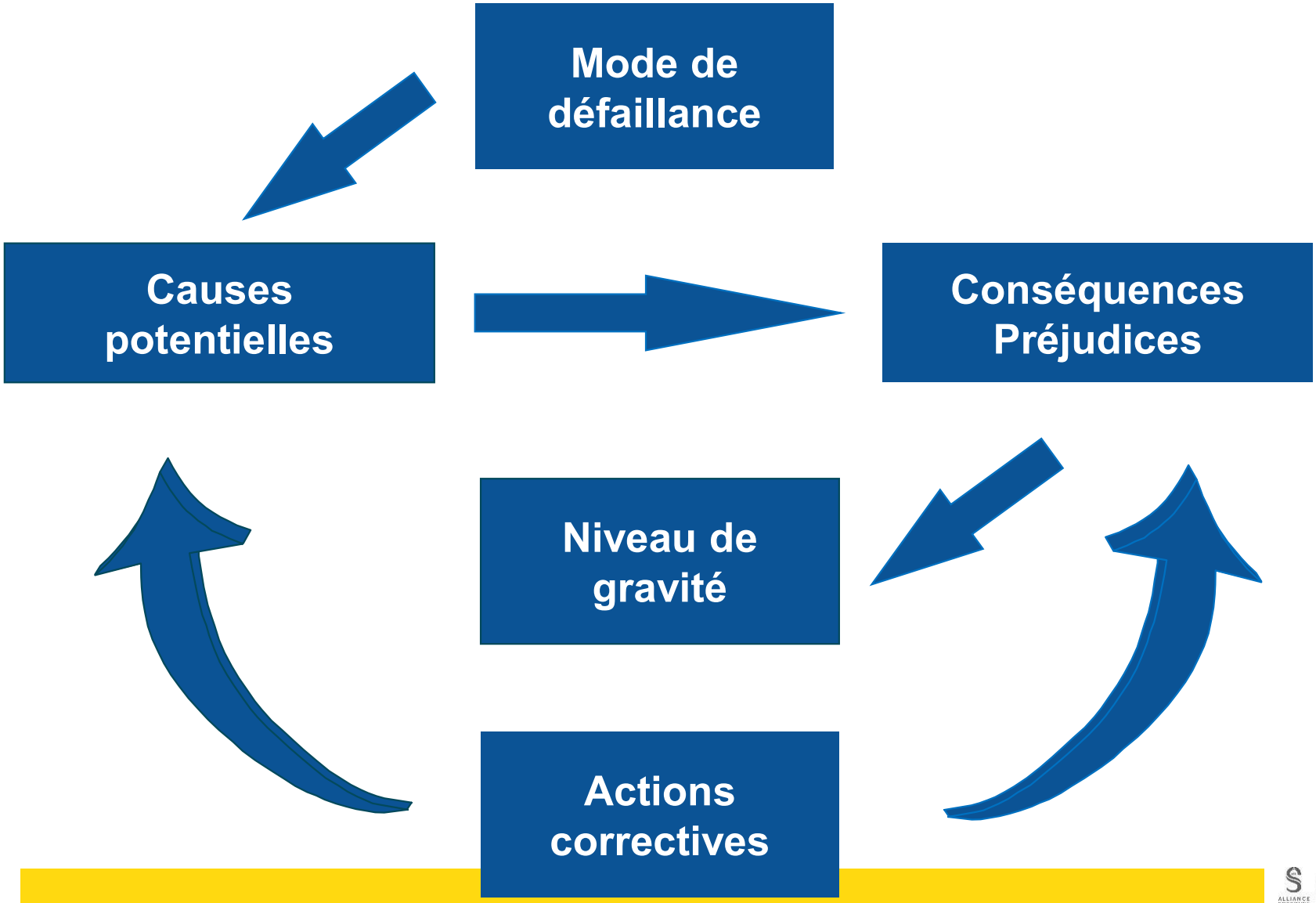
ANALYSE DES MODES DE DEFAILLANCE DES COMPOSANTS
DE LEURS EFFETS SUR LE SYSTEME ET DE LEUR CRITICITE

PROJET:
SYSTEMES:
SOUS–SYSTEME:

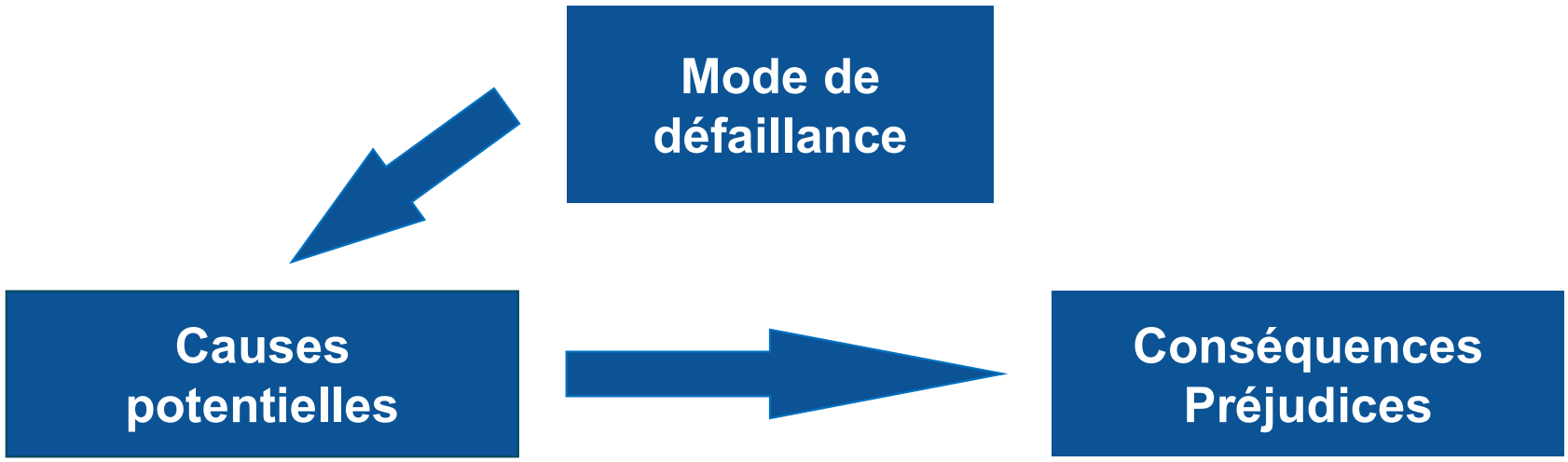
DATE:
DOCUMENTS:

IDENTIFICATION DU COMPOSANT	FONCTION ETATS	MODES DE DEFAILLANCE	CAUSES		EFFETS		PROBABILITE	CLASSE DE GRAVITE	MOYENS DE DETECTION DES DEFAILLANCES	ACTIONS CORRECTIVES	REMARQUES
			internes	externes	local	final					

Démarche

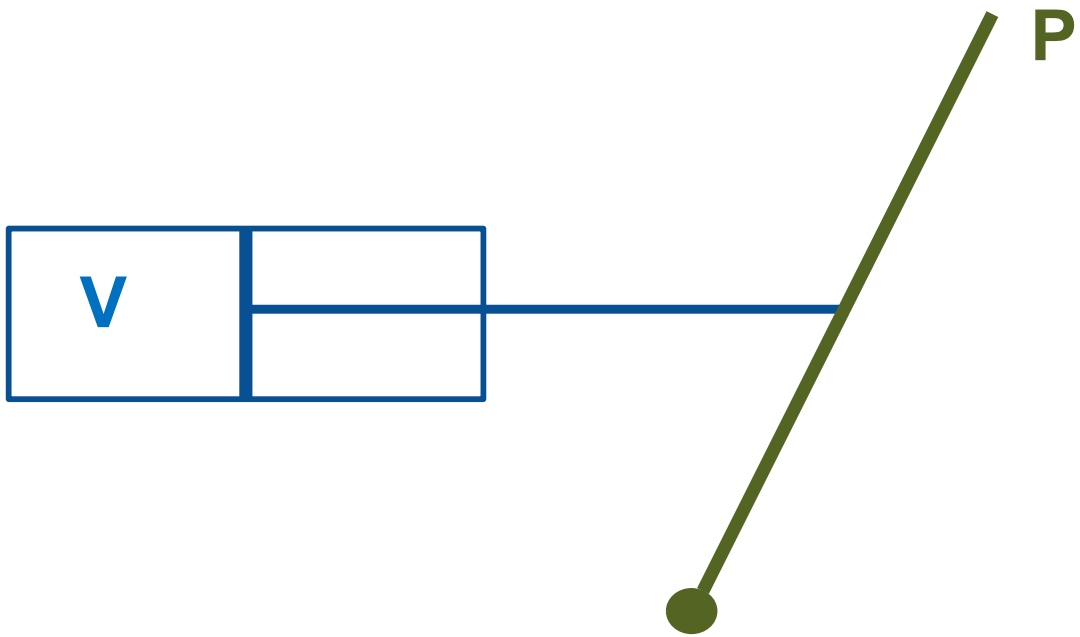

Mode de défaillance
Causes potentielles
Conséquences Préjudices
Niveau de gravité
Actions correctives

Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Lève-vitre	Refus de fermeture	Défauts internes mécaniques ou électriques Panne d'alimentation électrique	Gêne, inconfort (température,...) Vulnérabilité vis-à-vis du vol

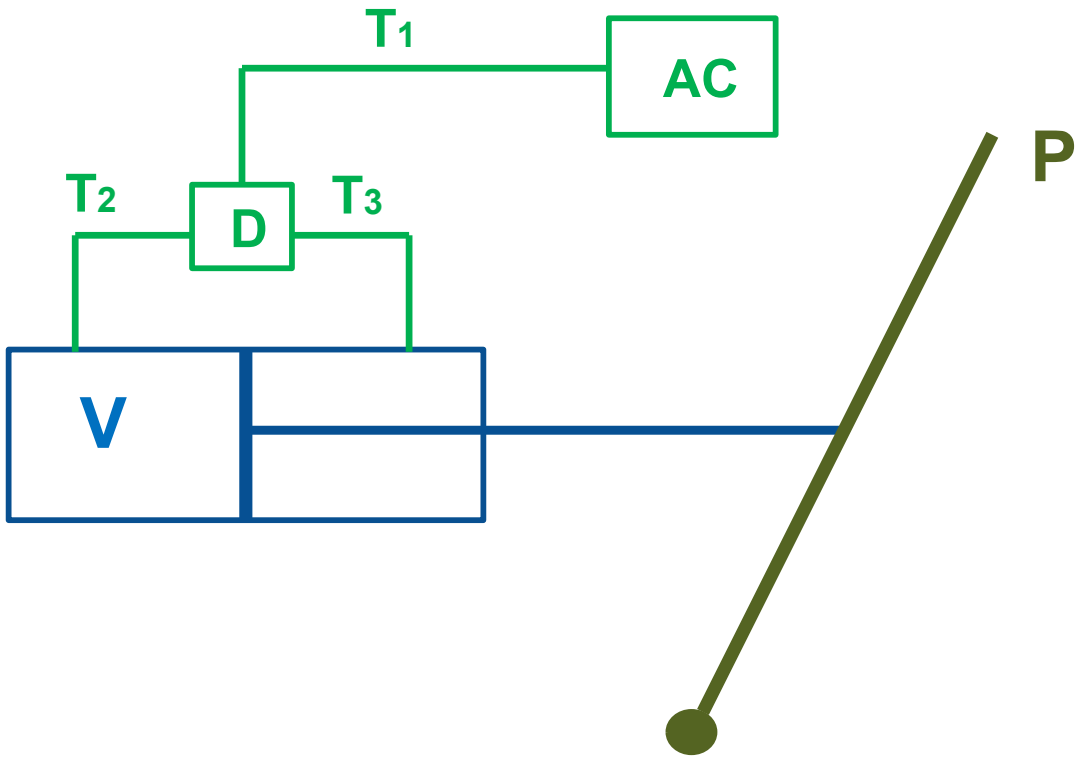


Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Lève-vitre	Refus de fermeture	Défauts internes mécaniques ou électriques Panne d'alimentation électrique	Gêne, inconfort (température,...) Vulnérabilité vis-à-vis du vol Indisponibilité du véhicule

Niveau de détail



Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Vérin	Pas de course (piston bloqué)	Défauts internes (détérioration des joints, fuite,…) Absence d'air comprimé Fuite alimentation	Non ouverture de la porte



Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Tuyauterie T_2	Rupture	Défaut interne (usure, corrosion,...) Accrochage par un engin	Non alimentation du vérin Pas de course du vérin, non ouverture de la porte

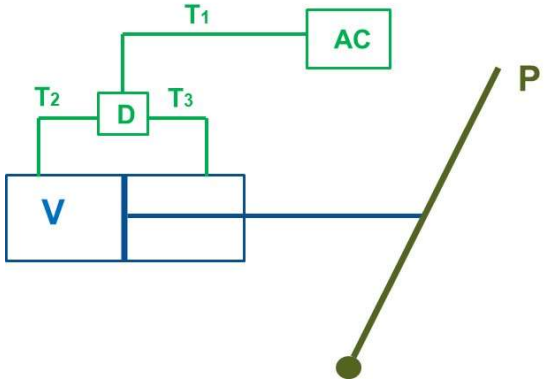
Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Vérin	Pas de course (piston bloqué)	Défauts internes (détérioration des joints, fuite,…) Absence d'air comprimé Fuite alimentation	Non ouverture de la porte

Composant	Mode de défaillance	Causes internes ou externes	Conséquences
Tuyauterie T_2	Rupture	Défaut interne (usure, corrosion,…) Accrochage par un engin	Non alimentation du vérin Pas de course du vérin, non ouverture de la porte

- Possibilité de faire des effets de zoom
- Nécessité d'être homogène dans la décomposition

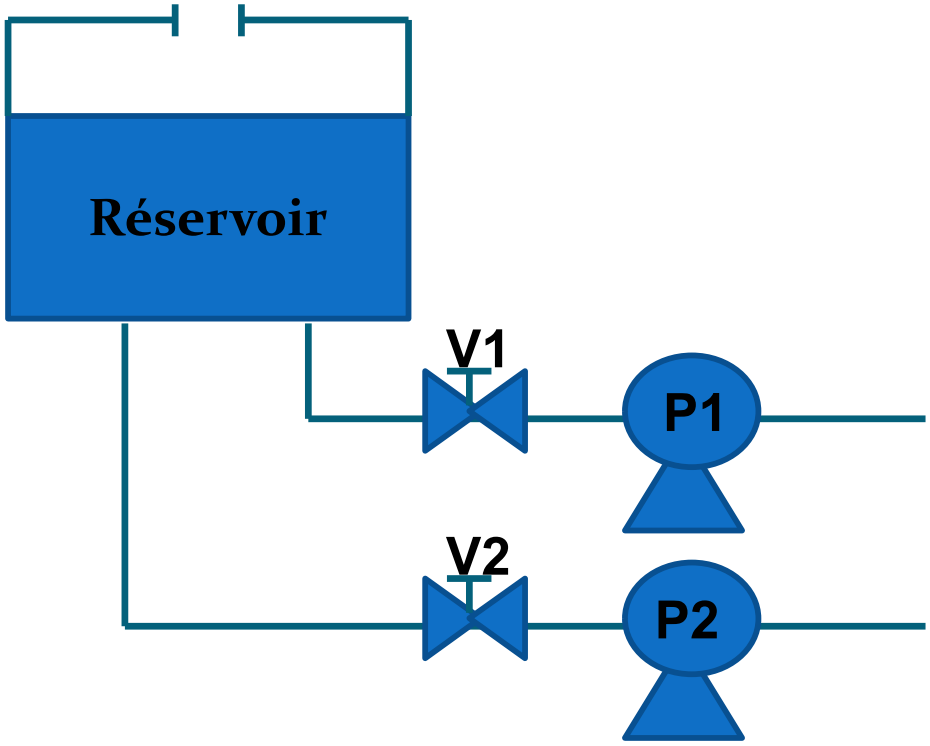
Bien définir la phase, l'état du composant

- Certaines défaillances ne sont pas possibles
- Certaines conséquences ne sont pas possibles
- Ou pour une même conséquence, la gravité est différente



Les modes communs

- Les utilités (électricité, eau, air,…)
- Les mêmes comportements (joints de la navette)
- Des parties communes dans un circuit, ….



Les limites

1. Hypothèse de bon fonctionnement des autres équipements
2. Effets de pannes uniques
3. Non utilisable ***directement*** en environnement accidentel

Mais un large éventail

- AMDEC Produit
- AMDEC Conception
- AMDEC Fonctionnelle
- AMDEC Composant
- AMDEC Matériel
- AMDEC Machine
- AMDEC Moyen de production
- AMDEC Service
- AMDEC Process
- AMDEC Procédé
- AMDEC Montage
- AMDEC Assemblage
- AMDEC Contrôle
- AMDEC Prestation de service

AMDEC Machine

Composant	Mode de défaillance	Causes	Effets / sous ensemble	Effets / installation de production	Effets / produit final
Vanne de vidange	Refus d'ouverture	Blocage mécanique Défaut de commande	Vidange de la cuve impossible Risque de prise en masse de la pâte	Arrêt de la production en aval (pas de stock intermédiaire de pâte)	Néant

AMDEC Procédé

Opération	Mode de défaillance	Causes	Effets / production	Effets / produit	Contrôle ou surveillance
Mise à épaisseur 150 mm +/- 0,05 mm	Epaisseur supérieure à 150,05 mm	Défaut machine Erreur de réglage Déformation de la pièce usinée	Montage impossible lors de l'assemblage final => retouches et ralentissement de la production		
	Epaisseur inférieure à 149,95 mm	Défaut machine Erreur réglage	Néant	Produit assemblé avec du jeu, non détecté Réduction durée de vie du produit Insatisfaction client	Contrôle impossible sur produit assemblés Prévoir des prélèvements après opération de mise en épaisseur

Bilan

Avantages

- Méthode relativement simple & accessible
- Outil puissant
- Domaine d'application large
- En conception & exploitation
- Systématique gage d'exhaustivité
- Liste des éléments critiques
- Tableaux assurent bonne traçabilité de la réflexion et des décisions

Inconvénients

- Lourdeur (volume & temps passé)
- Problèmes des combinaisons d'événements non pris en compte
- Problème potentiel des modes communs
- Problème des situations accidentelles

La catastrophe de Feyzin

Illustration de l'effet de la défaillance d'un composant

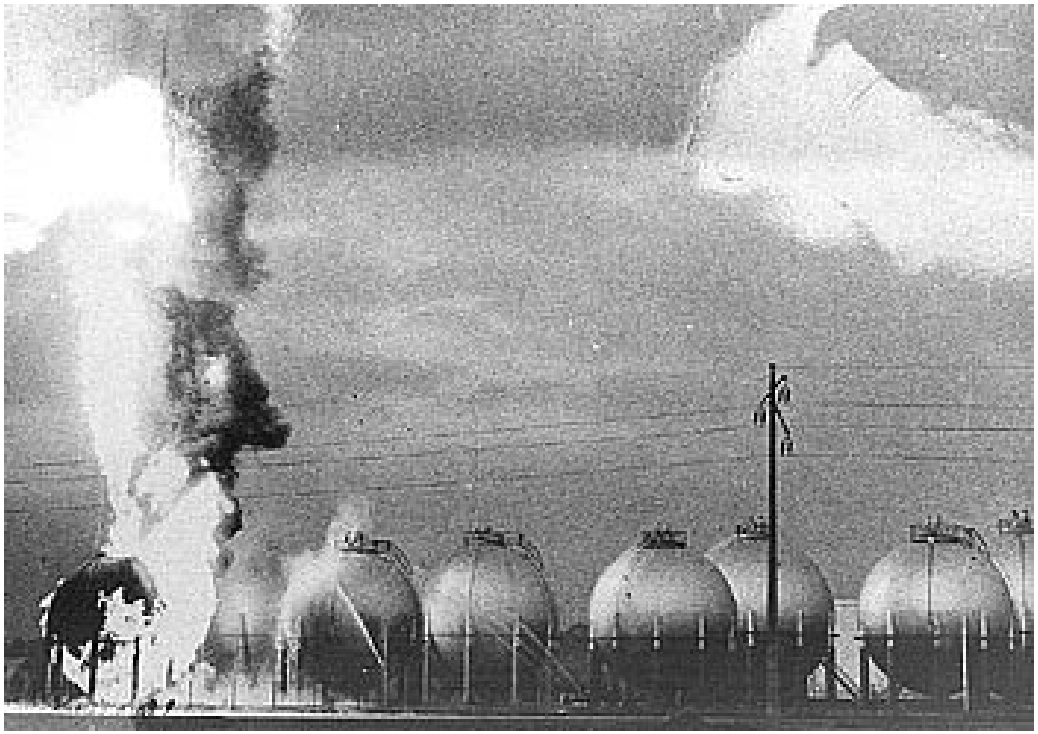

FEYZIN
4 janvier 1966
Le coup de semonce

Norton
Birmingham
Leicester
London
Cardiff
Bristol
Plymouth
Amsterdam
Nederland
Brussel
Bruxelles
Essen
Köln
Lille
België
Belgique
Luxembourg
Le Havre
Amiens
Reims
Paris
Caen
Brest
Rennes
Le Mans
Angers
Tours
Nantes
Dijon
Strasbourg
Schweiz
Suisse
Svizzera
France
Limoges
Bordeaux
Saint-Etienne
Grenoble
Torino
Toulouse
Montpellier
Monaco
Marseille
Toulon
Bilbao
Andorra
Perpignan
Zaragoza
Barcelona
España
Valladolid
Madrid

LYON
Villeurbanne

Contexte

- La raffinerie de Feyzin mise en service en 1964
- Stockage aérien d'hydrocarbures dont :
  - Quatre sphères de butane de 2000 m³
  - Quatre sphères de propane de 1200 m³



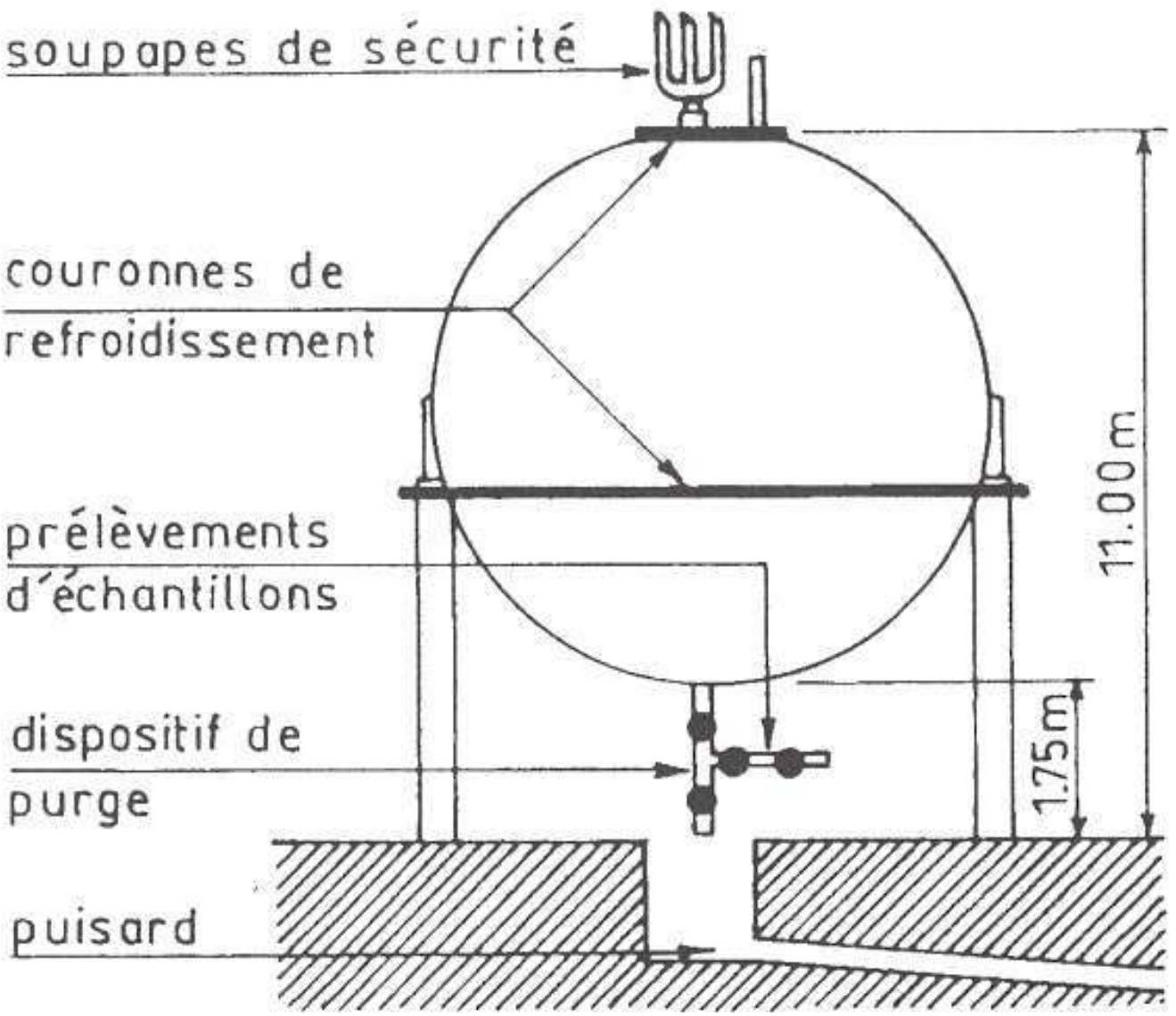
https://www.ina.fr/ina-eclaire-actu/video/s1043953_001/1966-la-catastrophe-de-la-raffinerie-de-feyzin

Lors d'opérations d'exploitation

- Phénomène de décantation d'eau et de soude => purges fréquentes
- Prise d'échantillons régulières (qualité produit)

- Ces opérations se font avec 2 vannes très proches (5 cm) en partie basse des sphères.
- Vannes manœuvrées par des clés carrées amovibles.

© Rotech France



CROQUIS SCHEMATIQUE D'UNE SPHERE

Des maladresses de conception

Retour exploitant

L'exploitation met rapidement en évidence les défauts :

1. vannes trop proches (peuvent givrer simultanément par détente du gaz liquéfié)
2. manœuvre par clés mobiles
3. vannes difficilement accessibles et difficiles à manœuvrer

REX

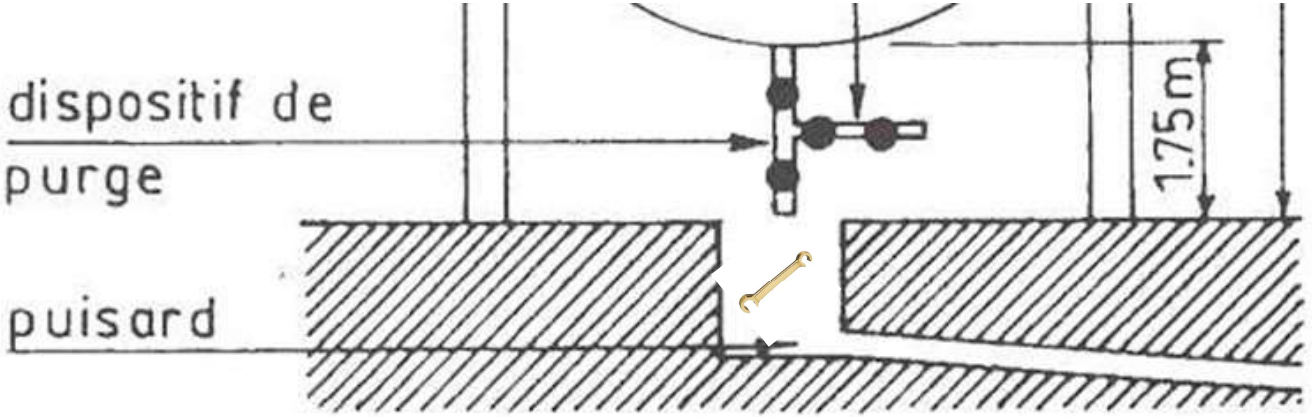
- Deux incidents graves se sont déjà produits
- Ils ont été heureusement maîtrisés
- Après 2ème incident, rédaction d'une note de service concernant la manœuvre des vannes
- Elle ne sera pas respectée le jour de l'accident

L'accident

- L'opération de purge débute à 6h40, il fait nuit noire, l'éclairage à cet endroit est très réduit
- L'opérateur ouvre à moitié la vanne inférieure puis en grand la vanne supérieure
- Les impuretés s'écoulent puis rapidement le propane jaillit, surprend l'opérateur

L’accident

- Chute de la clé
- Il ne peut pas la remettre, la vanne a givré
- Il renonce, tentative des agents de sécurité, échec
- Alerte en interne, mais pas à l’extérieur



L'accident

- Nappe de gaz lourd, vent nul.
- Le nuage atteint l'autoroute qui ne sera fermée que 10 mn après (7h05)
- A 7h15, une voiture sur une départementale enflamme le nuage (le conducteur décèdera à l'hôpital).
- Alerte des pompiers de Lyon qui arrivent à partir de 7h30
- Les pompiers de l'usine ont tenté de colmater la brèche, puis sont intervenus avec un camion poudre sans succès. Ils mettent en action les systèmes de refroidissement des sphères
- L'industriel voisin en fait autant => **manque d'eau**

L'accident

- Les pompiers lyonnais sont confrontés à ce manque d'eau => tentative de pomper dans le Rhône
  - Le camion s'embourbe, il faut 20 mn pour le dégager
  - Une clôture douanière doit être défoncée par un engin
- A 7h45 ouverture de la soupape de sécurité, le jet s'enflamme.
- Il y a 170 personnes sur place
- A 8h45 explosion de la 1ère sphère :17 morts et 84 blessés => repli des secours
- A 9h45 explosion de la 2ème sphère

Les dégâts

- Nombreux dégâts matériels jusqu'à Vienne (à 16 km) : 1475 constructions sur 21 communes
- Entre les 2 sphères volatilisées, un cratère

L= 35 m, l= 16 m, P= 2 m

Conséquences / Enseignements

Juridiques/législatives

- Sanctions pénales & civiles : (~ 1M€)
- Annexe Hydrocarbure au plan ORSEC (7/12/67)
- Nouvelles normes pour industrie pétrolière (refroidissement des sphères, distances d'isolement des stockages, protection incendie, organisation des secours,…)
- Refonte de l'organisation des inspecteurs des Installations Classées
- Refonte de la loi de 1917 => Loi des IC de 1976

Sur la « sécurité »

- Loi de Murphy
- Non réelle prise en compte du REX
- Corriger une erreur de conception par une procédure peu adaptée

Exemple d'AMDEC

1. En phase projet
2. En phase de modification d'installation

Exemple AMDEC en phase projet

Etude d'un projet de bouée de déchargement en mer de GNL

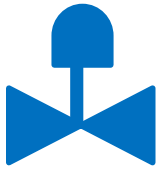
Travail basé

- sur les PID du projet
- l'interview
  - du chef de projet
  - du correspondant sécurité

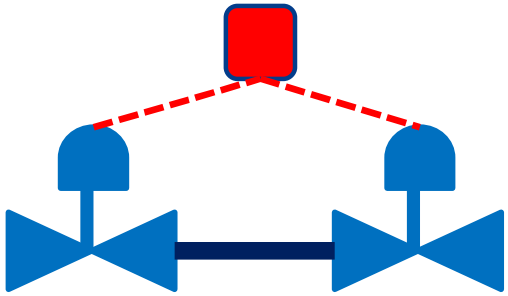
Nombreux points mis à jour dont celui des vannes FC piégeant du GNL
(le réchauffement par échange thermique avec l'eau => explosion liquide)

Détail de la démarche

AMDEC de la vanne



Travelling arrière: mode commun

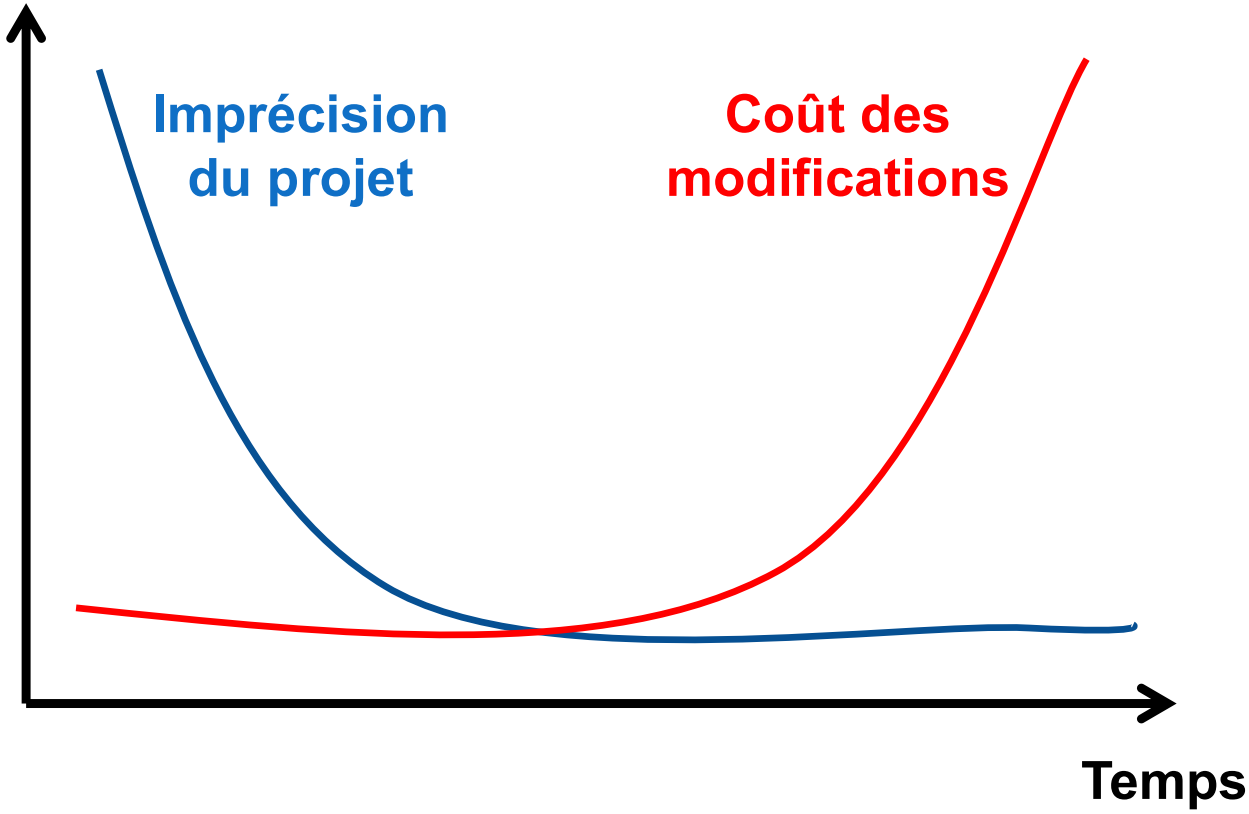


Science de l'ingénieur : physique

Retour d'expérience : explosion froide

Exemple AMDEC en phase projet

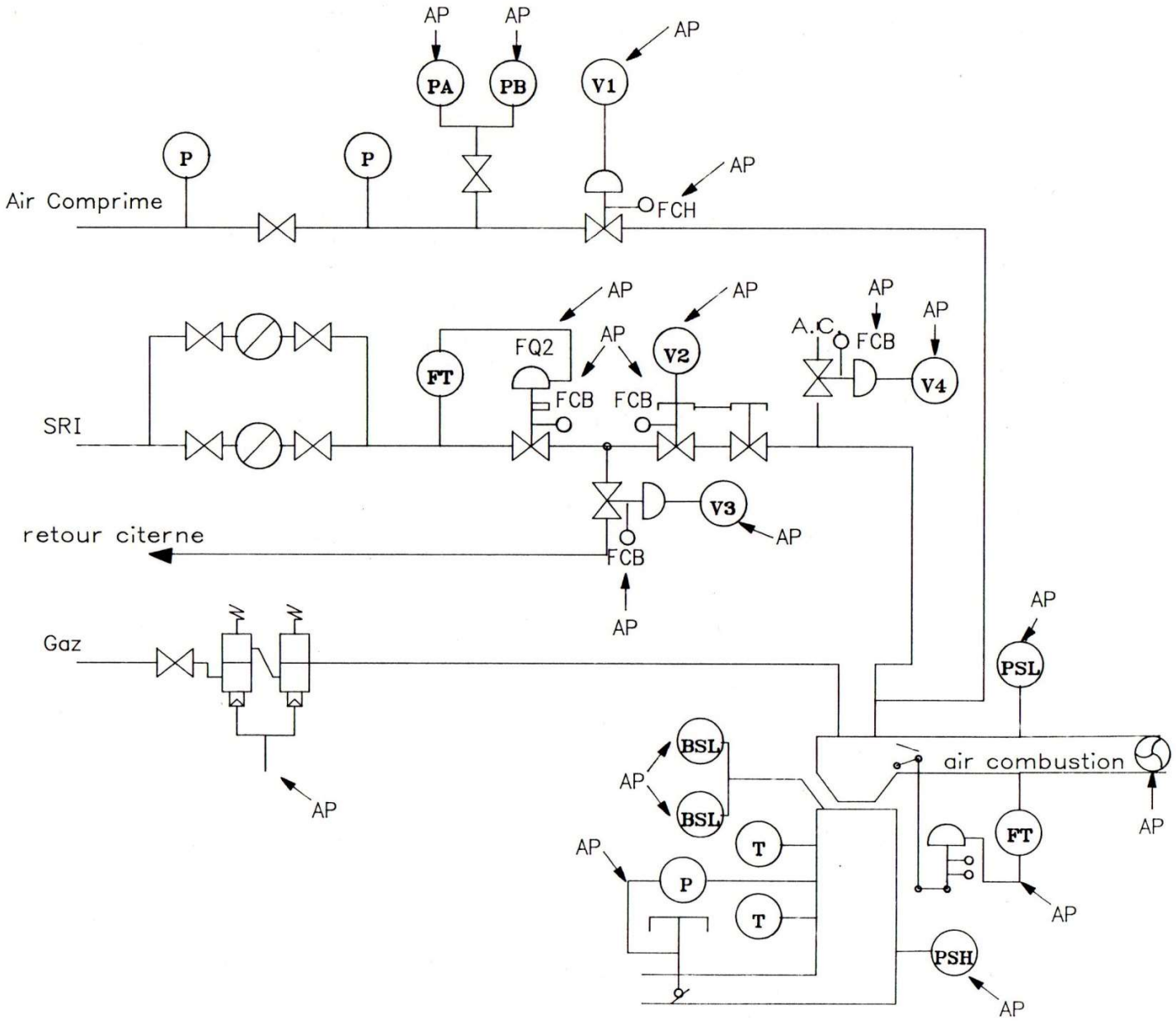
Coût de l'étude et des modifications



Implantation d'un nouvel Automate programmable

- Explosion d'une installation d'incinération de solvants et d'eaux chargées en solvant
- Reconstruction de l'installation
- Implantation d'un AP remplaçant un automate pneumatique
- Etude AMDEC des composants avec en parallèle le grafcet de l'AP

Schéma de l'incinérateur de solvants



ANALYSE DES MODES DE DEFAILLANCE DES COMPOSANTS DE LEURS EFFETS SUR LE SYSTEME ET DE LEUR CRITICITE

PROJET:

SYSTEMES: FOUR DE L'INCINERATEUR DATE:

SOUS–SYSTEME: CIRCUIT AIR DE COMBUSTION 1 DOCUMENTS:

IDENTIFICATION DU COMPOSANT	FONCTION ETATS	MODES DE DEFAILLANCE	CAUSES POSSIBLES D'UNE DEFAILLANCE	CONSEQUENCES		CLASSE DE GRAVITE	MOYENS DE DETECTION DES DEFAILLANCES	ACTIONS CORRECTIVES	REMARQU
				LOCALES	SUR LE SYSTEME				
Ventilateur V1	Creer la pression pour la circulation de l'air de combustion	Arret intempestif	–defaillance mecanique –perte d'alimentation	Arret de la circulation d'air	–en phase de balayage: non evacuation des vapeurs restant dans le four avant l'allumage Risque d'explosion	3	–capteur controlant l'alimentation du ventilateur (enclenchement du relais de commande) – capteur de pression seuil bas –surveillance du debit d'air en salle de controle	–commande par l'AP de la sequence defaut –declenchement de l'arret par le bouton poussoir	
					–en phase de combustion: combustion incomplete accumulation de solvant dans le four Risque d'explosion	3			
Ventels –regulation pneumatique –commande de mise en regulation par l'AP	Regler le debit d'air de combustion Phase de balayage	Refus d'ouverture (ou fermeture intempestive)	–defaillance mecanique –defaut de commande au niveau: –AP –commande pneumatique (distributeur ou alimentation)	Circulation d'air reduite	non evacuation des vapeurs restant dans le four avant l'allumage Risque d'explosion	3	idem –fin de course ferme (active) –fin de course ouvert (non active) –surveillance du debit d'air en salle de controle	idem –commande par l'AP de la sequence defaut –declenchement de l'arret par le bouton poussoir	

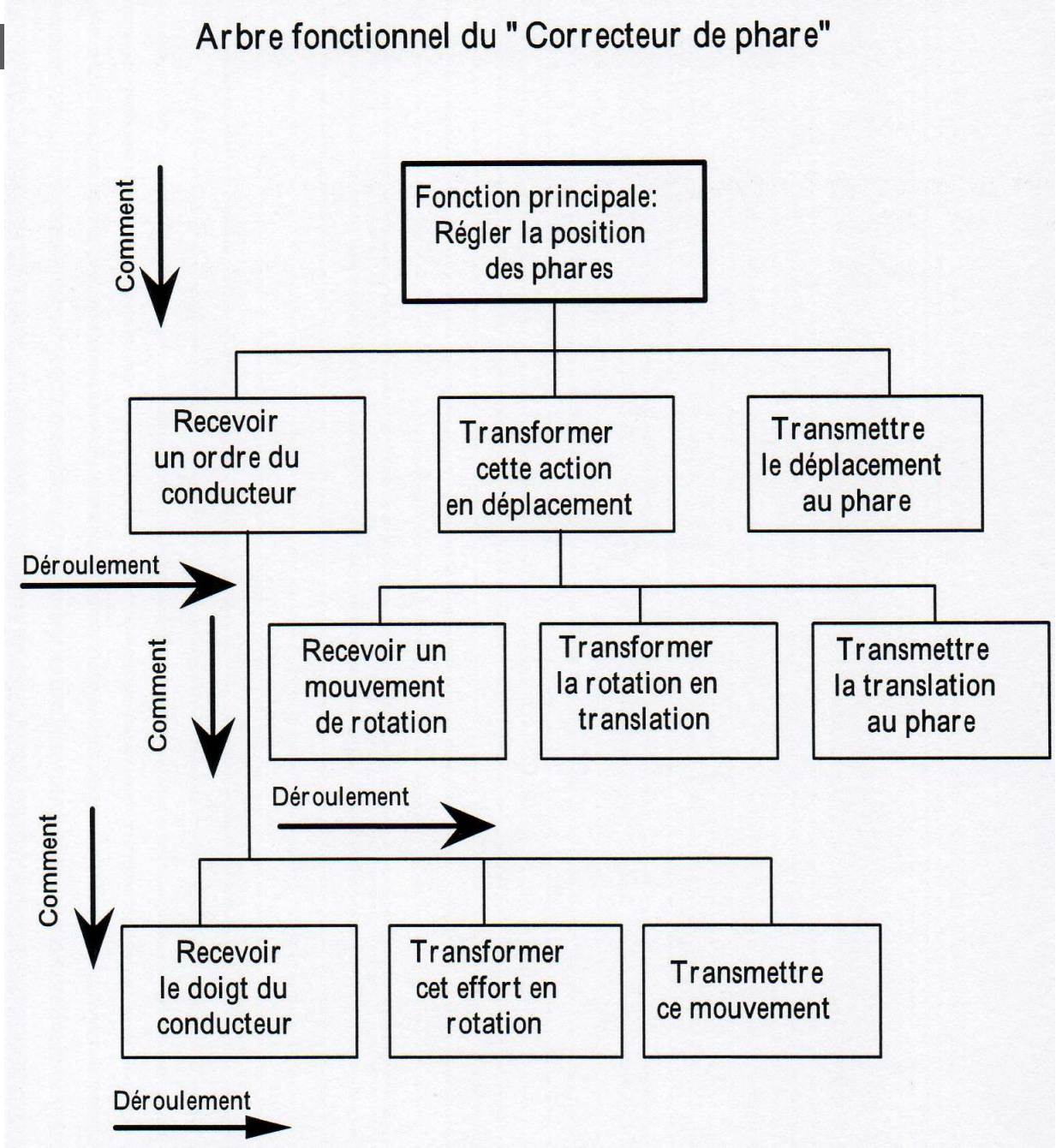
Résultats

- Très nombreuses remarques
  - Pilotage par AP « unique » :
    - Pour le pilotage du procédé & la sécurité
    - Absence de redondance (si on perd l'AP, on perd la sécurité)
  - Certaines fonctions de sécurité doivent être découplées
- Exemple de points soulevés
  - Beaucoup d'indéterminations :
    - De situations
    - De positions des actionneurs (capteurs sur FC)

La « Fiabilité » ou « sureté de fonctionnement »

…qui s’inspire de l’AMDEC

Analyse fonctionnelle : méthode RELIASEP



On identifie (AMDEC) puis on probabilise les défaillances

Taxonomy no	Item
1.2.1.2.2	Process Systems Valves Control Oil

Population	Installations	Aggregated time in service (10^6 hours)		No of demands
		Calendar time *	Operational time †	
77	15	1.3195		

Failure mode	No of failures	Failure rate (per 10^6 hours)			Active repair (hours)	Repair (manhours)		
		Lower	Mean	Upper		Min	Mean	Max
Critical	**21 ***	**8.55**	**15.76**	**25.02**	**10.5**	**2.0**	**17.3**	**45.0**
Delayed operation	1 *	0.17	0.75	3.36	26.3	45.0	45.0	45.0
Faulty indication	1 *	0.17	0.75	3.36	5.2	8.0	8.0	8.0
Fail to close	2 *	0.49	1.50	4.53	6.4	5.0	10.0	15.0
Fail to open	3 *	0.90	2.25	5.63	11.3	4.0	18.7	42.0
Internal leakage	3 *	0.34	2.25	6.19	11.8	14.0	19.7	24.0
Significant internal leakage	3 *	0.34	2.26	6.21	15.1	10.0	25.3	35.0
Spurious operation	2 *	0.49	1.50	4.53	5.5	2.0	8.5	15.0
Unknown	6 *	2.00	4.50	9.03	8.5	2.0	13.8	41.0
Degraded	**43 ***	**21.43**	**32.29**	**45.20**	**13.4**	**1.0**	**22.4**	**70.0**
Delayed operation	3 *	0.35	2.25	6.17	2.7	1.0	3.7	8.0
External leakage	3 *	0.90	2.26	5.65	11.8	6.0	19.7	28.0
Faulty indication	7 *	2.16	5.24	10.35	7.5	1.0	12.1	52.0
Internal leakage	7 *	2.55	5.27	10.02	11.7	1.0	19.4	70.0
Overhaul	5 *	0.59	3.79	9.02	16.7	20.0	28.2	36.0
Spurious operation	6 *	1.56	4.51	9.50	15.8	2.0	26.7	64.0
Unknown	12 *	4.66	8.99	15.36	18.3	3.0	31.0	53.0
Incipient	**21 ***	**9.82**	**15.82**	**23.86**	**14.8**	**2.0**	**24.9**	**79.0**
Delayed operation	1 *	0.17	0.76	3.39	2.3	3.0	3.0	3.0
External leakage	6 *	0.21	4.48	10.78	9.5	2.0	15.7	34.0
Faulty indication	3 *	0.91	2.26	5.67	1.7	2.0	2.0	2.0
Internal leakage	1 *	0.17	0.76	3.39	38.3	66.0	66.0	66.0
Overhaul	2 *	0.50	1.52	4.57	35.4	43.0	61.0	79.0
Seepage	1 *	0.17	0.76	3.39	37.1	64.0	64.0	64.0
Spurious operation	1 *	0.17	0.76	3.39	12.0	20.0	20.0	20.0
Unknown	6 *	1.97	4.54	9.13	14.7	10.0	24.7	42.0
Unknown	**12 ***	**4.37**	**9.00**	**15.66**	**13.8**	**4.0**	**23.2**	**60.0**
Overhaul	5 *	1.43	3.76	8.13	13.1	12.0	22.0	48.0
Unknown	7 *	1.47	5.24	11.07	14.3	4.0	24.1	60.0
All modes	**97 ***	**49.94**	**72.88**	**97.87**	**13.1**	**1.0**	**22.0**	**79.0**

Comments

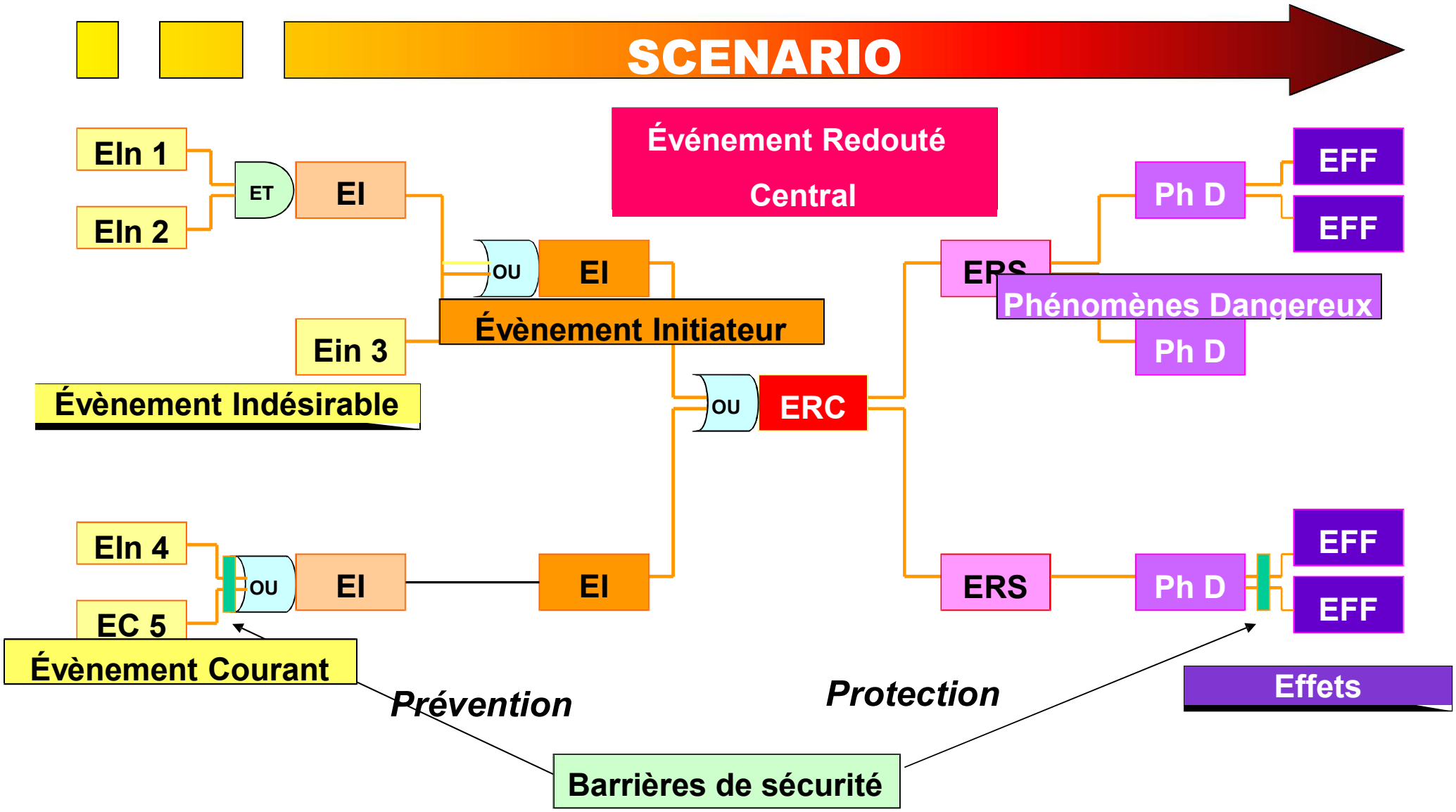
The estimates for the different failure modes were in some cases based on different subsets of data. This results from tests of statistical consistence among items, see sub chapter 3.4.

Et on quantifie un niveau de sureté de fonctionnement :

Tableau 5 – Niveau SIL suivant la norme CEI 61508			
Niveau d'intégrité de sécurité *(safety integrity level)* SIL	Probabilité annuelle de défaillance de la fonction		Facteur de réduction du risque (RRF)
	Fonctionnement en continu	Fonctionnement à la sollicitation	
	Taux de défaillance horaire	Probabilité de défaillance à la sollicitation (PFD_{avg})	
SIL 4	$10^{-8} < \lambda < 10^{-9}$	$10^{-4} < PFD_{avg} < 10^{-5}$	100 000 à 10 000
SIL 3	$10^{-7} < \lambda < 10^{-8}$	$10^{-3} < PFD_{avg} < 10^{-4}$	10 000 à 1 000
SIL 2	$10^{-6} < \lambda < 10^{-7}$	$10^{-2} < PFD_{avg} < 10^{-3}$	1 000 à 100
SIL 1	$10^{-5} < \lambda < 10^{-6}$	$10^{-1} < PFD_{avg} < 10^{-2}$	100 à 10

Taux de défaillance des « Barrières de sécurité »

…qui s’inspire de la sureté de fonctionnement


SCENARIO
EIn 1
EIn 2
ET
EI
Ein 3
OU
EI
Évènement Initiateur
Événement Redouté Central
Évènement Indésirable
OU
ERC
ERS
Ph D
EFF
EFF
Phénomènes Dangereux
Ph D
EIn 4
EC 5
OU
EI
EI
ERS
Ph D
EFF
EFF
Évènement Courant
Prévention
Protection
Effets
Barrières de sécurité
Arbre de défaillances
Arbre d'événements

Définitions

Fonction de sécurité (FS): Fonction ayant pour but la prévention et la protection d'événements redoutés. Les FS identifiées peuvent être assurées à partir de barrières techniques de sécurité, de barrières humaines (activités humaines) de sécurité, ou plus généralement par la combinaison des 2. Une même FS peut être réalisée par différentes barrières de sécurité. Une FS peut se décomposer en sous-fonction de sécurités liées.

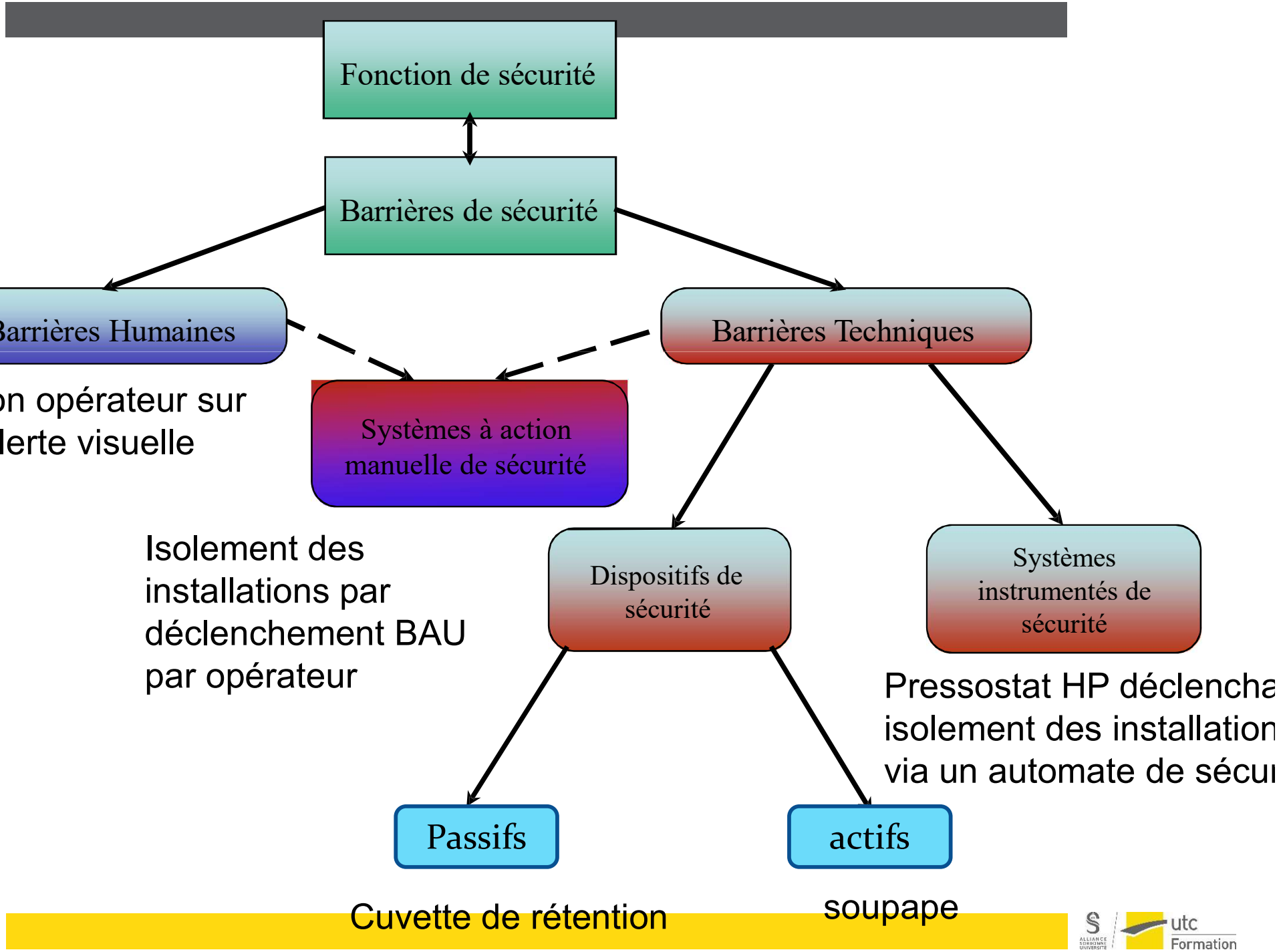
Barrière de sécurité (BS) : barrière qui permet d'assurer une fonction de sécurité. Elle peut être soit technique, soit humaine, soit combinée. Elle s'oppose à l'enchaînement d'événements susceptibles d'aboutir à un accident.

Définitions

Barrière technique de sécurité (BTS) : barrière de sécurité constituée d'un dispositif de sécurité ou d'un système instrumenté de sécurité.

- Dispositif de sécurité : élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité dans sa globalité.
- Système instrumenté de sécurité (SIS) : combinaison de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une ou plusieurs fonctions de sécurité.

- Barrière Humaine de sécurité (BHS) : tâche ou ensemble de tâches. Une BHS a pour fonction de s'opposer à l'apparition (vérification) ou à l'enchaînement d'événements susceptibles de générer un accident (rattrapage).


Fonction de sécurité
Barrières de sécurité
Barrières Humaines
Barrières Techniques
Action opérateur sur alerte visuelle
Systèmes à action manuelle de sécurité
Isolement des installations par déclenchement BAU par opérateur
Dispositifs de sécurité
Systèmes instrumentés de sécurité
Pressostat HP déclencha isolement des installation via un automate de sécu
Passifs
actifs
Cuvette de rétention
soupape

Critères

Une série d'action et/ou un dispositif technique est une BS si **dans son contexte d'utilisation** (i.e. dégradé) au minimum :

- **indépendant** du scénario d'accident ,
- **indépendant** des autres BS pour pouvoir les "agréger"
- « Testable et maintenable »

Ssi c'est une BS on étudie sa **performance** (critères indépendants):

- **Efficacité** (aptitude à remplir la fonction => dimensionnement adapté, résistance aux contraintes spécifiques, accessibilité,...)
- Temps de réponse ou **cinétique** (par rapport aux événements)
- **Niveau de confiance** (NC)

Niveau de confiance

Le “**niveau de confiance**” (NC).
Est une notion inspirée des techniques d’évaluation des “niveaux SIL” de la sureté de fonctionnement (ex: normes NF-EN 61508 et 61511).

Probabilité de non fonctionnement sur demande= 10^{-NC}

La méthode proposée est un outil d’évaluation qualitatif “simple” pour évaluer la performance des BS en groupe de travail notamment lors des séances d’analyse des risques (méthode INERIS).

Performance *globale* d'une BS

Avant tout, comprendre le fonctionnement de la barrière de sécurité

S'il s'agit d'un SIS d'une SAMS ou d'une BHS, le décomposer en 3 sous-fonctions :

- Détection
- Traitement de l'information
- Action

Efficacité (EF)	$EF_{sis}=Min(EF_{détection}, EF_{traitement}, EF_{action})$
Temps de réponse (TR)	$TR_{sis}=TR_{détection}+TR_{traitement}+TR_{action}$
Niveau de confiance (NC)	$NC_{sis}=Min(NC_{détection}, NC_{traitement}, NC_{action})$

Identification d'une BTS

Pour qu'un système technique puisse être considéré comme une BTS, il faut **absolument** que le système proposé soit :

- de concept éprouvé (a minima, déclaré de sécurité dans le cahier des charges)
- **indépendant** du procédé (qui est en mode dégradé…)
- à sécurité positive (si applicable)
- **indépendant** d'une autre BTS pour pouvoir les "agréger"

Performance d'une BTS

•**…Niveau de confiance (NC)** : adaptation des exigences des normes NF-EN 61508 et 61511.

Les niveaux de confiance sont discrets, du niveau "1" au niveau "4", NC "1" étant le niveau le plus bas, NC "4" le plus élevé. Un NC détermine une réduction du risque (proba scénario x 10^{-NC}).

2 catégories :

- les dispositifs passifs où la notion d'architecture n'a pas de sens (disque de rupture, mur coupe-feu…) => l'évaluation a lieu à partir du retour d'expérience, de l'état de l'art, voire de l'utilisation de bases de données de défaillances....
- Les systèmes actifs de type A (sans microprocesseur) ou B (avec) pour lesquelles on doit déterminer :
  - Le **taux de défaillances sûres (SFF)** : rapport de la somme des taux de défaillances sûres sur la somme des taux de défaillances **(AMDEC)**
  - La **tolérance aux anomalies matérielles** : équivalent à une redondance

Performance d'une BTS : type A

Passives = NC = 2 *voire 3 si dimensionnement et contrôle précis*

Actives

Taux de défaillances sûres (SFF)	Tolérance aux anomalies matérielles (*Redondance*)		
	0	1	2
< 60 %	NC 1	NC 2	NC 3
60 % < - < 90 %	NC 2	NC 3	NC 4
90 % < - < 99%	NC 3	NC 4	NC 4
≥ 99 %	NC 3	NC 4	NC 4

Autotest

Performance d'une BTS : type B

Taux de défaillances sûres (SFF)	Tolérance aux anomalies matérielles		
	0	1	2
< 60 %	Non autorisé	NC 1	NC 2
60 % < - < 90 %	NC 1	NC 2	NC 3
90 % < - < 99%	NC 2	NC 3	NC 4
≥ 99 %	NC 3	NC 4	NC 4

Performance d'une BTS : limites

En pratique :

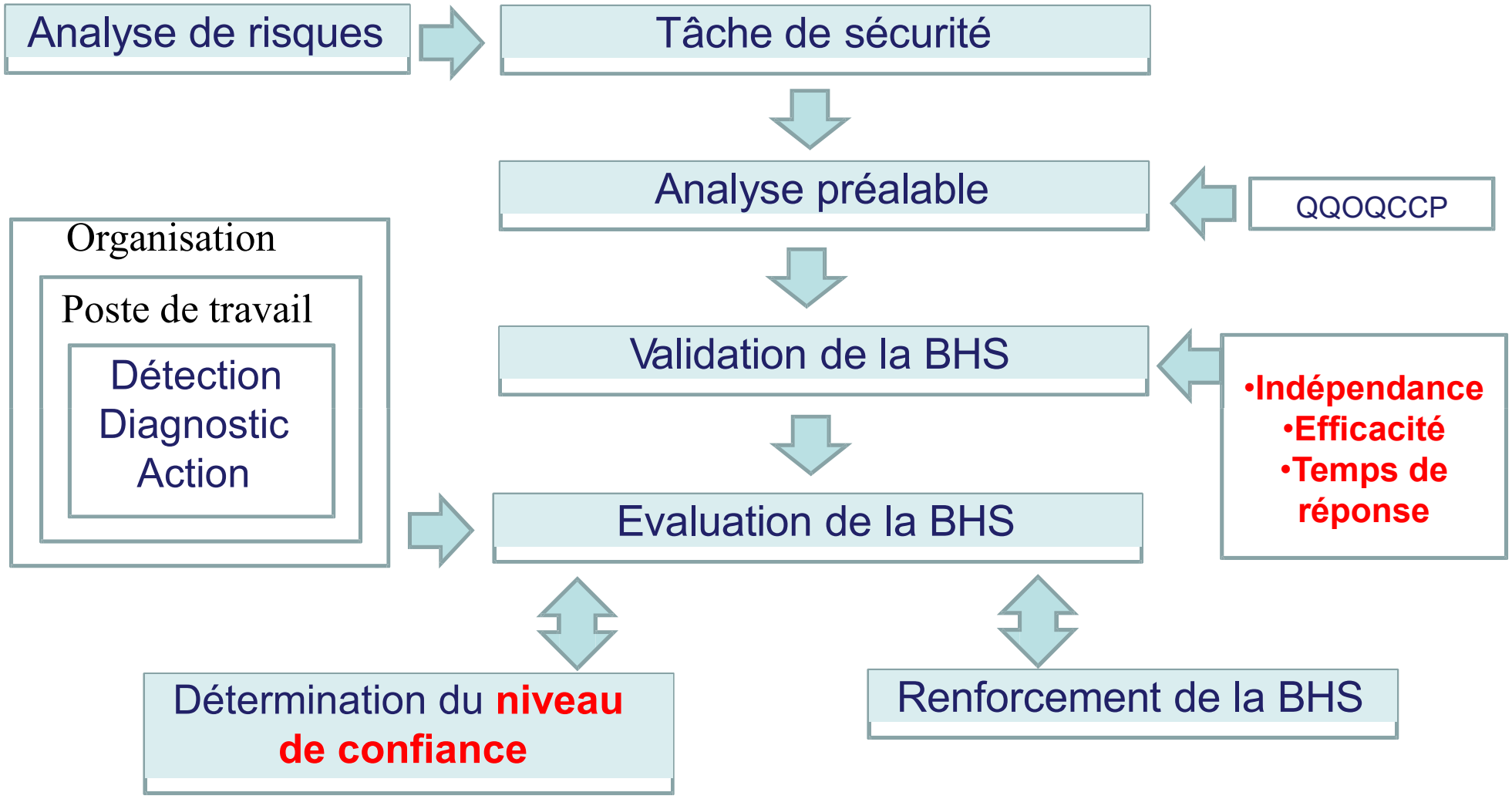
- Les technologies et connaissances actuelles ne permettent pas d'atteindre un NC de "4"
- Le SFF est supposé < 60 %, à moins de disposer d'une démonstration
- Le **NC attribué à un système sera en général <2**, sauf si:
  - auto-testé (et sauf cas particulier)
  - bon retour d'expérience formalisé
  - …avec au maximum un NC de "3"
- La performance (efficacité, temps de réponse et NC) des BTS doit être maintenue dans le temps par des tests et un entretien préventif

Identification d'une BHS

- Une Barrière Humaine de Sécurité (BHS) est une tâche ou un ensemble de tâches conçu pour assurer la maîtrise des paramètres de sécurité. Une BHS a pour fonction de s'opposer à l'apparition (**vérification**) ou à l'enchaînement d'événements susceptibles de générer un accident (**rattrapage**).

- Un Système à action manuelle de sécurité (SAMS) : Sous catégorie des BHS. La fonction de sécurité est réalisée par la mise en œuvre : d'une action et/ou décision humaine et d'un système instrumenté de sécurité

- Comme pour les BTS on veut :
  - **Sélectionner** des BHS
  - Evaluer leurs **performances**
  - Vérifier leur **maintenabilité** et leur **testabilité**


Analyse de risques
Tâche de sécurité
Analyse préalable
QQOQCCP
Organisation
Poste de travail
Détection
Diagnostic
Action
Validation de la BHS
•Indépendance
•Efficacité
•Temps de réponse
Evaluation de la BHS
Détermination du niveau de confiance
Renforcement de la BHS

Identification d'une BHS

On ne retient que le critère d'**indépendance** : La BHS est indépendante si l 'opérateur en charge de la barrière et les éléments techniques dont il se sert sont indépendants :

- de la cause du scénario ;
- ou du scénario lui-même (ou du procédé)

Critère d'indépendance d'une action de vérification est atteint si elle est menée :

§ par une autre personne
§ Ou dans une séquence de travail différente par rapport à l'exploitation

Performance d'une BHS: efficacité

« Dimensionnement adapté » : si la tâche de sécurité, telle qu'elle est prévue, permet de remplir l'objectif de sécurité visé dans le contexte du scénario (validité des actions requises) et :

- **si les besoins en connaissances de l'opérateur liés à la réalisation de la tâche de sécurité ont été identifiés et pourvus** (connaissance des enjeux de sécurité relatifs à la tâche à effectuer et aux conditions de sa réalisation, formation, compagnonnage, …),
- **si les besoins matériels de l'opérateur liés à la réalisation de la tâche de sécurité ont été identifiés et pourvus** (outils d'aide, documentation, procédures, … etc.) de sorte que la tâche de sécurité permette de remplir l'objectif de sécurité visé dans le contexte du scénario.

« Résistance aux contraintes spécifiques » : protection des opérateurs vis-à-vis du contexte accidentel - EPI, positionnement des moyens d 'intervention (Ex: Contrôle de l'état extérieur d'une canalisation transportant un liquide corrosif)

Performance d'une BHS: autres

Temps de réponse

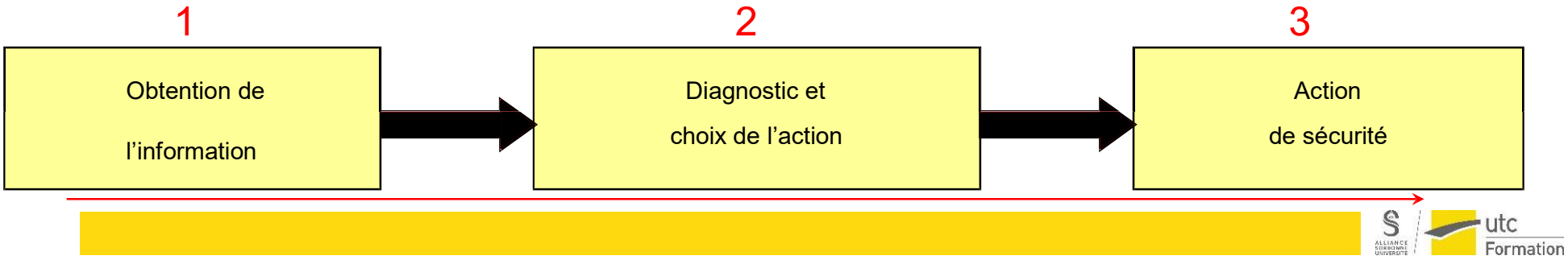
§ Temps de réponse obtenu à partir des exercices tant que possible.

§ Doit inclure toutes les étapes préalables nécessaires à la réalisation de l'action de sécurité - *revêtir les EPI, déployer les moyens, temps de communication et de coordination en cas d'actions impliquant plusieurs acteurs,...*

Cas des actions réalisées à une fréquence donnée (rondes de surveillance) : inclure la périodicité de la ronde dans le temps de détection

Niveau de confiance

§ **NCmax = 2**. Ce niveau de confiance décroît du moment que des facteurs défavorables sont identifiés.



Performance d'une BHS: autres

Décote	Caractéristiques de la situation de travail *Obtention de l'information – détection « passive »*
0	Information clairement perceptible et identifiable : Information disponible de façon hiérarchisée (par exemple : alarme dédiée visuelle et sonore clairement distincte des autres types d'alarmes) donnant l'état du système, quelles que soient les conditions environnementales (nuit, brouillard, …) qui seraient susceptibles d'empêcher ou de gêner la perception de ces informations. ET Totale disponibilité de l'opérateur : L'opérateur est présent à l'endroit où l'information est disponible et il peut interrompre toute autre activité en cours. Les conditions de travail sont favorables au maintien d'un bon niveau de vigilance.
- 1	Information perceptible et identifiable avec une difficulté modérée : Information disponible de façon non hiérarchisée au milieu d'un nombre limité d'autres informations, ET/OU Disponibilité de l'opérateur : L'opérateur est présent à l'endroit où l'information est disponible et il peut être amené à gérer un nombre acceptable d'autres tâches en même temps sans remise en cause de ses capacités de perception.
- 2	Information difficilement perceptible et identifiable : Information noyée parmi d'autres informations, ou information difficilement détectable (localisation des informations non adaptée à l'activité de l'opérateur, perception pouvant s'avérer difficile, notamment dans certaines conditions environnementales ou dans le cadre du déroulement du scénario). OU Faible disponibilité de l'opérateur : L'opérateur est rarement présent à l'endroit où l'information est disponible ou il est présent de façon aléatoire non prévisible ou il peut être amené à gérer un nombre important de tâches en même temps.

Performance d'une BHS: autres

Décote	· Caractéristiques de la situation de travail *Obtention de l'information – détection « active »*
0	Facilité d'obtention de la/des information(s) recherchée(s) : Identification ou obtention de l'information simple (information clairement identifiable, pas de confusion possible, …) par rapport au niveau de compétence attendu de l'opérateur et conditions de travail jugées non contraignantes (conditions environnementales favorables, bonne accessibilité à l'information…). ET Totale disponibilité et engagement de l'opérateur : Cette tâche est une activité planifiée, bien dimensionnée dans le plan de charge de l'opérateur, et perçue comme prioritaire par l'opérateur. Celui-ci dispose d'une marge de manœuvre suffisante pour faire face à d'éventuels aléas sans compromettre la réalisation de la tâche dans les conditions requises.
- 1	Conditions d'obtention de la/des information(s) recherchée(s) moyennement aisées : Identification ou obtention de l'information réalisée avec un effort (intellectuel et/ou physique) acceptable par rapport au niveau de compétence attendu de l'opérateur et aux conditions d'accès à l'information. ET/OU Disponibilité et engagement de l'opérateur : Cette tâche est une activité planifiée et dimensionnée dans le plan de charge de l'opérateur, et perçue comme importante par l'opérateur. Celui-ci dispose d'une marge de manœuvre plus réduite pour faire face à d'éventuels aléas.
- 2	Impossibilité ou difficulté d'obtention de la/des information(s) recherchée(s) : Identification ou obtention de l'information difficilement réalisable ou réalisée avec un effort (intellectuel et/ou physique) important ou conditions de travail jugées fortement contraignantes (accessibilité à l'information très difficile, forte pénibilité de l'activité, …). OU Faible disponibilité et engagement de l'opérateur : Cette tâche n'est pas prévue ou n'est pas correctement dimensionnée dans le plan de charge de l'opérateur ou cette tâche peut être perçue comme moins prioritaire vis-à-vis d'autres contraintes d'exploitation.

Performance d'une BHS: autres

Diagnostic permettant le choix de l'action

Décote	· Caractéristiques de la situation de travail
0	Bonne qualité et accessibilité des informations utiles au diagnostic : Présentation explicite et niveau suffisant d'informations : informations directes non sujettes à interprétation sur l'état du système (et la localisation de l'accident), de l'incident ou du défaut (respect des conventions de présentation des informations, le cas des indicateurs défaillants est signalé, …etc.). L'opérateur dispose si nécessaire d'un délai confortable pour prendre du recul sur la qualité et le niveau d'information utile, et approfondir le diagnostic. ET Niveau de guidage adapté à la situation : L'usage de procédure n'est pas nécessaire ou, dans le cas contraire, la décision est guidée par des procédures explicites (instruction claire et explicitation des conséquences de l'action sur le système) ou aide contextuelle fournie par le système (sur le système de conduite, signalisation à proximité des dispositifs de signalisation ou des organes de commande …) permettant de déterminer facilement l'action à réaliser.
- 1	Qualité acceptable des informations utiles au diagnostic : Présentation des informations non directement utilisables pour faire le diagnostic mais des modalités de traitement sont prévues pour obtenir les informations utiles au diagnostic mais qui peuvent parfois être source d'erreur (certains types de calculs, conversion d'unité, …) Ou niveau d'informations pas toujours suffisant mais il est possible d'approfondir le diagnostic par la recherche d'informations complémentaires (l'opérateur dispose alors d'un délai raisonnable pour prendre du recul et collecter les informations nécessaires) ET/OU Guidage prévu mais parfois insuffisant : Un certain niveau de guidage est nécessaire : les règles générales à appliquer sont connues ou formalisées mais un certain niveau d'interprétation des règles est nécessaire pour décider de la conduite à tenir (par exemple, les procédures traitent de nombreux cas connus mais une réflexion reste nécessaire pour décider).
-2	Qualité insuffisante des informations utiles au diagnostic : Informations insuffisamment explicites (ambigües, ou demandant des calculs complexes, des croisements de données, ou une réflexion mobilisant des connaissances non familières). Ou niveau d'informations insuffisant pour identifier le problème ou l'état du système, l'approfondissement du diagnostic est difficilement envisageable compte-tenu du contexte ou de l'organisation du travail (temps disponible insuffisant, isolement géographique, …). OU Guidage insuffisant : Application des règles difficilement envisageable compte-tenu de la situation : règle très générale ou trop précise qui demande des adaptations quasi-systématiques, ou nombre trop important de choix d'actions possibles, la prise de recul ou la sollicitation d'un avis extérieur étant difficile (ressources temporelles nécessaires insuffisantes par rapport au déroulement du scénario ou recours à un tiers non prévu dans l'organisation du travail).

Performance d'une BHS: autres

Décote	· Caractéristiques de la situation de travail *Action de sécurité*
0	Niveau de stress acceptable : Ressources nécessaires à la réalisation de l'action jugées suffisantes : absence de pression temporelle ou temps d'intervention largement inférieur à la cinétique de l'accident, pas d'exposition au danger, expérience significative de la situation, feed-back suffisant sur l'action engagée,... ET Tâche simple et peu exigeante : Nombre d'actions limité, sans enchaînement complexe (par exemple : fermer plusieurs vannes sans notion d'ordre), système robuste aux erreurs (détrompeur, temporisation, codes couleurs ou symboles évitant le risque de confusion,...) ou permettant d'alerter l'opérateur pour lui donner la possibilité de revenir en arrière. Les moyens d'actions étant facilement accessibles et facilement manœuvrables.
- 1	Niveau de stress possible mais tolérable : Ressources nécessaires à la réalisation de l'action jugées pouvant s'avérer insuffisantes, notamment dans certaines conditions difficiles (peu de marge temporelle, exposition au danger, …) ET/OU Tâche moyennement exigeante ou difficile : Nombre d'actions limité mais niveau d'exigence plus élevé : efforts importants de mémorisation ou de concentration, enchaînements stricts à respecter (par exemple : arrêter la pompe P1 puis seulement après, fermer la vanne V1 et ensuite la vanne V2. Modifier l'ordre de ces actions entraînerait un accident) mais le système permet à l'opérateur de revenir en arrière. Ou les moyens d'actions peuvent être moyennement accessibles et manœuvrables.
- 2	Niveau de stress important : Fort ressenti de pression : ressources nécessaires à la réalisation de l'action jugés inadaptées par rapport aux objectifs à atteindre (temps jugé insuffisant, exposition au danger, effet de panique, …). OU Tâche très exigeante, difficile ou impossible : Niveau d'exigence trop élevé (nombre d'actions important avec enchaînements stricts, impossibilité d'interrompre les effets d'une action engagée par erreur, …) et/ou accessibilité ou manœuvrabilité difficile ou impossible des moyens d'action.