

CONDUITE ET SÛRETE DES SYSTEMES AUTOMATISES

A. Mode de Fonctionnement des Systèmes Automatisés.

D) Le Guide d'Etude des Modes de Marches et d'Arrêts : GEMMA d'après l'ADEPA

1.1) Objectif:

Définir un vocabulaire précis décrivant sans ambiguïté les différents modes de marches et d'arrêts d'un système.

1.2) Présentation:

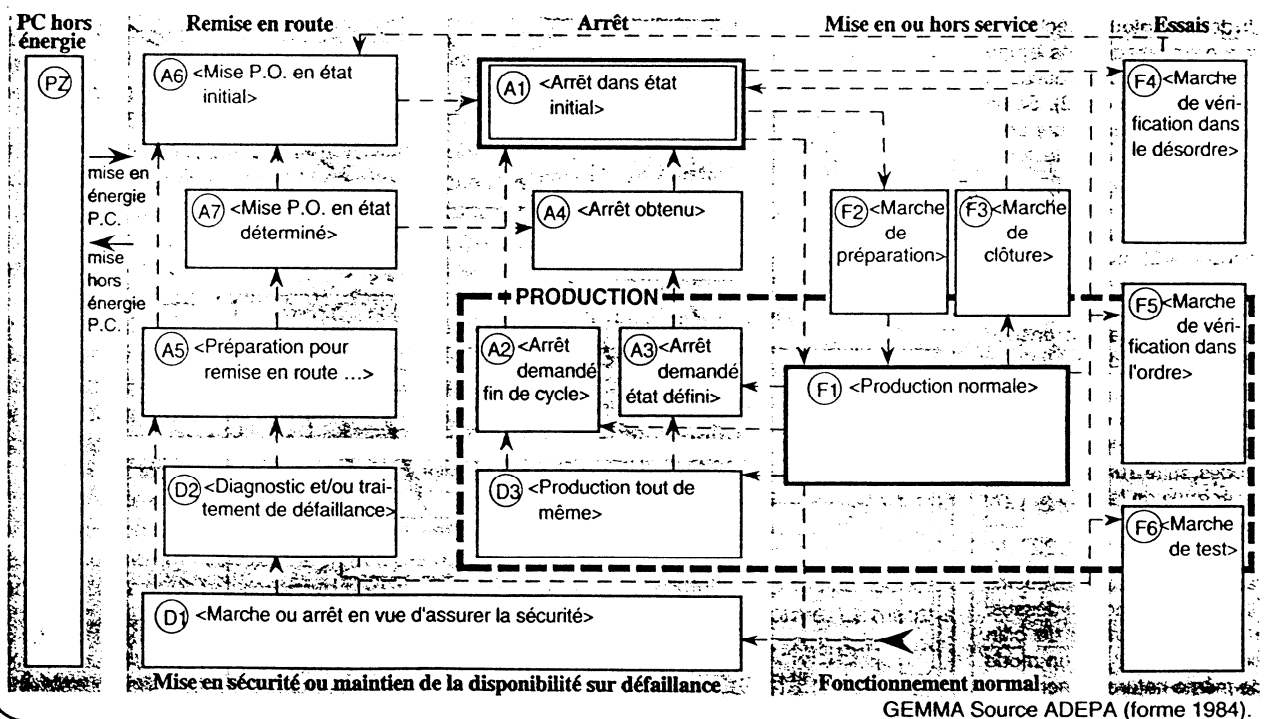
C'est un guide graphique basé sur quelques concepts de base qui propose une démarche en deux temps;

* Le recensement des différents modes envisagés et la mise en évidence des enchaînements qui les relie.

* La détermination des conditions de passage d'un mode à l'autre.

Le guide graphique GEMMA est constitué de deux zones :

- une zone correspondant à l'état « **hors énergie** » de la partie commande (**PC**)
- une zone permettant de décrire ce qui se passe lorsque la partie commande (**PC**) est « **sous énergie** » ; c'est la zone qui couvre la quasi totalité du guide graphique.



Remarque: Le GEMMA a apporté un cadre conceptuel et une rigueur de vocabulaire là où n'existaient qu'ambiguïté et imprécision.

On peut regretter que son utilisation soit insuffisamment développée dans l'industrie, mais cela peut s'expliquer en raison:

- * d'une diffusion insuffisante des méthodes de construction et d'interprétation matérielle et logicielle
- * de la difficulté d'appliquer le GEMMA à des unités de production complètes (ligne, module).

1.3) Concepts de base du GEMMA:

- Les modes de marches sont vus par la PC en Ordre de marche
- Le système est dit en production si la valeur ajoutée pour lequel il a été conçu est obtenue.

On y trouve 3 grandes familles de modes de marches et d'arrêts:

- * La Famille F; Procédures de Fonctionnement.
- * La Famille A; Procédures d'Arrêt.
- * La Famille D; Procédures de Défaillance.

<u>FAMILLE A:</u> Procédures d'Arrêt	<u>FAMILLE F:</u> Procédures de Fonctionnement
<u>FAMILLE D:</u> Procédures de Défaillance	

FAMILLE F:

FAMILLE A:

FAMILLE D:

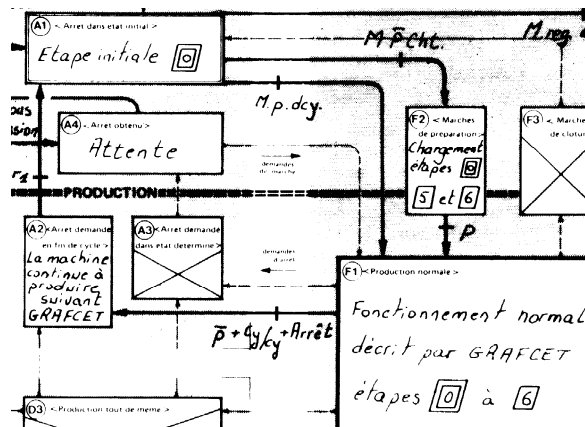
LES « RECTANGLES-ÉTATS »

Sur le guide graphique GEMMA (voir page 4), chaque mode de marche ou d'arrêt désiré peut être décrit dans l'un des «rectangles états » prévus à cette fin.

La position d'un rectangle état sur le guide graphique définit

- son appartenance à l'une des 3 familles ; procédure de **F**onctionnement, d'**A**rrêt ou de **D**éfaillance.
- le fait qu'il soit « en » ou « hors production ».

En pratique, pour une machine donnée, on ne choisira parmi les états proposés par le guide que ceux qui sont nécessaires, et on précisera le nom de chacun des états retenus, à l'intérieur du « rectangle état» correspondant.



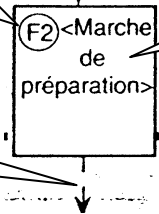
Pour effectuer ce choix, il est nécessaire de bien comprendre la signification de chacun des états de marches et d'arrêts proposés par le guide graphique.

Exemple de rectangle état

F2 est le repère du « rectangle état ». **F** signifie que l'état proposé fait partie des procédures de Fonctionnement. (A pour procédures d'Arrêt, et D pour procédures en Défaillance).

< Marche de préparation > est la dénomination générale de l'état proposé. Les signes < et > indiquent l'emploi du « langage général ».

Les principales possibilités de liaisons d'état à état sont suggérées.



1.4) Présentation du guide GEMMA complet:

■ **Les rectangles états**

Sur le guide graphique GEMMA, chaque mode de marches ou d'arrêts désiré peut être décrit dans un rectangle d'état portant une désignation qui utilise un vocabulaire ne pouvant pas prêter à confusion. Cette description pourra se faire en langage machine propre au concepteur. Par exemple en « Production normale », on pourra trouver la description « Marche semi-automatique ».

La position d'un rectangle état sur le guide graphique définit :

- son appartenance à l'une des trois familles,
- le fait qu'il soit « en » ou « hors production ».

• **Les états F**

Ce sont les états de marche situés dans la zone « procédures de fonctionnement » du guide graphique GEMMA.

F1 « Production normale » : Dans cet état, la machine produit normalement : c'est l'état pour lequel elle a été conçue. C'est à ce titre que le « rectangle-état » a un cadre particulièrement renforcé. On peut souvent faire correspondre à cet état un grafcet que l'on appelle grafcet de base.

Remarque : A cet état ne correspond pas nécessairement une marche automatique.

F2 « Marche de préparation » : Cet état est utilisé pour les machines nécessitant une préparation préalable à la production normale : préchauffage de l'outillage, remplissage de la machine, mises en routes diverses, etc.

F3 « Marche de clôture » : C'est l'état nécessaire pour certaines machines devant être vidées, nettoyées, etc., en fin de journée ou en fin de série.

F4 « Marche de vérification dans le désordre » : Cet état permet de vérifier certaines fonctions ou certains mouvements sur la machine, sans respecter l'ordre du cycle.

F5 « Marche de vérification dans l'ordre » : Dans cet état, le cycle de production peut être exploré au rythme voulu par la personne effectuant la vérification, la machine pouvant produire ou ne pas produire.

F6 « Marche de test » : Les machines de contrôle, de mesure, de tri..., comportent des capteurs qui doivent être réglés ou étalonnés périodiquement : a « Marche de test » F6 permet ces opérations de réglage ou d'étalonnage.

• **Les états A**

Situés dans la zone « procédures d'Arrêt de la partie opérative », ces états correspondent à des arrêts normaux ou à des marches conduisant à des arrêts normaux.

A1 « Arrêt dans l'état initial » : C'est l'état « repos » de la machine. Il correspond en général à la situation initiale du grafcet : c'est pourquoi, comme une étape initiale, ce rectangle-état est entouré d'un double cadre.

Pour une étude plus facile de l'automatisme, il est recommandé de représenter la machine dans cet état initial.

A2 « Arrêt demandé en fin de cycle » : Lorsque l'arrêt est demandé, la machine continue de produire jusqu'à la fin du cycle. A2 est donc un état transitoire vers l'état A1.

A3 « Arrêt demandé dans état déterminé » : La machine continue de produire jusqu'à un arrêt en une position autre que la fin du cycle : c'est un état transitoire vers A4.

A4 « Arrêt obtenu » : La machine est alors arrêtée en une autre position que la fin du cycle.

A5 « Préparation pour remise en route après défaillance » : C'est dans cet état que l'on procède à toutes les opérations (dégagements, nettoyages,...) nécessaires à une remise en route après défaillance.

A6 « Mise P.O. dans état initial » : La machine étant en A6, on remet manuellement ou automatiquement la partie opérative en position pour un redémarrage dans l'état initial.

A7 « Mise P.O. dans état déterminé » : La machine étant en A7, on remet la P.O. en position pour un redémarrage dans une position autre que l'état initial.

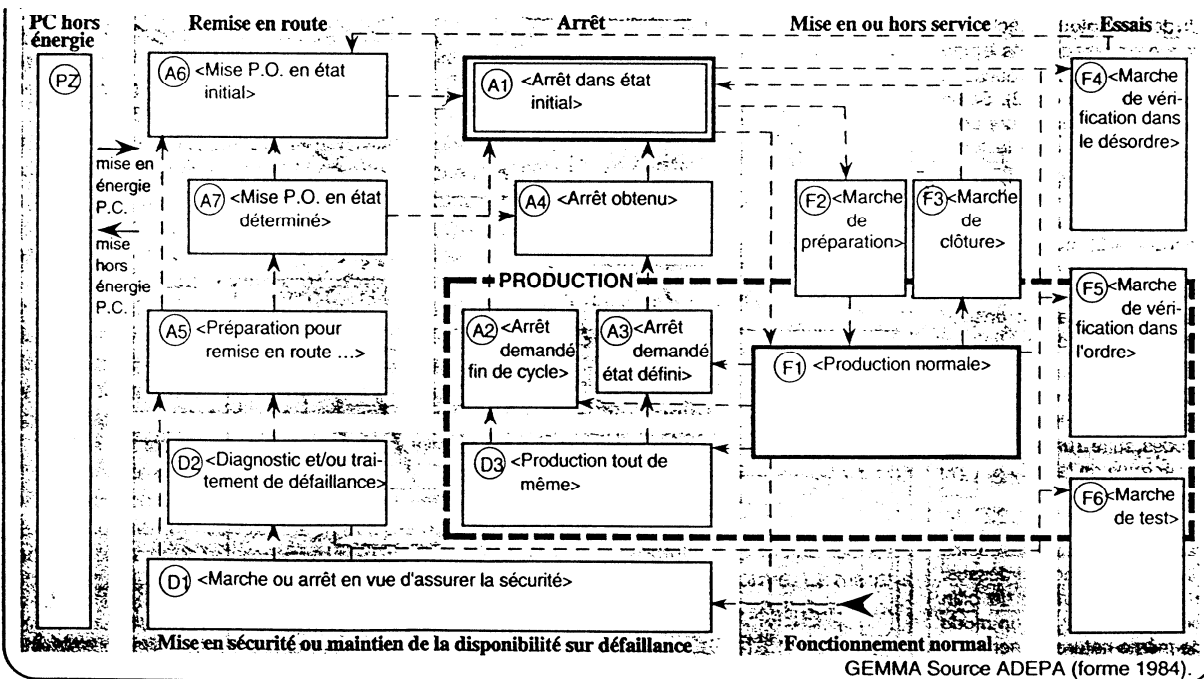
• **Les états D**

Ce sont les états de Marches et d'Arrêts situés dans la zone « procédures ou défaillances » de la partie opérative.

D1 « Arrêt d'urgence » : C'est l'état pris lors d'un arrêt d'urgence : on y prévoit non seulement les arrêts, mais aussi les cycles de dégagements, les procédures et précautions nécessaires pour éviter ou limiter les conséquences dues à la défaillance.

D2 « Diagnostic et/ou traitement de défaillance » : C'est dans cet état que la machine peut être examinée après défaillance et qu'il peut être apporté un traitement permettant le redémarrage.

D3 « Production tout de même » : Il est parfois nécessaire de continuer la production même après défaillance de la machine : on aura alors une « production dégradée », ou une « production forcée », ou une production aidée par des opérateurs non prévus en « Production normale ».



1.5) Méthode d'utilisation:

Séquence d'étude.

Phase 1

- Etude du processus d'action.

Parallèlement

- Définition du cycle de production (GRAF CET fonctionnel).

Phase 2

- Définition de la partie opérative et des capteurs.

Parallèlement

- Etablissement du GRAF CET opérationnel de base

Phase 3

- Mise en oeuvre du guide graphique GEMMA pour la sélection des modes de marches et d'arrêts avec mise en évidence des liaisons entre ces modes.

Phase 4

- Définition à l'aide du GEMMA des conditions d'évolution entre les états de marches et d'arrêts

parallèlement

- Définition des fonctions du pupitre de commande.
- Etablissement du GRAF CET complété.

Phase 5

- Choix d'une technologie de commande : électrique, électronique ou pneumatique, câblée ou programmée...

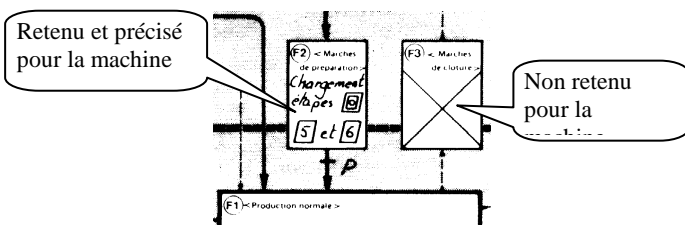
Phase 6

- Conception du schéma ou du programme de commande dans la technologie choisie.

Sélection des modes de marches et d'arrêts.

a) Envisager tous les « rectangles-états » proposés par le GEMMA. Avec ses « rectangles-états », le guide graphique constitue une « check list » des différents types de modes de marches et d'arrêts nécessaires en automatisation industrielle courante. Pour une machine donnée, il est donc important d'examiner le cas de chaque « rectangle-état » :

- si le mode proposé est retenu, il sera précisé en « langage machine », dans le rectangle-état » ; au besoin, plusieurs variantes de ce mode seront distinguées;
- si le mode proposé n'est pas nécessaire pour la machine, une croix sera portée dans le « rectangle-état », pour bien signifier qu'il n'est pas retenu.



b) Rechercher les évolutions d'un état à l'autre. Deux états essentiels, définis dès le début de l'étude, se retrouvent sur toutes les machines

- l'état A1, dit « état initial » ou « état repos » de la machine,
- l'état F1, mode de « production normale », pour lequel la machine a été conçue.

En parlant de chacun des deux états essentiels, A1 et F1, il est intéressant de rechercher Les évolutions vers d'autres états, dont la nécessité est moins évidente au premier abord.

- On pourra commencer par réfléchir au démarrage de la machine, c'est-à-dire passer de A1 à F1, en se posant la question : une « marche de préparation » F2 est-elle nécessaire ?

- Comment arrêter la machine, au choix :

- en fin de cycle → circuit F1 → A2 → A1
- dans une autre position → circuit F1 → A3 → A4

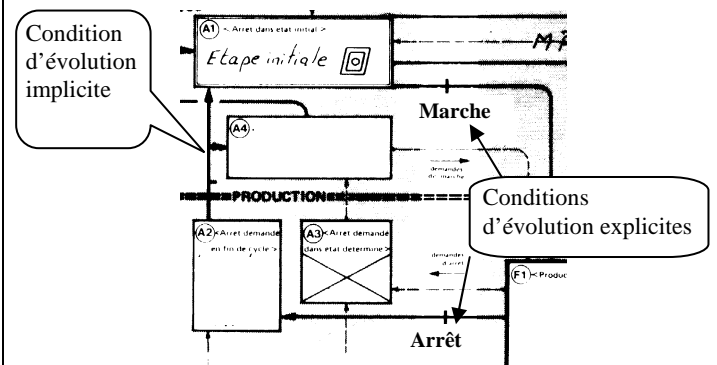
- On examinera les cas de défaillance,

- avec « Arrêt d'urgence », D1
- avec « Production tout de même », D3.
- etc....

Conditions d'évolution.

On peut passer d'un état à l'autre de deux manières :

- 1 Avec une condition d'évolution : elle est portée sur la liaison orientée entre états la condition peut être liée à l'action sur un bouton du pupitre de commande, ou à l'actionnement d'un capteur situé sur la machine.
- 2 Sans condition d'évolution : dans certaines évolutions entre états, l'écriture d'une condition n'apporterait aucune information utile c'est le cas lorsque celle-ci est évidente (exemple, passage de A2 à A1 ci-dessous), ou parce que l'état atteint dépend de l'intervenant.



Conclusion

Comme nous venons de le voir dans les exemples précédents, on peut apercevoir les conséquences de l'intervention du GEMMA dans la séquence d'étude de la machine.

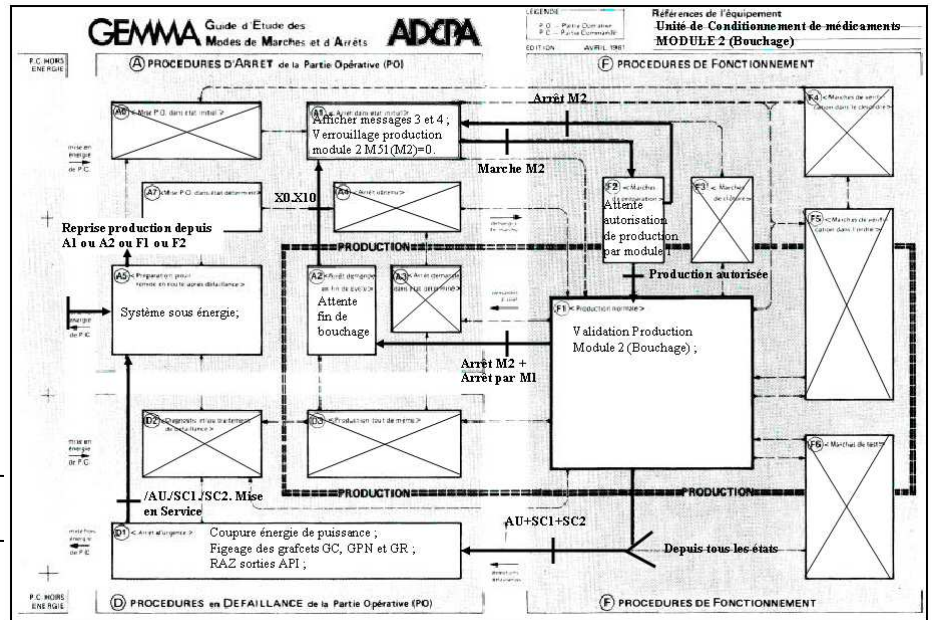
- ✓ la machine est mieux conçue, donc sa réalisation et sa mise en route se font avec moins de tâtonnements et de modifications
- ✓ comme le GRAF CET, le GEMMA suivra ensuite la machine, facilitant les dépannages ou modifications.

1.6) Représentation hiérarchisée de la P.C. induite par le GEMMA .

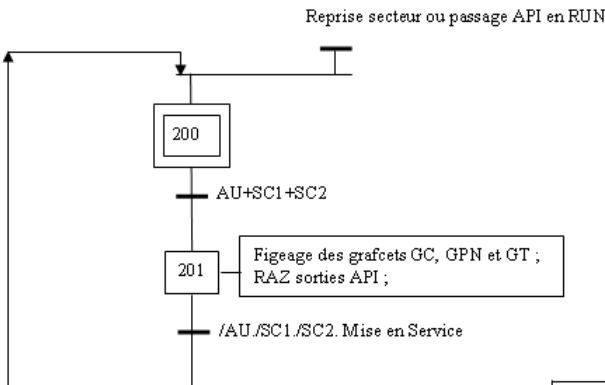
La P.C. peut alors être structurée en plusieurs niveaux hiérarchisés. La représentation la plus simple en utilise deux.

Exemple d'une structure hiérarchisée de P.C.

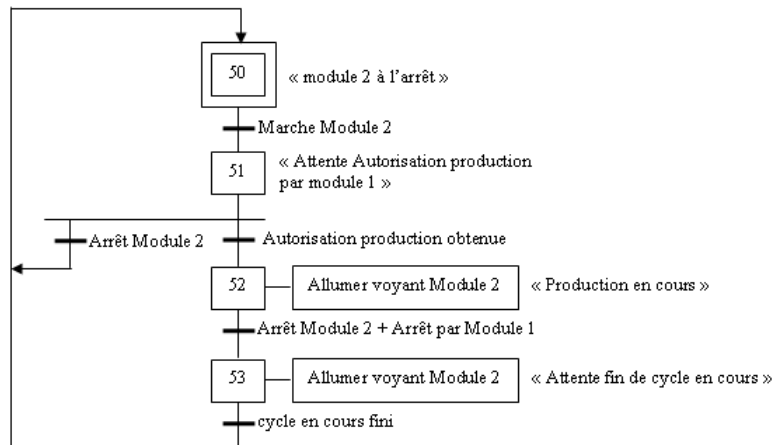
(structuration de la PC du module 2 machine Ravoux)



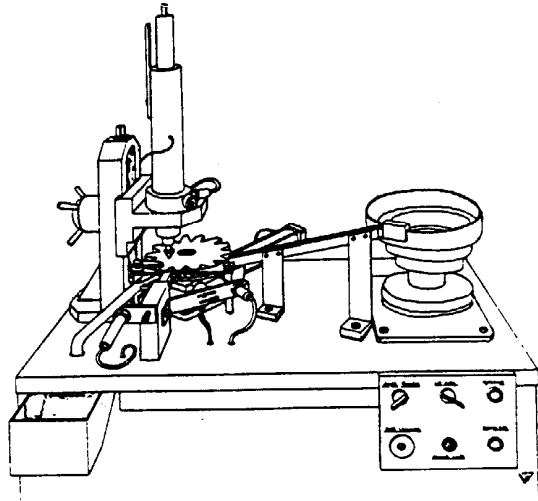
Grafctet de Sécurité:



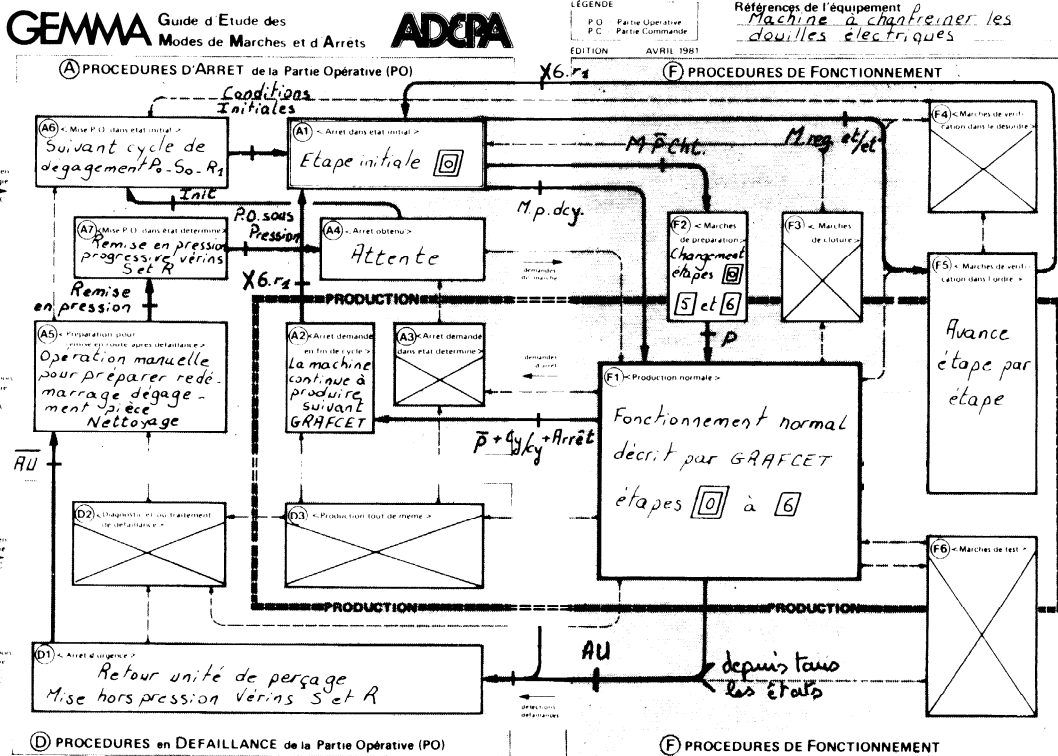
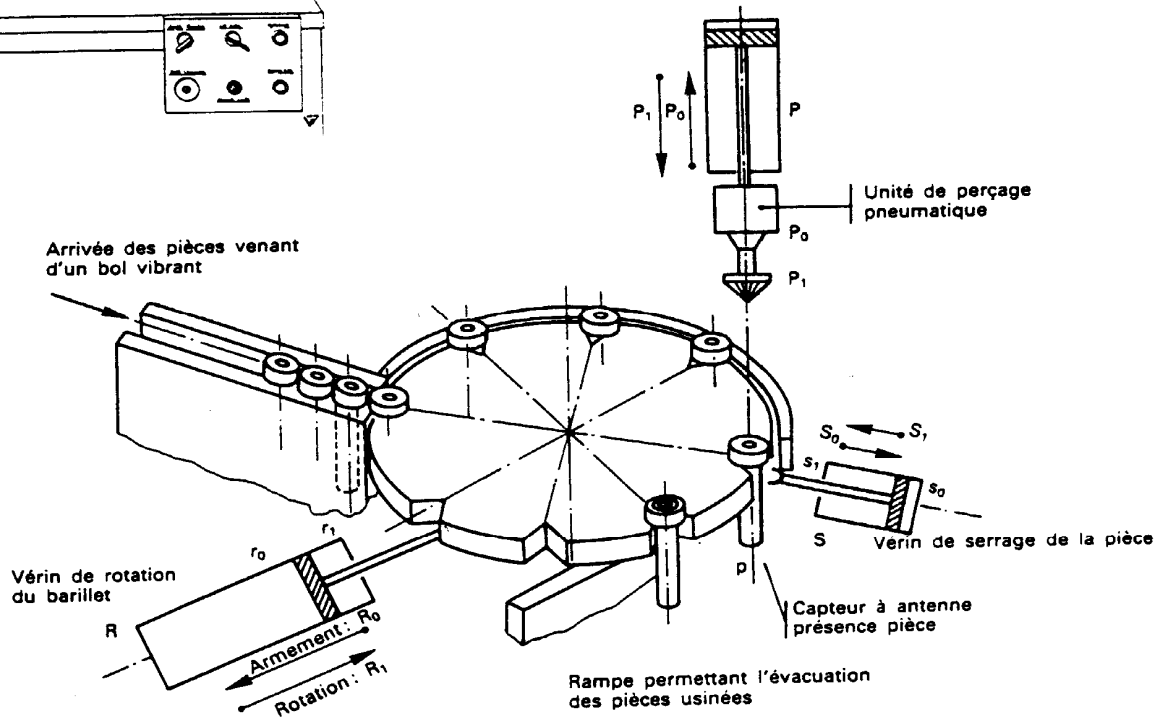
Grafctet de Conduite:



II) Exemple d'exploitation d'un GEMMA et de réalisation d'une PC Hiérarchisée

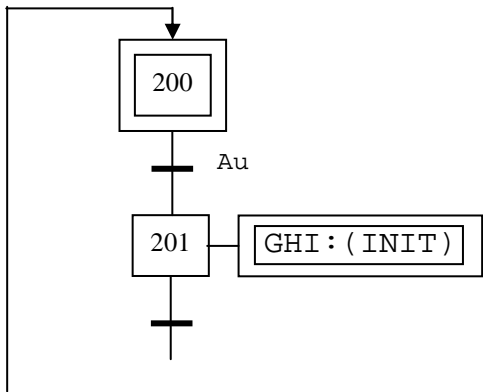


Machine à Chanfreiner des Douilles Électriques

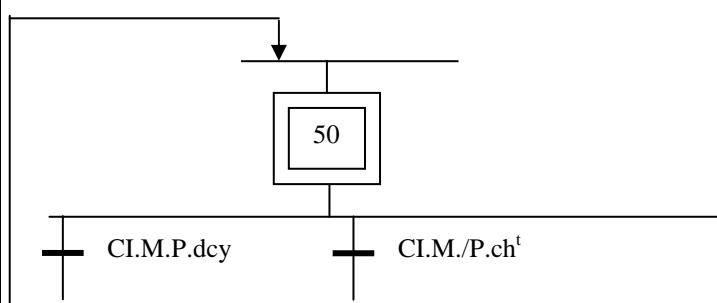


Réalisation des grafjets associés au GEMMA donné page 7

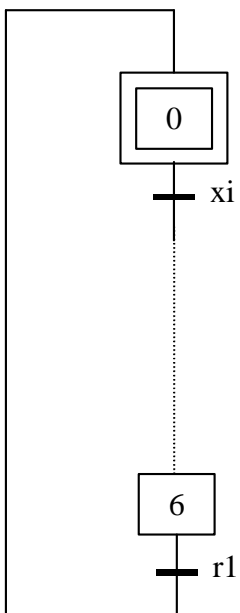
Grafjet de Sécurité



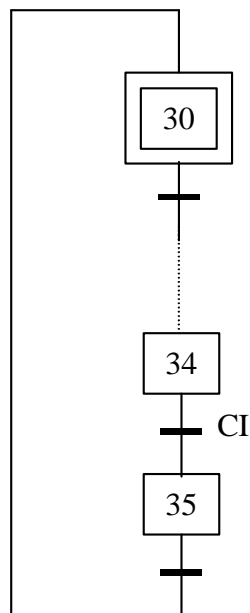
Grafjet de Conduite



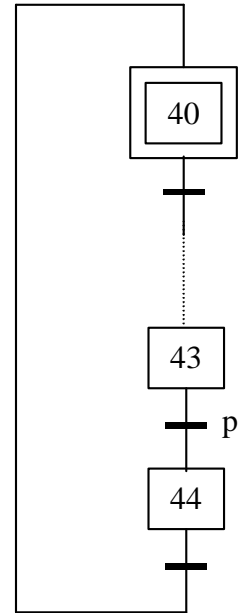
Grafjet de Production



Tâche « mise PO en CI »



Tâche « marche de prépa »



B. Sûreté des systèmes automatisés

I) Définition

Le concept de Sûreté caractérise le fonctionnement d'un système et repose sur deux critères qui sont :

- Un critère _____
- Un critère _____

Remarque :

II) Eventail des méthodes d'analyse de sûreté existantes

2.1 Présentation :

Il existe deux classes de méthode :

- Les méthodes déductives ou descendantes :

Va du modèle vers les faits, du général vers le particulier

En sûreté elle part des dangers ou effets redoutés pour aller jusqu'aux causes.

Elle est bien adaptée lors de la conception des systèmes afin d'identifier les fonctions les plus critiques pour l'obtention des objectifs de sûreté.

- Les moyens à mettre en œuvre d'un point de vue PC seront abordés un peu plus loin (principe de sécurité positive, redondance, surveillance ...)

- Les méthodes inductives ou ascendantes

C'est l'approche inverse, en sécurité, on part des causes et on remonte jusqu'aux incidences et leurs effets.

Un échantillon des principales méthodes d'analyse de Sûreté utilisées dans le monde vous est présenté page suivante

Principales méthodes d'analyse de la sûreté ⁽²⁾									
Méthode	Source	Démarche	Eléments de départ	Outil de représent.	Types de résultats	Système	Domaine application	Lien entre méthodes	
								Amont	Aval
APR* ou APD*	USA-1960 Militaire	Inductive Qualitative	Entités dangereuses	Tableaux d'analyse	Liste situations-dangereuses	Réparable Statique	Chimie	Analyse fonction.	AMDE ou HAZOP
AMDE(C)*	USA-1960 Aéronautique	Inductive Qualitative	Modes de défaillance composants	Tableaux et grille	Répertoire classifié des défaillances	Réparable Statique	Système matériel essentiel	Analyse fonctionnelle et/ou APR	AEE, AdD, DDC
HAZOP*	RU-1970 Chimie	Inductive Qualitative	Paramètres mesurables	Tableaux	Répertoire des dérives	Réparable Statique	Chimie	APR	AdD, DDC
MAC(AdD)*	USA-1961 Aérospatial	Déductive	Evénement redouté (ER)	Arbre des causes	Coupes minimales de l'ER	Réparable Non séqu.	Processus non stoch.**	Méthodes inductives	GdM, RdP GRAFCET
MEE* ou GdM*	F-1976 USA-1950	Déductive Quantitative	Etats de fonctionnement et de panne	Graphes d'états	Différentes configurations de disponibilité	Réparable Dynamique	Processus markovien Petite taille	AMDE	AdD éventuel
DCC* ou MDCC*	DK-1970 Nucléaire	Mixte	Evénement initiateur	Diagr. causes-effets	Conséquences Coupes mini.	Statique	Processus non stoch.**	AMDE	
RdP* GRAFCET*	RFA-1962 F-1977 Automatique	Déductive Quantitative	Etats de fonctionnement et de panne	Graphes d'états	Modélisation des évolutions	Réparable Evolutif	Processus séquentiel automatisé	AMDE	GdM

* APD/APR = Analyse préliminaire des dangers/risques
 AMDE(C) = Analyse des modes de défaillance, de leurs effets (et de leur criticité)
 HAZOP = Analyse des conséquences et de la criticité des dérives des paramètres de conduite
 MAC = Méthode de l'arbre des causes
 AdD = Arbre de défaillances (ou arbre des causes)
 MEE = Méthode de l'espace des états
 GdM = Graphe de Markov
 (M)DCC = (Méthode) Diagramme causes-conséquences
 RdP = Réseau de Petri
 ** Processus non stochastique

⁽²⁾ Tableau d'après :
 E. Fadier "Les facteurs humains de la fiabilité dans les systèmes complexes, sous la direction de J. Leplat et G. de Terssac, OCTARES, 1990, et :
 "Sûreté de fonctionnement des systèmes industriels" par A. Villemeur, Eyrolles, 1988.

➤ L'outil d'analyse AMDEC vous est présenté en cours de Maintenance

2.2 Méthode de l'Arbre des Causes (AdC) ou de l'Arbre des Défaillances (AdD) :

C'est une méthode déductive qui permet de représenter, de manière logique, l'enchaînement des causes nécessaires à la manifestation de la défaillance constatée (ou du danger redouté pour une analyse de sécurité).

- Voir cours de maintenance
- Application sur blocage grafcet (Exemple DOC-IV B22)
- Formalisme : voir DOC-IV AdC

2.3 Diagramme Causes Effets ou diagramme d'Ishikawa:

- Voir cours de maintenance

III) Technique de conception et de réalisation de systèmes Sûrs.

3.1 Objectif :

3.2 Les Principes de base :

La **Prévention Intrinsèque** (suppression du risque) est toujours préférable à sa réduction.

En cas d'impossibilité les **solutions les plus simples et les plus directes sont toujours les meilleures**. Pour cela on s'attachera à appliquer :

Le principe _____

Par ailleurs, lorsque tout a été fait pour minimiser la probabilité de défaillance (fiabilisation), trois grands principes permettent de réduire les risques jusqu'au niveau requis afin d'atteindre la **Sûreté Totale** :

Le principe _____

et/ou

Le principe _____

Le principe de protection, qui reste le recours incontournable lorsque les risques ne peuvent pas être supprimés.

3.3 Solutions et moyens d'obtention de la sûreté.

3.31 démarche d'étude :

Définir le comportement souhaité pour la fonction et son effecteur :

- Sécurité positive
- Sûreté Totale

En déduire successivement le comportement à obtenir :

- Sur l'actionneur.
- Sur le préactionneur.
- Sur les sorties API.

....

Choisir des constituants à comportement orienté sur défaillance :

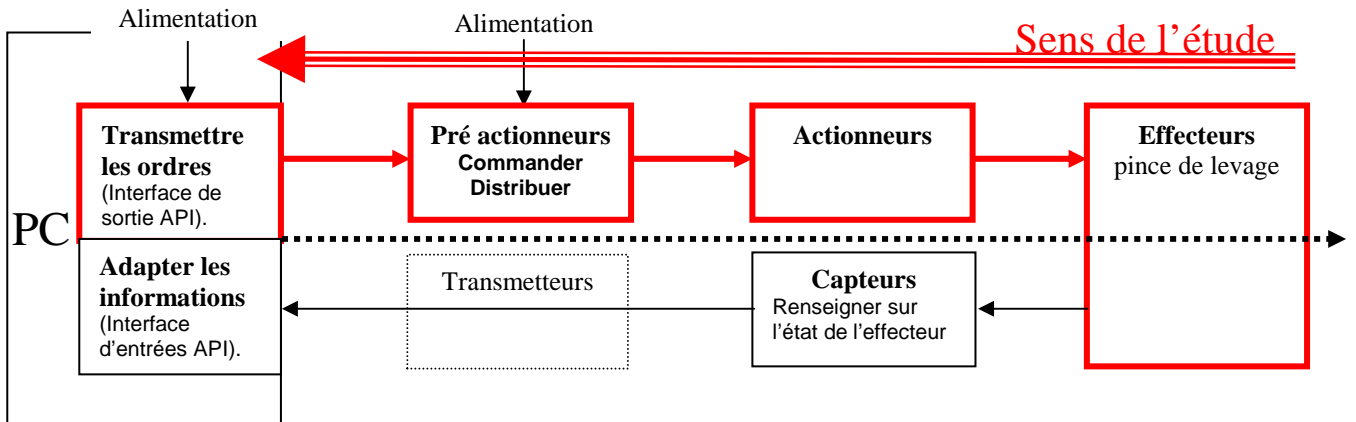
- Voir typologie des matériels de sécurité (DOC-IV B331)

Vérifier que votre solution garantit bien le comportement attendu.

3.32 Exemple de comportement orienté vers la sécurité : **Sécurité Positive**.

Choisir les éléments de la chaîne d'action ci-dessous pour une pince de levage qui au repos (non commandée) doit-être fermée.

L'actionneur est pneumatique et a pour fonctionnement : tige rentrée = pince fermée.

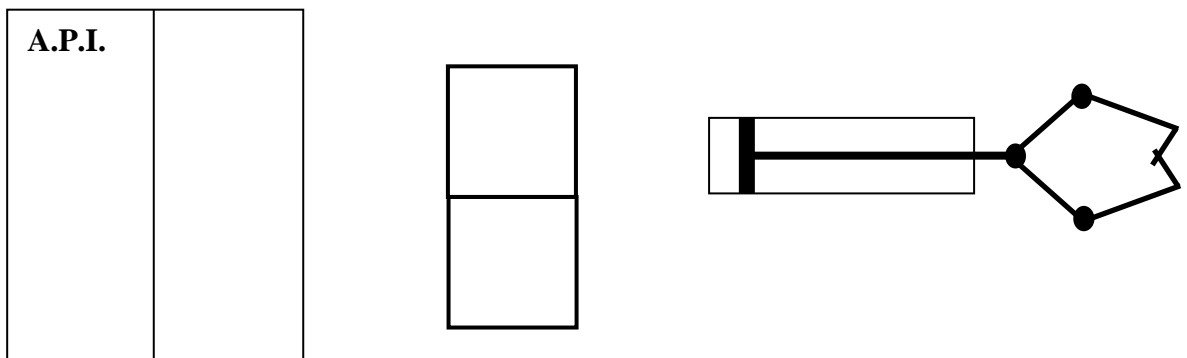


La sécurité anti-incendie impose un comportement orienté _____

L'obtention de ce comportement sur défaillance conduit à retenir successivement :

- Un actionneur _____
- Un préactionneur _____
- Un module de sortie API _____

réalisation du schéma fonctionnel :



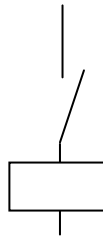
Remarque :

3.4 Solutions et moyens redondants.

3.41 Rôle et utilité de la redondance

Analyse des risques potentiels liés à l'utilisation d'un **contact à action mécanique NO** dans une chaîne fonctionnelle de sécurité, **orientée vers l'arrêt** du fonctionnement (coupure).

Modes de défaillances pénalisants pour l'obtention de la sécurité :



Modes de défaillances pénalisant pour la disponibilité :

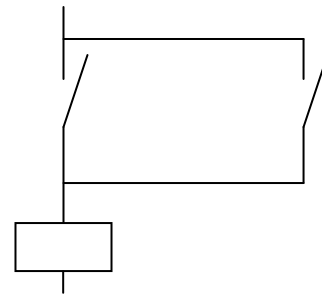
solutions redondantes possibles



Ici la redondance est un moyen d'amélioration ?

- La sécurité
- disponibilité

Justification :



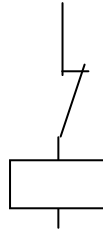
Ici la redondance est un moyen d'amélioration ?

- La sécurité
- disponibilité

Justification :

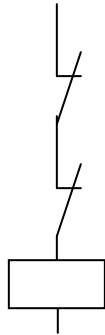
- a) Analyse des risques potentiels liés à l'utilisation d'un **contact à action mécanique NF** dans une chaîne fonctionnelle de sécurité, **orientée vers l'arrêt** du fonctionnement (coupure).

Modes de défaillances pénalisants pour l'obtention de la sécurité :



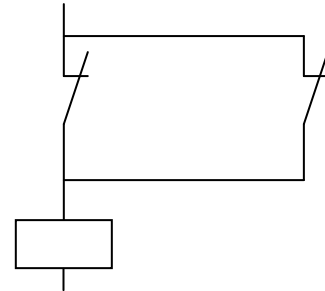
Modes de défaillances pénalisant pour la disponibilité :

solutions redondantes possibles



Ici la redondance est un moyen d'amélioration ? La sécurité disponibilité

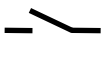
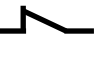
Justification :



Ici la redondance est un moyen d'amélioration ? La sécurité disponibilité

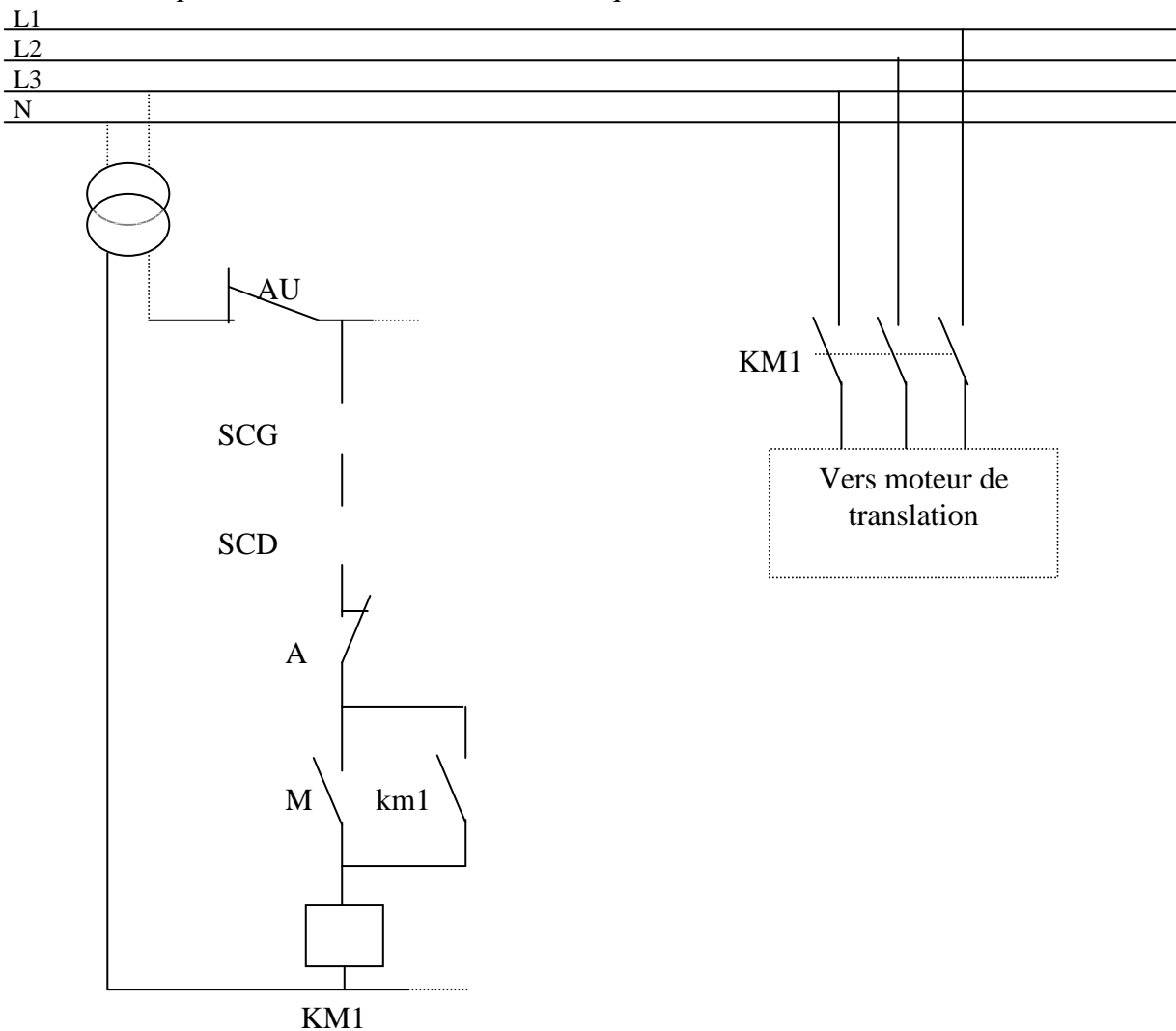
Justification :

3.42 Synthèse :

Capteur de sécurité	Logique associée	Défaillance possible	prévision du risque
			
			

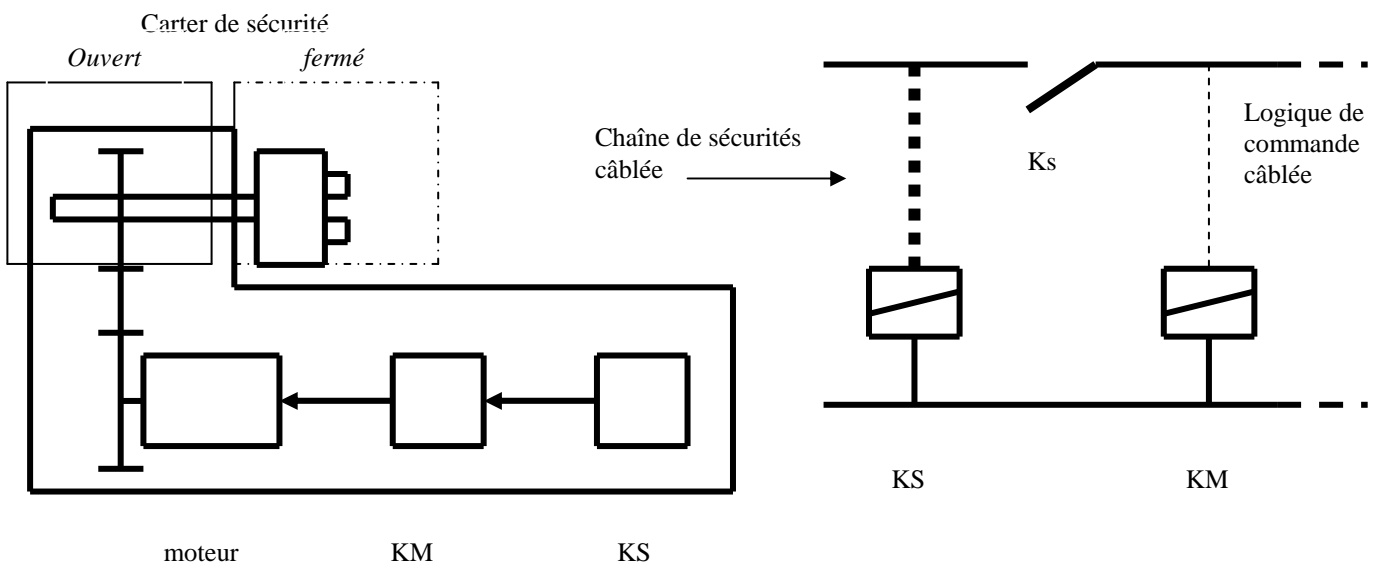
3.43 Conclusion :

Exemple : Choix des sur courses mécaniques Droit et Gauche d'un moteur de translation :



3.5 La Redondance.

3.51 Exemple de mise en œuvre « carter sur tour conventionnel » :



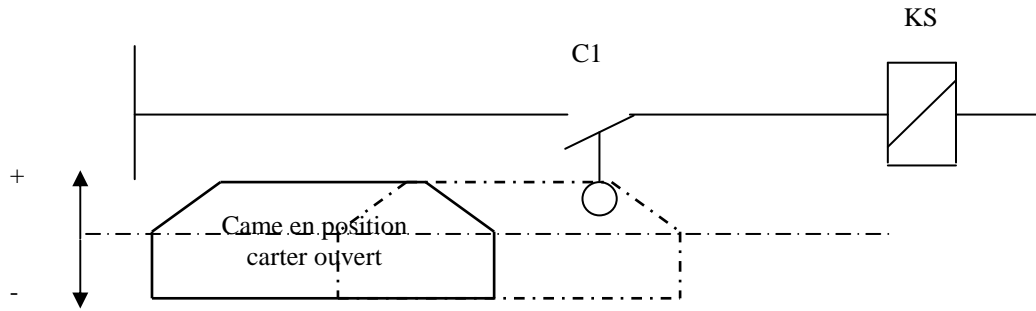
Risques

Types de défaillances possibles du système.

A :

B :

Solution N°1 : contact à fermeture (NO)

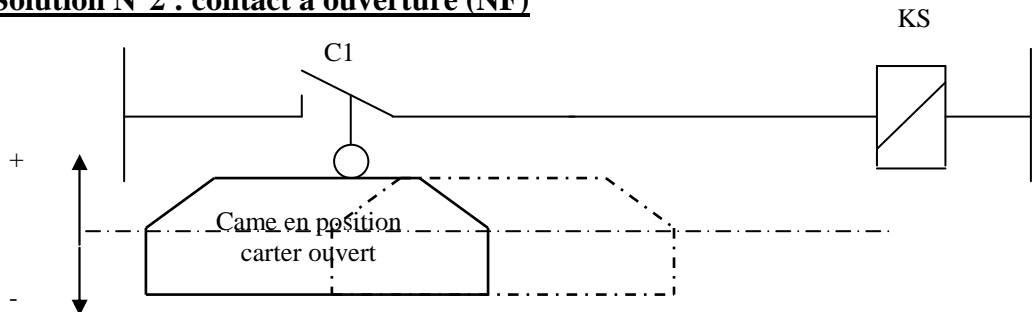


N°	Modes de défaillances possibles	Risque de défaillance	Effets induits KS	DANGER ?
1	Contact C1 fermé (collage ou ressort cassé)	B		
2	Contact Ks fermé (collage ou ressort cassé)	B		
3	Came déréglée en +			
4	Came déréglée en -	A		

Remarque sur la prévision des risques



Solution N°2 : contact à ouverture (NF)

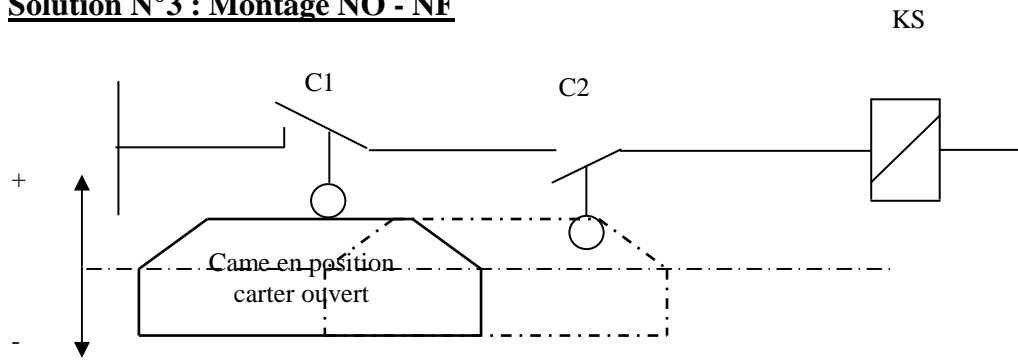


N°	Modes de défaillances possibles	Risque de défaillance	Effets induits KS	DANGER ?
1	Contact C1 fermé	B		
2	Contact Ks fermé (collage ou ressort cassé)	B		
3	Came déréglée en +			
4	Came déréglée en -	B		

Remarque sur la prévision des risques

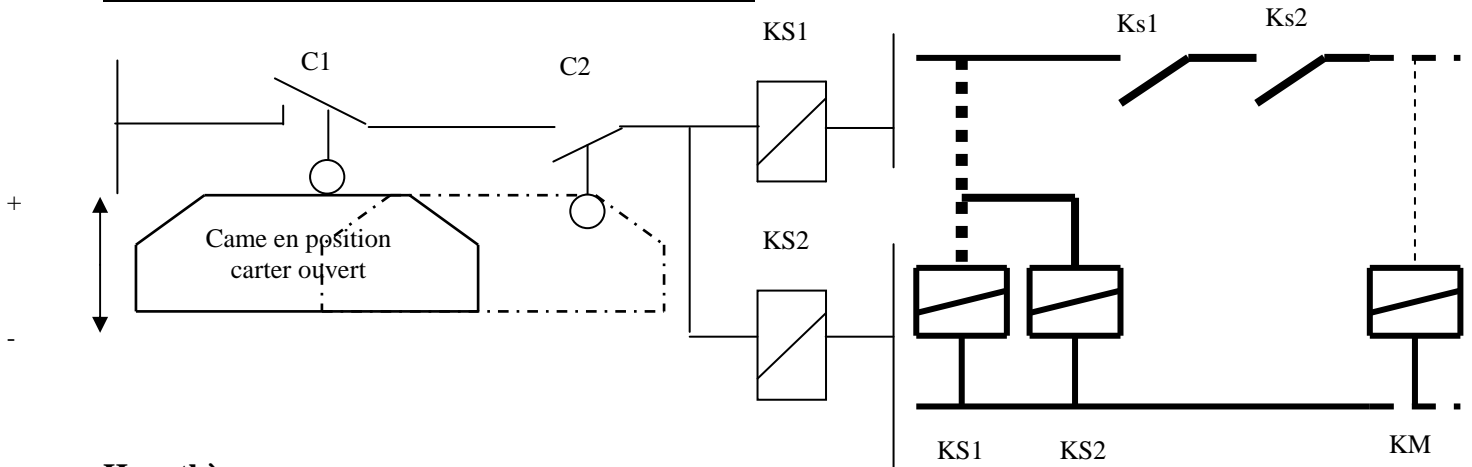


Solution N°3 : Montage NO - NF



N°	Modes de défaillances possibles	Risque de défaillance	Effets induits KS	DANGER ?
1.1	Contact C1 fermé Contact C2 ouvert	A		
1.2	Contact C1 ouvert Contact C2 fermé	A		
2	Contact Ks fermé (collage ou ressort cassé)	B		
3	Came dérégulée en + : Contact C1 ouvert Contact C2 ouvert			
4	Came dérégulée en - : Contact C1 fermé Contact C2 ouvert	A		

Solution N°4 : Mise en redondance du relais KS



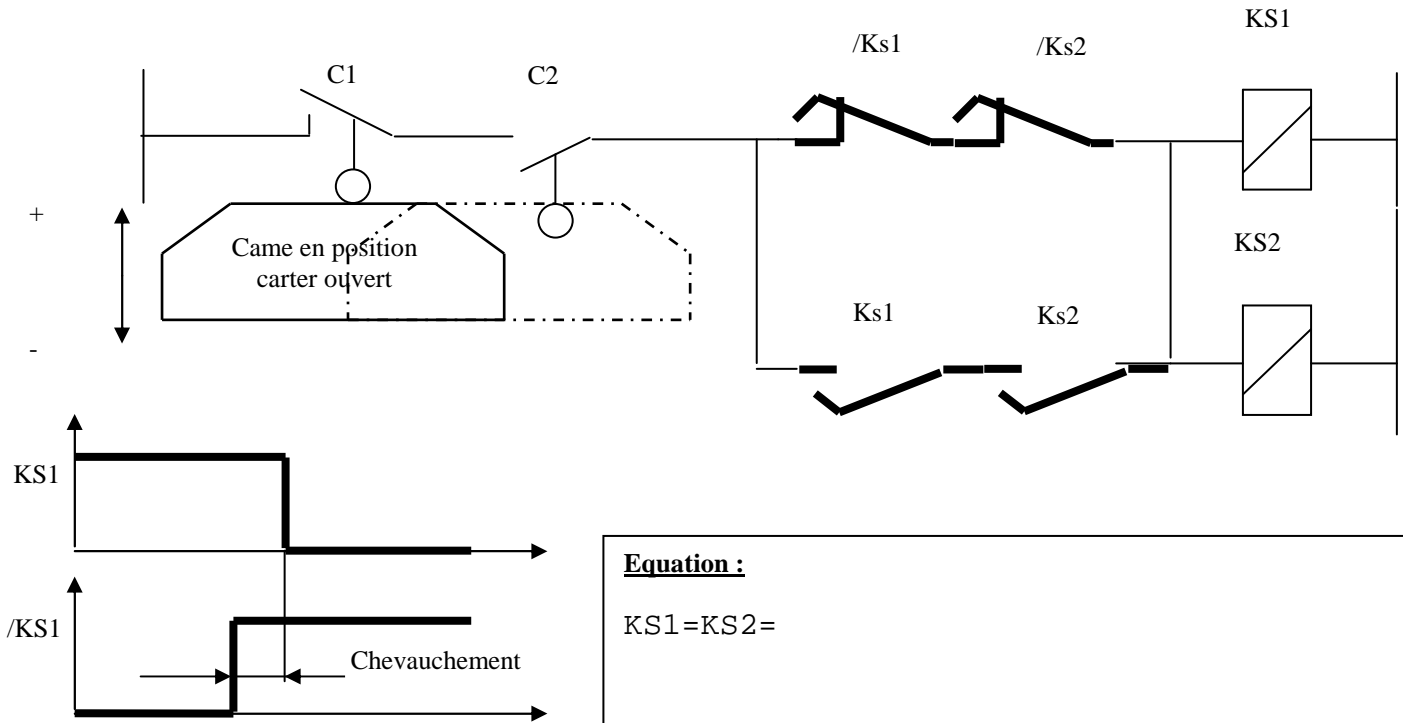
Hypothèse

N°	Modes de défaillances possibles	Risque de défaillance	Effets induits KS _i	DANGER ?
1.1	Identique à l'étude précédente	A	KS1=0,KS2=0	NON
1.2	Identique à l'étude précédente	A	KS1=0,KS2=0	NON
2.1	Contact Ks1 fermé (collage ou ressort cassé) Contact Ks2 ouvert			
2.2	Contact Ks1 ouvert Contact Ks2 fermé (collage ou ressort cassé)			
3	Identique à l'étude précédente		KS1=0,KS2=0	NON
4	Identique à l'étude précédente	A	KS1=0,KS2=0	NON

Remarque

ATTENTION !

Solution N°5 : Montage avec auto-contrôle (emploi de contacts à chevauchement)



Equation :
 $KS1 = KS2 =$

N°	Modes de défaillances possibles	Risque de défaillance	Effets induits KS _i	DANGER ?
1.1	Identique à l'étude précédente	A	$KS1=0, KS2=0$	NON
1.2	Identique à l'étude précédente	A	$KS1=0, KS2=0$	NON
2.1	Contact Ks1 collé Contact Ks2 ouvert	A		
2.2	Contact Ks1 ouvert Contact Ks2 collé	A		
3	Identique à l'étude précédente		$KS1=0, KS2=0$	NON
4	Identique à l'étude précédente	A	$KS1=0, KS2=0$	NON

CONCLUSION :

3.52 Caractérisation de la redondance.

Généralement, une redondance est caractérisée par un doublet noté _____ ;
avec :

m = _____

et

n = _____

suiivi d'un ensemble d'attributs qui peuvent être :

- Son principe qui est fonction du besoin de Sûreté ;
 - o **Active** _____

 - ou
 - o **Passive** _____

- Son caractère technologique ;
 - o **Homogène** _____

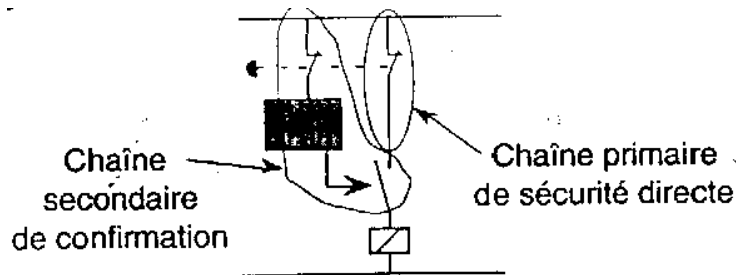
 - ou
 - o **Hétérogène** _____

- La nature des moyens utilisés ;
 - o **Matérielle** _____

 - ou
 - o **Logicielle** _____

- etc...

➤ Exemple de redondance 2/2 active hétérogène (logicielle et câblée) :



➤ Exemples de mise en œuvre redondante sur tout ou partie d'une production industrielle : industrielle : cf. DOC-IV B352

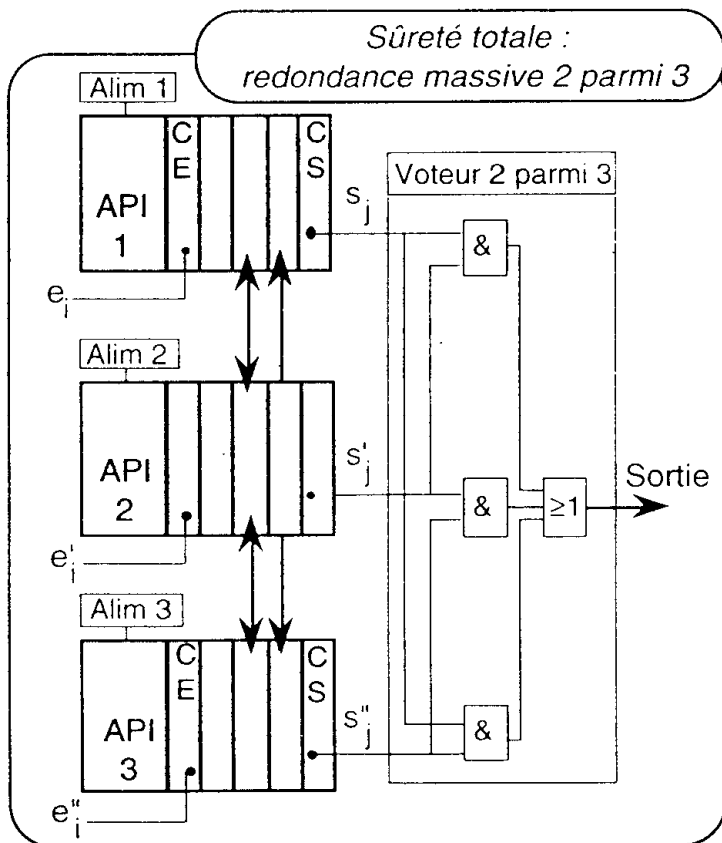
3.53 Solution juste nécessaire aux besoins de Sûreté.

A chaque besoin de Sûreté doit correspondre une solution de redondance appropriée :

Besoins de sûreté	Solution juste nécessaire
Disponibilité seulement avec état transitoire toléré.	Redondance _____
Sécurité orientée seulement.	Redondance _____
Sécurité orientée et disponibilité améliorée*.	Redondance _____ _____ _____ _____
Sûreté Totale	Redondance _____

*Remarque 1 :

- Exemple de redondance 2/3 avec voteur ; Sûreté Totale que l'on retrouve que sur des éléments très critiques (sécurité nucléaire par ex.) ou qui ne peuvent pas être réparé durant leur vie (satellite par ex.) :



Remarque 2 :

API	M	M	M	M
	S	S	E	E
	1	2	1	2

API	M	M	M	M
	S	S	E	E
	1	2	1	2

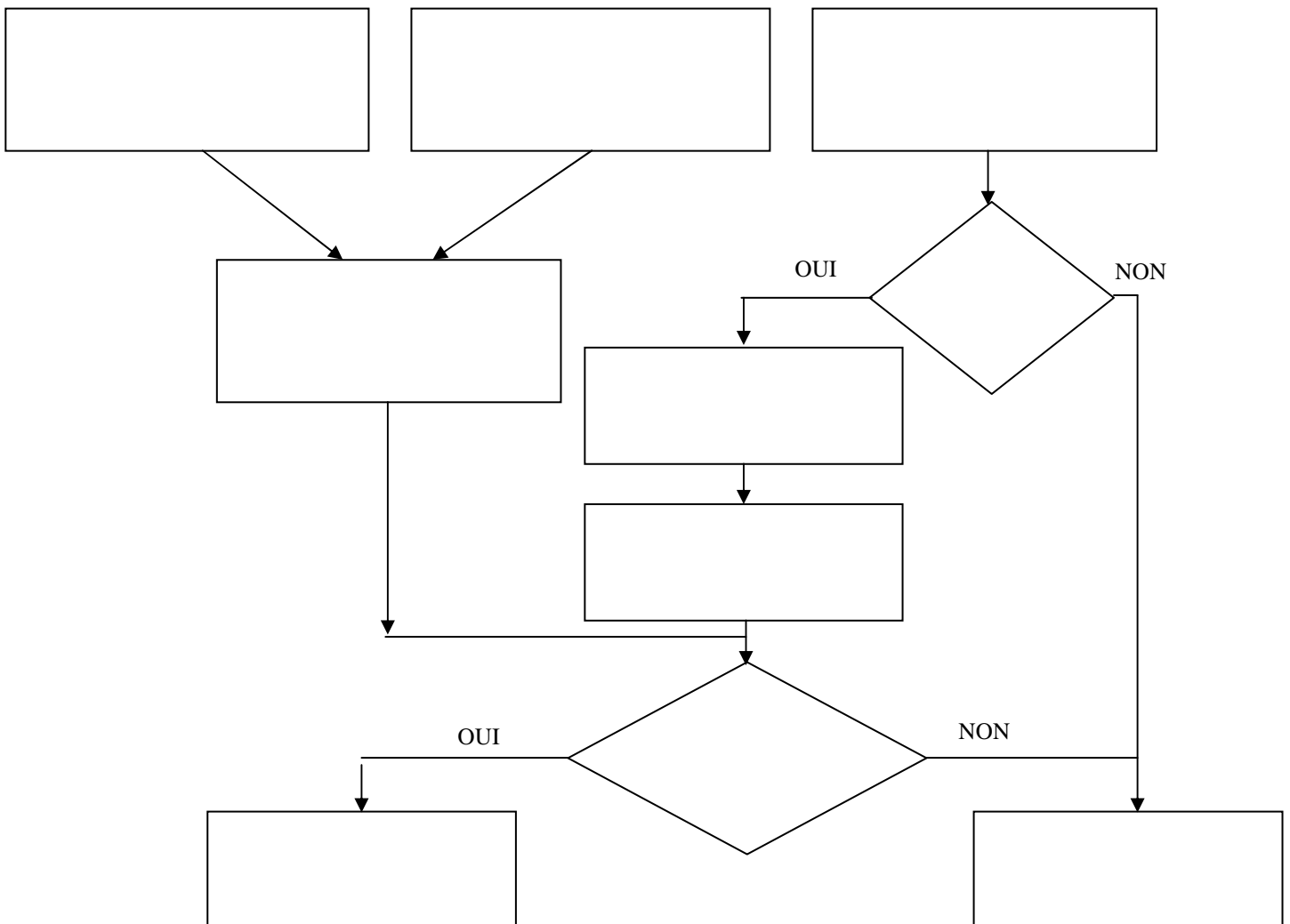
Chaîne
fonctionnelle 1

Chaîne
fonctionnelle 1

Chaîne
fonctionnelle
redondante 2

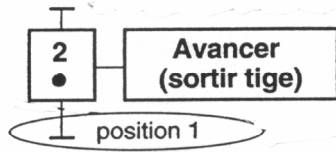
Chaîne
fonctionnelle
redondante 2

3.54 Organigramme de synthèse sur la redondance.



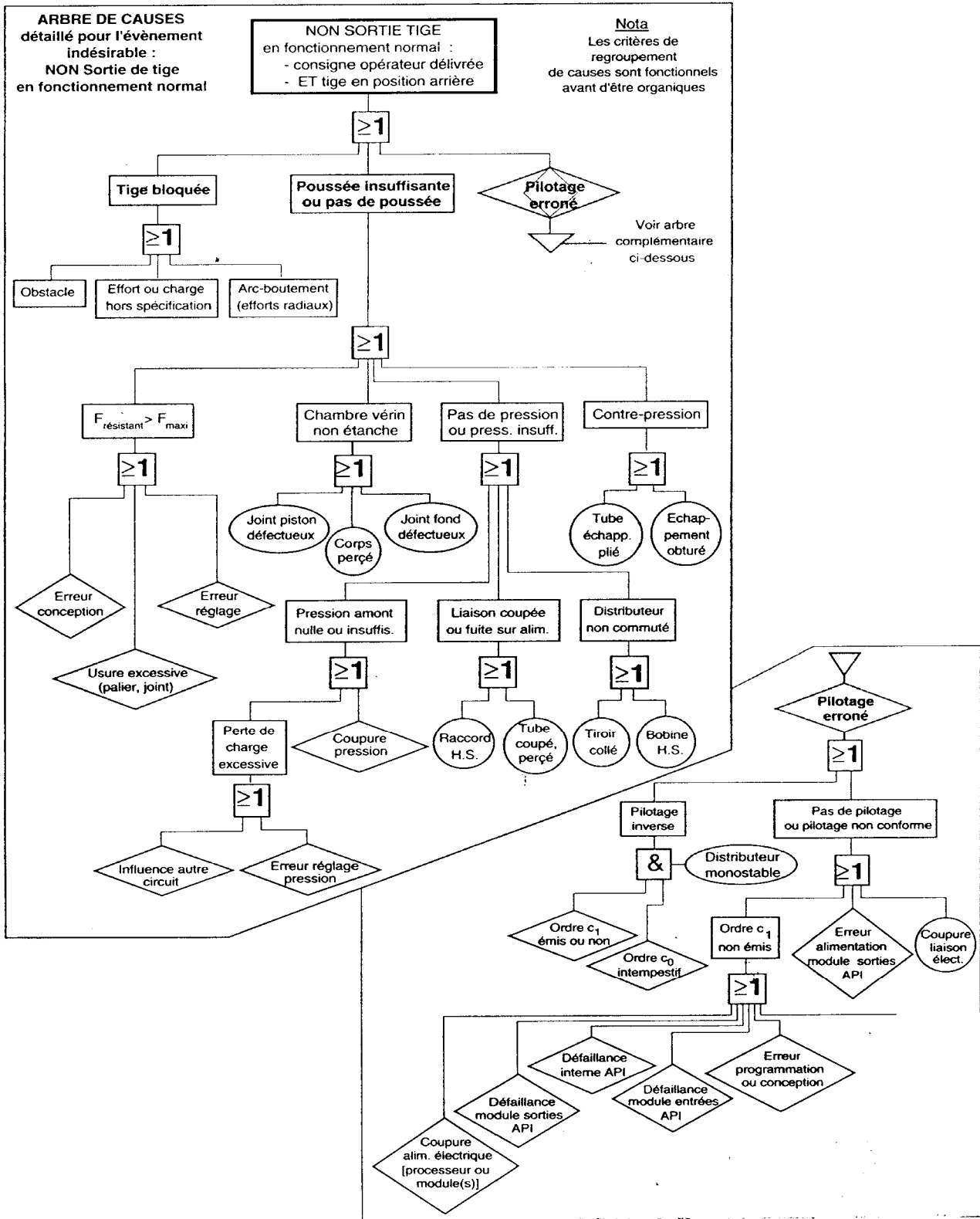
DOC-IV B22

Exemple d'un grafcet bloqué à une étape:



Ici, après observation du technicien, ce dernier s'aperçoit que la tige du vérin incriminé n'est pas sortie.

Représentation de l'AdC « non sortie de tige du vérin »:



DOC-IV AdC

Arbre Des Causes

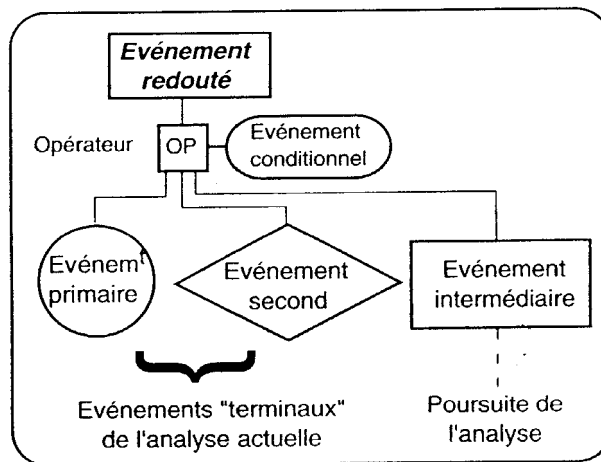
C'est une méthode déductive, c'est à dire qui part du contexte général et qui va vers les éléments en particulier.

Méthodologie

En premier lieu, on détermine quelle est la panne sur laquelle va porter l'étude. Ensuite, on va chercher les combinaisons logiques des événements jugés responsables.

Formalisme

Agencement des éléments graphiques d'un AdC

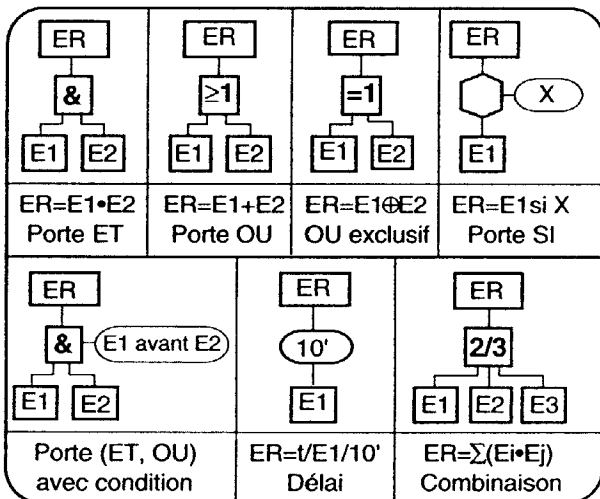


Evénement primaire : l'effet de la cause est lié directement à la défaillance (ex : un voyant ne s'allume pas parce que la lampe est hors service)

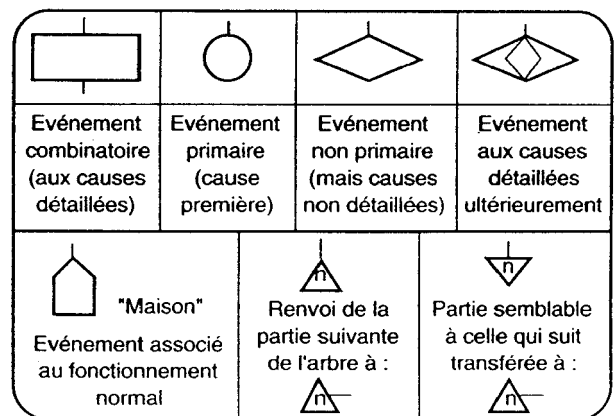
Evénement secondaire : l'effet de la cause est lié directement ou indirectement à une défaillance d'un autre composant ou de l'opérateur (ex : pas de pilotage d'un distributeur suite à la défaillance de la sortie API)

Evénement intermédiaire : l'effet de la cause est lié directement ou indirectement à une défaillance dont l'origine doit être recherchée en remontant à ses causes premières ou secondes.

Principaux opérateurs logiques:

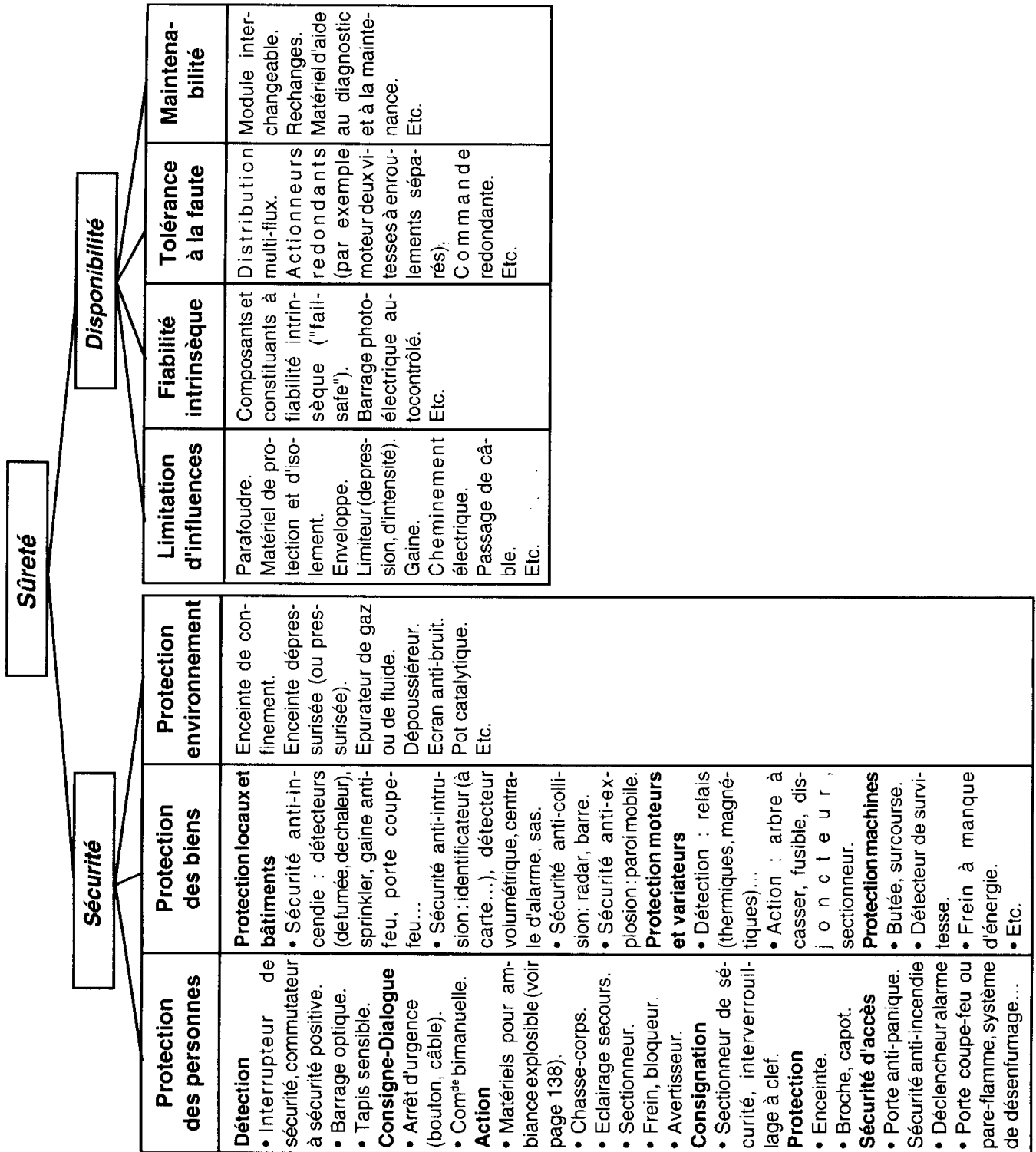


Principales représentations d'événements:



DOC-IV B331

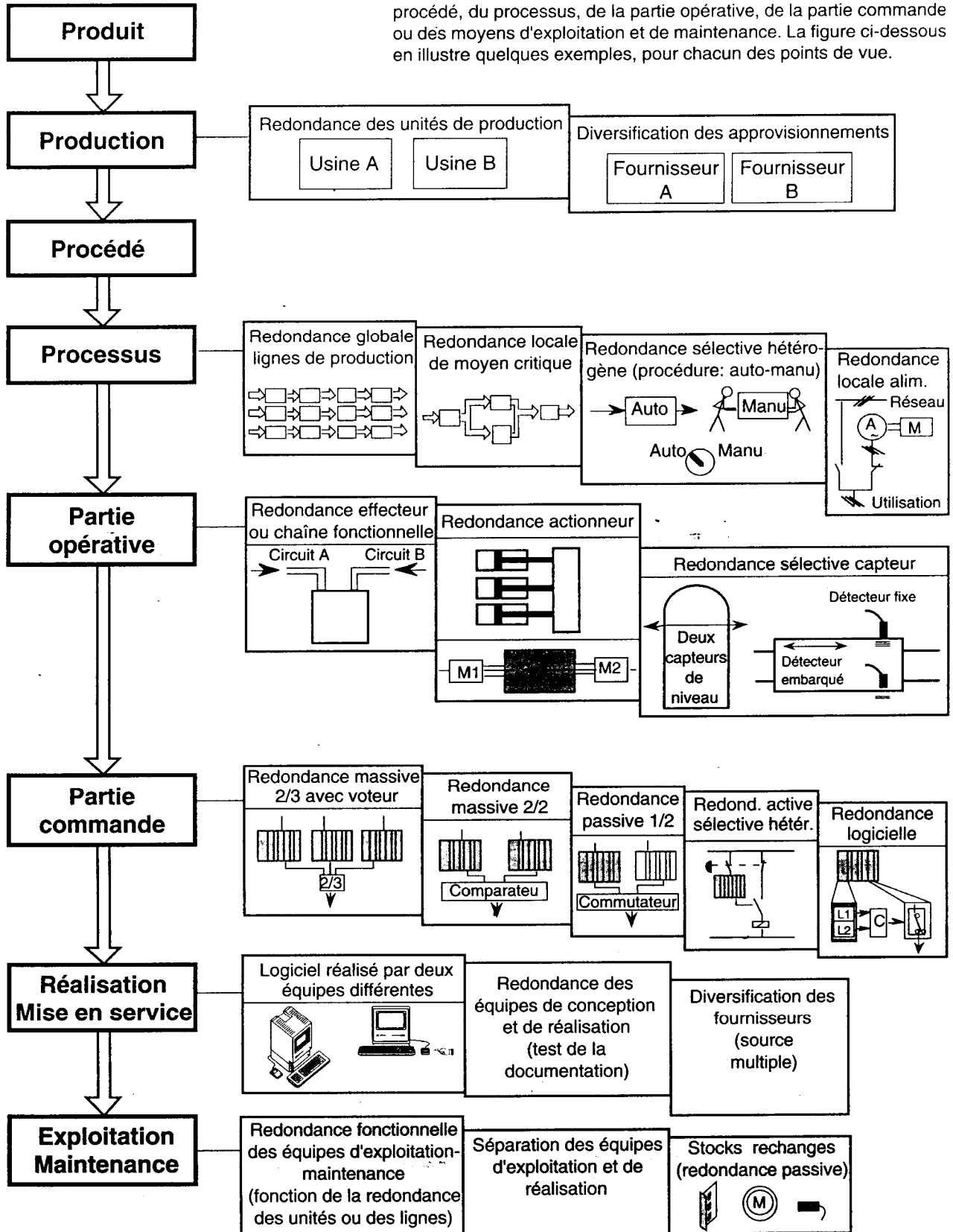
TYPOLOGIE DES MATERIALS DE SECURITE



DOC-IV B352

Exemples de mise en œuvre de solutions redondantes pour les différents points de vue

La redondance peut porter sur tout ou partie de la production, du procédé, du processus, de la partie opérative, de la partie commande ou des moyens d'exploitation et de maintenance. La figure ci-dessous en illustre quelques exemples, pour chacun des points de vue.



DOC-IV B362

Exemples de DISCORDANCE "LOGIQUE"

Discordance d'antivalence

L'antivalence est un procédé de recherche de discordance par redondance complémentaire à partir, par exemple, soit de deux capteurs différents, soit de contacts N.O. et N.F. d'un même capteur.

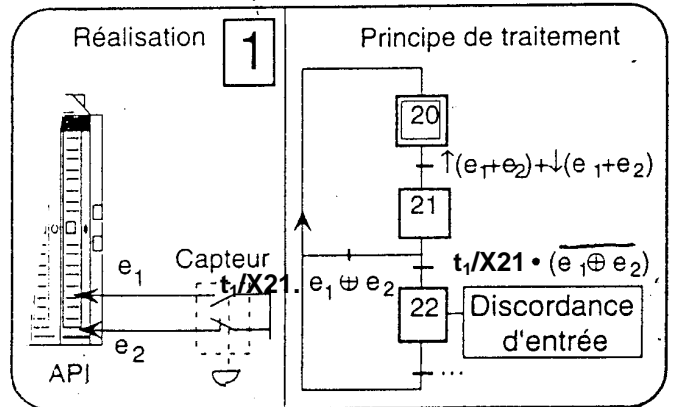
Pour s'affranchir des aléas d'asynchronisme il est recommandé de valider la discordance par une temporisation (figure 1, ci-contre) ou sur deux cycles de traitement.

Discordance d'informations

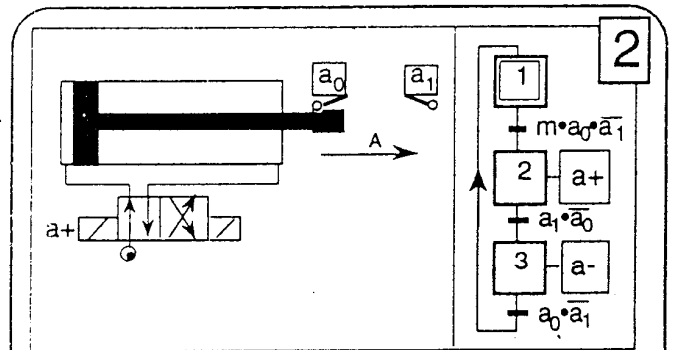
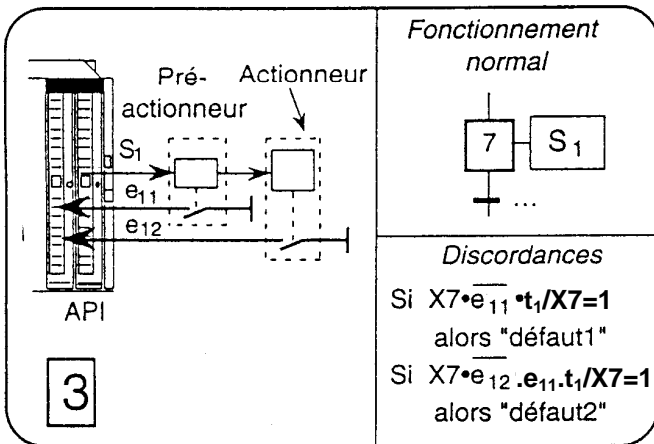
Ce procédé exploite l'exclusion physique normale entre l'état logique de capteurs dans des situations définies pour tester leur bon fonctionnement (voir figure 2).

Discordance de commande ou discordance d'action

Ce procédé de surveillance des chaînes d'action exploite un retour d'état du préactionneur ou du capteur pour tester une éventuelle discordance avec l'ordre émis. (voir principe, figure 3 ci-dessous).



Discordance et antivalence d'entrées.



Diagnostic de défauts sur discordances

- Si $X1 \cdot a_0 = 1$ alors "défaut 1"
- Si $X1 \cdot a_1 = 1$ alors "défaut 2"
- Si $X2 \cdot a_0 \cdot a_1 = 1$ alors "défaut 3"
- Si $X3 \cdot a_0 \cdot a_1 = 1$ alors "défaut 4"
- Si $X1 \oplus X2 \oplus X3 = 0$ ou $X1 \cdot X2 \cdot X3 = 1$ alors "défaut PC"

"Défaut 1" correspond ici soit à un défaut dans la chaîne d'acquisition de a_0 , soit à un défaut de positionnement de la tige (suite à une action manuelle par exemple)

Discordance et exclusion physiques d'états.

Autres discordances

- Discordance de combinaisons logiques autorisées (informations sur mots, combinaisons d'un code).
- Discordance de situations de graphes (situation atteinte incompatible avec le fonctionnement normal).