












## SPECIFICATIONS DU SERVICE ELECTRIQUE ONERA DU CENTRE DE MODANE AVRIEUX

### CONCEPTION DE SYSTEME DE CONTROLE COMMANDE : RESPECT DE LA CONFORMITE MACHINE

#### HISTORIQUE

Version Révision	Date de mise à jour	Cause et /ou nature de l'évolution
1.0	28/11/12	Création

	Rédacteur	Vérificateurs	Approbateur
Groupe	GTE	GTE	GT
Nom	M.Marchand	T.Coudurier, S.Bouvier, C.Chiaberto, D.Charvin, O.Giraud, P.Magnin, N. Sari, D. Bertino	C. Chargy
Visa		       	



## SOMMAIRE

<b>1. OBJET.....</b>	<b>4</b>
<b>2. LEXIQUE.....</b>	<b>4</b>
<b>3. CONFORMITE MACHINE .....</b>	<b>4</b>
3.1. Généralités.....	4
3.2. Analyse du risque : définition du niveau de sécurité .....	4
<b>4. CONCEPTION DES SYSTEMES DE CONTROLE COMMANDE .....</b>	<b>5</b>
4.1. Généralités.....	5
4.2. Principes de conception.....	6
4.3. Exemples de schémas électriques : aide à la conception .....	7
4.3.1. Fonction d'arrêt et contrôle arrêt.....	7
4.3.2. Fonction contre la mise en marche intempestive .....	7
4.3.3. Fonction arrêt d'urgence .....	11
4.3.4. Disponibilité des installations : redondance des sécurités.....	15
<b>5. VALIDATION .....</b>	<b>23</b>
<b>6. FICHE DE CONTROLE ONERA.....</b>	<b>25</b>

## 1. **OBJET**

Le document a pour but de décrire un certain nombre de règles de conception pour les systèmes de contrôle commande, dans le but de respecter la conformité machine. Dans une première partie, un rappel sera fait sur la réglementation et dans une seconde partie, nous donnerons des règles et des exemples de conception pouvant être utilisés par les concepteurs pour les systèmes de contrôles commandes du CMA (Centre Modane Avrieux).

### Nota :

- Ce document est une aide à la conception de système de contrôle commande dans le cadre de la conformité machine et n'est en aucun cas exhaustif pour cette partie. Le concepteur (sous-traitant) pourra se baser sur ce document, mais c'est à lui de mettre tous les moyens en œuvre pour respecter la réglementation en vigueur.
- Le document ne traite pas toutes les parties pour les systèmes de contrôles commandes. Le document ne traite pas aussi les parties mécaniques, hydrauliques, pneumatiques... des systèmes (objet d'autres normes).

*Norme applicable: ISO 13849-1 et : ISO 13849-2*

## 2. **LEXIQUE**

Concepteur : personne, groupes de personnes dont le travail consiste à concevoir et/ou à mettre en place toutes parties en lien avec le domaine de l'électrotechnique et/ou l'automatisme.

PI : Performance Level.

API : Automate Programmable Industriel

CCF : Défaillance de cause commune

## 3. **CONFORMITE MACHINE**

### 3.1. **Généralités**

Les systèmes commandés (systèmes intelligents) peuvent être potentiellement dangereux pour l'homme, compte tenu des énergies importantes mise en œuvre (grosses installations = grosse puissance) et des nombreux organes et pièces en mouvement.

La société moderne ne tolère et n'accepte plus le risque d'accident du travail.

Par conséquent, l'entreprise doit être constamment soucieuse de ces notions de dangers en se tournant vers la sécurité.

Le code du travail et les directives européennes (directive machines) définissent la réglementation à respecter.

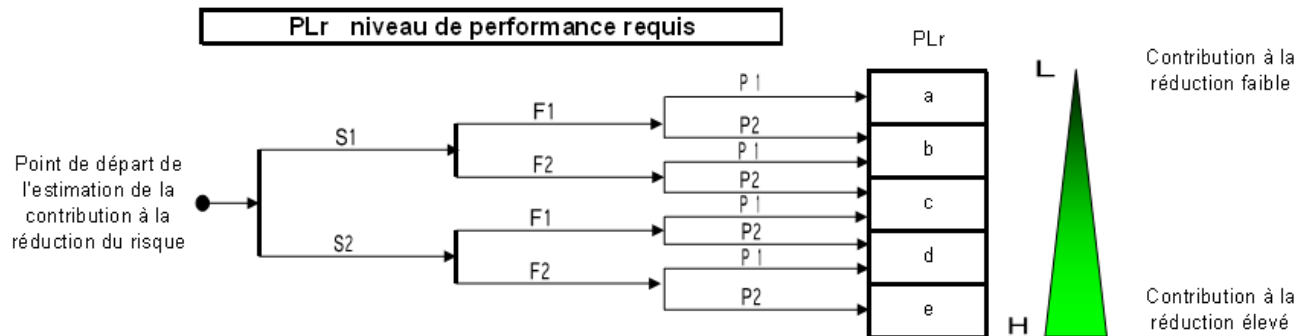
Les installations du CMA sont considérées comme des machines ou process et doivent obéir à ces règles. Les travaux de rénovations ou les travaux neufs obligent à prendre en compte dans la conception des systèmes le respect de cette réglementation.

### 3.2. **Analyse du risque : définition du niveau de sécurité**

Pour chaque projet contrôle commande (rénovation de systèmes existants ou travaux neufs), un groupe de travail ONERA réalise une analyse de risque et détermine le niveau de sécurité requis pour chaque fonction de l'installation à sécuriser. Pour chaque fonction de sécurité l'ONERA fournira au concepteur le niveau de sécurité à atteindre.

**Le concepteur à l'obligation de mettre en place le matériel adéquat pour satisfaire au niveau de sécurité requis.**

La méthode utilisée par l'ONERA est le graphe de risque issu de la norme **ISO 13849-1** qui définit ce niveau de performance requis.



A chaque embranchement de l'arbre sont estimés les facteurs clés d'appréciation du risque, classiquement on retrouve :

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

Au bout de chaque branche est indiqué un niveau de risque résultant du phénomène dangereux considéré, appelé PI (performance level ou niveau de performance).

## 4. CONCEPTION DES SYSTEMES DE CONTROLE COMMANDE

### 4.1. Généralités

Les systèmes automatisés de sécurité se caractérisent par l'utilisation de capteurs, relais ou automates, actionneurs, ... pour réaliser des fonctions de sécurité, qui devront, suivant l'ampleur du risque couvert, garantir un certain niveau d'intégrité de sécurité (PL Performance Level dans le secteur des machines) afin d'amener le risque à des limites de tolérances acceptables.

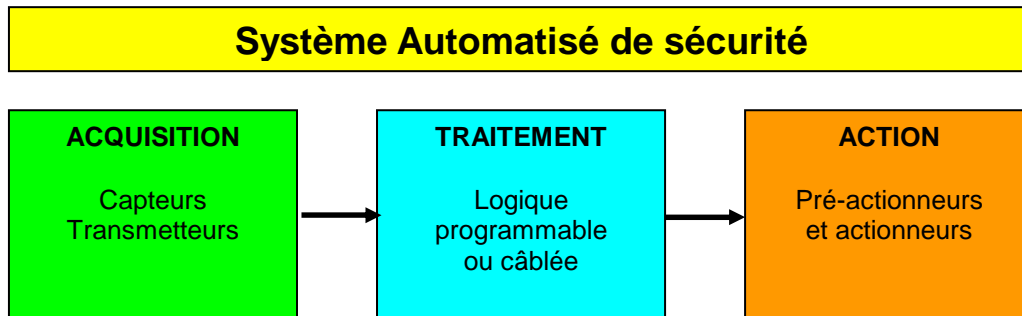
La norme ISO 13849 énumère des fonctions de sécurité types :

- **Fonction d'arrêt**
- Fonction de mise en marche et remise en marche
- **Fonction contre la mise en marche intempestive**
- Fonction de réarmement manuel
- Fonction d'isolation et dissipation d'énergie
- Fonction de temps de réponse
- Fonction de commande et sélection de mode
- **Fonction d'arrêt d'urgence**

Cette spécification parle de la fonction d'arrêt, la fonction contre la mise en marche intempestive et la fonction d'arrêt d'urgence.

Ces fonctions peuvent être combinées dans un même ensemble dont les caractéristiques sont adaptées à celles de la machine à protéger.

Le système automatisé de sécurité doit comprendre l'ensemble de la chaîne de contrôle commande relative à la sécurité, depuis l'acquisition, en passant par la logique de traitement, jusqu'aux actionneurs finaux.



Pour chaque fonction de sécurité définie, le système devra répondre au niveau de performance souhaité sur **toute sa chaîne** (acquisition, traitement, action).

#### 4.2. Principes de conception

Le tableau ci-joint donne pour chaque niveau de sécurité à atteindre le type de traitement à mettre en place à minima, s'il faut mettre des fonctions de surveillance, de redondance et décrit le comportement du système attendu.

Niveau de PL	Type de traitement	Diagnostic	Redondance	Comportement du système
a	Automate	non	Non	Si un défaut se produit, il peut conduire à la perte de la fonction de sécurité.
b	Automate	oui	Non	Des composants éprouvés et des principes de sécurité fiables doivent être utilisés. La survenue d'un défaut peut mener à la perte de la fonction de sécurité mais la probabilité qu'elle se produise est plus faible.
c	Câblé (hors automate)	Oui (partiel)	Non	La fonction de sécurité doit être contrôlée à intervalles convenables par le système de commande de la machine. - L'occurrence d'un défaut peut mener à la perte de la fonction de sécurité entre les intervalles de test. - La perte de la fonction est détectée par la vérification.
d	Câblé (hors automate)	Oui (partiel)	Oui	Les parties relatives à la sécurité doivent être conçues de façon à ce que : (a) Un défaut unique dans n'importe laquelle de ces parties ne doit pas mener à la perte de la fonction de sécurité ; et (b) Si cela est raisonnablement faisable, le défaut unique doit être détecté. Lorsqu'un défaut unique se produit, la fonction de sécurité est toujours assurée. Certains défauts seront détectés, mais pas tous. - L'accumulation de défauts non détectés peut conduire à la perte de la fonction de sécurité.
e	Câblé (hors automate)	Oui (total)	Oui	Le système de commande doit être conçu de façon à ce que : (a) Un défaut unique du système de commande ne

				<p>doit pas mener à une perte de la fonction de sécurité.</p> <p>(b) le défaut unique doit être détecté au prochain appel à la fonction de sécurité ou avant.</p> <p>(c) l'accumulation de défaut et les CCF doivent être pris en compte.</p> <p>Lorsqu'un défaut apparaît dans l'une quelconque de ces parties, la fonction de sécurité opère toujours.</p> <p>Les défauts seront détectés à temps pour empêcher une perte de la fonction de sécurité.</p> <p>Si les diagnostics décèlent un défaut sur les deux canaux, ou bien découvrent une discordance entre les résultats de chaque voie, sans pouvoir diagnostiquer le canal fautif, le système se positionne en situation sûre</p>
--	--	--	--	---

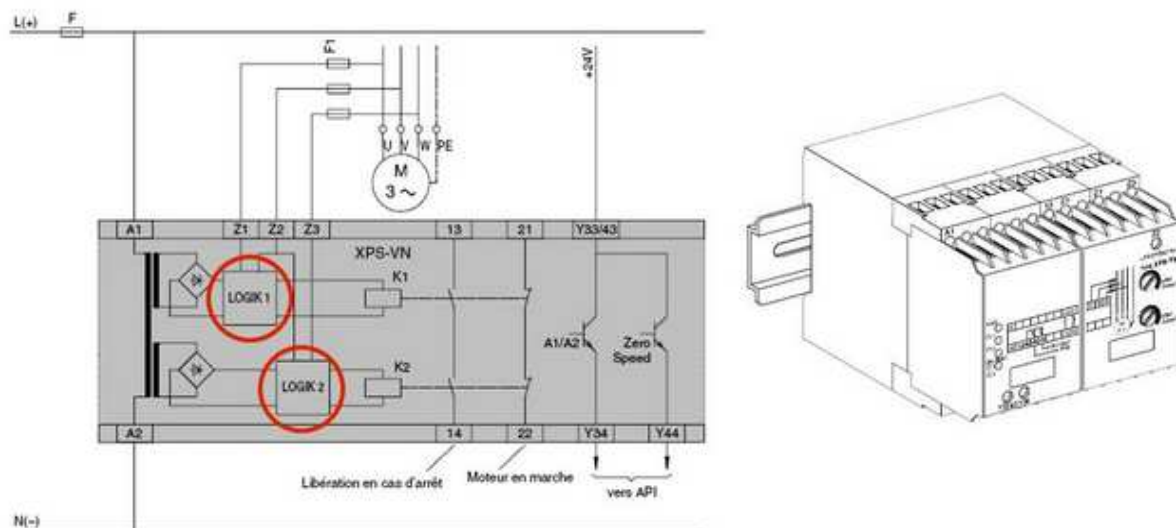
Suivant le niveau de sécurité à atteindre défini par l'ONERA, **le concepteur du système devra donner, pour chaque sous ensemble de la chaine, le niveau de sécurité global atteint.**

### 4.3. Exemples de schémas électriques : aide à la conception

#### 4.3.1. Fonction d'arrêt et contrôle arrêt

Lorsqu'une fonction d'arrêt liée à la sécurité doit être mise en place, la fonction doit mettre l'installation à l'arrêt après l'actionnement du dispositif de sécurité. De manière sécurisée la fonction doit aussi contrôler que le système est bien à l'arrêt.

Pour assurer cette fonction de contrôle, un contrôle peut être fait soit par automate soit hors automate (relais de sécurité par exemple) selon le niveau de sécurité demandé. L'exemple ci-après contrôle la détection de vitesse nulle via un relais de sécurité.



#### 4.3.2. Fonction contre la mise en marche intempestive

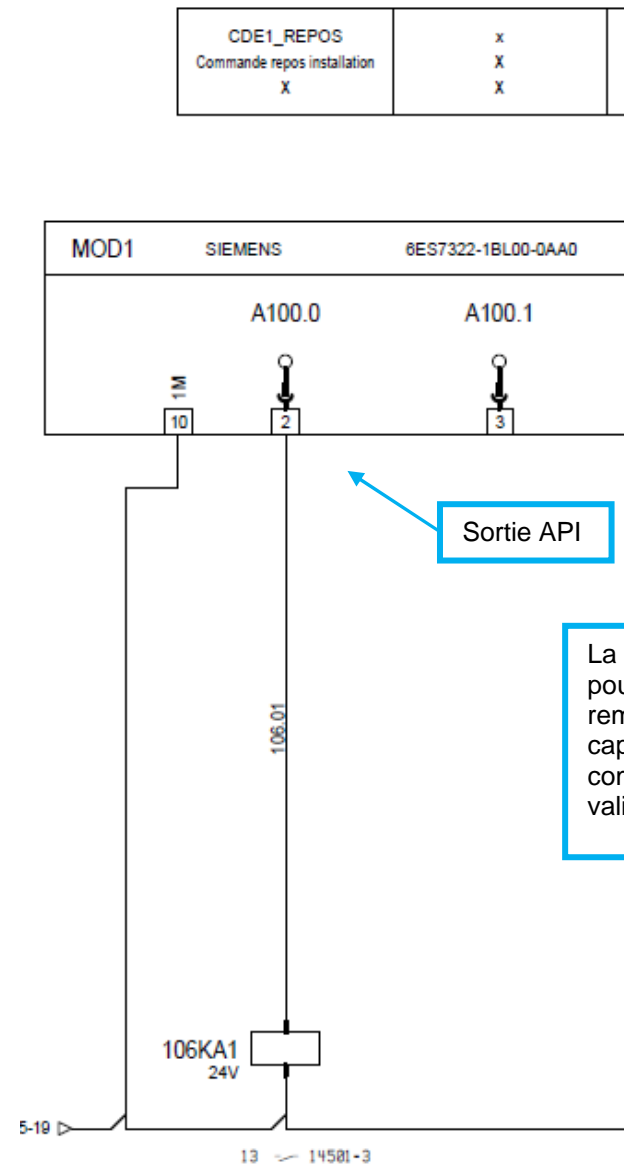
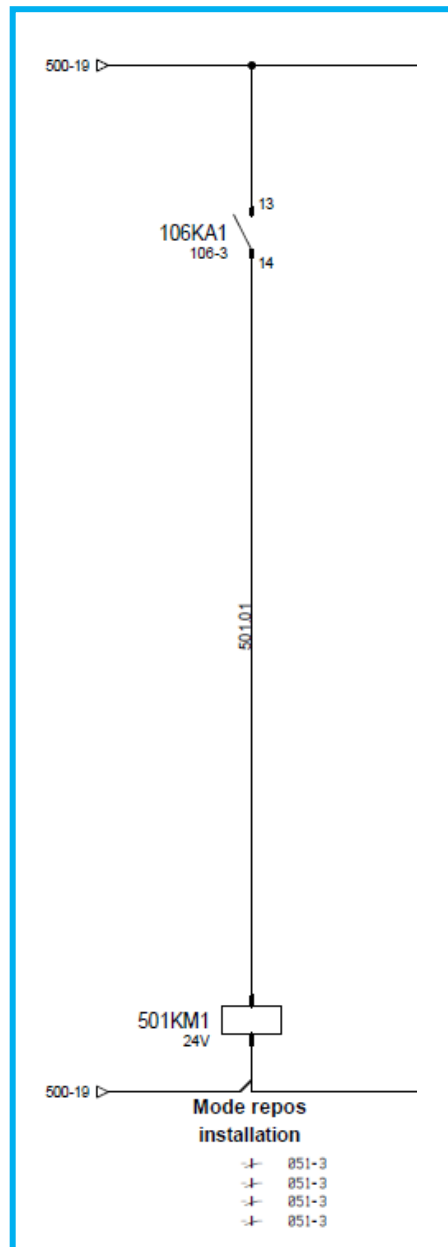
De manière générale, la non mise en marche intempestive d'une installation au CMA est assurée par un commutateur de mode sur lequel on trouve plusieurs positions dont l'une étant « Repos installation ». Dans cet état, l'installation se trouve au repos, c'est-à-dire que les différents actionneurs qui présentent un risque pour les utilisateurs doivent avoir leur puissances et commande coupées selon le niveau de sécurité demandé.

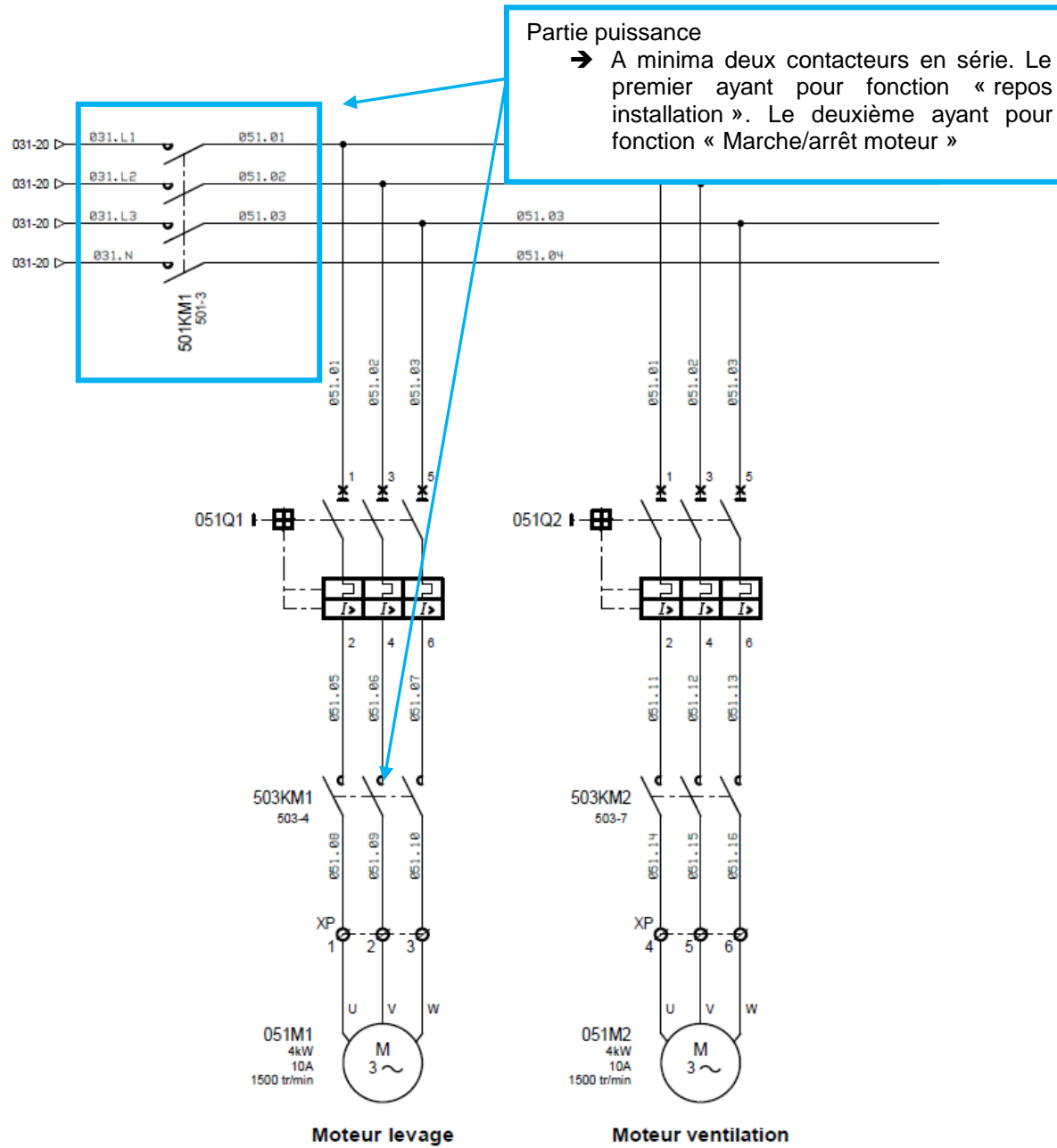
Afin d'assurer cette fonction de non mise en marche intempestive, sur la partie commande et sur la partie puissance un faux défaut (enclenchement d'un contact, contacteur,...) ne doit pas mettre en marche l'installation (=actionneur(s)). Pour ce faire, sur la partie commande il doit y avoir à minima deux équipements en série, idem sur la partie puissance. Un faux défaut sur un des équipements, ne doit pas faire une mise en marche intempestive.

On privilégiera un câblage hors automate lorsque cela est possible.

**A minima, le concepteur du système devra respecter le principe des schémas donnés ci-après pour les niveaux Pla, b.**







Pour les **niveaux PLc,d,e** d'autres principes devront être mise en œuvre :

- câblage hors automate, redondance contacteurs, gestion des différentes discordances.
- Utilisation d'un automate de sécurité programmé par une personne certifiée,

Nota :

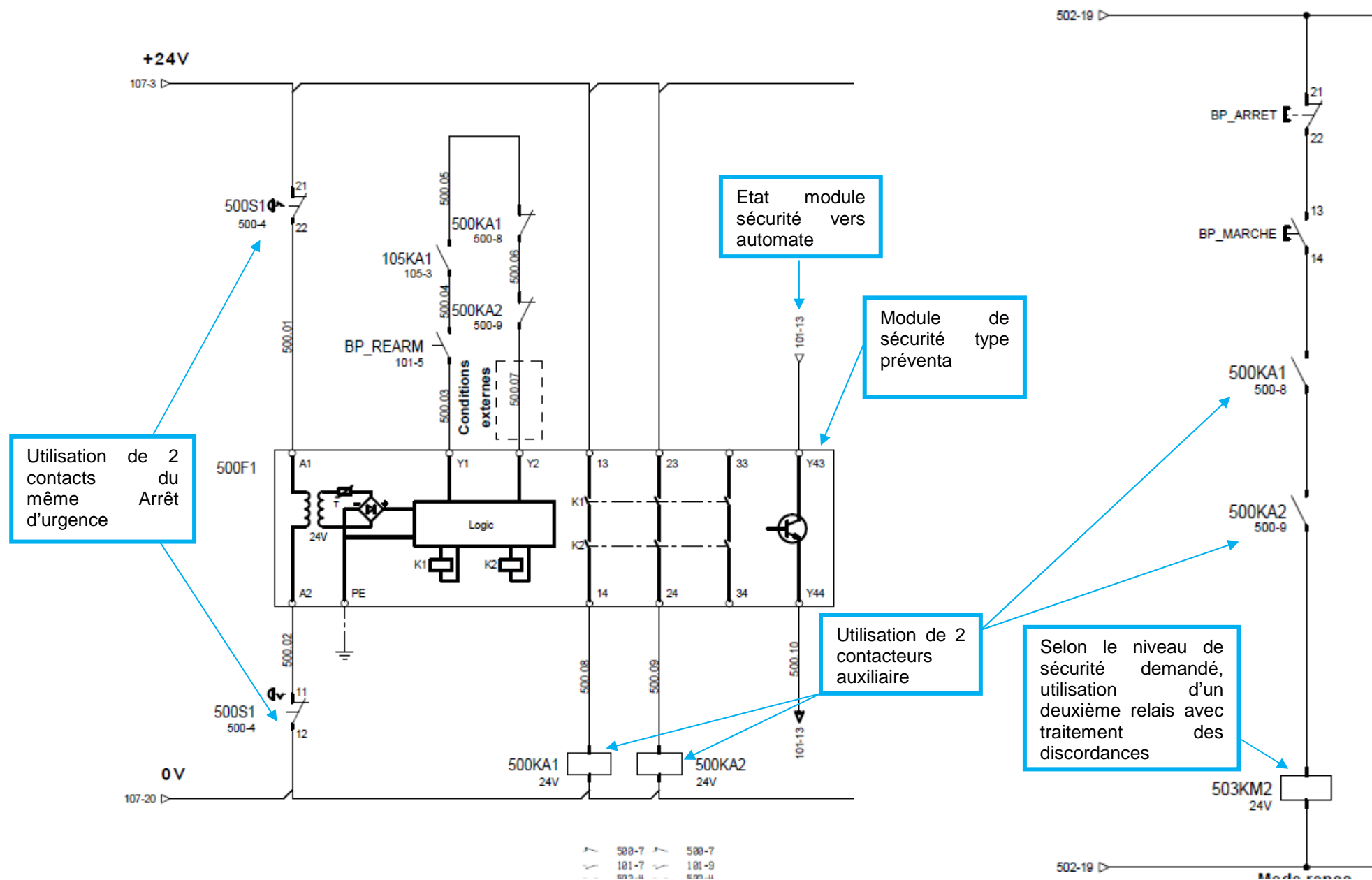
Si l'installation est en marche, un faux défaut sur la chaîne de sécurité devra assurer la fonction de sécurité (repos installation = coupure des puissances et des commandes) ce qui entraîne généralement aussi l'arrêt d'une partie de l'installation voir l'arrêt complet.

Pour éviter l'arrêt de l'installation sur un faux défaut des solutions avec redondance sont proposées dans le § »  
Disponibilité des installations : redondance des sécurités »

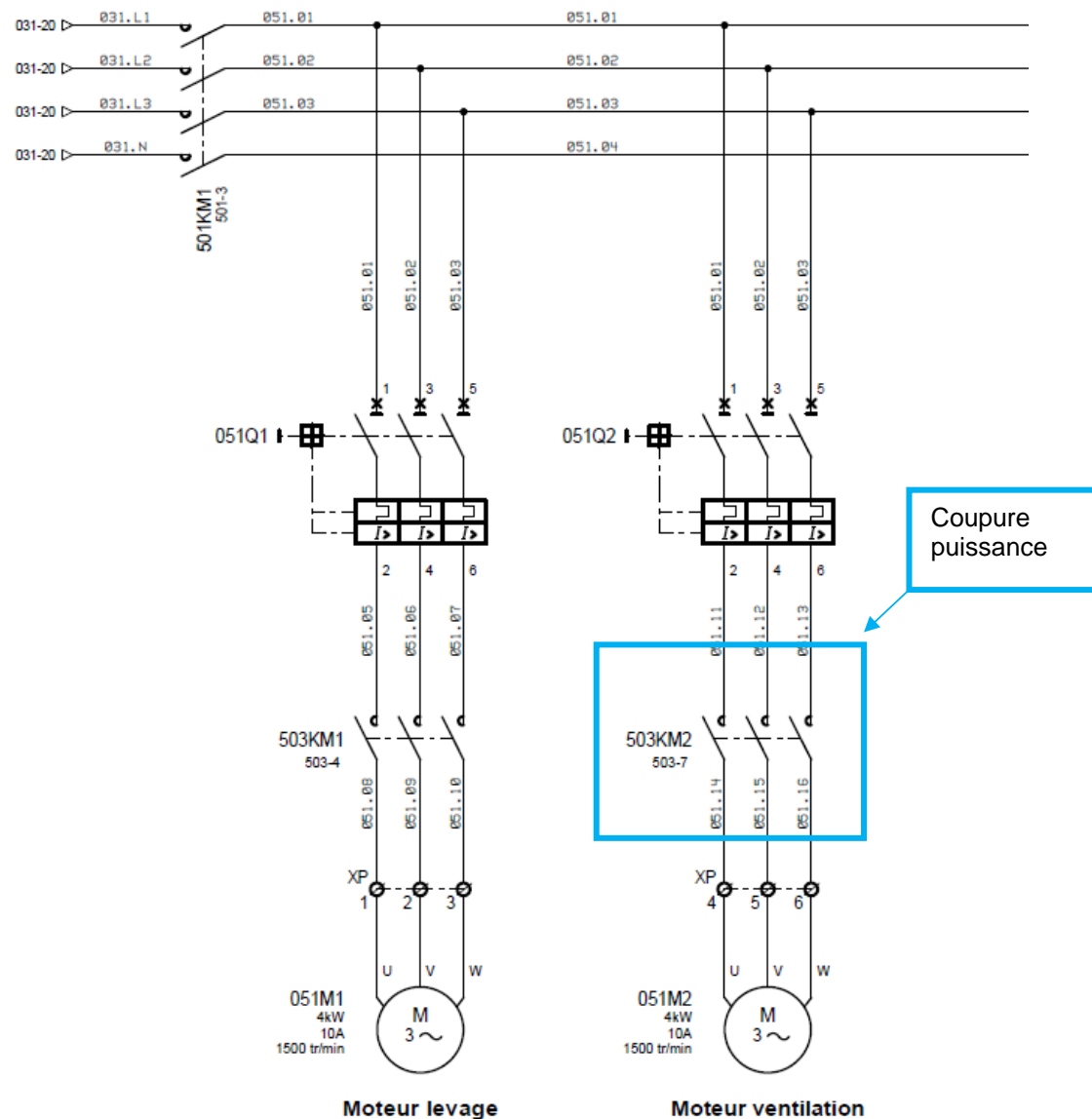
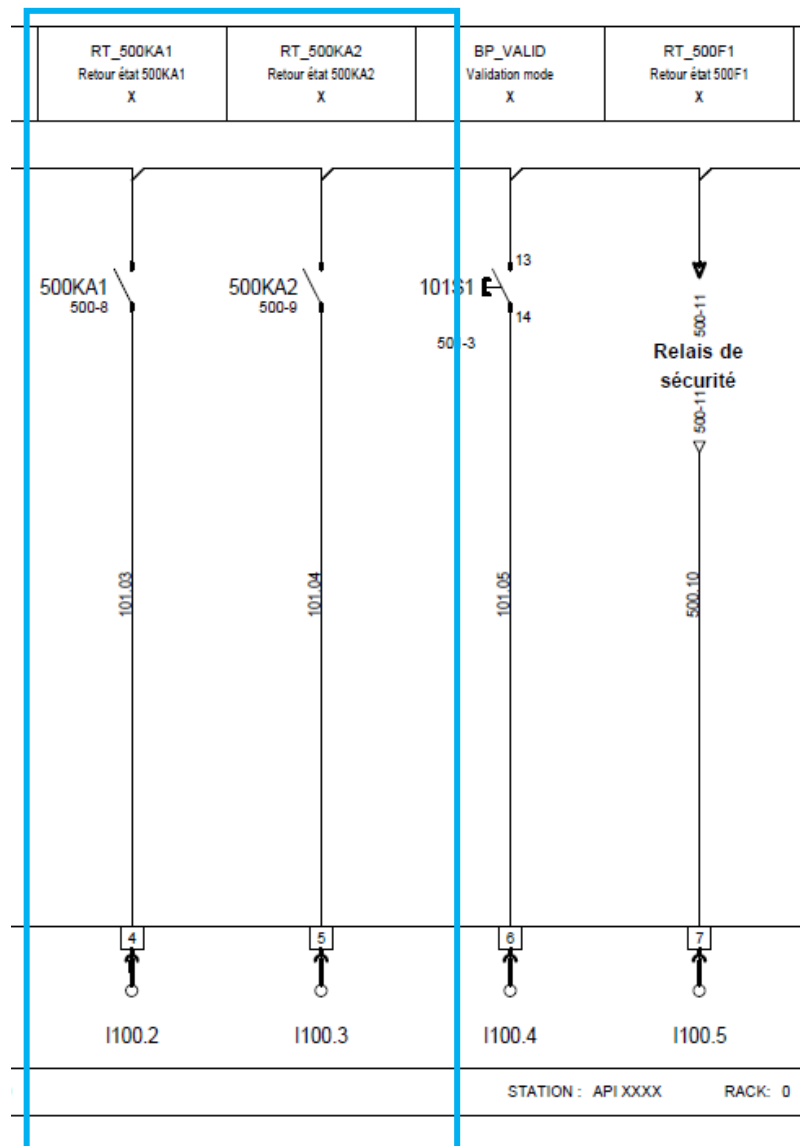
#### **4.3.3. Fonction arrêt d'urgence**

**A minima, le concepteur du système devra respecter le principe des schémas ci-après pour les niveaux Pla, b.**





Mise à disposition dans l'automate des retours d'état des contacteurs pour gestion des discordances (une alarme doit être traitée dans l'automate et devra être remonté au poste de pilotage)



Pour les **niveaux PLc,d,e** d'autres principes devront être mise en œuvre :

- câblage hors automate, redondance contacteurs, gestion des différentes discordances.
- Utilisation d'un automate de sécurité programmé par une personne certifiée,

#### **4.3.4. Disponibilité des installations : redondance des sécurités**

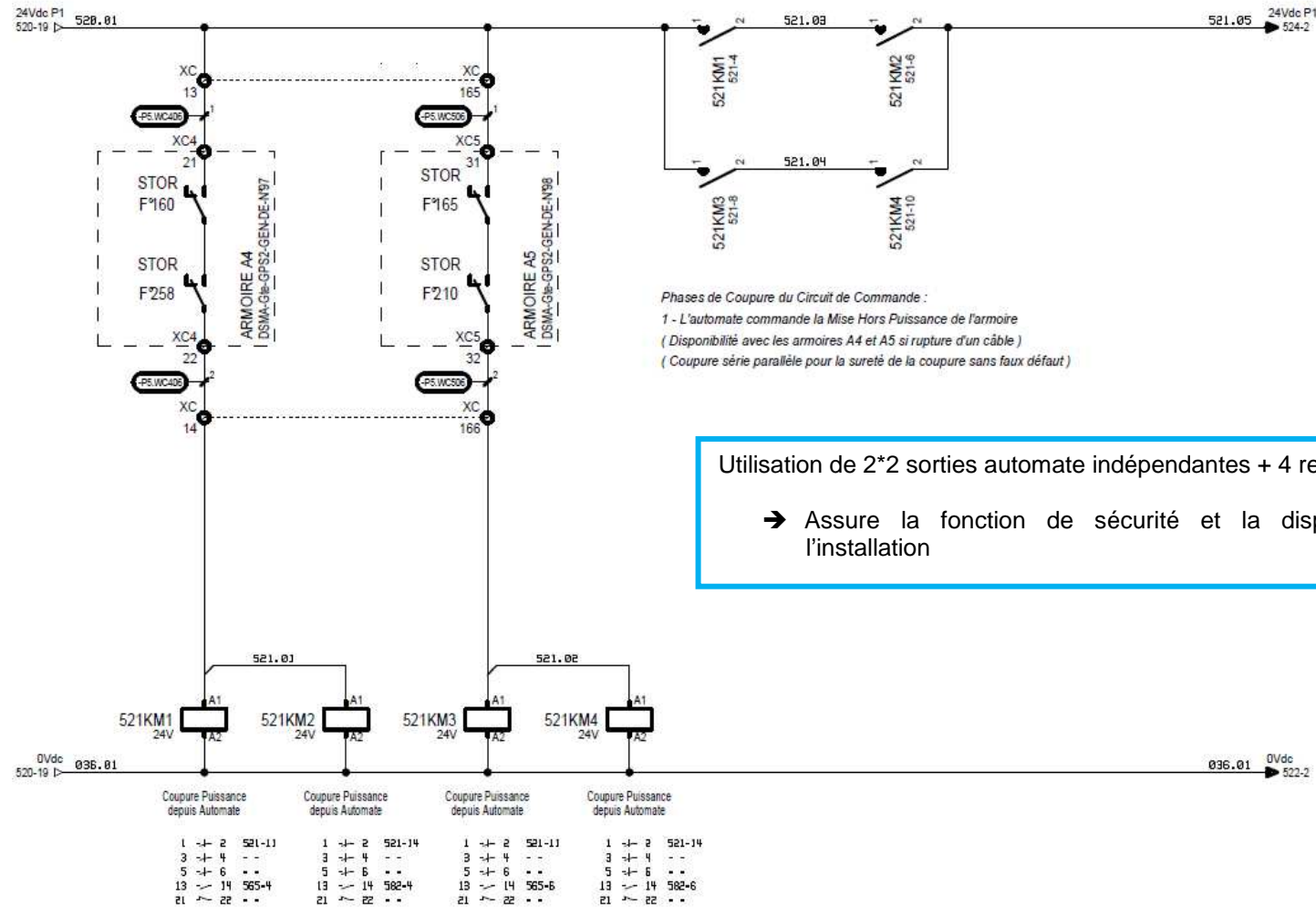
Certaines installations doivent être disponible : un défaut intempestif ne doit en aucun cas arrêter la machine (peut engendrer une casse matériel= perte financière importante).

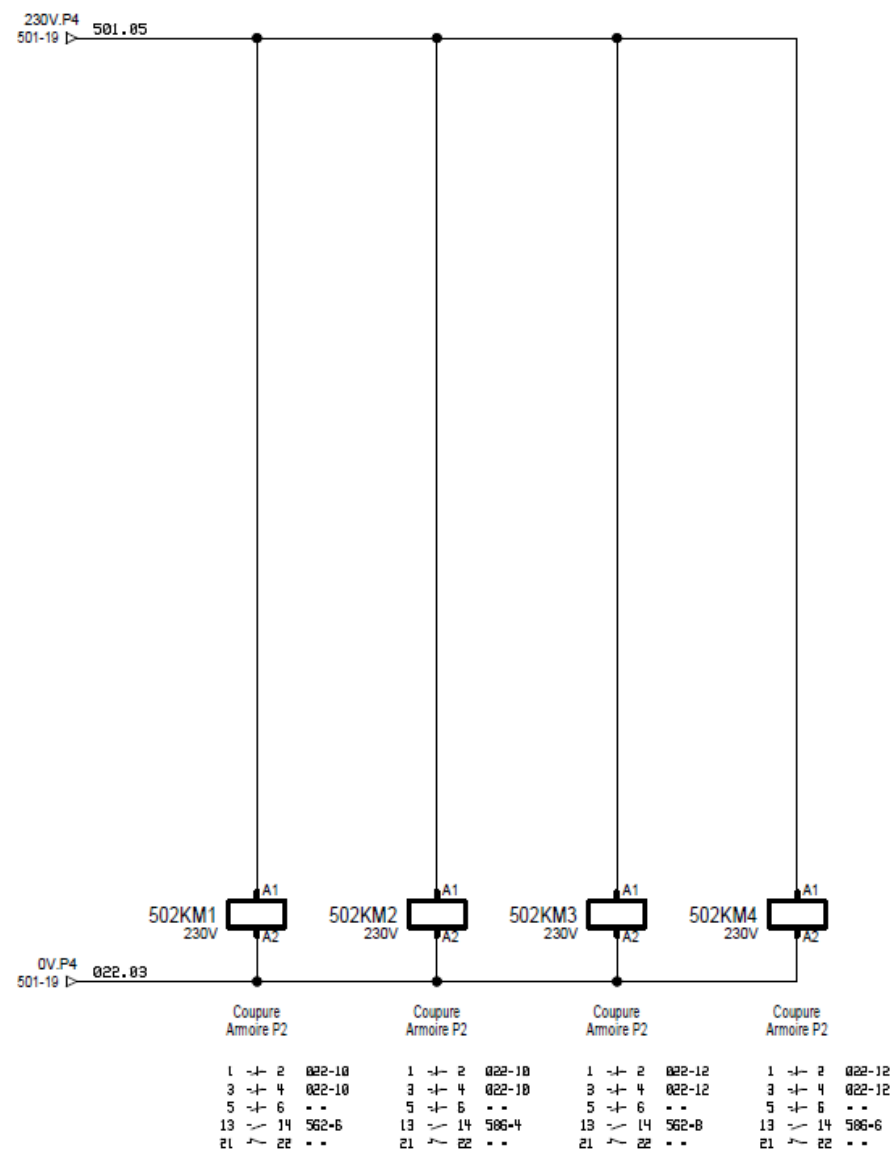
Pour pallier à ce genre de problème, lorsque cela est nécessaire, les systèmes de contrôle commande doivent être conçu de telle sorte à assurer la continuité de service tout en respectant le niveau de sécurité définit. Pour respecter ces critères, la partie sécurité doit être redondée. Ci-après quelques exemples qui pourront aider le concepteur à mettre ces principes en œuvres.

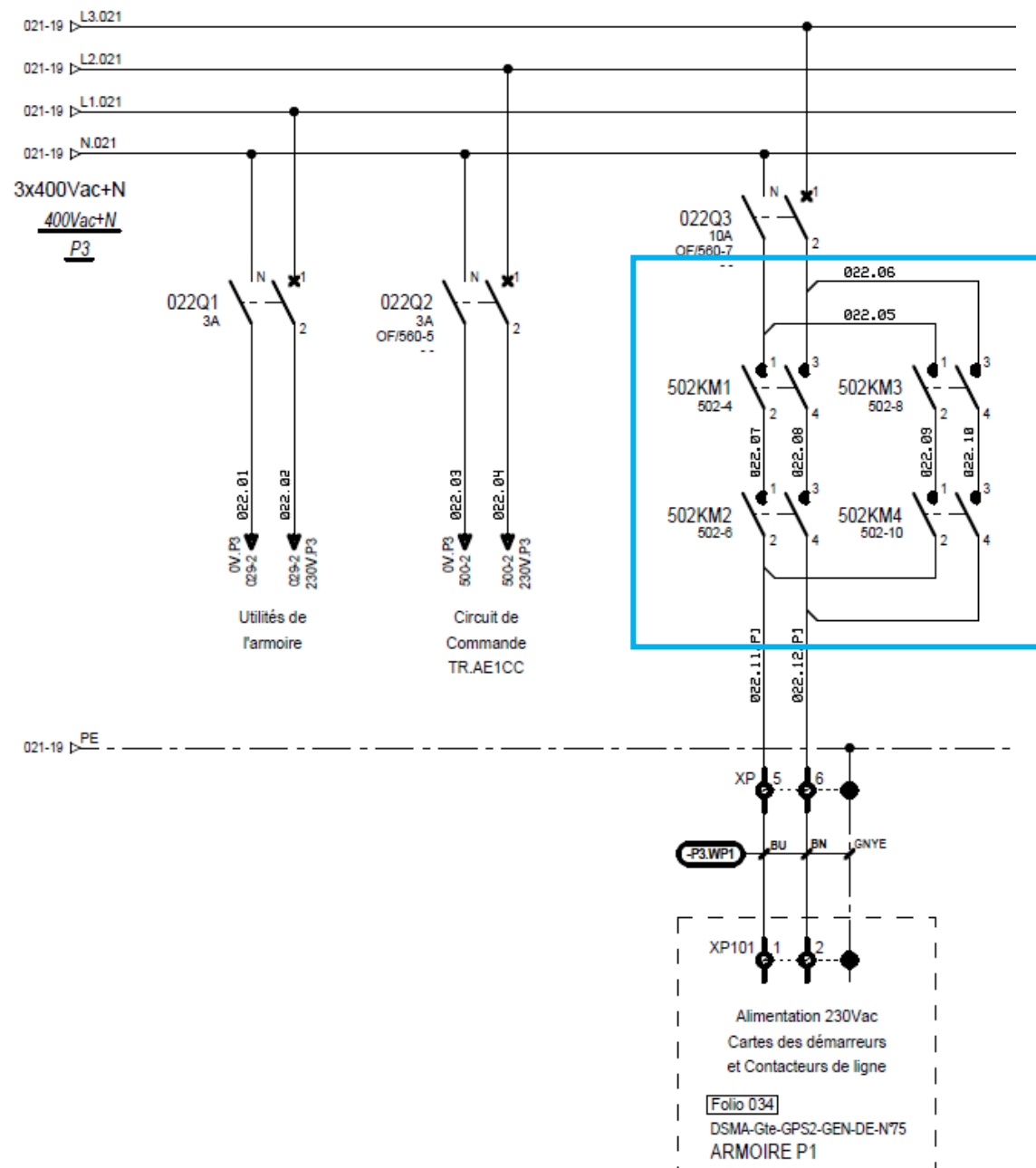




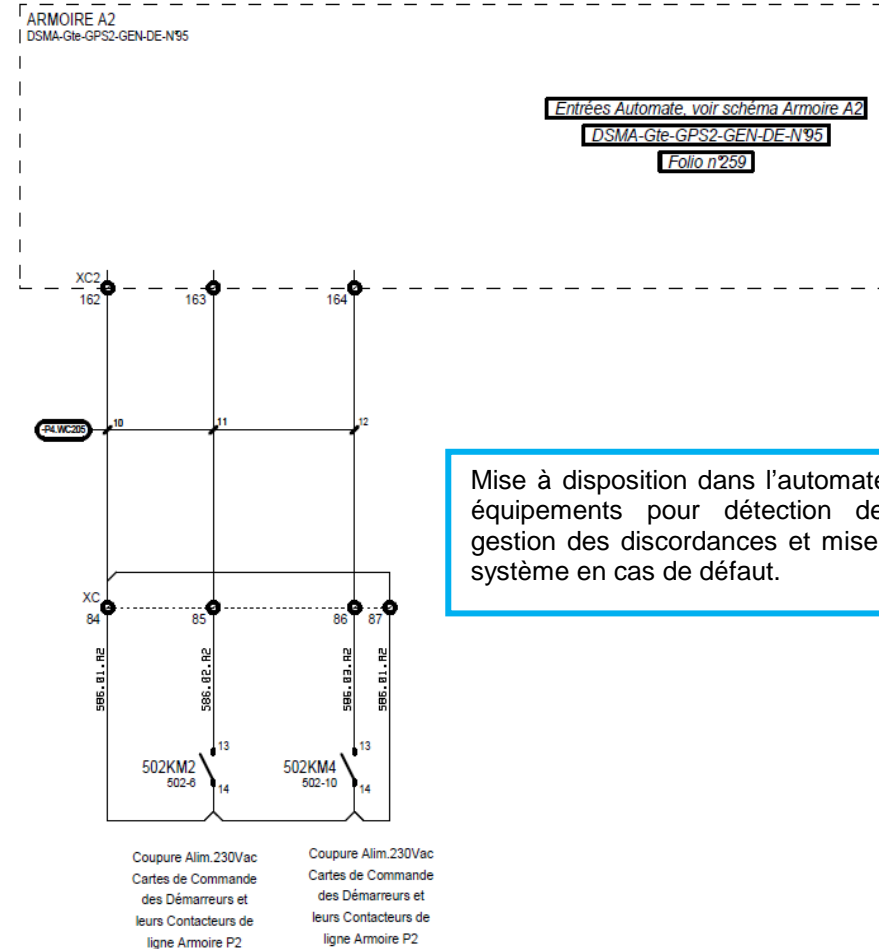
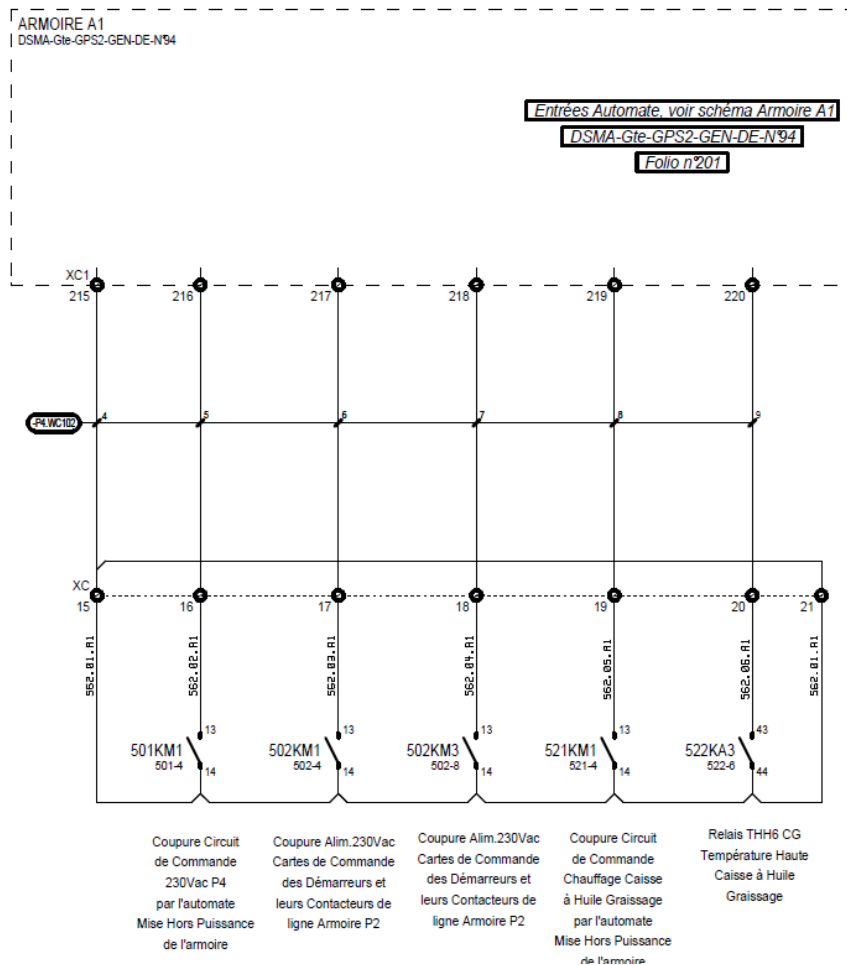
## Fonction Repos installation avec redondance







4 relais pour couper l'alimentation sur des démarreurs en respectant le niveau de sécurité et assurant la continuité de service en cas de faux défaut.

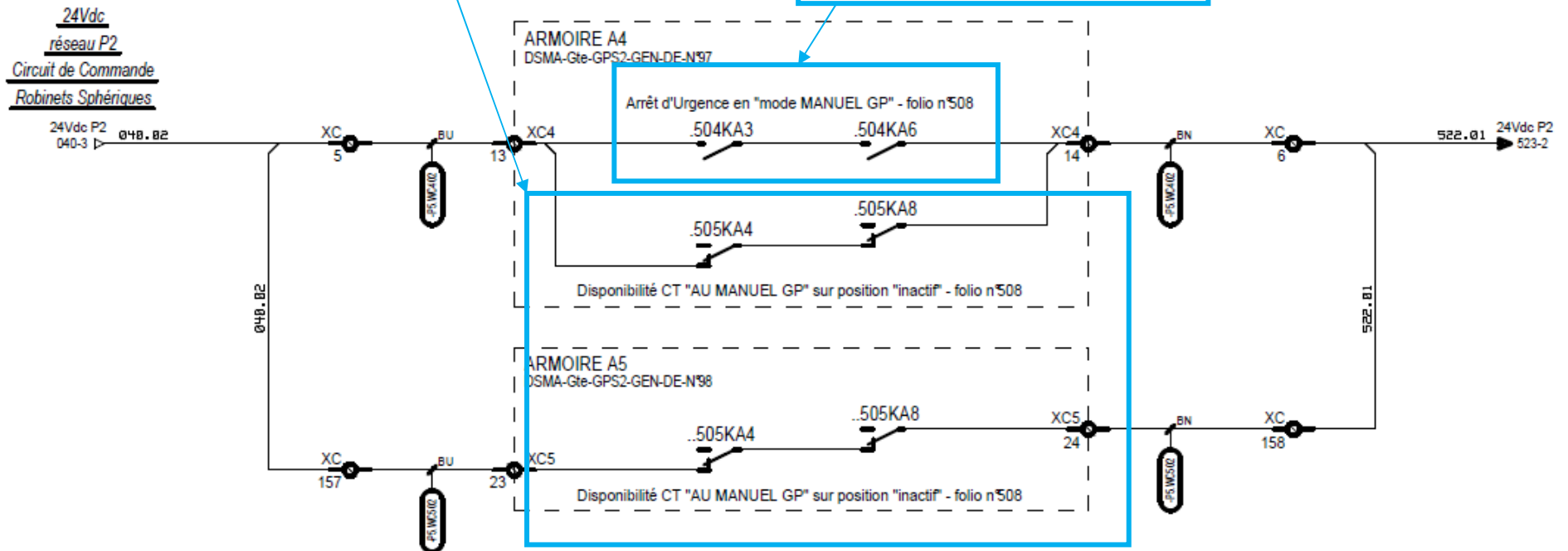


Mise à disposition dans l'automate des états des équipements pour détection des défauts de gestion des discordances et mise en sécurité du système en cas de défaut.



Disponibilité élevée (2 branches en parallèle)

Sécurité élevée (2 contacts en série)



API en mode MANUEL GP et CT "AU MANUEL GP" en position "actif" :

Phases de Coupure du Circuit de Commande :

- 1 - Passage du CT "AU MANUEL GP" en position "actif" -> Attente du Réarmement du Préventa
- 2 - Action sur AU
- 3 - Perte du 24Vdc alimentant le Préventa
- 4 - Rupture du câble venant de l'armoire A4

API hors mode MANUEL GP et CT "AU MANUEL GP" en position "inactif" :

- 1 - Inhibition des AU et du préventa
- 2 - Redondance de la position du CT "AU MANUEL GP" en position "inactif" dans Armoire A4 avec alimentation différente
- 3 - Redondance de la position du CT "AU MANUEL GP" en position "inactif" dans Armoire A5 avec alimentation différente
- 4 - Mise en parallèle de la redondance de la position du CT "AU MANUEL GP" en position "inactif"
- 5 - Câbles différents pour Armoire A4 et Armoire A5 si rupture d'un câble

0Vdc 521-19 036.01 0Vdc 523-2

Chaque cas est unique et doit être étudié en fonction du niveau de sécurité requis, du matériel disponible sur le marché, du processus de la machine.

## **5. VALIDATION**

A minima, le concepteur devra établir un cahier de validation pour les fonctions de sécurité. Cette partie pourra être intégrée au dossier de validation globale du système de contrôle commande mais sera bien identifiée.


Dans ce cahier de validation, à minima le concepteur prévoira :

- Les tests exhaustifs de toutes les fonctions de sécurité,
- Selon le niveau de sécurité à atteindre, les tests des défauts possibles et la validation du comportement du système.





**6. FICHE DE CONTROLE ONERA**

N° fiche				 <b>FICHE DE CONTROLE:</b> <b>CONFORMITE MACHINE</b>	
Nom du projet					
Date du contrôle		/ /			
Nom(s) vérificateur(s)					
<b>N° Fonction de sécurité</b>	<b>Description de la fonction de sécurité</b>	<b>Niveau de sécurité à atteindre (établis par ONERA)</b>	<b>Niveau de sécurité atteint par la chaîne de sécurité (concepteur)</b>	<b>Nom et signature du concepteur</b>	<b>Nom et signature du représentant ONERA (Chef unité ou responsable sécurité)</b>
1					
2					
3					
4					
5					