

## Contrôleur CS9

### Manuel de sécurité



Un document "readme.pdf" peut être livré avec le DVD du robot. Il contient des ajouts et errata, à la documentation.

## TABLE DES MATIÈRES

|  |           |
|--|-----------|
| <b>1- INTRODUCTION.....</b>  | <b>5</b>  |
| 1.1- Avant propos.....   | 5         |
| 1.2- Définition et glossaire.....                                      | 6         |
| <b>2- DESCRIPTION.....</b>   | <b>9</b>  |
| 2.1- Description.....  | 9         |
| 2.2- Situations d'utilisation de la sécurité.....                      | 11        |
| 2.3- Composants de sécurité.....                                       | 13        |
| 2.4- Fonctions de sécurité.....  | 14        |
| <b>3- CONCEPTION DE LA MACHINE.....</b>                                | <b>19</b> |
| 3.1- Exigences de sécurité.....  | 19        |
| 3.2- Niveau de performances/d'intégrité des fonctions de sécurité..... | 23        |
| 3.3- Réalisation.....  | 29        |
| <b>4- SAFE PMT.....</b>  | <b>51</b> |
| 4.1- Installation et paramètres.....                                   | 51        |
| 4.2- Description.....  | 52        |
| 4.3- Actualisation des paramètres de sécurité.....                     | 53        |
| 4.4- Rapport de validation.....  | 55        |
| 4.5- Sauvegarde et restauration des paramètres de sécurité.....        | 55        |
| 4.6- Maintenance.....  | 59        |
| <b>5- PARAMÈTRES DE SÉCURITÉ.....</b>                                  | <b>63</b> |
| 5.1- (SafeCell) Activation de la surveillance de sécurité.....         | 63        |
| 5.2- (SafeCell) Fonctions de sécurité d'arrêt.....                     | 65        |
| 5.3- (SafeCell) Fonctions de sécurité de limitation.....               | 69        |
| 5.4- Fonctions de sécurité de contrôle.....                            | 81        |
| 5.5- Entrées/sorties de sécurité.....                                  | 82        |
| 5.6- (SafeCell) Fonctions de diagnostic.....                           | 83        |
| <b>6- MISE EN SERVICE.....</b>   | <b>85</b> |
| 6.1- Informations pour la validation.....                              | 85        |
| 6.2- Validation des alimentations électriques.....                     | 86        |
| 6.3- Validation des fonctions de sécurité de contrôle.....             | 86        |
| 6.4- Validation des fonctions de sécurité d'arrêt.....                 | 86        |
| 6.5- Validation des distances de séparation.....                       | 87        |
| 6.6- Validation des fonctions de sécurité de limitation.....           | 87        |
| 6.7- Validation de l'espace de travail restreint.....                  | 89        |
| 6.8- Validation des fonctions de sécurité des entrées/sorties.....     | 89        |
| 6.9- Validation des fonctions de diagnostic.....                       | 90        |
| 6.10- Validation des mesures de sécurité.....                          | 90        |

6.11- Remise en service..... 91

**7- ANNEXES.....93**

7.1- Liste de vérifications pour la mise en service..... 93

7.2- RSI9 IOs..... 97

7.3- Entrées-sorties de DSI9 (système)..... 101

7.4- Version de sécurité..... 102

7.5- Versions de SafeCell..... 108

# 1 - INTRODUCTION

## 1.1 - AVANT PROPOS

M0000242.1

Les informations contenues dans le présent document sont la propriété de Stäubli et elles ne peuvent être reproduites, pour tout ou partie, sans notre accord préalable écrit.

Les spécifications contenues dans le présent document peuvent être soumises à modifications sans préavis. Bien que toutes les précautions soient prises pour assurer l'exactitude des informations données dans ce document, Stäubli ne peut être considéré comme responsable des erreurs ou omissions pouvant apparaître dans les illustrations, les plans et les spécifications du dit document.

Les schémas électriques inclus dans ce manuel sont fournis à titre informatif uniquement. La référence pour les schémas électriques du robot est donnée dans un manuel spécifique. Les photographies sont utilisées pour faciliter la compréhension, elles n'ont aucun caractère contractuel.

Merci de rapporter les erreurs et omissions au contact du Support Clients Stäubli Robotique de votre pays, que vous pouvez trouver sur :

- <http://www.staubli.com/en/contacts/division/robotics/>

**STÄUBLI, UNIMATION, VAL, Stericlean**

**sont des marques enregistrées par Stäubli INTERNATIONAL AG.**



EtherCAT® est une marque déposée et une technologie brevetée sous licence de Beckhoff Automation GmbH, Allemagne.



Safety over EtherCAT® est une marque déposée et une technologie brevetée sous licence de Beckhoff Automation GmbH, Allemagne.

### 1.1.1 - BUT DE CE MANUEL

M0004671.1

Ce manuel a pour objectif de donner des informations relatives à la configuration et à la validation correctes des paramètres de sécurité du robot. Il apporte une aide aux personnes intervenant sur cet appareil à titre de référence seulement. Stäubli propose des formations pour faciliter la compréhension de ce manuel, l'utilisation du robot, ainsi que sa maintenance.

### 1.1.2 - MESSAGES SPÉCIAUX CONCERNANT LA SÉCURITÉ, PRÉCAUTIONS ET INFORMATIONS

M0005317.1

Dans ce document, plusieurs pictogrammes signalent des dangers importants.

Ces avertissements se présentent comme suit (par ordre d'importance décroissant) :



#### SÉCURITÉ

Consigne qui attire l'attention du lecteur sur l'engagement de sa responsabilité si les mesures indiquées ne sont pas respectées. Le respect de cette consigne est indispensable pour conserver le niveau de sécurité du robot.



Instructions attirant l'attention du lecteur sur les risques de détérioration ou de panne du matériel si les consignes ne sont pas respectées. Le respect de cette consigne est indispensable pour préserver la fiabilité et les performances du matériel.



Fournit un complément d'information, souligne un point ou une procédure importante. Cette information doit être mémorisée pour faciliter la mise en oeuvre et assurer le bon déroulement des opérations décrites.

## 1.2 - DÉFINITION ET GLOSSAIRE

M0004672.1

**Personne** : Terme général désignant quiconque peut se trouver à proximité d'une machine Stäubli.

**Personnel** : Désigne les personnes affectées et formées à l'installation, l'utilisation et la maintenance de la machine Stäubli.

**Utilisateur** : Désigne les personnes ou la société responsable de l'utilisation de la machine Stäubli.

**Opérateur** : Désigne la personne qui démarre, stoppe ou contrôle le fonctionnement du robot.

**Intégrateur** : Désigne les personnes ou la société responsable de la conception et de la fabrication de la cellule robotisée.

**Responsable sécurité** : Désigne les personnes responsables de la mise en service de sécurité.

|                    |   |  |
|--------------------|---|--|
| B <sub>10d</sub>   |   | Nombre moyen de cycles pour atteindre 10% de défaillances dangereuses (ISO 13849-1, C4)  |
| DSI9               | Digital Sensor Interface                                  | Carte interface codeur : carte de sécurité dans le socle du robot  |
| FMEA               | Failure Mode and Effects Analysis                         | AMDEC : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité   |
| IP code            | Ingress Protection Code                                   | Standard international (IEC 60529) définissant le degré de protection contre les intrusions  |
| PFH <sub>d</sub>   | Probability of dangerous Failure per Hour                 | Probabilité de défaillance dangereuse par heure : composante de la mesure des performances des fonctions de sécurité nécessaire pour définir les niveaux PL ou SIL |
| PL                 | Performance Level   | Niveau de performance : mesure des performances pour les fonctions de sécurité selon ISO 13849-1   |
| RBR                | Remote Brake Release                                      | Libération des freins déportée : boîtier manuel de commande des freins   |
| RSI9               | Robot Safety Interface                                    | Carte Interface de sécurité : carte de sécurité dans le tiroir calculateur CS9   |
| SBC <sup>(1)</sup> | Safe Brake Control  | Commande de frein sûre : fonction de sécurité pour la commande de l'alimentation électrique des freins   |
| SELV/<br>PELV      | Separated Extra Low Voltage / Protected Extra Low Voltage | TBTS/TBTP : Très Basse Tension de Sécurité / Très Basse Tension de Protection  |
| SIL                | Safety Integrity Level                                    | Niveau d'intégrité de sécurité : mesure des performances pour les fonctions de sécurité selon IEC 61508 ou IEC 62061   |
| SLO                | Safely Limited Orientation                                | Orientation limitée de sécurité : fonction de sécurité limitant l'orientation de l'outil   |
| SLP <sup>(1)</sup> | Safely Limited Position                                   | Position limitée de sécurité : fonction de sécurité limitant la position du robot  |
| SLS <sup>(1)</sup> | Safely Limited Speed                                      | Vitesse limitée de sécurité : fonction de sécurité limitant la vitesse du robot  |
| SOS <sup>(1)</sup> | Safe Operating Stop                                       | Arrêt sûr opérationnel : Fonction de sécurité empêchant le mouvement du robot  |
| SP2                |   | Stäubli pendant  |
| SRC                | Stäubli Robotics Control                                  | Logiciel embarqué sur le robot   |
| SS0 <sup>(1)</sup> | Safe Stop 0   | Arrêt sûr 0 : fonction de sécurité pour un arrêt de catégorie 0 selon IEC 60204-1  |

|                    |                        |   |
|--------------------|------------------------|---|
| SS1 <sup>(1)</sup> | Safe Stop 1            | Arrêt sûr 1 : fonction de sécurité pour un arrêt de catégorie 1 selon IEC 60204-1                                 |
| SS2 <sup>(1)</sup> | Safe Stop 2            | Arrêt sûr 2 : fonction de sécurité pour un arrêt de catégorie 2 selon IEC 60204-1                                 |
| STO <sup>(1)</sup> | Safe Torque Off        | Absence sûre de couple : fonction de sécurité pour le contrôle du couple des moteurs                              |
| SVC                | Safe Valve Control     | Commande de sécurité des électrovannes : fonction contrôlant l'alimentation en énergie des électrovannes          |
| TDO                | Test Digital Output    | Sortie numérique de test : sortie numérique couplée à une entrée numérique sûre pour détecter les courts-circuits |
| USI                | User Safe Input        | Entrée sûre utilisateur : entrée numérique sûre sur le tiroir calculateur CS9                                     |
| USO                | User Safe Output       | Sortie sûre utilisateur : sortie numérique sûre sur le tiroir calculateur CS9                                     |
| WMS9               | Working Mode Selection | Sélection du mode de marche : interface de sélection de la touche de mode de marche                               |

(1) Selon la définition de la norme EN 61800-5-2:2016





## 2 - DESCRIPTION

### 2.1 - DESCRIPTION

#### 2.1.1 - SÉCURITÉ FONCTIONNELLE

M0004629.1

Le contrôleur CS9 comprend un contrôleur de sécurité qui est capable non seulement d'arrêter le robot sur demande (par ex. après un arrêt d'urgence) mais aussi de surveiller des conditions de sécurité avancées basées sur la position et la vitesse du bras. Pour cela, il s'appuie sur des microprocesseurs redondants pour exécuter un programme de sécurité du robot qui peut être configuré (mais pas modifié) par l'intégrateur du robot. L'utilisation de systèmes électroniques programmables pour la sécurité est appelée « sécurité fonctionnelle ».

La sécurité fonctionnelle offre de nouvelles possibilités telles que la réduction de l'encombrement de la cellule ou la taille de la barrière et rend possibles différentes sortes d'applications collaboratives dans lesquelles l'homme et la machine peuvent interagir de façon plus proche et plus fréquente. Des cas typiques d'utilisation de la sécurité fonctionnelle sont décrits dans le chapitre 2.2.

Le contrôleur de sécurité est indépendant du contrôleur de mouvement mais leurs configurations sont synchronisées, de sorte que la plupart des limites de sécurité configurées sont respectées automatiquement, sans qu'il faille modifier le programme d'application. Par exemple, la réduction de la vitesse de sécurité maximale est automatiquement appliquée aux mouvements du robot.



La plupart des paramètres de sécurité peuvent être mis au point sans toucher au programme d'application.

Les avantages de la sécurité fonctionnelle ont toutefois une contrepartie : une gestion rigoureuse de la configuration de sécurité est nécessaire et, selon les fonctions de sécurité utilisées, un référencement du robot et des essais de freins doivent être régulièrement prévus. Pour les configurations de sécurité complexes, la mise au point et la validation des paramètres de sécurité peut demander un temps considérable.



La faisabilité des projets basés sur les nouveaux concepts de sécurité doit être soigneusement étudiée. Toute erreur dans le concept de sécurité peut avoir des répercussions graves sur toute la cellule.

Le programme de sécurité du robot existe dans 3 versions distinctes :

- La version Initial (programme de sécurité 200.x) est destinée à des applications qui ne nécessitent pas de sécurité fonctionnelle. C'est la version qui est livrée avec chaque robot.
- La version SafeCell (programme de sécurité 100.x) est une version intermédiaire qui permet de configurer tous les arrêts de sécurité, la position des articulations et les limites de vitesse.
- La version SafeCell+ (programme de sécurité 1.x) est une version complète qui permet en outre de configurer des zones de sécurité, avec des limites de position cartésienne et de vitesse.



Les versions SafeCell et SafeCell+ du programme de sécurité ne sont pas disponibles pour les bras TS2.



- Utiliser le programme de sécurité Initial quand aucune fonction de sécurité avancée n'est nécessaire.
- Consulter le manuel d'instruction de la CS9 comme référence pour le programme de sécurité Initial.

### 2.1.2 - PROCESSUS DE SÉCURITÉ

M0004630.1

La gestion rigoureuse de la configuration de sécurité du robot s'effectue en trois étapes principales :

#### 1) Concept de sécurité et faisabilité

Le concept de sécurité doit clairement définir à quoi sert la sécurité du robot et quelles fonctions sont nécessaires à cette fin. Il doit démontrer qu'il permet une réduction adéquate des risques et confirmer que la solution identifiée est réalisable. Le chapitre 3 donne les informations nécessaires à l'exécution de cette étape.

#### 2) Configuration de la sécurité

Au cours de l'intégration de la cellule, les fonctions de sécurité nécessaires sont configurées avec les valeurs de paramètres identifiées dans le concept de sécurité et mises au point sur site si nécessaire. Le chapitre 5 est le manuel de référence des paramètres de sécurité.

#### 3) Validation de la sécurité

Quand l'application est prête à fonctionner, une validation de la sécurité doit être effectuée afin de s'assurer que toutes les fonctions de sécurité se comportent de la manière prévue. Le chapitre 6 détaille les essais de validation à effectuer ; une liste de vérifications est donnée en annexe, à l'appui de la phase de validation.

### 2.1.3 - FONCTIONS DE SÉCURITÉ

M0004631.1

Le concept de sécurité fait le lien entre les risques identifiés dans la cellule et les fonctions de sécurité du robot qui servent à les maîtriser. Le but principal du présent manuel de sécurité est de décrire en détail les fonctions de sécurité du robot afin de permettre leur bonne utilisation.

Le principe général des fonctions de sécurité du robot est de surveiller des conditions de sécurité prédéfinies et, soit de signaler l'état surveillé à d'autres périphériques, soit de mettre le robot dans un état sûr quand certaines conditions de sécurité ne sont plus satisfaites :

- Les conditions de sécurité sont contrôlées par la surveillance des retours des entrées et codeurs sûrs. Selon la réaction souhaitée, cette surveillance entraîne un arrêt sûr et/ou l'inhibition d'une sortie sûre afin de déclencher la réaction adéquate d'autres dispositifs dans la cellule.
- L'état sûr du robot est obtenu par la désactivation des actionneurs qu'il contrôle : moteurs, freins et électrovannes. L'état sûr des autres dispositifs dans la cellule peut éventuellement être contrôlé par des sorties sûres.



Tous les robots CS9/TX2 sont dotés de l'équipement de sécurité nécessaire pour les fonctions de sécurité documentées. Les fonctions de sécurité avancées sont protégées par la licence d'exécution SafeCell+.

### 2.1.4 - PROGRAMME DE SÉCURITÉ

M0004632.1

Les fonctions de sécurité du robot sont implémentées dans un prédéfini programme de sécurité du robot qui garantit la gestion adéquate des moteurs, freins, électrovannes et des modes de marche du robot. Ce programme de sécurité n'est pas modifiable ; il est seulement possible de configurer ses paramètres.

Le programme de sécurité implémente :

- la prise en charge de différents modes de marche et les interfaces de commande du redémarrage.
- la sécurité SP2 : arrêt d'urgence, dispositif d'activation configurable, retrait du boîtier sans arrêt d'urgence.
- les limites de vitesse de sécurité de l'articulation et cartésiennes (SafeCell+) en mode manuel et automatique.
- les limites de sécurité des articulations.
- (SafeCell+) 2 zones sûres permanentes avec accès interdit ou vitesse limitée.
- 4 entrées de sécurité configurables pour déclencher soit un arrêt de sécurité, soit une limite de vitesse de sécurité, avec un temps de réaction configurable.
- (SafeCell+) Pour 2 entrées, l'arrêt de sécurité ou la limite de vitesse peut être circonscrit à une zone sûre.
- 3 sorties sûres configurables pour transmettre des informations de sécurité à d'autres appareils.
- un profil de sécurité esclave EtherCAT FSoE qui s'interface avec un PLC sécurisé externe.
- Gestion du référencement de sécurité.
- Gestion des essais de frein.

Une zone de sécurité est définie comme une position articulaire sécurisée et des limites de vitesse cartésiennes dans un volume cartésien (cube/cylindre/face d'un plan vertical). Les limites de position cartésienne et de vitesse du robot sont vérifiées sur le TCP en un maximum de 4 points de contrôle différents fixés à la bride du robot et éventuellement en 1 point de contrôle fixé au coude du robot.



La complexité de la solution de sécurité est limitée par le nombre d'E/S sûres et de zones de sécurité. Il est important de vérifier attentivement la faisabilité des nouveaux concepts de sécurité dans la phase de conception initiale.

Stäubli Robotics Suite 2019 inclut un éditeur de configuration de la sécurité qui vérifie les ressources de sécurité requises et identifie les incompatibilités possibles entre les paramètres de sécurité.

## 2.2 - SITUATIONS D'UTILISATION DE LA SÉCURITÉ

### 2.2.1 - INTERVENTIONS À PROXIMITÉ DU ROBOT

M0004633.1

Il n'est pas nécessaire de faire intervenir la sécurité fonctionnelle du robot pour arrêter celui-ci au cours d'une intervention dans son espace de travail. La sécurité fonctionnelle du robot apporte toutefois de nouvelles possibilités :

- L'utilisation d'un arrêt sûr SS2 au lieu de SS1 simplifie la programmation de l'application : l'arrêt et le redémarrage peuvent être entièrement commandés par le contrôleur de sécurité, indépendamment du programme d'application.

Quand un redémarrage automatique après intervention est possible (par ex. pour les très petites cellules ou celles qui peuvent toujours détecter la présence d'une personne), l'utilisation d'un arrêt SS2 optimise la durée de l'intervention.

- La mise au point du temps d'arrêt peut servir à réduire les distances de séparation (voir le chapitre 2.2.2) ou permettre de concevoir une zone d'échange de pièces simple et efficace, avec des barrières immatérielles, tandis que l'intervention rapide de l'opérateur a peu d'impact sur le temps de cycle de la production.

En outre, le très bon niveau de sécurité de l'arrêt sûr du CS9/TX2 rend possibles des interventions régulières dans l'espace de travail du robot, lorsque l'estimation du risque montre que le fonctionnement SIL2/PLd habituel ne suffit pas pour les interventions fréquentes.

### 2.2.2 - RÉDUCTION DE LA DISTANCE DE SÉPARATION / ENCOMBREMENT DE LA CELLULE

M0004634.1

La distance de séparation entre le robot et les dispositifs de protection est déterminée de telle manière que le robot ait le temps de s'arrêter avant qu'une personne qui s'en approche puisse l'atteindre. En faisant du temps d'arrêt un paramètre de sécurité configurable, on peut optimiser la distance de séparation. Quand la distance de séparation a un effet sur l'encombrement de la cellule, cette optimisation réduit en conséquence l'encombrement de la cellule.

Plus le robot est rapide, plus sa capacité de décélération est importante, plus le temps d'arrêt possible est réduit. Le temps d'arrêt minimum possible dépend de la charge et de la fréquence d'arrêt, de façon à préserver la durée de vie du robot.

### 2.2.3 - DIMENSIONNEMENT OPTIMISÉ DES BARRIÈRES

M0004635.1

Quand des barrières sont placées dans l'espace accessible du robot, il faut s'assurer, soit qu'elles puissent arrêter le robot sans être dangereusement déformées, soit que le robot puisse toujours s'arrêter avant de les atteindre.

- Une déformation dangereuse peut être empêchée en réduisant l'énergie maximale du robot au moyen de limites de vitesse de sécurité.
- L'arrêt du robot avant les barrières peut être réalisé avec des limites de position de sécurité, mais il faut prévoir une zone d'arrêt entre les barrières et les limites de sécurité afin que le robot ait le temps de s'arrêter sur ses freins en cas de défaillance du système (par ex. coupure de courant).
- Les deux solutions peuvent être couplées afin de trouver le meilleur compromis possible entre temps de cycle et encombrement de la cellule.

L'estimation de la distance d'arrêt la plus défavorable ou de l'énergie aux limites nécessite des simulations complexes : en pratique, il faut formuler des estimations conservatrices.

### 2.2.4 - ESPACE DE TRAVAIL PARTAGÉ ENTRE L'OPÉRATEUR ET LE ROBOT

M0004636.1

Les limites de sécurité de position et de vitesse activées par un signal de sécurité peuvent être utilisées pour ne laisser manœuvrer le robot que dans une partie de son espace de travail, à vitesse réduite, quand l'opérateur pénètre dans une autre partie de la cellule, par exemple pour le déchargement et le rechargement d'une palette. Un changement de palette peut ainsi être effectué sans arrêter l'application.

### 2.2.5 - APPLICATIONS COLLABORATIVES

M0004637.1

Les applications collaboratives peuvent représenter des solutions très différentes :

- Au sens le plus large, il s'agit d'applications avec lesquelles l'opérateur peut entrer et sortir librement de l'espace de travail du robot : des interventions régulières près du robot ou un partage de l'espace de travail peuvent prendre la forme d'opérations collaboratives avec les robots CS9, dont les performances de sécurité élevées permettent des passages fréquents dans l'espace de travail du robot.
- Dans un sens plus restrictif, le terme désigne des applications avec lesquelles le contact avec un robot en mouvement, même s'il n'est pas souhaité, est possible et sans danger. Il faut généralement pour cela un capteur de sécurité qui détecte le contact.



#### SÉCURITÉ

Les robots CS9/TX2 ne sont PAS équipés d'une fonction de surveillance adéquate pour une détection du contact : une telle fonction doit être implémentée par l'ajout de dispositifs de protection externes.

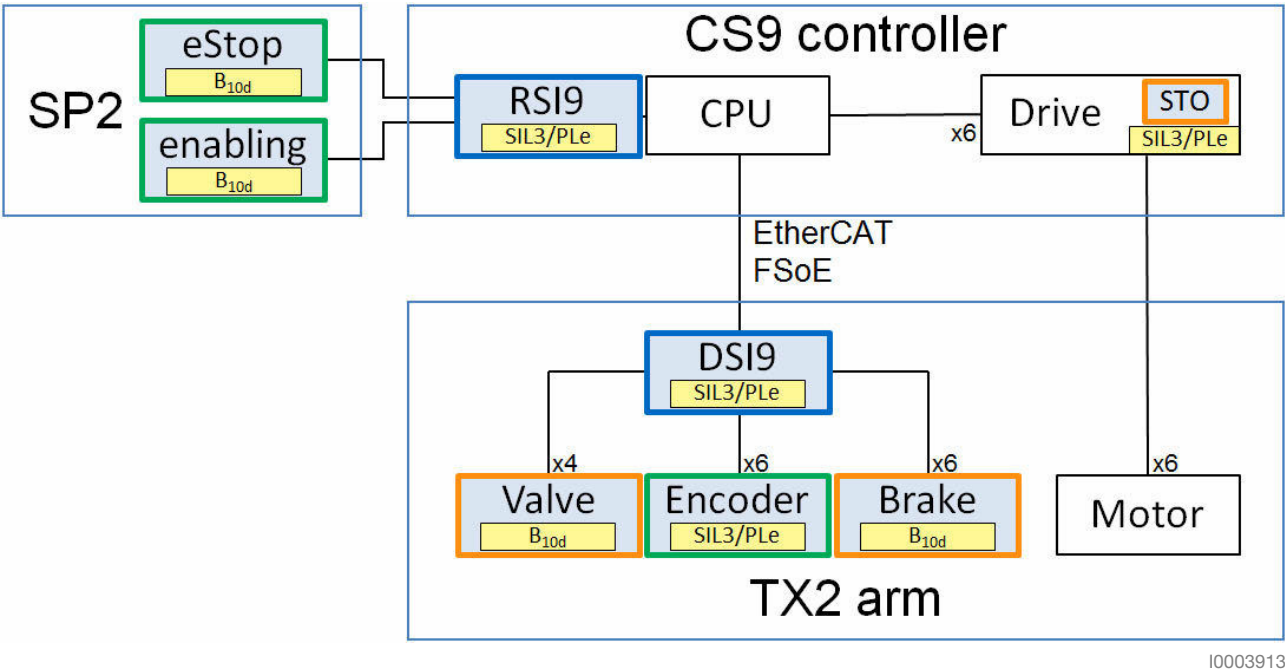
- Dans son sens le plus restrictif, le terme désigne des opérations dans lesquelles l'opérateur et le robot travaillent de façon coordonnée sur la même tâche, avec des contacts possibles. Certaines de ces applications collaboratives, par exemple le guidage manuel, sont possibles avec les robots CS9, moyennant l'ajout d'équipement de sécurité sur l'effecteur.

2.3 - COMPOSANTS DE SÉCURITÉ

2.3.1 - ARCHITECTURE

M0004638.1

L'architecture de sécurité d'un robot CS9/TX2 est résumée dans la figure ci-dessous :



I0003913

| Anglais        | Traduction          | Anglais | Traduction |
|----------------|---------------------|---------|------------|
| eStop          | Arrêt d'urgence     | Encoder | Codeur     |
| Enabling       | Bouton d'activation | Brake   | Frein      |
| CS9 controller | Contrôleur CS9      | Motor   | Moteur     |
| Drives         | Amplificateurs      | TX2 arm | Bras TX2   |
| Valve          | Electrovanne        |         |            |

Figure 2.1

Cette figure met en évidence les composants de sécurité du contrôleur CS9 et du bras TX2 qui lui est rattaché. Le contrôleur comprend un PLC (RSI9) sécurisé et des amplificateurs qui utilisent la fonction de sécurité des entrées sûres utilisateur (STO) pour mettre les moteurs hors tension. Le bras est équipé d'une carte d'E/S de sécurité (DSI9) pour commander les électrovannes et les freins et transmettre le retour de position de sécurité des codeurs à la carte de sécurité RSI9.

L'alimentation du contrôleur délivre en outre les 24V TBTS/TBTP nécessaires pour faire fonctionner l'équipement de sécurité.

### 2.3.2 - INTERFACES DE SÉCURITÉ

M0004639.1

La carte de sécurité RSI9 possède des entrées et sorties numériques sûres, accessibles par l'interface du contrôleur. Elle utilise également des protocoles de sécurité Ethernet en temps réel tels que FSoE en EtherCAT, de sorte que les ports Ethernet en temps réel du contrôleur font également partie de l'interface de sécurité.

Les entrées sûres de la carte RSI9 sont utilisées pour connecter les dispositifs de sécurité suivants :

- Le bouchon de maintenance livré avec chaque robot pour sécuriser les phases d'intégration et d'entretien du robot.
- Le pendant d'apprentissage SP2 (en option), équipé d'un bouton d'activation et d'un arrêt d'urgence, et d'un bouchon qui permet le fonctionnement quand le pendant d'apprentissage est enlevé.
- Le sélecteur de mode de marche (WMS9) en option, qui comprend un commutateur de mode, un arrêt d'urgence et un bouton-poussoir d'acquiescement du redémarrage de sécurité (réinitialisation manuelle).

La carte DSI9 comprend également une série d'entrées numériques sûres, destinées à connecter l'interface de libération des freins déportée (RBR) (en option) et permettant la commande manuelle des freins, même quand le contrôleur n'est pas connecté ou en panne.

Les arrêts sur butées mécaniques sont également des dispositifs de sécurité qui permettent de réduire le rayon d'action du bras, mais elles n'utilisent pas d'électronique programmable et ne font donc pas partie de la sécurité fonctionnelle.

L'utilisation de cet équipement est décrite dans les manuels d'utilisation du contrôleur et du bras.

### 2.3.3 - SAFE PMT

M0004640.1

SafePMT est le logiciel pour PC nécessaire pour éditer les paramètres de sécurité, les transmettre à la carte de sécurité et fournir le rapport de référence nécessaire pour valider la sécurité. Il communique avec la carte de sécurité par une connexion Ethernet sécurisée. SafePMT est livré avec Stäubli Robotics Suite ou peut être téléchargé dans la bibliothèque d'assistance technique en ligne de Stäubli. Son installation et son utilisation sont décrites dans le chapitre 4.

## 2.4 - FONCTIONS DE SÉCURITÉ

M0004641.1

Une fonction de sécurité est une fonction du contrôleur de sécurité qui sert à supprimer ou réduire un risque d'accident corporel. Les fonctions de sécurité sont implémentées à l'aide de matériel et de logiciels spécifiques, conformes aux exigences des normes de sécurité internationales, afin que le risque de leur défaillance dangereuse (PFH<sub>d</sub>) puisse être calculé de façon à définir leur niveau d'intégrité de sécurité SIL (selon IEC 62061) ou leur niveau de performances PL (selon ISO 13849-1).

Différentes fonctions de sécurité peuvent avoir des niveaux de performances de sécurité différents, selon les composants auxquels elles font appel. Le niveau de performances de sécurité nécessaire pour une fonction de sécurité dépend de l'évaluation du risque que cette fonction contrôle : plus le risque est grand, plus le niveau de performances de sécurité est élevé. Les normes sur la sécurité ISO 13849-1 et IEC 62061 définissent des méthodes pour estimer le niveau de performances de sécurité. Le niveau de performances de sécurité SIL2/PLd est habituellement suffisant pour les fonctions d'arrêt sûr dans les applications où les interactions homme-machine sont limitées ; en revanche, les applications nécessitant des interactions fréquentes avec du matériel en mouvement à grande vitesse nécessitent un niveau plus élevé, SIL3/PL<sub>e</sub>, pour les fonctions d'arrêt sûr ou de limitation de vitesse.

Les fonctions de sécurité du robot peuvent être utilisées pour contrôler :

- Les risques liés aux pièces en mouvement (collision, écrasement, coincement par le robot, son outil ou la pièce).
- Les risques liés à la chute de pièces (axe du robot ou pièce).
- Les risques liés à la position ou à l'orientation du robot (par ex. source laser sur le robot).
- Les risques liés à d'autres dispositifs connectés au robot.

Elles peuvent être classées en différentes catégories :

- Fonctions de sécurité d'inhibition, qui amènent de force les actionneurs dans un état sûr.
- Fonctions de sécurité d'arrêt qui commandent la phase d'arrêt du robot et le gardent arrêté.
- Fonctions de sécurité de limitation, qui activent un arrêt sûr quand une limite surveillée est atteinte.
- Fonctions de sécurité de sortie, émettant en sortie des états contrôlés par le contrôleur de sécurité.
- Fonctions de sécurité de commande, implémentant des interfaces de commande : mode de marche, commande du redémarrage.

Il est possible de construire des fonctions de sécurité complexes en calculant les fonctions avancées associées aux retours des capteurs et en définissant des combinaisons logiques d'états sûrs, par exemple de définir des zones de sécurité par une combinaison de conditions de sécurité pour la position et la vitesse.

#### 2.4.1 - FONCTIONS DE SÉCURITÉ D'INHIBITION

M0004642.1

Le contrôleur du robot CS9 commande 3 sortes d'actionneurs : les moteurs du robot, les freins et les électrovannes. D'autres actionneurs spécifiques de l'application peuvent être commandés par les sorties sûres utilisateur (USO) du contrôleur de sécurité.

- (STO) (Safe Torque Off) est la fonction de sécurité qui inhibe le couple des moteurs ; elle est implémentée au niveau matériel, directement dans les amplificateurs du contrôleur.
- (SBC) (Safe Brake Control) est la fonction de sécurité qui coupe l'alimentation des freins et les contraint ainsi à se fermer immédiatement. La fonction de sécurité SBC contrôle l'ouverture inopinée des freins mais n'assure pas que le couple de freinage sera correct : un essai de freins régulier est nécessaire pour cela.
- (SVC) (Safe Valve Control) est la fonction de sécurité qui coupe l'alimentation des électrovannes. Le comportement qui en résulte dépend du circuit pneumatique, qui doit être conçu de telle façon que l'effecteur (et éventuellement la pièce qu'il porte) reste dans un état sûr quand les électrovannes sont inhibées.
- Les actionneurs spécifiques de l'utilisateur peuvent être commandés à l'aide d'une sortie sûre utilisateur (USO) reflétant soit l'état d'alimentation du robot (état STO), soit l'état d'arrêt sûr (état SS2).



Les fonctions de sécurité STO, SBC et SVC sont de niveau SIL3/PLe.

#### 2.4.2 - FONCTIONS DE SÉCURITÉ D'ARRÊT

M0004643.1

- La catégorie d'arrêt sûr 0 (SS0) est l'activation simultanée des fonctions de sécurité d'inhibition (STO, SBC et SVC). Elle entraîne un arrêt sur les freins non contrôlé et, dans la mesure du possible, n'est utilisée que s'il n'y a aucune autre solution.
- La catégorie d'arrêt sûr 1 (SS1) est une fonction de sécurité qui déclenche un arrêt contrôlé du robot ; le temps d'arrêt est un paramètre de sécurité configurable. La fonction de sécurité SS0 est ensuite activée quand le robot est arrêté ou quand le délai spécifié est écoulé.
- La catégorie d'arrêt sûr 2 (SS2) est une fonction de sécurité qui déclenche un arrêt contrôlé du robot ; le temps d'arrêt est un paramètre de sécurité configurable. La fonction de sécurité de surveillance SOS et la fonction de sécurité d'inhibition SVC sont activées lors de l'arrêt du robot. Tout mouvement déclenche ensuite l'activation immédiate de la fonction de sécurité SS0.



Les fonctions de sécurité SS0, SS1 et SS2 sont de niveau SIL3,PLe.



### 2.4.3 - FONCTIONS DE SÉCURITÉ DE LIMITATION

M0004644.1

Les entrées sûres utilisateur et les codeurs sûrs du robot CS9 sont contrôlés en continu afin d'exécuter des fonctions de sécurité supplémentaires :

- (SOS) (Safe Operating Stop) est la fonction de sécurité qui vérifie que les axes du robot restent dans une position fixe (dans des limites de tolérance réduites) ; la fonction de sécurité SS0 est activée si la tolérance est dépassée.
- (SLP) (Safely-Limited Position) est la fonction de sécurité qui surveille la position du robot, à la fois sur les coordonnées articulaires (SLPj) et sur les coordonnées cartésiennes (SLPc), en la comparant à des limites configurables. Les limites cartésiennes sont définies avec des volumes géométriques ; la présence dans les limites cartésiennes est surveillée pour un ensemble de points de contrôle configurables (« outil sûr »). Les fonctions de sécurité SLPj et SLPc nécessitent un référencement de sécurité dans la cellule ; les zones interdites nécessitent habituellement un essai de freins régulier au cas où le robot devrait être stoppé sur ses freins après une panne du système (par ex. coupure de courant).
- (SLS) (Safely-Limited Speed) est la fonction de sécurité qui surveille la vitesse du robot, à la fois sur les vitesses articulaires (SLSj) et sur les vitesses cartésiennes (SLSc), en la comparant à des limites configurables. La vitesse cartésienne est surveillée pour un ensemble de points de surveillance configurables. La fonction de sécurité SLSj peut être utilisée sans contrainte mais la fonction SLSc nécessite un référencement de sécurité dans la cellule. En raison de la précision limitée de la vitesse de sécurité, la vitesse commandée par le contrôleur de mouvement est jusqu'à 20% inférieure à la limite de vitesse de sécurité. La vitesse est contrôlée à l'aide de VAL 3 TCP et de l'outil, qui peut être différent du TCP de sécurité et des protections.
- La surveillance de zone sûre (SZM) est une combinaison de limites de position sûres, et d'arrêt de sécurité ou de limite de vitesse sûre : l'arrêt de sécurité ou la limite de vitesse sûre ne prend effet que dans les limites de position.
- Les entrées sûres utilisateur (USI) sont surveillées en continu afin de déclencher une réaction du robot : arrêts sûrs SS1 ou SS2, positions limitées de sécurité (SLP), vitesse limitées de sécurité SLS ou zones de sécurité SZM. Les quatre entrées sûres du contrôleur de sécurité peuvent être configurées indépendamment, à quelques restrictions près :
  - L'entrée sûre USIA est réservée à l'arrêt d'urgence WMS quand l'interface WMS est utilisée.
  - L'entrée sûre USID peut être utilisée pour le référencement sûr quand celui-ci est requis.
- Le profil esclave FSoE est un autre moyen de déclencher une réaction du robot à partir d'un PLC sûr externe. N'importe quelle entrée sûre utilisateur peut être remplacée par un signal FSoE équivalent.



Les fonctions de sécurité SOS, SLP, SLS et SZM sont de niveau SIL3,PLe.

### 2.4.4 - FONCTIONS DE SÉCURITÉ DE CONTRÔLE

M0004645.1

- Les modes de contrôle définissent des états de sécurité utilisés pour commander l'activation ou l'inhibition d'autres fonctions de sécurité ; les modes de sécurité du robot CS9/TX2 sont définis par le mode de marche, le mode de maintenance, le mode SP2 et le mode RBR.
- Le contrôle du redémarrage est la fonction de sécurité qui maintient le robot dans l'état sûr après un arrêt sûr ou après le démarrage de la machine, jusqu'à ce qu'il reçoive un signal d'acquiescement explicite du redémarrage (réinitialisation manuelle).

Le programme de sécurité propose des conditions de redémarrage configurables spécifiques après un arrêt SS2 sans réinitialisation manuelle.

- Le mode et le redémarrage peuvent aussi être contrôlés à partir du profil esclave FSoE.
- La connexion/déconnexion de SP2 sans arrêt d'urgence est une autre fonction de contrôle implémentée par le contrôleur de sécurité.



### 2.4.5 - FONCTIONS DE SÉCURITÉ DES SORTIES

Les trois sorties sûres du contrôleur de sécurité peuvent être configurées pour commander des périphériques externes ou pour envoyer des informations de sécurité à un PLC sûr externe.

- État en cours d'arrêt ou arrêté (arrêt d'urgence, arrêt de protection, arrêt sûr opérationnel).
- État d'alimentation.
- État du mode de marche.
- Informations pour le contrôle du redémarrage.
- État de vitesse réduite activé par USID.

Ces états de sécurité sont également disponibles dans le profil esclave FSoE.



## 3 - CONCEPTION DE LA MACHINE

### 3.1 - EXIGENCES DE SÉCURITÉ

#### 3.1.1 - RÈGLEMENTATIONS EN MATIÈRE DE SÉCURITÉ

M0000550.1

##### Usage préconisé

Un robot n'est pas un produit prêt à l'emploi. C'est une "quasi-machine" conçue pour être intégrée à une "machine" : la cellule robotisée. L'ensemble de cette machine doit être conforme aux réglementations de sécurité en vigueur avant d'être exploité.

Le robot Stäubli est conçu pour les applications industrielles, où l'opérateur est séparé d'un robot mobile par divers dispositifs de protection. Une proximité temporaire entre l'opérateur et le robot est possible en cas de collaboration ou lors des opérations de mise au point et de maintenance. Les risques supplémentaires encourus doivent être gérés par l'intégrateur.

##### Réglementations européennes

Au sein de l'Union européenne, les réglementations de sécurité en vigueur pour les machines sont définies par la Directive Machines 2006/42/CE. Cette directive stipule qu'une évaluation des risques doit être effectuée afin de déterminer les exigences applicables en matière de santé et de sécurité. La machine doit alors être conçue et fabriquée en tenant compte des résultats de l'évaluation des risques. La directive définit les exigences essentielles et obligatoires en matière de santé et de sécurité.

Les normes internationales ont été développées pour fournir un cadre à l'application correcte de la Directive Machines. La Directive Machines et la liste des normes harmonisées sont disponibles à l'adresse <http://eur-lex.europa.eu>. En termes d'intégration du robot, l'application des spécifications de la norme EN ISO 10218-2:2011, d'après l'évaluation des risques réalisée par l'intégrateur, suppose la conformité aux exigences essentielles en matière de santé et de sécurité de la Directive Machines, couvertes par la norme.

La Directive Machines définit les procédures permettant d'évaluer la conformité des machines. Pour les machines complètes, la marque CE, accompagnée de la déclaration de conformité CE, suppose la conformité à la Directive. Pour les quasi-machines, la déclaration d'incorporation définit les exigences essentielles en matière de santé et de sécurité, ainsi que d'autres Directives applicables, qui sont satisfaites.

Le robot est livré avec sa déclaration d'incorporation. Une copie électronique de la déclaration, avec plusieurs traductions, est disponible sur le DVD du robot. Il est également possible de les demander au Support Clients Stäubli.

La déclaration d'incorporation du robot est basée sur la réalisation des exigences applicables des normes harmonisées suivantes :

- |   |   |
|---|---|
| ■ EN ISO 10218-1:2011                   | Robots et dispositifs robotiques - Exigences de sécurité pour les robots industriels - Partie 1                                   |
| ■ EN ISO 13849-1:2015                   | Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1                                       |
| ■ EN 60204-1:2006 et EN 60204-1/A1:2009 | Sécurité des machines - Équipement électrique   |
| ■ EN 61000-6-4:2007 / A1:2011           | Compatibilité électromagnétique - Norme générique sur les émissions   |
| ■ EN 61000-6-2:2005                     | Compatibilité électromagnétique - Norme générique sur l'immunité  |
| ■ IEC/EN 62061:2005                     | Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables |

Il n'existe pas de norme réglementaire de l'OHSA (Occupational Safety and Health Administration) concernant les robots aux États-Unis. Cependant, la norme ANSI/RIA R15.06-2012 est référencée comme étant la norme applicable aux systèmes robotisés. Cette norme est harmonisée pour être essentiellement identique aux normes ISO 10218-1:2011 et ISO 10218-2:2011, comme l'est la norme CAN/CSA-Z434-03 (R2013) pour le Canada. Ces normes ISO pour les robots industriels ont également été adoptées en Corée.

Chaque pays peut définir des normes de sécurité supplémentaires, et avoir des règlements locaux spécifiques. Par exemple, la norme UL pour les robots et les équipements robotisés UL 1740 contient des exigences supplémentaires pour le robot et la sécurité électrique.

Pour la version UL, le robot a été contrôlé par rapport aux normes suivantes :

- Norme UL 1740      Robots et matériel robotique
- Norme RIA15-06      Norme nationale américaine pour les robots industriels et les systèmes robotiques. Exigences de sécurité.
- Norme CSA Z434-03      Robots industriels et systèmes robotiques. Exigences générales de sécurité.
- Norme NFPA 79      Norme électrique pour les machines industrielles
- Norme NFPA 70      NEC code national de l'électricité

Pour des informations relatives au règlement (CE) REACH 1907/2006, consulter l'adresse internet suivante : <https://www.staubli.com/en/robotics-reach/>

### 3.1.2 - EXIGENCES ESSENTIELLES DE SANTÉ ET DE SÉCURITÉ

M0000591.1

Lors de la prise en compte des exigences essentielles de santé et de sécurité établies par la Directive Machines, l'intégrateur devra satisfaire aux exigences liées au robot non satisfaites ou partiellement satisfaites par Stäubli. Ces exigences sont décrites dans les manuels d'utilisation du robot.

Les exigences générales liées au robot sont les suivantes :

#### Principes d'intégration de la sécurité

La machine finale doit être conçue de manière à ce que le robot qui y est intégré fonctionne conformément à ses caractéristiques et qu'il soit utilisé, mis au point et entretenu sans risque.

#### Ergonomie

Les conditions de mise au point du robot (apprentissage de points, réglage des mouvements) seront définies lors de la conception de l'effecteur et de l'environnement de la cellule.

#### Dispositifs de contrôle et d'information

Les moyens d'interaction entre le robot et l'opérateur doivent satisfaire les exigences de la Directive Machines.

En présence de plusieurs robots fonctionnant en mode automatique, le système de contrôle doit être conçu de manière à ce que l'utilisation d'un robot empêche l'utilisation des autres, à l'exception des commandes d'arrêt et d'arrêt d'urgence.

#### Risques liés aux éléments mobiles

Les risques de contact entre le robot et l'opérateur doivent être prévenus au moyen de dispositifs de protection appropriés.

#### Instructions

Si le robot est intégré dans une machine finale utilisée dans un pays différent de celui où le robot a été livré, il est possible que la notice d'instructions du robot doive être traduite par l'intégrateur.

La notice d'instructions de la machine finale doit inclure la notice du robot ou les parties de cette notice qui sont nécessaires pour utiliser, mettre au point et entretenir le robot.

La documentation commerciale de la machine finale doit être conforme à la notice d'instructions du robot.

### 3.1.3 - CONCEPT DE SÉCURITÉ

Afin d'assurer une sécurité adéquate de la machine et de satisfaire les exigences réglementaires de sécurité, une stratégie de réduction des risques, telle que la propose par exemple la norme ISO 12100-1:2010, doit être mise en place. Cette stratégie identifie les risques en présence et les moyens de les réduire : ceci constitue le concept de sécurité. Les fonctions de sécurité à implémenter sont déterminées dans le cadre du concept de sécurité. Les exigences concernant la définition et la conception des fonctions de sécurité sont exposées dans les normes ISO 13849-1 ou IEC 62061.

Certaines fonctions de sécurité de la machine se basent sur les fonctions de sécurité du robot. Il importe de s'assurer que ces dernières soient utilisées de façon adéquate et que le comportement de la machine en résultant atteigne les objectifs de sécurité attendus. La mise au point et la validation des paramètres de sécurité du robot ne peuvent donc être effectués que dans le contexte du concept de sécurité de la machine entière.

Les informations du concept de sécurité nécessaires pour la configuration de sécurité du robot comprennent :

- **Alimentations électriques de sécurité**  
Le concept de sécurité doit identifier les caractéristiques électriques des appareils à interfacer avec les pièces liées à la sécurité du robot.
- **Mode de marche**  
Le concept de sécurité doit identifier la manière dont les modes de marche sont définis et partagés entre les différents dispositifs de la machine.
- **Contrôle du redémarrage**  
Le concept de sécurité doit identifier la manière dont les signaux d'acquiescement du redémarrage (réinitialisation manuelle) sont déclenchés et partagés entre les différents dispositifs de la machine.
- **Arrêts d'urgence**  
Le concept de sécurité doit identifier la manière dont les signaux d'arrêt d'urgence sont déclenchés et partagés entre les différents dispositifs de la machine.
- **Arrêts de protection**  
Le concept de sécurité doit identifier les signaux de sécurité qui vont arrêter le robot, avec leurs caractéristiques : mode de marche, contrôle du redémarrage, catégorie d'arrêt, temps d'arrêt, répercussions sur d'autres dispositifs.
- **Les fonctions de sécurité de limitation (limites de position et de vitesse)**  
Le concept de sécurité doit identifier les fonctions de sécurité de limitation à utiliser et leur but ainsi que leurs caractéristiques : limites de position et de vitesse, mode de marche pour l'activation et signaux (le cas échéant).
- **Distances de séparation**  
Le concept de sécurité doit identifier les distances de séparation entre le robot et les dispositifs de protection de la machine, en précisant les contraintes associées de position du robot, de vitesse et de distance.
- **Espace de travail restreint**  
Le concept de sécurité doit identifier les limites dans l'espace que le robot ne doit pas dépasser, le principe sur lequel elles se fondent (limites logicielles, arrêts sur butées, solidité des barrières) et les contraintes associées de position et de vitesse du robot.

### 3.1.4 - VALIDATION DU CONCEPT DE SÉCURITÉ, FAISABILITÉ

M0004648.1

Il est préférable de revoir le concept de sécurité avec le responsable de la sécurité des machines dès les premières étapes de la conception, afin de s'assurer que les différentes parties soient d'accord sur les mesures de réduction des risques : tout changement dans le concept de sécurité peut avoir des répercussions importantes sur la conception de la machine.

Il convient également de s'assurer que les différents composants de sécurité présentent les fonctions attendues et peuvent être interfacés. Les points typiques à vérifier pour les composantes de sécurité concernant le robot sont les suivants :

- Niveau de performances/d'intégrité PL/SIL

Le niveau de performances des fonctions de sécurité de la machine doit être calculé à partir de la caractéristique de sécurité des composants de sécurité en question et comparé au niveau de performances de sécurité visé.

- Compatibilité entre les alimentations électriques de sécurité

Différentes technologies d'E/S numériques sûres peuvent ne pas être compatibles : par exemple, il convient de vérifier que les impulsions de test d'autodiagnostic des sorties numériques sûres sont acceptées (ignorées) par le dispositif connecté.

- Détection des défauts du câblage de sécurité

Les alimentations électriques de sécurité doivent être compatibles mais avoir néanmoins une détection des défauts de câblage compatible avec le niveau de performances de sécurité visé (par ex. détection des courts-circuits au 0V, 24V ou entre les signaux de sécurité). La désactivation du contrôle des impulsions de test sur les entrées sûres peut créer des alimentations compatibles mais inadéquates.

- Codage de signaux redondants

Les signaux de sécurité redondants peuvent être codés de différentes manières, par exemple avec 2 contacts normalement fermés (NF) ou 1 contact normalement fermé et 1 normalement ouvert. Les dispositifs interfacés doivent prendre en charge les codages compatibles.

- Nombre d'entrées et sorties numériques sûres

Le robot permet de nombreuses configurations différentes de ses entrées et sorties sûres mais ne possède qu'un nombre limité de contacts. Il faut veiller à ce qu'un nombre suffisant d'entrées et de sorties numériques soient disponibles, y compris pour des usages spécifiques tels que des entrées pour le référencement sûr ou des sorties pour les avertissements de sécurité.

- Boucles de blocage

Le chaînage des arrêts d'urgence, des arrêts de protection ou du signal de contrôle du redémarrage peut produire des boucles de blocage si deux appareils s'attendent mutuellement pour annuler une condition d'arrêt.

- Nombre et capacités des fonctions de surveillance de la position et de la vitesse

Le robot possède un nombre limité de fonctions de position et de vitesse et n'est pas conçu pour coder des volumes complexes autour de lui-même ou de son outil : plus les volumes sont complexes, plus les phases de conception et de validation le sont également.

Les volumes de sécurité doivent être conçus pour résoudre seulement les problèmes de sécurité et non pour empêcher les collisions matérielles, pour lesquelles le contrôle des mouvements offre de meilleures solutions. Il importe de s'assurer que les capacités des fonctions de position et de vitesse permettent de coder les volumes entourant le robot et son outil.

Afin d'éviter les fausses alertes, une marge est toujours prévue entre les limites de sécurité et celles du contrôleur de mouvement : le robot bouge toujours à une vitesse inférieure à la limite de sécurité configurée.

- Distances de séparation

Une distance de séparation doit être calculée à l'aide du temps de réaction complet de la fonction de sécurité correspondante, qui inclut les temps de réaction de ses composants, avec des délais de détection et de transmission. Si le temps d'arrêt du robot est significativement réduit, il faut vérifier si le temps d'arrêt configuré peut être réalisé et si les conséquences sur la durée de vie du robot sont acceptables.

- Espace de travail restreint

Il existe toujours une marge entre les limites de position vérifiées par le contrôleur de sécurité et les positions que le robot peut atteindre dans les conditions les plus défavorables, par exemple après une coupure de courant. Cette marge doit être prise en compte dans la conception de la cellule.

- Capteur de référencement

La procédure de référencement sûr nécessite le montage d'un capteur de référencement dans la cellule ; la technologie et le placement du capteur doivent convenir pour la procédure de référencement.

## **3.2 - NIVEAU DE PERFORMANCES/D'INTÉGRITÉ DES FONCTIONS DE SÉCURITÉ**

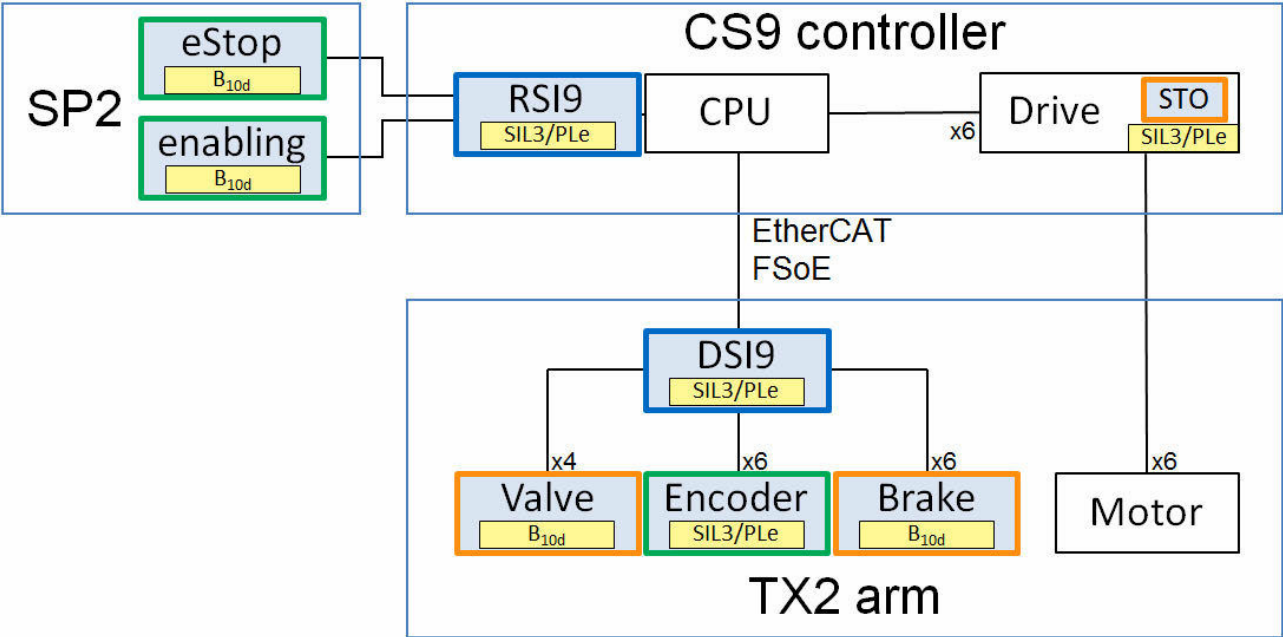
M0004649.1

Les niveaux de performances et d'intégrité des fonctions de sécurité (PL/SIL) sont spécifiés uniquement pour des conditions d'utilisation adéquates, qui sont détaillées dans les manuels, notamment :

- Les conditions générales d'utilisation (conditions d'environnement, alimentation électrique).
- Les conditions d'utilisation spécifiques des fonctions (paramétrage, tests réguliers, comportement en cas de défaut).
- Les conditions d'utilisation organisationnelles (recherche des défauts de sécurité, contrôle des accès à la configuration de sécurité et à la maintenance).

3.2.1 - ÉLÉMENTS DE SÉCURITÉ

M0004650.1



I0003913

| Anglais        | Traduction          | Anglais | Traduction |
|----------------|---------------------|---------|------------|
| eStop          | Arrêt d'urgence     | Encoder | Codeur     |
| Enabling       | Bouton d'activation | Brake   | Frein      |
| CS9 controller | Contrôleur CS9      | Motor   | Moteur     |
| Drives         | Amplificateurs      | TX2 arm | Bras TX2   |
| Valve          | Electrovanne        |         |            |

Figure 3.1

|                   | Element                     | B <sub>10d</sub> (nb. de cycles) | PFH <sub>d</sub> (h <sup>-1</sup> ) | SIL <sup>(1)</sup> | PL <sup>(1)</sup> |
|-------------------|-----------------------------|----------------------------------|-------------------------------------|--------------------|-------------------|
| Capteur/entrée    | SP2 arrêt d'urgence         | 250000                           | -                                   | -                  | -                 |
|                   | Bouton de validation du SP2 | 1000000                          | -                                   | -                  | -                 |
|                   | WMS arrêt d'urgence         | 250000                           | -                                   | -                  | -                 |
|                   | Encoder                     | -                                | 0.02 10 <sup>-7</sup>               | HFT1 - SIL3        | Cat 4 - PLe       |
| Logique           | RSI9                        | -                                | 0.09 10 <sup>-7</sup>               | HFT1 - SIL3        | Cat 4 – PLe       |
|                   | DSI9                        | -                                | 0.18 10 <sup>-7</sup>               | HFT1 - SIL3        | Cat 4 – PLe       |
| Actionneur/sortie | Électrovanne                | Voir le manuel du bras           | -                                   | -                  | -                 |
|                   | STO (6 amplificateurs)      | -                                | 0.13 10 <sup>-7</sup>               | HFT1 - SIL3        | Cat 4 – PLe       |

(1) Temps de mission 20 ans.



### 3.2.2 - FONCTIONS DE SÉCURITÉ D'INHIBITION

M0004651.1

|     | Description  | Act. (1) | Cod. (2) | PFH <sub>d</sub> (h <sup>-1</sup> ) | SIL (3)         | PL (3)          |
|-----|--|----------|----------|-------------------------------------|-----------------|-----------------|
| STO | Maintenir les phases du moteur ouvertes                  | -        | -        | 0.22 10 <sup>-7</sup>               | HFT1 - SIL3     | Cat 4 - PLe     |
| SBC | Maintenir les contacts d'alimentation des freins ouverts | -        | -        | 0.27 10 <sup>-7</sup>               | HFT1 - SIL3 (4) | Cat 4 - PLe (4) |
| SVC | Maintenir les contacts d'alimentation des vannes ouverts | OFF      | -        |                                     |                 |                 |

- (1) Activation : - = toujours activé. ON/OFF : configurable, MARCHE ou ARRÊT par défaut. Opt. = option. Lic. = avec licence pour logiciel SafeCELL+.
- (2) Codeurs : Ret. = retour du codeur nécessaire, pas de référencement requis. Réf. = référencement requis. - = non requis.
- (3) Temps de mission 20 ans.
- (4) Les freins et les électrovannes sont commandés par un seul conducteur ; une exclusion des défauts est utilisée pour empêcher la possibilité d'un court-circuit au 24V dans le bras.

#### Conditions d'activation :

- Les fonctions de sécurité STO et SBC sont toujours activées sur tous les robots CS9/TX2. Certains bras ne sont pas équipés d'un frein sur tous les axes : voir le manuel du bras. La fonction de sécurité SVC est présente sur tous les robots CS9/TX2 mais désactivée par défaut. Voir le chapitre 3.3.6 pour l'activation de SVC.

#### Conditions d'utilisation :

- Les fonctions de sécurité d'inhibition ne sont pas directement accessibles : elles sont déclenchées après un arrêt sûr SS1 (voir le chapitre 3.2.3) ou après une alarme de sécurité (arrêt SS0).
- Pour un arrêt SS1, le délai et les conditions pour atteindre l'état sûr sont définis dans les fonctions de sécurité SS1.
- Pour un arrêt SS0, les fonctions de sécurité des freins suivantes sont définies au point 3.3.8.
- Les fonctions de sécurité SBC et SVC contrôlent la sécurité des commandes de freins et de électrovannes mais pas les freins ni les électrovannes eux-mêmes : un essai de frein régulier est nécessaire pour contrôler la sécurité des freins (voir le chapitre 3.3.10) ; la sécurité des électrovannes dépend de la conception et de la condition d'utilisation du circuit pneumatique dans lequel elles sont utilisées.

#### Comportement en cas de défaut :

- Un défaut unique dans les fonctions de sécurité SBC et SVC est sans conséquences. Une exclusion des défauts est utilisée pour justifier l'impossibilité d'un court-circuit au 24V dans le câblage à l'intérieur du bras.
- Un défaut unique de la fonction de sécurité STO peut entraîner la présence de haute tension sur une phase du moteur, sans possibilité de produire un couple moteur.

## 3.2.3 - FONCTIONS D'ARRÊT

M0004652.1

|     |        | Description  | Act. (1) | Cod. (2) | PFH <sub>d</sub> (h <sup>-1</sup> ) | SIL (3)     | PL (3)      |
|-----|--------|--|----------|----------|-------------------------------------|-------------|-------------|
| SS0 |        | Activation immédiate de STO, SBC et (en option) SVC.                     | - (4)    | -        | 0.40 10 <sup>-7</sup>               | HFT1 - SIL3 | Cat 4 - PLe |
| SS1 | SP2-ES | Arrêt contrôlé dans un délai configurable, suivi de l'activation de SS0. | -        | -        | 0.57 10 <sup>-7</sup>               |             |             |
|     | SP2-EN |  | -        | -        | 0.82 10 <sup>-7</sup>               |             |             |
|     | WMS-ES |  | Opt.     | -        | 0.57 10 <sup>-7</sup>               |             |             |
|     | USER   |  | ON       | -        | 0.40 10 <sup>-7</sup>               |             |             |
| SS2 | SP2-EN | Arrêt contrôlé dans un délai configurable, suivi de l'activation de SOS. | OFF      | Ret.     | 0.94 10 <sup>-7</sup>               | HFT1 - SIL3 | Cat 4 - PLe |
|     | USER   |  | OFF      | Ret.     | 0.52 10 <sup>-7</sup>               |             |             |

- (1) Activation : - = toujours activé. ON/OFF : configurable, MARCHE ou ARRÊT par défaut. Opt. = option. Lic. = avec licence pour logiciel SafeCELL+.
- (2) Codeurs : Ret. = retour du codeur nécessaire, pas de référencement requis. Réf. = référencement requis. - = non requis.
- (3) Temps de mission 20 ans.
- (4) SS0 n'est pas directement activable mais est activée après un arrêt SS1 ou une alarme de sécurité.

Conditions d'activation :

- Les arrêts sûrs par les dispositifs d'urgence et le bouton d'activation SP2-ES et SP2-EN sont toujours activés quand le SP2 est connecté au contrôleur CS9.
- L'arrêt d'urgence WMS est activé quand l'option WMS est utilisée ; l'utilisation de WMS est un paramètre de sécurité (voir chapitre 5.4.1).
- Les arrêts sûrs SS1-USER sont déclenchés par les 4 entrées sûres différentes du contrôleur CS9 ; ils peuvent être modifiés ou désactivés au moyen des paramètres de sécurité.
- Chaque entrée sûre du contrôleur CS9 peut être configurée pour déclencher un arrêt SS2 au lieu du comportement SS1 par défaut.

Conditions d'utilisation :

- Le temps d'arrêt du système et les arrêts sûrs utilisateur sont un paramètre de sécurité (voir chapitre 3.3.7).
- L'activation de la fonction SVC avec des arrêts SS0 est un paramètre de sécurité (voir chapitre 3.3.6).
- Le dispositif d'activation SP2 peut être configuré pour déclencher un arrêt SS2 au lieu de SS1 (voir chapitre 3.3.4.2).
- Les arrêts SS1 décrits contrôlent la sécurité des commandes de freins et de électrovannes mais pas des freins et électrovannes eux-mêmes (voir chapitre 3.2.2).
- Le PFH<sub>d</sub> du bouton d'activation SP2 est basé sur une utilisation moyenne ≤ 10 fois/jour et une utilisation moyenne de la position de panique ≤ 1 fois/jour.
- Le PFH<sub>d</sub> de l'arrêt d'urgence SP2 est basé sur une utilisation moyenne ≤ 1 fois/jour et un test annuel.

Comportement en cas de défaut :

- Un défaut pendant le temps d'arrêt entraîne un arrêt SS0 ; dans ce cas, le temps d'arrêt peut ne pas être respecté.
- Voir aussi le comportement des fonctions de sécurité STO, SBC et SVC en cas de défaut (voir chapitre 3.2.2).

## 3.2.4 - FONCTIONS DE SÉCURITÉ DE LIMITATION

|                  | Description  | Act. (1) | Cod. (2) | PFH <sub>d</sub><br>(h <sup>-1</sup> ) | SIL (3)        | PL (3)        |
|------------------|--|----------|----------|--|----------------|---------------|
| SOS              | Surveillance de l'immobilisation du robot, SS0 quand la limite de déplacement est dépassée   | OFF (4)  | Ret.     | 0.52<br>10 <sup>-7</sup>               | HFT1 -<br>SIL3 | Cat4 -<br>PLe |
| SLPj             | Surveillance des positions articulaires du robot avec anticipation basée sur la décélération maximale, SS0 quand une limite est dépassée | OFF      | Repère   |  |                |               |
| SLSj             | Surveillance de la vitesse des articulations du robot, SS0 quand une limite est dépassée   | ON       | Ret.     |  |                |               |
| SLPc             | Surveillance de la position cartésienne des points de contrôle, SS0 quand une limite est dépassée  | Lic.     | Repère   |  |                |               |
| SLS <sub>c</sub> | Surveillance de la vitesse cartésienne des points de contrôle, SS0 quand une limite est dépassée   | Lic.     | Repère   |  |                |               |
| SZM              | Surveillance des zones cartésiennes, SS0 quand une limite de vitesse est dépassée dans la zone   | Lic.     | Repère   |  |                |               |

- (1) Activation : - = toujours activé. ON/OFF : configurable, MARCHE ou ARRÊT par défaut. Opt. = option. Lic. = avec licence pour logiciel SafeCELL+.
- (2) Codeurs : Ret. = retour du codeur nécessaire, pas de référencement requis. Réf. = référencement requis. - = non requis.
- (3) Temps de mission 20 ans.
- (4) SOS n'est pas directement activable mais est activée après un arrêt SS2.

## Conditions d'activation :

- La fonction de sécurité SOS n'est pas directement accessible : elle est déclenchée après un arrêt sûr SS2 (voir chapitre 3.2.3).
- Les fonctions de sécurité utilisant la position ou la vitesse cartésienne du robot nécessitent l'installation de la licence SRC SafeCELL+.
- Les fonctions de sécurité de limitation SOS-SLP-SLS-SZM nécessitent l'activation du retour du codeur sûr (voir chapitre 5.1).
- Les fonctions de sécurité de limitation SLP-SLS<sub>c</sub>-SZM nécessitent l'implémentation d'un référencement sûr (voir chapitre 3.3.9).
- Les fonctions de sécurité de limitation SLP-SLS-SZM peuvent être configurées pour être permanentes ou activées par une entrée sûre, dans tous les modes de marche ou seulement les modes automatiques.

## Conditions d'utilisation :

- Toutes les fonctions de sécurité de limitation sont configurables avec plusieurs paramètres de sécurité définissant les limites de surveillance.

## Comportement en cas de défaut :

- Un défaut au cours de la surveillance entraîne un arrêt SS0.
- Voir aussi le comportement des fonctions de sécurité STO, SBC et SVC en cas de défaut (voir chapitre 3.2.2).

## 3.2.5 - FONCTIONS DE SÉCURITÉ DES ENTRÉES/SORTIES

M0004654.1

|            | Description  | Act. (1) | Cod. (2)  | PFH <sub>d</sub> (h <sup>-1</sup> ) (3) | SIL (4)     | PL (4)     |
|------------|--|----------|-----------|---|-------------|------------|
| FS-BUS     | Bus de communication et de sécurité fonctionnelle                                    | Opt.     | -         | Négligeable                             | HFT1 - SIL3 | Cat4 - PLe |
| ES-OUT     | État d'arrêt d'urgence du robot (y compris le dispositif d'arrêt d'urgence du robot) | ON       | -         | 0.26 10 <sup>-7</sup>                   |             |            |
| ES-RST-OUT | État d'arrêt d'urgence du robot avec commande du redémarrage                         | OFF      | -         |   |             |            |
| SS2-OUT    | État d'arrêt d'urgence du robot (y compris le bouton d'activation)                   | OFF      | -         | 0.51 10 <sup>-7</sup>                   |             |            |
| RST-OUT    | État et signal de commande du redémarrage  | OFF      | -         | 0.09 10 <sup>-7</sup>                   |             |            |
| MODE-OUT   | Mode de marche MANU/AUTO   | ON       | -         |   |             |            |
| PWR-OUT    | État de l'alimentation du bras (STO)   | ON       | -         |   |             |            |
| VAL 3-OUT  | Inhibition d'une sortie sûre contrôlée par VAL 3                                     | OFF      | -         |   |             |            |
| SOS-OUT    | État de SOS  | OFF      | Ret.      | 0.39 10 <sup>-7</sup>                   |             |            |
| SLSD-OUT   | État de USID SLS   | OFF      | Ret./Cod. |   |             |            |

- (1) Activation : - = toujours activé. ON/OFF : configurable, MARCHE ou ARRÊT par défaut. Opt. = option. Lic. = avec licence pour logiciel SafeCELL+.
- (2) Codeurs : Ret. = retour du codeur nécessaire, pas de référencement requis. Réf. = référencement requis. - = non requis.
- (3) La PFH<sub>d</sub> inclut les dispositifs d'entrée du robot (WMS et arrêts d'urgence SP2, dispositif d'activation SP2) mais n'inclut pas les dispositifs d'entrée utilisateur (arrêt d'urgence supplémentaire ou capteur d'activation).
- (4) Temps de mission 20 ans.

## Conditions d'activation :

- Le PFH<sub>d</sub> du canal de communication sur un bus de sécurité fonctionnelle est négligeable, à condition que le robot et son câble d'interconnexion soient installés de la manière spécifiée dans le mode d'emploi du contrôleur.
- La fonction de sécurité de surveillance SOS-OUT nécessite un retour de l'encodeur sûr (voir chapitre 5.1.1).
- La fonction de sécurité de surveillance SLSD-OUT nécessite un retour de l'encodeur sûr (voir le chapitre 5.1.1), éventuellement un référencement sûr (voir le chapitre 3.3.9) selon la configuration de USID SLS.

## Conditions d'utilisation :

- La SS2-OUT PFH<sub>d</sub> se base sur une valeur moyenne du bouton d'activation SP2 de ≤ 10 fois/jour et une utilisation moyenne de la position de panique de ≤ 1 fois/jour.
- La ES-OUT PFH<sub>d</sub> se base sur une utilisation moyenne de l'arrêt d'urgence de ≤ 1 fois/jour et sur un test annuel.
- La sortie ES-OUT correspond à la position du bouton d'arrêt d'urgence, tandis que ES-RST-OUT reste au 0V jusqu'à ce que le signal d'acquiescement du redémarrage (réinitialisation manuelle) soit reçu. ES-RST-OUT ne revient pas en boucle dans un arrêt sûr, afin d'empêcher une boucle de blocage (voir chapitre 3.3.3).

Comportement en cas de défaut :

- Les sorties sûres (0V) sont inhibées en cas de défaut.

### 3.3 - RÉALISATION

M0005310.1



Consulter le manuel d'instruction de la CS9 comme référence pour le programme de sécurité Initial.

#### 3.3.1 - AMBIANCE DE TRAVAIL

M0004655.1

Les niveaux de performances et d'intégrité PL/SIL des fonctions de sécurité sont définis seulement quand le contrôleur et le bras sont utilisés dans les conditions d'environnement spécifiées en ce qui concerne :

- Température de fonctionnement.
- Température de stockage.
- Humidité.
- Altitude/Pression.
- Conditions d'installation.
- Vibrations.
- Indice de protection (IP).
- Propreté de l'air.

Les exigences de sécurité relatives à l'environnement de fonctionnement ne sont pas les mêmes pour le bras et le contrôleur : voir les chapitres des manuels correspondants concernant les conditions d'environnement. Nous consulter à propos des environnements spécifiques (rayons X, soudage laser,...).

#### 3.3.2 - INTERFACES ÉLECTRIQUES

##### 3.3.2.1 - Alimentations

M0004656.1

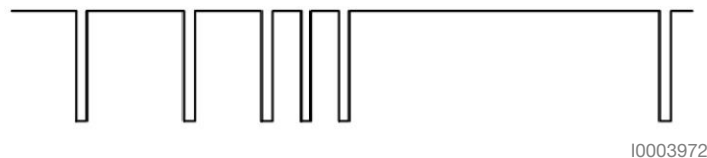
Afin d'assurer la sécurité électrique, l'alimentation électrique du robot doit être conforme à ses spécifications : voir le chapitre « Réseau électrique » du manuel du contrôleur.

L'équipement de sécurité fonctionnel doit être alimenté en basse tension sous 24V (TBTS/TBTP selon EN 61131-2) ; pour cela, le contrôleur du robot contient une alimentation électrique TBTP 24V interne. Une alimentation 24V externe peut être utilisée en option pour le contrôleur (J213) ou le bras (J711 sur l'interface RBR). Elle fournit un courant TBTS/TBTP de 24V.

##### 3.3.2.2 - Impulsions de test sur les entrées et sorties sûres

M0004657.1

Afin d'atteindre un niveau élevé de performances de sécurité, les signaux de sécurité numériques sous 24V sont marqués avec une séquence de brèves impulsions de test, répétées toutes les 16ms, comme le montre la figure ci-dessous :



I0003972

Figure 3.2

Différents motifs d'impulsions sont utilisés pour différents signaux de sécurité, afin qu'un court-circuit vers 0V, 24V et entre les signaux de sécurité soit rapidement détecté par la vérification de la présence des impulsions attendues.

Pour cela :

- des entrées sûres (USI) sont connectées aux sorties de test 24V dédiées (TDO) émettant les impulsions de test, de sorte que l'entrée sûre peut vérifier la présence des impulsions attendues.
- les sorties sûres (USO) comprennent, à l'intérieur du contrôleur CS9, une entrée de test qui recherche le signal de sortie afin de détecter les perturbations inattendues (impulsions manquantes ou surnuméraires).

L'utilisation d'impulsions de test peut imposer des contraintes au périphérique interfacé avec les signaux numériques de sécurité :

- Sur les entrées sûres, elles imposent l'utilisation de contacts secs ou d'optotransistors pour ouvrir et fermer le contact entre l'entrée sûre (USI) et la sortie de test dédiée (TDO).
- Sur les sorties sûres (USO), il faut s'assurer que le périphérique interfacé n'est pas affecté par les impulsions ni ne filtre celles-ci.

### 3.3.2.3 - Désactivation du contrôle des impulsions de test sur les entrées sûres

M0004658.1

Il est possible de désactiver les contrôles des impulsions de test sur les entrées sûres afin de pouvoir connecter directement celles-ci à la sortie 24V d'un dispositif externe. C'est typiquement la solution employée pour connecter un dispositif qui utilise lui aussi des impulsions de test, par exemple un PLC de sécurité.

Cette possibilité doit toutefois être utilisée avec prudence afin d'empêcher une diminution du niveau de performances de la fonction de sécurité en question. Le contrôle des impulsions de test est désactivé :

- par l'utilisation d'un programme de sécurité « noPulses » qui le désactive sur toutes les entrées sûres utilisateur (USIA/B/C/D, WMS). Les impulsions de test sur les entrées sûres système (arrêt d'urgence SP2 et bouton d'activation) sont maintenues.
- par l'utilisation d'un programme de sécurité « noPulsesJ101 » qui les désactive seulement sur J101-1/2/3/4 (entrées de mode de marche et de réinitialisation manuelle). Les contrôles des impulsions de test sur J101-7/8 et USIA/B/C/D sont maintenus.

Les impulsions de test sur les entrées sûres peuvent être désactivées sans risque quand le signal 24V connecté possède ses propres impulsions de test : le diagnostic des courts-circuits est alors effectué par l'équipement émetteur au lieu du robot.



## SÉCURITÉ

Quand le signal 24V connecté ne possède pas d'impulsion de test, il faut effectuer une AM-DEC pour déterminer les conséquences des courts-circuits non détectés au 24V ou entre les signaux de sécurité : il peut être nécessaire d'abaisser en conséquence le niveau de performances de la fonction de sécurité correspondante.

Pour connecter une sortie 24V externe à une entrée sûre du robot :

- La sortie de test (TDO) du robot n'est pas utilisée.
- Le dispositif externe et le contrôleur de sécurité doivent avoir la même masse 0V : le 0V du dispositif externe doit être connecté au contact J213-4 du contrôleur du robot.

Pour connecter une sortie sûre du robot à l'entrée sûre d'un dispositif externe :

- L'entrée du dispositif externe doit être configurée pour désactiver le contrôle des impulsions de test, qui est déjà assuré par le contrôleur du robot.
- Le dispositif externe et le contrôleur de sécurité doivent avoir la même masse 0V : le 0V du dispositif externe doit être connecté au contact J213-4 du contrôleur du robot.

Voir les instructions de câblage dans le manuel des schémas électriques du contrôleur CS9.

**3.3.2.4 - Codage de signaux de sécurité**

Selon le signal et l'équipement, certains signaux de sécurité peuvent être codés avec 2 contacts normalement fermés (NF) ou un contact normalement ouvert (NO) et un normalement fermé (NF). L'utilisation de 1 contact NO et 1 contact NF n'est toutefois pas prise en charge sur les entrées sûres avec le programme de sécurité du robot.

3.3.3 - PROFIL ESCLAVE (FSOE)

3.3.3.1 - Activation du profil

M0004660.1

L'activation du profil esclave nécessite :

- le programme de sécurité Initial (200.003 et versions supérieures), SafeCell ou SafeCell+ (1.000 et versions supérieures).



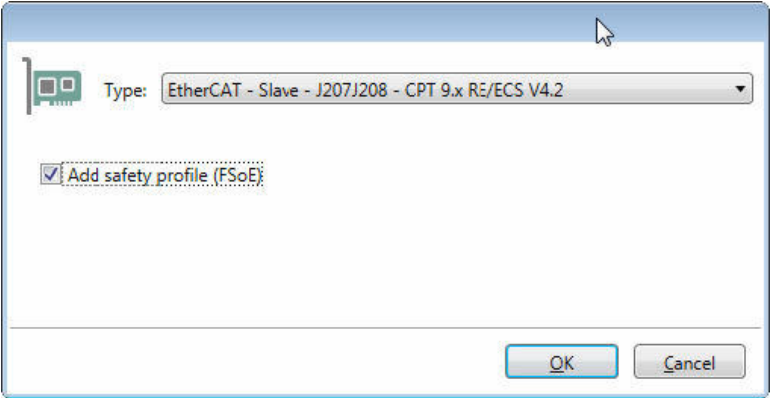
Les caractéristiques disponibles avec le profil esclave dépendent de la version du programme de sécurité : le dispositif d'activation et la commande d'arrêt SS2 ne sont pas disponibles dans la version Initial.

- Le profil esclave n'est pas disponible avec le programme de sécurité 200.x.
- L'activation du paramètre de sécurité profile\_activate.

Les entrées et sorties du profil sont activées par défaut, mais le robot ne détecte pas la coupure de la connexion entre le robot et le FSoE maître : le FSoE maître n'a alors pas le contrôle sûr du robot. Le contrôle sûr du robot par un PLC externe est activé avec le paramètre de sécurité profile\_activate.

- La configuration des esclaves Ethernet du contrôleur CS9.

Celle-ci est décrite dans le manuel d'instructions du contrôleur CS9 (configuration des esclaves RT Ethernet). Il ne faut pas oublier de sélectionner le profil de sécurité et de transférer la configuration de l'esclave au contrôleur CS9.



I0003914

Figure 3.3

- La configuration du FSoE maître.

La configuration de l'esclave (fichier ESI) peut être exportée à partir de l'outil Physical IOs de SRS.



Le temps de réponse le plus défavorable avec une communication FSoE est donné par le délai configuré du chien de garde du protocole de configuration. Ce temps influe sur le calcul des distances de séparation (voir chapitre 3.3.7).

- La configuration de l'adresse du FSoE esclave du contrôleur CS9.

L'adresse par défaut est 1. Elle peut être modifiée à l'aide du paramètre de sécurité profile\_address.



L'utilisation du profil de sécurité n'inhibe pas les entrées de sécurité sur J100 et J101 :

- Le choix d'un mode de marche sur J100 entre en conflit avec le choix du mode de marche du profil de sécurité.
- Les entrées sûres de J100 et J101 (7/8) doivent être câblées ou désactivées en mode automatique comme manuel, afin d'empêcher l'activation systématique des fonctions de sécurité correspondantes.

|                  |                        |
|------------------|------------------------|
| profile_activate | Voir le chapitre 5.5.1 |
| profile_address  | Voir le chapitre 5.5.1 |



### 3.3.3.2 - Entrées de profil

Les entrées de profil sont les signaux de sécurité envoyés par le RSI9 au PLC sûr externe.

| Bit | Nom               | Description  |
|-----|-------------------|--|
| 0   | manualSlow        | <b>ON</b> : Le mode de marche actuel est manuel lent.  |
| 1   | manualFast        | <b>ON</b> : Le mode de marche actuel est manuel rapide.  |
| 2   | autoLocal         | <b>ON</b> : Le mode de marche actuel est automatique local.  |
| 3   | autoRemote        | <b>ON</b> : Le mode de marche actuel est automatique déporté.  |
| 4   | maintenanceMode   | <b>ON</b> : Le mode de maintenance est activé.   |
| 5   | reducedSafety     | <b>ON</b> : Le mode de sécurité réduite est activé (vitesse rapide en mode manuel rapide).   |
| 16  | safeState         | <b>ON</b> : Le robot est dans l'état sûr (puissance des moteurs coupée, freins serrés).  |
| 17  | armPower          | <b>ON</b> : Les moteurs du robot sont mis sous puissance.  |
| 18  | fastSpeed         | <b>ON</b> : Les limites de vitesse du robot sont les limites en mode automatique ou les limites spécifiques de l'application (zones ou limites USI).<br><b>OFF</b> : Les limites de vitesse du robot sont les limites du mode manuel lent. |
| 19  | sosState          | <b>ON</b> : Le robot est dans l'état sûr ou arrêté sous tension avec la fonction de sécurité SOS activée.  |
| 20  | ss2state          | <b>ON</b> : Une condition d'arrêt sûr est active (SS0, SS1 ou SS2).  |
| 21  | ss1state          | <b>ON</b> : Une condition d'arrêt sûr est active (SS0 ou SS1).   |
| 22  | waitingRestartAck | <b>ON</b> : Un acquittement du redémarrage (réinitialisation manuelle) sera demandée pour le redémarrage quand la condition d'arrêt sûr sera levée.  |
| 23  | restartAck        | Signal d'acquiescement du redémarrage (réinitialisation manuelle) du robot.  |
| 24  | mcpRemoval        | <b>ON</b> : Le MCP est en cours de déconnexion ou de reconnexion.  |
| 25  | mcpPlug           | <b>ON</b> : Le bouchon du MCP est branchée.  |
| 26  | mcpEnabling       | <b>ON</b> : Le bouton d'activation du MCP est activé.<br><b>OFF</b> : Le bouton d'activation du MCP est débloqué ou doit être débloqué pour des essais.  |
| 27  | mcpEstop          | <b>ON</b> : L'arrêt d'urgence du MCP est activé.   |
| 40  | usiA              | État de l'entrée sûre USIA.  |
| 41  | usiB              | État de l'entrée sûre USIB.  |
| 42  | usiC              | État de l'entrée sûre USIC.  |
| 43  | usiD              | État de l'entrée sûre USID.  |
| 48  | zone1             | <b>ON</b> : Une protection de surveillance du robot se trouve dans la zone 1.  |

| Bit | Nom   | Description   |
|-----|-------|---|
| 49  | zone2 | <b>ON</b> : Une protection de surveillance du robot se trouve dans la zone 2. |
| 50  | zone3 | <b>ON</b> : Une protection de surveillance du robot se trouve dans la zone 3. |
| 51  | zone4 | <b>ON</b> : Une protection de surveillance du robot se trouve dans la zone 4. |


### 3.3.3.3 - Sorties de profil

M0004662.1

Les sorties de profil sont les signaux de sécurité envoyés par le PLC sûr externe au RSI9.

| Bit | Nom                           | Description  |
|-----|-------------------------------|--|
| 0   | manualSlow                    | <b>ON</b> : Sélectionne le mode de marche manuel lent <sup>(1)</sup> .   |
| 1   | manualFast                    | <b>ON</b> : Sélectionne le mode de marche manuel rapide <sup>(1)</sup> .   |
| 2   | autoLocal                     | <b>ON</b> : Sélectionne le mode de marche automatique local <sup>(1)</sup> .   |
| 3   | autoRemote                    | <b>ON</b> : Sélectionne le mode de marche automatique déporté <sup>(1)</sup> .   |
| 8   | ss1Ctrl                       | Quand le profil de sécurité est activé, ss1Ctrl doit rester <b>ON</b> pour permettre les mouvements du robot : <b>OFF</b> déclenche un arrêt SS1.<br>Quand le profil de sécurité n'est pas activé, <b>ON</b> déclenche un arrêt SS1. |
| 9   | enablingDeviceCtrl (SafeCell) | <b>ON</b> : Un bouton d'activation <sup>(2)</sup> est activé ; les mouvements sont autorisés dans les modes manuels.<br><b>OFF</b> : Le bouton d'activation SP2 doit être activé pour permettre les mouvements en mode manuel.       |
| 10  | ss2Ctrl (SafeCell)            | Quand le profil de sécurité est activé, ss2Ctrl doit rester <b>ON</b> pour permettre les mouvements du robot : <b>OFF</b> déclenche un arrêt SS2.<br>Quand le profil de sécurité n'est pas activé, <b>ON</b> déclenche un arrêt SS2. |
| 12  | restartAck                    | Un front descendant <b>ON</b> ↓ <b>OFF</b> déclenche un acquittement de redémarrage (réinitialisation manuelle).   |
| 13  | referencing                   | <b>ON</b> : Un capteur de référencement détecte le robot dans l'une des positions de référencement (voir chapitre 3.3.9.3).  |
| 24  | monitoringA                   | <b>ON</b> : La fonction de sécurité configurée pour USIA est activée <sup>(3)</sup> .  |
| 25  | monitoringB                   | <b>ON</b> : La fonction de sécurité configurée pour USIB est activée <sup>(3)</sup> .  |
| 26  | monitoringC                   | <b>ON</b> : La fonction de sécurité configurée pour USIC est activée <sup>(3)</sup> .  |
| 27  | monitoringD                   | <b>ON</b> : La fonction de sécurité configurée pour USID est activée <sup>(3)</sup> .  |

(1) Actif uniquement quand le mode de marche n'est pas choisi à partir de SP2 : mode\_WMS = 1 ou mode\_WMS=0 et mode\_MCP=0.

(2)  enablingDeviceCtrl permet d'utiliser un bouton d'activation externe pour commander le robot ou pour imposer l'utilisation simultanée de deux boutons d'activation.

(3) Voir l'avertissement au chapitre 3.3.3.1.

|                        |                        |
|------------------------|------------------------|
| mode_WMS               | Voir le chapitre 5.4.1 |
| Working mode selection | Voir le chapitre 5.5.1 |

### 3.3.4 - ARRÊTS DE SÉCURITÉ

#### 3.3.4.1 - Arrêts d'urgence et de protection

M0004663.1

Les arrêts d'urgence sont des arrêts sûrs spécifiques, facilement reconnaissables (bouton-poussoir rouge sur fond jaune), toujours efficaces quand ils sont activés et qui coupent la puissance motrice des actionneurs du robot et des autres actionneurs de la cellule. Le signal des dispositifs d'arrêt d'urgence connectés au robot est donc propagé au reste de la cellule via une sortie sûre (voir chapitre 3.2.5).

Les arrêts de protection sont des arrêts sûrs qui peuvent être configurés selon les risques qu'ils contrôlent : efficaces en mode manuel, automatique ou les deux, avec ou sans commande de redémarrage (réinitialisation manuelle), arrêt SS1 ou SS2, propagation à d'autres périphériques ou limitée au robot...

Par défaut, le contrôleur CS9 est configuré de telle façon que l'entrée sûre USIA soit connectée au dispositif d'arrêt d'urgence et que la sortie sûre USOA propage le signal d'arrêt d'urgence aux autres périphériques de la cellule.

USIB, USIC et USID sont configurées par défaut comme des arrêts de protection SS1, respectivement dans les modes manuels seulement, les modes automatiques seulement et tous les modes de marche.

Seule USIA peut être configurée comme un arrêt d'urgence. Quand l'interface WMS ne sert pas, elle peut aussi être configurée librement comme arrêt de protection.



L'arrêt d'urgence WMS utilise en interne les mêmes contacts que l'entrée USIA : quand l'interface WMS est utilisée, USIA est toujours configurée comme un arrêt d'urgence.

#### 3.3.4.2 - Dispositif d'activation

M0005311.1

Le dispositif d'activation est un arrêt de protection qui est déclenché, dans les modes manuels, quand le dispositif d'activation est relâché ou enfoncé à fond. Il est configuré, par défaut, comme un arrêt de protection SS1. Il peut être configuré comme un arrêt de protection SS2 à l'aide du paramètre de sécurité enabling\_SS2. Le profil esclave sur le bus de sécurité permet un contrôle avancé du dispositif d'activation à partir d'un automate programmable sûr externe :

- L'état du dispositif d'activation SP2 (enfoncé / relâché) peut être lu.
- L'arrêt de protection du dispositif d'activation peut être contrôlé.

Il est ainsi possible de partager un dispositif d'activation entre plusieurs dispositifs ou d'obliger à utiliser plusieurs dispositifs d'activation pour protéger plusieurs personnes dans la cellule.

|              |                          |
|--------------|--------------------------|
| enabling_SS2 | Voir le chapitre 3.3.4.2 |
|--------------|--------------------------|

#### 3.3.4.3 - États d'arrêt d'urgence

M0004664.1

Le contrôleur de sécurité définit différents états d'arrêt d'urgence accessibles dans VAL 3 ou au moyen d'une sortie sûre :

| État d'arrêt | Description   |
|--------------|---|
| ES-OUT       | Un bouton d'arrêt d'urgence relié au robot est activé.  |
| ES-RST-OUT   | Un bouton d'arrêt d'urgence relié au robot est activé ou a été relâché mais sans acquittement (en attente de réinitialisation manuelle).  |
| SS2-OUT      | Un arrêt sûr est actif, quelle que soit la condition (SS1 ou SS2). Peut être utilisé comme image de l'état du bouton d'activation en mode manuel.   |
| SOS-OUT      | Un arrêt sûr est actif et le robot est arrêté. Alors que le signal d'état SS2 est activé pendant que le robot s'arrête mais n'est pas encore arrêté, l'état SOS peut être utilisé pour n'autoriser une action que lorsque le robot est vraiment arrêté. |

#### 3.3.4.4 - Prévention des boucles de blocage

M0004665.1

Quand un état d'arrêt sûr du robot est utilisé comme signal d'arrêt pour d'autres périphériques de la cellule, il faut s'assurer que ce signal d'arrêt n'est pas renvoyé en boucle comme entrée d'arrêt sûr dans le contrôleur du robot : cela produirait une boucle de blocage et le robot ne pourrait pas sortir de l'état d'arrêt sûr.

Quand un PLC sûr est responsable de la commande d'arrêt d'urgence de la cellule :

- La sortie d'arrêt d'urgence du robot USOA, configurée comme ES-OUT, doit être connectée au PLC sûr afin que celui-ci puisse arrêter tous les autres périphériques de la cellule.
- L'acquittement de sécurité de l'arrêt d'urgence (réinitialisation manuelle) doit être géré par le PLC sûr et non par le robot. Ne pas utiliser la configuration ES-RST-OUT d'USOA
- Le PLC sûr doit utiliser une entrée d'arrêt de protection SS1 du robot, et non son entrée d'arrêt d'urgence, pour l'arrêter quand un arrêt d'urgence de la cellule est activé.

L'entrée d'arrêt d'urgence du robot USIA peut éventuellement être reconfigurée comme un arrêt de protection SS1 si elle n'est pas connectée à un dispositif d'arrêt d'urgence et si le WMS du robot n'est pas utilisé.



Configurée en entrée d'arrêt d'urgence, USIA doit être connectée à un dispositif d'arrêt d'urgence et non à un PLC sûr externe. Pour être connectée à un PLC sûr externe, elle doit être reconfigurée en arrêt de protection.

USOA, connectée à un PLC sûr, doit être configurée en ES-OUT ; la configuration ES-RST-OUT est destinée à contrôler un équipement autonome.

### 3.3.5 - INTERFACES DE CONTRÔLE

#### 3.3.5.1 - Mode de marche et acquittement de sécurité

M0004666.1

Le robot a besoin d'interfaces de contrôle de la sécurité pour sélectionner son mode de marche et confirmer les arrêts de sécurité (réinitialisation manuelle). Différentes solutions sont possibles, selon le résultat de l'analyse des risques :

- Le mode de marche et l'acquittement de sécurité du robot peuvent être contrôlés par des entrées sûres ; l'interface en option WMS9 offre une interface prête à l'emploi à cette fin, mais elle peut être remplacée par un système équivalent spécifique de l'utilisateur, connecté à l'interface J101-WMS.

Voir dans le manuel de schémas électriques de la CS9 (chapitre sur les entrées/sorties de sécurité) les spécifications de l'interface J101-WMS (sélection du mode de marche, redémarrage, arrêt d'urgence).



Les entrées d'arrêt d'urgence de l'interface J101-WMS sont câblées en interne vers des entrées sûres USIA. L'USIA doit rester configuré comme un arrêt d'urgence. Il peut être nécessaire de désactiver les impulsions de test vers l'USIA (voir chapitre 3.3.2).

- Le mode de marche et l'acquittement de sécurité du robot peuvent aussi être sélectionnés par le logiciel, à partir de l'interface SP2. Le mode de marche peut éventuellement être contrôlé par le logiciel, à l'aide de l'option remoteMcp du contrôleur. L'acquittement de sécurité peut être contrôlée dans VAL 3 à l'aide de la sortie logicielle RSI9 Qrestart ou par la cartographie des entrées/sorties (voir les entrées/sorties système du contrôleur). Lorsqu'il est sélectionné par logiciel, le profil utilisateur peut être utilisé pour contrôler l'accès à certains modes de marche.
- L'acquittement de sécurité peut aussi être désactivé sur le robot quand la commande du redémarrage est entièrement implémentée par un PLC externe ou dans VAL 3.
- Le redémarrage automatique après un arrêt SS2 peut être contrôlé avec différentes temporisations, afin d'imposer une réinitialisation manuelle après un arrêt prolongé, de déclencher un avertissement avant le redémarrage ou de redémarrer d'abord à petite vitesse.

Le choix des interfaces de contrôle de la sécurité fait partie du concept de sécurité. Il doit prendre en compte les risques potentiels, tels que :

- Le risque qu'une personne s'approche du robot en mode automatique sans arrêt sûr, en particulier lors des mises au point ou de la maintenance.
- Le risque que le mode de marche sélectionné ou affiché par le logiciel diffère du mode de marche effectif du contrôleur de sécurité ; le mode de marche effectif commande différentes fonctions de sécurité telles que les limites de vitesse de sécurité et les arrêts sûrs.
- Le risque que le robot redémarre dès qu'une condition d'arrêt de sécurité disparaît, en particulier lors de la maintenance.



Le risque d'un redémarrage inopiné du robot doit faire l'objet de davantage d'attention dans les applications collaboratives. Un signal visuel peut être utile pour indiquer quand le robot va probablement redémarrer ou quand un acquittement de sécurité (réinitialisation manuelle) est nécessaire pour le redémarrage.

Les interfaces de contrôle doivent se trouver à l'extérieur de l'espace protégé afin de dégager la vue sur l'espace restreint du robot.

Quelle que soit l'interface de sélection du mode de marche choisie, elle sert à demander un changement de mode au contrôleur de sécurité : le mode de marche ne change effectivement qu'après l'arrêt du robot, quand celui-ci est dans l'état sûr.

L'acquiescement du redémarrage de sécurité avec J101-4 est déclenchée par un front descendant du signal ; l'acquiescement du redémarrage de sécurité par la sortie logicielle RSI9 Qrestart est déclenchée en réglant celle-ci à 1. Le signal d'acquiescement du redémarrage du robot peut être transmis aux autres périphériques sur une sortie sûre (voir chapitre 5.5.4).

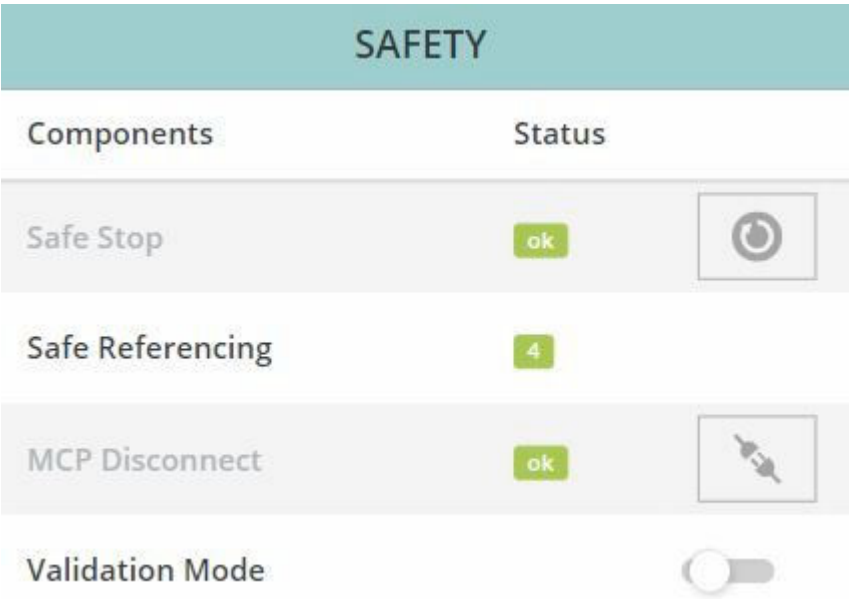


Après un dépassement de la position de sécurité de l'articulation ou des limites de vitesse (SLPj, SLSj), l'acquiescement par le logiciel Qrestart n'est pas effectif : le signal de confirmation du redémarrage de sécurité n'est accepté qu'à partir des entrées sûres J101-4 et FS-bus restartAck.

3.3.5.2 - Partage du MCP

M0004667.1

Un même MCP peut être partagé par plusieurs robots. Quand un robot fonctionne en mode automatique déporté, il est possible de le brancher et de le débrancher sans arrêt d'urgence, après en avoir fait la commande sur l'interface de sécurité du SP2. La commande désactive temporairement l'arrêt d'urgence du boîtier de commande manuel. Afin d'éviter les abus, après la commande, le MCP doit être remplacé à temps par un bouchon MCP spécifique.



I0005261

Figure 3.4

Le MCP peut être reconnecté par la suite, sans commande préalable, dans les 30s suivant le retrait du bouchon MCP.



SÉCURITÉ

Un MCP qui n'est connecté à aucun contrôleur de robot doit être rangé ou couvert afin que son bouton d'arrêt d'urgence inactif ne soit pas visible dans la cellule.

### 3.3.5.3 - Mode maintenance

Le contrôleur est livré avec un bouchon de maintenance permettant de commander le robot pendant son intégration dans la machine et les opérations de maintenance, quand les arrêts d'urgence des équipements de protection ne sont pas opérationnels. Quand le shunt de maintenance est connecté, le robot peut être commandé à partir du MCP, et ce quel que soit l'état des équipements périphériques :

- Les fonctions de sécurité d'arrêt et de limitation définies par l'utilisateur sont désactivées (USIA, USIB, USIC, USID, zones, limites de position et de vitesse).
- L'arrêt d'urgence MCP et le bouton de validation du MCP sont opérationnels.
- La sélection du mode de marche et l'acquiescement du redémarrage sont commandés depuis l'interface du MCP.

Le mode de marche automatique est possible mais à une vitesse limitée et sous le contrôle du bouton de validation, comme en mode manuel. Le mode automatique sans restriction avec le bouchon de maintenance est possible, mais dans le cadre d'opérations de maintenance spécifiques et uniquement par un personnel dûment formé.



#### SÉCURITÉ

- L'accès au bouchon de maintenance est réservé à un personnel formé.
- En mode maintenance, l'accès à la zone dangereuse doit être protégé au moyen de barrières amovibles ou balisé par des bandes de sécurité, et contrôlé par le personnel en service.
- (ISO 10218-1: 2011, 5.7.3) Le mode de marche manuel doit être, dans la mesure du possible, utilisé lorsque personne ne se trouve dans la zone dangereuse.

La fiche d'entretien active simultanément les modes de fonctionnement manuel lent, automatique local et automatique à distance (J101-1/2/3/5 câblés ensemble). Un automate programmable sûr externe peut imposer le mode maintenance de la même manière, en activant ces 3 modes de fonctionnement ensemble, à l'aide de l'interface J101 ou de celle du profil esclave.

### 3.3.6 - CONTRÔLE SÛR DES ACTIONNEURS EXTERNES

Le robot CS9/TX2 peut être utilisé pour contrôler de manière sûre un actionneur spécifique de l'utilisateur, soit à l'aide des électrovannes du bras, soit par les sorties de sécurité du contrôleur CS9.

Par défaut, les électrovannes sont entièrement commandées dans VAL 3 et les sorties de sécurité ne peuvent pas être contrôlées. Toutefois, il est possible de modifier la configuration par défaut afin que les électrovannes et les sorties sûres soient contrôlées dans VAL 3, du moment que le robot ne se trouve pas en arrêt SS0, SS1 ou SS2. Si le robot est en arrêt SS0, SS1 ou SS2, l'alimentation électrique des électrovannes et les sorties sûres sont mises de force à 0V.

Le contrôleur de sécurité s'assure ainsi que l'actionneur connecté ne peut plus être activé tant que le robot est en arrêt sûr.



#### SÉCURITÉ

Le comportement de l'actionneur externe reste sûr quand ses signaux de commande sont commutés sur 0V par le contrôleur de sécurité.

Le contrôle sûr des électrovannes est activé avec le paramètre `valves_safeControl` ; la commande par VAL 3 des sorties sûres est activée par les paramètres de sécurité `USOx_VAL3`.



Quand la commande sûre d'un actionneur est utilisée, l'application VAL 3 doit prendre en compte l'inhibition de l'actionneur lorsqu'un arrêt de sécurité est actif. L'état effectif de la sortie peut alors ne pas correspondre à l'état de la commande VAL 3.

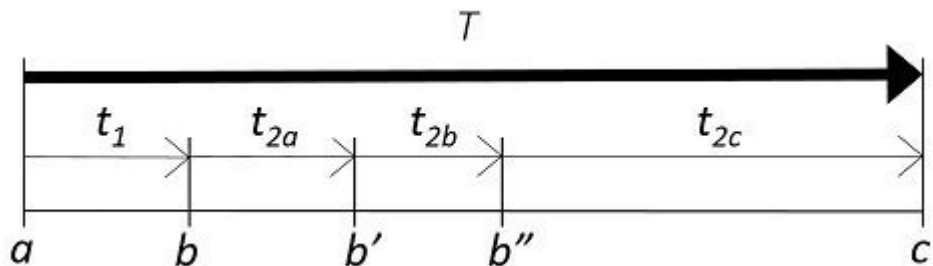


|                    |                        |
|--------------------|------------------------|
| valves_safeControl | Voir le chapitre 5.5.5 |
| USOx_VAL3          | Voir le chapitre 5.5   |

### 3.3.7 - DISTANCES DE SÉPARATION

M0004669.1

Une distance de séparation adéquate entre le robot et l'opérateur élimine le risque de contacts dangereux en assurant l'arrêt du robot avant que l'opérateur ait le temps de l'atteindre. Les exigences de sécurité pour le calcul des distances de séparation sont définies dans la norme ISO 13855:2010 :



I0005273

Figure 3.5

- $T$  : temps de réponse total, pour calculer la distance de séparation.
- $t_1$  : temps de réaction maximal du capteur.
- $t_{2a}$  : temps de transmission maximal du capteur au contrôleur de sécurité du robot.
- $t_{2b}$  : temps de réaction maximal du contrôleur du robot (32 ms).
- $t_{2c}$  : temps d'arrêt maximal du robot.

Le contrôleur de sécurité CS9/TX2 permet d'optimiser les distances de séparation en rendant le temps d'arrêt du robot  $t_{2c}$  configurable :

- Le temps d'arrêt maximal est défini par le paramètre de sécurité maxStopTime. Par défaut, celui-ci est réglé à 0.5s. Ce temps d'arrêt est utilisé pour les arrêts SP2 (dispositif d'activation ou arrêt d'urgence).
- Un temps d'arrêt réduit peut être assigné à chaque signal d'entrée de sécurité USIA, USIB, USIC et USID par la modification du paramètre de sécurité USIx\_maxStopTime.



### SÉCURITÉ

Le temps de réponse total est  $T = t_1 + t_{2a} + t_{2b} + t_{2c} + t_{2d}$ , où :

- $t_1$  et  $t_{2a}$  dépendent de l'équipement de la cellule ;  $t_{2a}$  doit inclure le délai du chien de garde FSoE pour les demandes d'arrêt FSoE.
- $t_{2b} = 32$  ms.
- $t_{2c} = \text{maxStopTime}$  pour l'arrêt d'urgence SP2.
- $t_{2c} = \text{maxStopTime}$  pour les demandes d'arrêt SS1/SS2 FSoE.
- $t_{2c} = \text{USIA\_maxStopTime}$  pour l'arrêt d'urgence WMS.
- $t_{2c} = \text{USIx\_maxStopTime}$  pour les arrêts USIx.



Le temps d'arrêt minimum dépend du robot et il est d'environ 100ms ; le robot peut ne pas être capable de s'arrêter sans erreur dans ce temps, selon sa vitesse, son accélération et sa charge. Typiquement, un robot qui marche à la vitesse nominale et la charge nominale s'arrête en 350ms environ avec la décélération nominale.



Le robot peut s'arrêter dans un temps très court mais les efforts accrus qui en résultent sur son mécanisme peuvent affecter sa durée de vie, selon la charge et la fréquence des arrêts. Les répercussions du temps d'arrêt sur la durée de vie doivent être évaluées à l'aide de l'outil Optimize Lab.



## SÉCURITÉ

Un temps d'arrêt très court peut entraîner une erreur du robot au cours de la phase d'arrêt : il en résulterait une usure prématurée des freins, auquel cas le temps d'arrêt paramétré ne pourrait plus être garanti. Il convient de vérifier que le robot peut s'arrêter sans erreur dans les conditions les plus défavorables.

|                  |  |
|------------------|--|
| maxStopTime      | Voir le chapitre <a href="#">5.2.3.1</a> |
| USlx_maxStopTime | Voir le chapitre <a href="#">5.2.3</a>   |

### 3.3.8 - ESPACE RESTREINT : DISTANCES D'ARRÊT ET ÉNERGIE RESTANTE

M0004670.1

Quand le robot est utilisé seulement sur une partie de son rayon d'action maximal, il est souvent judicieux de réduire les dimensions du périmètre de protection qui l'entoure afin d'optimiser l'encombrement de la cellule. Afin de protéger les personnes qui gravitent autour de la cellule, il faut s'assurer que le robot ne puisse pas outrepasser les limites du périmètre de protection. Il ne suffit pas de limiter le contrôleur de mouvement à une zone de travail réduite : la protection doit rester efficace en cas de défaillance du robot à grande vitesse, par exemple de défaut d'un variateur ou de coupure d'électricité inattendue.

Différentes solutions sont possibles :

- Des barrières suffisamment solides pour que le robot ne puisse pas les déformer dangereusement peuvent être disposées autour du robot. Elles doivent supporter l'énergie maximale du robot avec sa charge (à la vitesse maximale possible). L'énergie maximale du robot peut être réduite en abaissant sa vitesse maximale possible à l'aide des fonctions de sécurité SLS.
- L'espace maximal du robot peut être restreint à l'aide de la fonction de sécurité SLP ; l'espace qui peut être couvert par le robot et son terminal (espace restreint) doit être évalué à partir des limites de SLP et de la distance d'arrêt maximale du robot quand la limite est atteinte. La distance d'arrêt maximale du robot peut être réduite en abaissant la vitesse maximale possible.
- Ces deux solutions peuvent être combinées en calculant l'énergie maximale du robot au cours de son arrêt après les limites de SLP ; les barrières peuvent alors être placées à l'intérieur de l'espace restreint, de telle sorte que l'énergie restante du robot ne puisse pas causer de déformation dangereuse.

La réduction de la vitesse peut aussi n'être appliquée que lorsque des personnes sont détectées autour de la cellule, le robot continuant à pleine vitesse quand il n'y a pas de risque.

Dans tous les cas, l'optimisation de l'espace protégé s'appuie sur une estimation de la distance d'arrêt maximale et/ou de l'énergie du robot. Cette estimation est complexe car elle doit prendre en compte :

- tous les mouvements autorisés dans la plage de positions et de vitesse du robot, dans l'espace des articulations aussi bien que l'espace cartésien.
- la charge utile (masse et inertie) et le montage du robot.
- d'autres paramètres tels que le moment de freinage, les frictions internes, etc.

Stäubli propose une procédure de test pour mesurer les distances d'arrêt afin d'assurer la conformité à la norme ISO 10218-1, annexe B. Toutefois, les mesures de la distance d'arrêt ne sont représentatives de l'état du robot qu'au moment des essais car le comportement du robot peut varier en fonctionnement normal.

La norme ISO 10218-1, annexe B, précise que le fabricant doit prévoir la dégradation des performances d'arrêt et faire des recommandations sur le moment où un entretien est nécessaire. Par ailleurs, elle autorise l'utilisation d'un outil de simulation à la place d'essais réels.

La solution de Stäubli pour assurer la conformité à ces exigences est le calculateur de distance de freinage (BDC). Cet outil de simulation estime les distances d'arrêt et l'énergie restante au niveau de l'obstacle, en tenant compte de la dégradation des performances d'arrêt.

Prenez contact avec votre centre d'assistance clientèle Stäubli Robotics pour avoir accès à l'outil BDC et à la procédure d'essai.



## SÉCURITÉ

Quand l'espace restreint entourant le robot est calculé selon la distance d'arrêt, un essai de frein régulier doit être effectué afin de s'assurer que l'état des freins est encore compatible avec la distance d'arrêt estimée.

L'espace restreint peut ne pas être nécessaire en mode manuel, quand il est probable que les risques à petite vitesse soient déjà réduits à un niveau acceptable. Le paramètre de sécurité `jointLimits_manu` permet de définir aussi l'espace restreint dans les modes manuels ; un axe hors limites ne peut alors être ramené dans les limites qu'après la libération manuelle des freins ou en utilisant le mode de maintenance.

|                               |                                     |
|-------------------------------|-------------------------------------|
| <code>jointLimits_manu</code> | Voir chapitre <a href="#">5.3.1</a> |
|-------------------------------|-------------------------------------|

### 3.3.9 - RÉFÉRENCEMENT SÛR

M0005090.1

#### 3.3.9.1 - Principe

M0004674.1

Une procédure de calibrage est nécessaire pour configurer la géométrie du bras dans le contrôleur de mouvement. Les offsets de calibrage définissent la position de chaque codeur quand le robot se trouve dans sa position zéro. La précision du mouvement du TCP dépend de celle des offsets de calibrage.

Le contrôleur de sécurité a besoin de ses propres offsets de calibrage pour calculer les positions et vitesses cartésiennes sûres : la procédure de référencement sûr consiste à copier dans le contrôleur de sécurité les offsets de calibrage du contrôleur de mouvement.



## SÉCURITÉ

La procédure de référencement sûr est nécessaire pour les fonctions de sécurité SLPj, SLPc, SLSc et SZM.



La procédure de référencement sûr n'est pas nécessaire pour les fonctions de sécurité SS1, SS2 ni SLSj.

Afin de s'assurer que la position de sécurité est correcte, la procédure de référencement sûr peut être exécutée uniquement dans des positions fixes, définies comme des paramètres de sécurité et correspondant à l'emplacement d'un capteur connecté au contrôleur de sécurité. En outre, parce qu'un robot peut éventuellement atteindre la même position cartésienne dans différentes configurations, un contrôle de référencement dans une deuxième position est nécessaire pour vérifier que le premier référencement a été fait avec la configuration correcte.



Le capteur de référencement ne doit pas nécessairement être sûr (aucune redondance n'est nécessaire).



## SÉCURITÉ

La seconde position de référencement doit être définie de manière à ce que le capteur ne puisse pas être activé, si le premier référencement a été fait avec une configuration incorrecte du bras.

Différents capteurs peuvent être utilisés pour deux positions de référencement, mais il est habituellement possible d'utiliser un seul capteur qui peut être atteint dans deux positions différentes. Le programme de sécurité définit une seule entrée sûre pour le retour du ou des capteurs de référencement. Il n'est pas nécessaire que le capteur de référencement soit très précis car la position de sécurité est synchronisée avec la position de mouvement ; la portée de détection du capteur peut aller jusqu'à 10 ou 20 mm.. Différentes technologies de capteurs sont possibles ; il faut simplement vérifier qu'il n'est pas possible d'activer le(s) capteur(s) dans les deux positions de référencement différentes si le robot n'est pas correctement calibré.

Une fois les positions de référencement configurées dans les paramètres de sécurité refPos1\_Jx et refPos2\_Jx, la procédure de référencement consiste simplement à amener le bras dans la première position et à couper sa puissance puis, après 2.5 s, à l'amener dans la deuxième position et à s'y arrêter 0.5 s (ou davantage). Il n'est pas nécessaire de désactiver l'alimentation du bras dans la deuxième position. Le référencement peut être effectué en mode manuel ou automatique.



- L'état de référencement en cours est affiché sur la page Sécurité du MCP.
- Un programme VAL 3 de référencement sûr automatique est proposé avec le modèle safeCalibration VAL 3 livré avec chaque robot.

|            |                                     |
|------------|-------------------------------------|
| refPos1_Jx | Voir chapitre <a href="#">5.1.2</a> |
| refPos2_Jx | Voir chapitre <a href="#">5.1.2</a> |

### 3.3.9.2 - Test du référencement et restauration

M0004675.1

Le référencement sûr est conservé dans le temps et automatiquement restauré après le redémarrage, sauf si un axe du robot a bougé pendant l'arrêt du robot : dans ce cas, le référencement sûr doit être restauré en déplaçant le robot et en désactivant l'alimentation du bras dans la première position de référencement.

Il est en outre réinitialisé automatiquement chaque fois que le calibrage du contrôleur de mouvement est modifié, afin de s'assurer que les positions sûres et non sûres concordent toujours : un nouveau référencement sûr doit être effectué après une opération de maintenance qui a modifié certains offsets de calibrage.

Une fois établi, le référencement sûr reste valable tant qu'un décalage significatif d'un composant mécanique ne modifie pas sa géométrie, ce qui ne risque de se produire qu'après une collision grave du robot. Le risque de décalage mécanique non détecté après une collision doit être prévu au niveau de l'application par le redémarrage à petite vitesse jusqu'à ce que le calibrage du robot soit à nouveau vérifié, par exemple à l'aide d'une position applicative précise.

Cette procédure de test du référencement après une collision peut être renforcée à l'aide du contrôleur de sécurité : la sortie QforceRefTest RSI9 peut être utilisée pour réinitialiser le contrôle du référencement sûr ; le robot peut encore bouger mais seulement à petite vitesse, jusqu'à ce qu'il ait été ramené dans la deuxième position de référencement.

Il est possible aussi d'imposer un contrôle régulier du référencement sûr en activant le paramètre de sécurité `referencing_timeout` ; l'intervalle de test est alors défini par les paramètres de sécurité `refWarningDelay` et `refTimeoutDelay` :

- Après le délai d'avertissement, l'état du référencement passe à 1 « Avertissement ».
- Après l'écoulement du délai supplémentaire, le contrôle de référencement sûr est réinitialisé (état du référencement 2 « Initialisé » dans le tableau ci-dessous) et un nouveau contrôle du référencement par déplacement du robot dans la deuxième position de référencement est demandé.

|                                  |                        |
|----------------------------------|------------------------|
| <code>referencing_timeout</code> | Voir le chapitre 5.6.1 |
| <code>refWarningDelay</code>     | Voir le chapitre 5.6.1 |
| <code>refTimeoutDelay</code>     | Voir le chapitre 5.6.1 |

### 3.3.9.3 - Réalisation

M0004676.1

La réalisation du référencement sûr consiste dans les étapes suivantes :

#### 1) Activation du référencement sûr

Le référencement sûr est désactivé par défaut et doit être activé à l'aide du paramètre de sécurité `referencing_auto`. Le paramètre `referencing_manu` doit également être activé si les limites de position de sécurité sont nécessaires en mode manuel.



Si `referencing_manu` est activé, le bouchon de maintenance doit être branché pour déplacer un robot non référencé en mode manuel.

Quand `referencing_auto` est activé, les mouvements automatiques sont encore autorisés si le robot n'est pas référencé, mais seulement à petite vitesse (ils ne sont cependant pas autorisés si `safeEncoder_auto` est réglé à 1).

| <code>referencing_auto</code> | <code>safeEncoder_auto</code> | Perte du référencement           |
|-------------------------------|-------------------------------|----------------------------------|
| 1                             | 0                             | Pas d'arrêt sûr, vitesse réduite |
| 1                             | 1                             | Arrêt sûr                        |

#### 2) Positionnement et câblage du ou des capteurs de référencement.

Par défaut, le capteur de référencement doit être câblé sur l'entrée sûre USID1 (J100 13-15). Quand le paramètre de sécurité `referencing_USID1` est réglé à 0, le capteur de référencement peut être câblé sur n'importe quelle entrée numérique du contrôleur CS9. Le contrôleur doit ensuite être configuré pour définir le signal qui doit être utilisé pour le référencement de sécurité (entrée `referencingSensor` dans l'éditeur de cartes Stäubli Robotics Suite IO ; voir aussi le chapitre "Configuration du logiciel" dans le mode d'emploi de CS9).

Le capteur de référencement peut aussi être câblé sur une entrée d'un automate programmable sûr externe, connectée au contrôleur du robot via l'interface du profil esclave (voir chapitre 3.3.3). Le paramètre de sécurité `referencing_USID1` doit être réglé à 0. Aucune configuration supplémentaire du contrôleur n'est nécessaire.

Le câblage peut être testé en vérifiant la rétrosignalisation du capteur de référencement sur la carte Rsi9IO :

- L'état du signal USID est visible sous la forme d'une entrée numérique RSI9.
- Quand `referencing_USID` est à 0 et que le signal à utiliser pour le référencement est défini dans le contrôleur, son état est reflété dans la sortie numérique du système RSI9 QrefSensor.

### 3) Apprentissage des positions de référencement

Aller dans les positions de référencement et saisir les coordonnées de l'articulation (un chiffre après le point suffit) comme paramètres de sécurité refPos1\_Jx et refPos2\_Jx.

Pour les bras TX2-40 et TX2-60, à cause du couplage mécanique au niveau du poignet, les paramètres de sécurité refPosX\_J6 sont formés par la somme des positions de référencement pour les articulations 5 et 6.

$\text{refPos1\_J6} = \text{joint5\_pos1} + \text{joint6\_pos1}$ .

$\text{refPos2\_J6} = \text{joint5\_pos2} + \text{joint6\_pos2}$ .

### 4) Test des positions de référencement en mode manuel

Les positions de référencement définies comme paramètres de sécurité sont automatiquement prêtes à l'emploi dans le contrôleur : sur SP2, elles sont définies comme les positions 'safeReference1' et 'safeReference2' dans la page de calibrage. Le processus de référencement peut être testé en mode manuel à partir de cette interface.

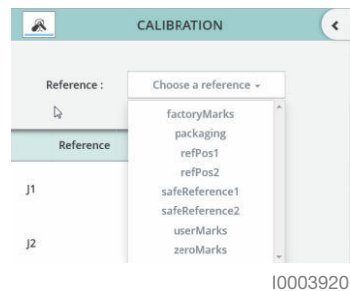


Figure 3.6

### 5) Réalisation des procédures de référencement automatiques

Dans VAL 3, les positions de référencement peuvent être lues à l'aide de l'instruction **"getJntRef"**, en utilisant le paramètre "safeReference1" ou "safeReference2".

Le test de référencement régulier, destiné à empêcher l'expiration du référencement, consiste simplement en un arrêt pendant 0.5 s dans l'une de ces positions. La réussite du test de référencement peut être vérifiée par la lecture de l'entrée lreferencingOK Rsi9 : l'entrée est **ON** quand le délai d'expiration du référencement est réinitialisé. Le délai d'expiration du référencement est également réinitialisé au moment du démarrage si le robot se trouve dans la position de référencement ; il reste réinitialisé tant que le robot est arrêté dans cette position.

Le tableau ci-dessous donne les indications complètes pour la gestion du référencement sûr. L'état de référencement est donné par l'instruction getSafeRefStatus() de VAL 3. «Safe position», «Safe velocity» et «Safe recovery» sont les trois entrées de la carte Rsi9IO qui définissent l'état de référencement (voir chapitre 7.2.2).

Un programme VAL 3 de référencement sûr automatique est proposé avec le modèle safeCalibration VAL 3 livré avec chaque robot.

| État de référencement | Safe position | Safe velocity | Safe recovery | Description   |
|-----------------------|---------------|---------------|---------------|---|
| 0 : Référencé         | <b>ON</b>     | OFF           | OFF           | Le référencement sûr est vérifié : le fonctionnement normal est activé.   |
| 1 : Attention         | <b>ON</b>     | OFF           | OFF           | Dépassement du délai : Arrêt dans la première ou la deuxième position de référencement pour empêcher l'expiration du référencement.                           |
| 2 : Initialisé        | <b>ON</b>     | OFF           | <b>ON</b>     | Le référencement sûr est défini mais non vérifié ou n'a pas été testé à temps ; arrêter le robot dans la deuxième position de référencement pour le vérifier. |

| État de référen-<br>cement | Safe<br>posi-<br>tion | Safe<br>velo-<br>city | Safe<br>reco-<br>very | Description  |
|----------------------------|-----------------------|-----------------------|-----------------------|--|
| 3 : Perdu                  | OFF                   | OFF                   | ON                    | Le référencement sûr est perdu à la suite d'un redémarrage : une articulation du robot a bougé pendant l'arrêt du robot. Aller dans la première position de référencement et mettre le bras hors tension pour refaire le référencement.  |
| 4 : Réin-<br>itialisé      | OFF                   | ON                    | OFF                   | Le référencement sûr est réinitialisé : aller dans la première posi-<br>tion de référencement et mettre le bras hors tension pour le défi-<br>nir.   |
| 5 : Invali-<br>de          | OFF                   | OFF                   | OFF                   | Le référencement sûr est incorrect ou le retour de position sûre<br>est invalide : <ul style="list-style-type: none"><li>■ Vérifier que la carte DSI9 fonctionne et la réinitialiser si néces-<br/>saire</li><li>■ Vérifier que le retour de position sûre est activée<br/>(QnoSafePos OFF)</li><li>■ Réinitialiser le référencement sûr (QresetRef ON puis OFF)</li></ul> |

| RsI9IO IOs         |             |           |            |
|--------------------|-------------|-----------|------------|
| Digital In         | Digital Out | Analog In | Analog Out |
| « 21 - 43 / 46 »   |             |           |            |
| Safe Brake Control | OFF         | direct    |            |
| Fast speed         | OFF         | direct    |            |
| Safe position      | ON          | direct    |            |
| Safe velocity      | OFF         | direct    |            |
| Safe recovery      | ON          | direct    |            |

| RsI9IO IOs          |             |           |            |
|---------------------|-------------|-----------|------------|
| Digital In          | Digital Out | Analog In | Analog Out |
| « 41 - 46 / 46 »    |             |           |            |
| MCP plug            | OFF         | direct    |            |
| MCP removal         | OFF         | direct    |            |
| Referencing timeout | OFF         | direct    |            |
| Brake test timeout  | OFF         | direct    |            |
| lbrakeTestOK        | OFF         | direct    |            |
| lreferencingOK      | OFF         | direct    |            |

| RsI9IO IOs      |             |           |            |
|-----------------|-------------|-----------|------------|
| Digital In      | Digital Out | Analog In | Analog Out |
| « 1 - 16 / 16 » |             |           |            |
| usoB2 (J102-6)  | OFF         | direct    |            |
| usoC1 (J102-9)  | OFF         | direct    |            |
| usoC2 (J102-10) | OFF         | direct    |            |
| QforceRefTest   | OFF         | direct    |            |
| QresetRef       | OFF         | direct    |            |
| QnoSafePos      | OFF         | direct    |            |
| Qrestart        | OFF         | direct    |            |
| QmcpRemoval     | OFF         | direct    |            |
| QredSafety      | OFF         | direct    |            |
| QsosEnable      | OFF         | direct    |            |
| QrefPos1        | OFF         | direct    |            |
| QrefPos2        | OFF         | direct    |            |

6) Exécution du test automatique du référencement

En raison de contraintes de temps (voir le chapitre 3.3.9.4, 4)), la procédure de référencement qui fonctionne en manuel doit aussi être testé en mode automatique.

|                  |                        |
|------------------|------------------------|
| referencing_auto | Voir le chapitre 5.1.2 |
| referencing_manu | Voir le chapitre 5.1.2 |
| referencing_USID | Voir le chapitre 5.1.2 |
| safeEncoder_auto | Voir le chapitre 5.1.2 |
| refPos1_Jx       | Voir le chapitre 5.1.2 |
| refPos2_Jx       | Voir le chapitre 5.1.2 |
| refPosX_J6       | Voir le chapitre 5.1.2 |
| refPos1_J5       | Voir le chapitre 5.1.2 |

### 3.3.9.4 - Essais et débogage

La procédure de référencement sûr peut ne pas aboutir pour différentes raisons :

**1) Référencement sûr non activé.**

- Vérifier que le paramètre de sécurité `referencing_auto` est réglé à 1.

**2) Pas de retour du capteur de référencement ou retour invalide.**

- Quand `referencing_USID` est à 1 : Vérifier que l'entrée sûre `USID1` est **ON** quand le robot est dans la position de référence et **OFF** quand il n'y est pas.
- Quand `referencing_USID` est à 0 : vérifier la configuration du contrôleur `referencingSensor` (Editeur de cartes IO). Vérifier que la sortie numérique système `RSI9 QrefSensor` est **ON** quand le robot est dans la position de référencement et **OFF** quand il n'y est pas.

**3) Les positions de référencement ne sont pas définies, ou pas correctement.**

Pour la première position de référencement :

- Vérifier que la sortie `QrefPos1 Rsi9` est déclenchée quand le bras est mis hors tension dans la première position.

Pour la deuxième position de référencement (dans l'état de référencement « Initialisé » ou « Référencé », selon les définitions du chapitre 3.3.9.3).

- Vérifier que la sortie `QrefPos2 Rsi9` est déclenchée quand le robot s'arrête dans la deuxième position de référence.
- Pour les bras TX2-40 et TX2-60 : vérifier que le paramètre de sécurité `refPos2_J6` a été calculé comme deuxième position de référencement de l'axe 6 + `refPos2_J5`.
- Comparer la position de l'articulation du robot dans SP2 à la position dans SafePMT.

**4) Le robot s'arrête trop tard ou trop tôt dans la position de référencement.**

Le robot doit s'arrêter dans la position de référencement dans la 0.5s qui suit l'activation du capteur.

- Le capteur peut être activé trop tôt si le robot vient lentement dans sa position de destination. Essayer de le faire bouger plus vite.
- Le capteur peut être activé trop tard si le robot atteint la position de destination avant que le signal du capteur soit entièrement transmis (peu probable, mais possible). Essayer de le faire bouger plus lentement.

**5) Position de référencement incorrecte.**

- Vérifier le tableau d'états de référencement pour savoir quelle position de référencement doit être utilisée (première ou seconde).



### 3.3.10 - ESSAIS DES FREINS

#### 3.3.10.1 - Risques liés aux freins

M0004678.1

Les robots à 6 axes sont équipés de freins de moteur qui retiennent le robot quand le bras est hors tension. Les freins de moteur sont souvent appelés « freins de sécurité » parce qu'ils sont serrés automatiquement lorsque leur mise sous puissance est coupée. Cela ne suffit pas, toutefois, pour éliminer complètement les risques liés aux freins :

- La commande de la mise sous puissance des freins doit être sécurisée afin d'assurer qu'ils se serreront lorsque cela sera nécessaire et ne se desserreront pas inopinément. Sur le robot CS9/TX2, c'est la fonction de sécurité SBC (Safe Brake Control) qui l'assure : chaque frein est contrôlé individuellement par une sortie sûre d'une carte de sécurité SIL3/PLe.
- Le frein lui-même peut être défaillant : sa fiabilité est caractérisée par une valeur de délai moyen avant défaillance dangereuse (MTTFd) mais, comme il n'y a pas de redondance intrinsèque de ses composants mécaniques, une défaillance unique peut l'empêcher de fonctionner comme prévu.

Les 3 principaux risques que les freins de robot représentent pour la sécurité sont les suivants :

- Lors de la coupure de la puissance du bras, le frein ne peut pas retenir un segment du bras, qui peut alors blesser une personne se trouvant dessous.
- Lors du contact avec un robot désactivé (par ex. opération de maintenance de l'effecteur), un frein ne peut pas supporter l'effort externe supplémentaire et le segment commence à glisser.
- Quand l'espace restreint est réalisé avec la fonction SLP (Safe Limited Position), il compte sur la distance de freinage sur les freins, qui est estimée à l'aide d'un moment de freinage minimum. Les limites restreintes du robot peuvent être outrepassées si le moment de freinage effectif est inférieur à la valeur utilisée pour cette estimation.

#### 3.3.10.2 - Mesures de contrôle des risques

M0004679.1

Les mesures permettant de contrôler les risques liés aux freins consistent, tout d'abord, à réduire au minimum l'exposition du personnel aux conséquences d'un défaut des freins en évitant que des personnes se trouvent sous le bras pendant le fonctionnement et la maintenance, ou dans l'emprise maximale du robot en fonctionnement.



### SÉCURITÉ

- Si une intervention humaine régulière est nécessaire sous un robot non sécurisé, les freins doivent être testés dans les 10 heures précédant l'intervention.
- Si une intervention humaine régulière est nécessaire sous un robot en mouvement, la puissance du bras ne doit être coupée que dans des situations exceptionnelles (arrêt d'urgence) ; dans les conditions normales, on utilisera des arrêts SS2 à la place. Les freins doivent être testés dans les 10 heures précédant l'intervention ; le paramètre de sécurité brakeTest\_manu doit être activé afin de permettre les mouvements manuels en dessous du bras.
- Quand des personnes se trouvent dans l'emprise maximale du robot, protégées uniquement par l'espace restreint défini, les freins doivent être testés chaque jour (en supposant qu'ils servent effectivement à retenir le robot dans l'espace restreint jusqu'à 3 fois par an).

Le paramètre brakeTest\_auto doit être activé ; l'intervalle de test peut être augmenté si l'exposition est réduite (par ex. une fois par semaine si l'exposition est peu fréquente).



L'intervalle des essais de frein est défini par les paramètres de sécurité `brakeTestWarningDelay` et `brakeTestTimeoutDelay` :

- Après le délai d'avertissement, l'entrée d'expiration de l'intervalle d'essai de frein RSI9 Brake test timeout passe à **ON**.
- Après le délai supplémentaire, la vitesse des mouvements est réduite dans les modes automatiques si `brakeTest_auto` est réglé à 1. Les mouvements ne sont pas autorisés dans les modes manuels si `brakeTest_manu` est réglé à 1 (le bouchon de maintenance est alors nécessaire pour faire bouger le robot manuellement).

L'essai de frein lui-même est exécuté selon l'instruction VAL 3 "**brakeTest**".

- L'application VAL 3 doit fonctionner en mode automatique déporté pour permettre l'activation et la désactivation automatiques de la puissance du bras.
- L'essai de frein peut être effectué dans presque n'importe quelle position, pourvu qu'il y ait un espace libre autour de la position d'essai en prévision d'un échec du test. L'instruction "**brakeTest**" doit être appelée après l'arrêt dans la position d'essai.
- L'essai de frein compense automatiquement la gravité pour le test des moments de freinage. Un échec de l'essai est possible, avec une charge lourde, si le moment à compenser est trop important ; une position moins sensible à la gravité doit alors être choisie.



Le mouvement produit par l'essai de frein sur un frein défectueux est inférieur à 1° pour les axes 1 et 2, 2° pour les axes 3 et 4 et 3° pour les axes 5 et 6.

|                                    |  |
|------------------------------------|--|
| <code>brakeTest_manu</code>        | Voir le chapitre <a href="#">5.6.2</a> |
| <code>brakeTest_auto</code>        | Voir le chapitre <a href="#">5.6.2</a> |
| <code>brakeTestWarningDelay</code> | Voir le chapitre <a href="#">5.6.2</a> |
| <code>brakeTestTimeoutDelay</code> | Voir le chapitre <a href="#">5.6.2</a> |



## 4 - SAFE PMT

### 4.1 - INSTALLATION ET PARAMÈTRES

M0004680.1

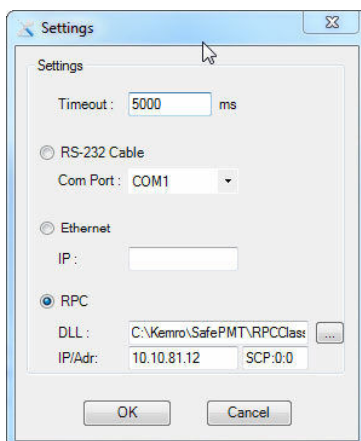
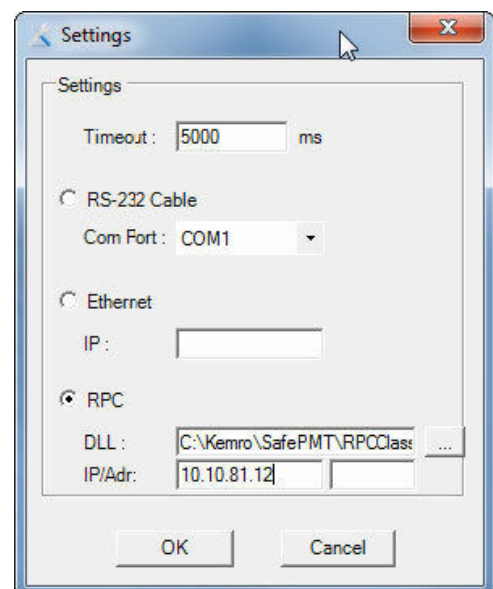
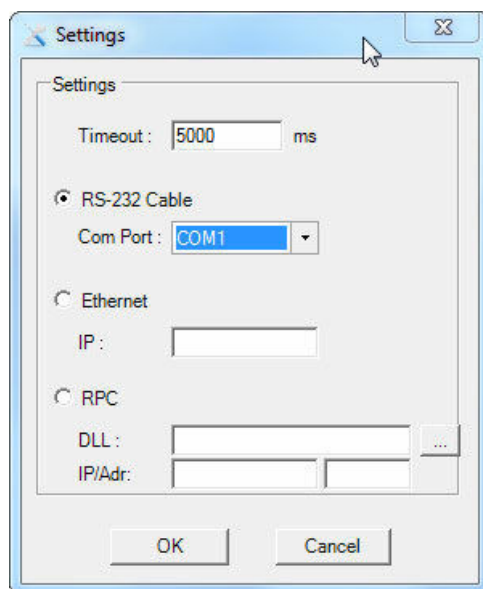
La version actuelle de SafePMT est livrée avec un fichier d'installation et un autre de configuration. Vous devez disposer des droits d'administrateur pour installer le logiciel. SafePMT nécessite l'installation de Microsoft .NET Framework 3.5 : voir les instructions de Microsoft relatives à l'installation de ce cadre si celui-ci n'est pas installé dans votre version de Windows :

<https://docs.microsoft.com/en-us/dotnet/framework/install/dotnet-35-windows-10>

Pour terminer l'installation :

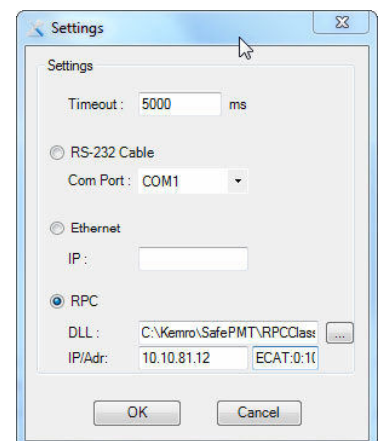
- Supprimer le fichier de configuration datar.dat dans le répertoire d'installation de SafePMT.
- Copier le fichier de configuration datas.dat dans le répertoire d'installation de SafePMT.

Une fenêtre de paramètres s'affiche lors du premier démarrage de SafePMT. Elle doit être configurée avec l'adresse IP du robot, en utilisant le choix « RPC » (et non « Ethernet ») et la DLL "RPCClassLibrary.dll" (voir ci-dessous) :



RSi9

Au démarrage, SafePMT est toujours configuré pour se connecter à la carte RSi9 ("SCP:0:0"). L'adresse « ECAT:0:1002 » doit être utilisée à la place pour le connecter à la carte DSI9, pour le diagnostic ou pour la mise à jour du firmware.

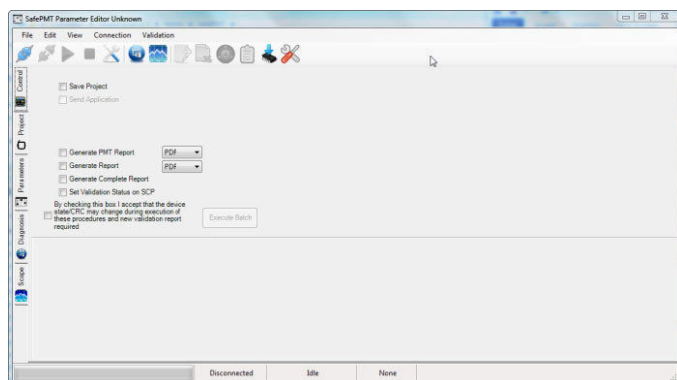


DSi9

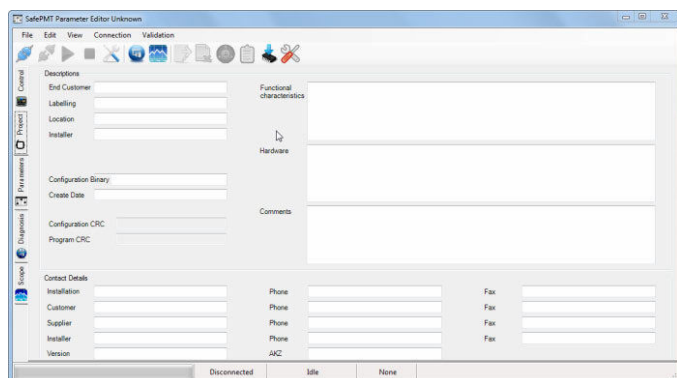
## 4.2 - DESCRIPTION

M0004681.1

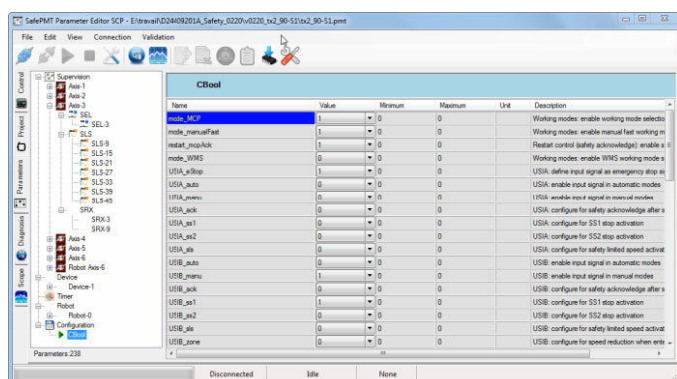
SafePMT affiche 5 onglets à gauche de l'interface :



L'onglet Control apparaît au démarrage.



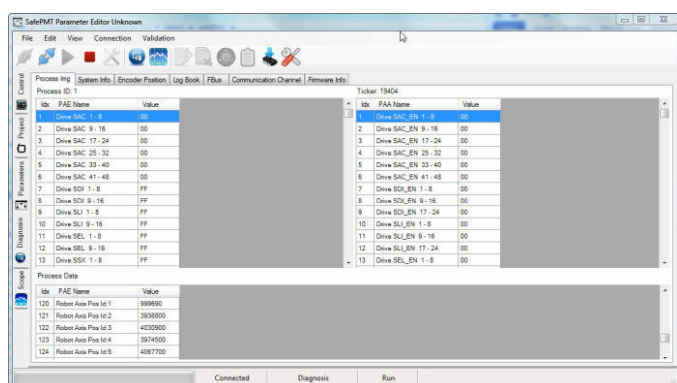
L'onglet Project est destiné à recueillir les informations du projet, qui sont enregistrées avec les paramètres de sécurité et affichées dans le rapport de validation.



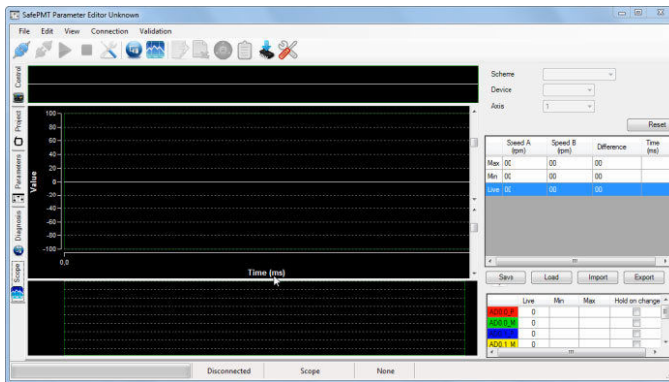
L'onglet Parameters est l'éditeur des paramètres de sécurité ; le fichier de paramètres .pmt doit être ouvert pour que les paramètres apparaissent dans cet onglet.

Les paramètres sont triés en quatre catégories :

- Supervision/Axis x : Paramètres articulaires
- Timer : paramètres de temporisation
- Robot/Robot-0 : Paramètres cartésiens
- Configuration/Cbool : Paramètres booléens



L'onglet Diagnosis est réservé au diagnostic et à la maintenance (mise à jour du firmware) en recherche et développement avancés.



L'onglet Scope peut être utilisé pour des diagnostics par l'utilisateur, afin de vérifier la position sûre et l'état de certaines fonctions de sécurité.

Les icônes en haut de l'écran donnent accès directement aux principales fonctions de l'outil :



Contrôle de la connexion Ethernet (connexion/déconnexion).



Contrôle du programme de sécurité du robot (démarrage/arrêt).



Accès aux paramètres pour modifier l'adresse IP du robot.



Actualisation des paramètres de sécurité.



Téléchargement du rapport de validation.



Validation de la connexion (attente de validation/prêt pour l'actualisation).

### 4.3 - ACTUALISATION DES PARAMÈTRES DE SÉCURITÉ

M0004682.1

Les paramètres de sécurité sont stockés dans un fichier .pmt avec le programme de sécurité correspondant. Pour actualiser le programme de sécurité et ses paramètres :

Ouvrir le fichier .pmt.

File > Open

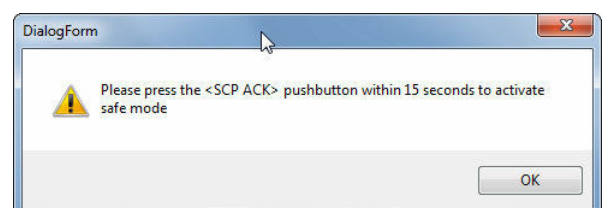
Modifier les paramètres de sécurité (si nécessaire).

Parameters tab

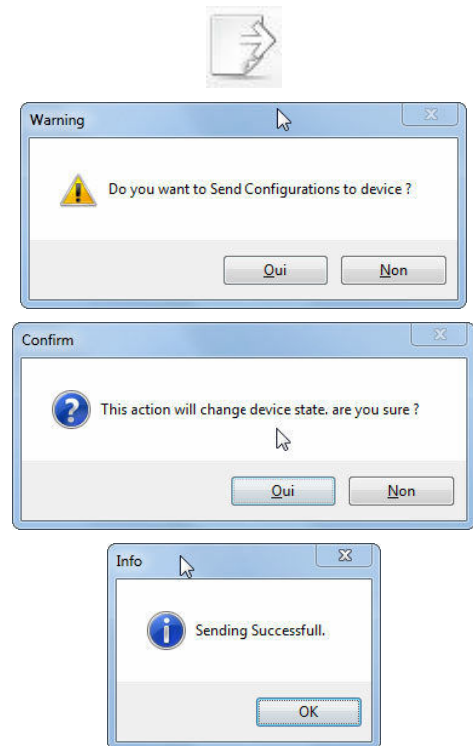
Se connecter au robot.



Confirmer la connexion sur le robot (« mode sécurisé ») : appuyer sur le bouton Update (SCP ACK) sur le tiroir central du CS9 pour s'assurer que la mise à jour est destinée au bon robot.



Envoyer le programme de sécurité et ses paramètres.  
Un pop-up annonce la fin de la mise à jour 30 secondes plus tard environ.



Déconnecter, attendre 15 secondes puis appuyer sur 'Update' pour remettre le robot en marche (ou redémarrer le contrôleur après la déconnexion).



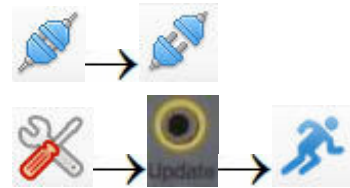
## 4.4 - RAPPORT DE VALIDATION

Le rapport de validation est un support pour les tests de validation, qui donne une description de référence détaillée de la configuration de sécurité du robot. Pour générer le rapport de validation :

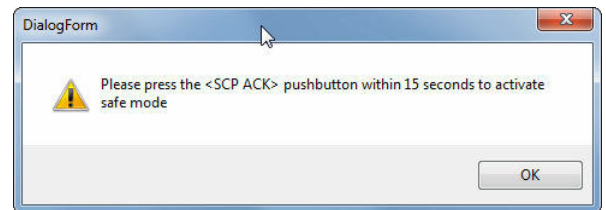
Mettre à jour les informations du projet.

Se connecter au robot.

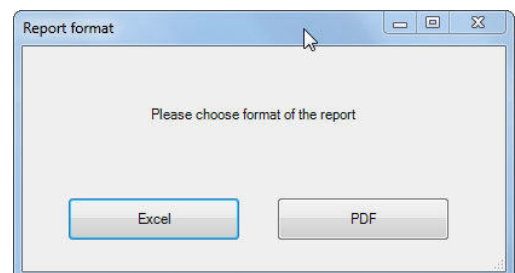
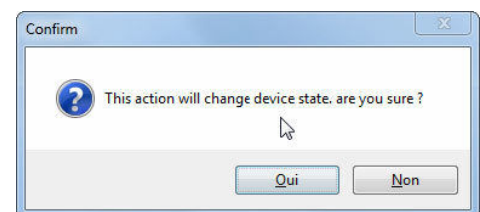
Project tab



Confirmer la connexion sur le robot (« mode sécurisé ») : appuyer sur le bouton Update (SCP ACK) sur le tiroir central du CS9 pour s'assurer que la mise à jour est destinée au bon robot.



Générer le rapport de PMT. SafePMT met environ 1.5 minute à télécharger les données avant de demander quel doit être le format du rapport (Excel ou PDF). La génération du rapport prend 2 minutes de plus.



## 4.5 - SAUVEGARDE ET RESTAURATION DES PARAMÈTRES DE SÉCURITÉ

Une fois qu'une application de sécurité est validée, des mesures doivent être prises pour :

- Empêcher toute mise à jour non autorisée en contrôlant l'accès à l'outil SafePMT (qui ne doit pas être accessible dans la zone de production) et à la configuration .pmt de sécurité.
- Enregistrer une sauvegarde de la configuration de sécurité modifiée (fichier .pmt), de l'outil safePMT et du rapport de validation de sécurité dans un lieu sûr et accessible pour les opérations de maintenance de sécurité.

L'application de sécurité validée peut être restaurée à partir du fichier source (.pmt), comme pour la mise à jour des paramètres de sécurité (chapitre 4.3), ou d'une sauvegarde binaire. La sauvegarde binaire est préférable pour la maintenance ou la duplication du programme : la restauration est plus rapide et le fichier source ne peut pas être modifié.

Quelle que soit la méthode de restauration, la configuration de sécurité qui en résulte doit être validée, de la manière décrite dans le chapitre 4.5.3.

### 4.5.1 - SAUVEGARDE BINAIRE

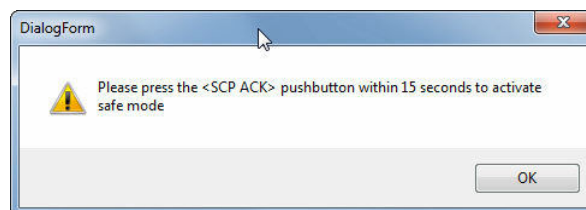
M0004685.1

Pour enregistrer une sauvegarde binaire de la configuration de sécurité actuelle :

Se connecter au robot.

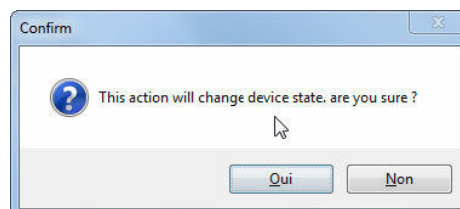
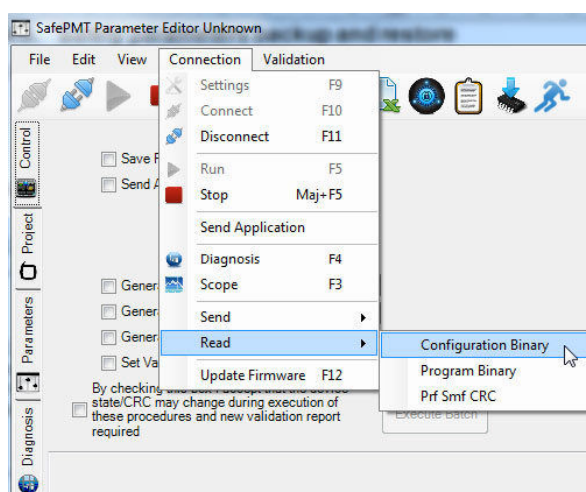


Confirmer la connexion sur le robot (« mode sécurisé ») : appuyer sur le bouton Update (SCP ACK) sur le tiroir central du CS9 pour s'assurer que la mise à jour est destinée au bon robot.

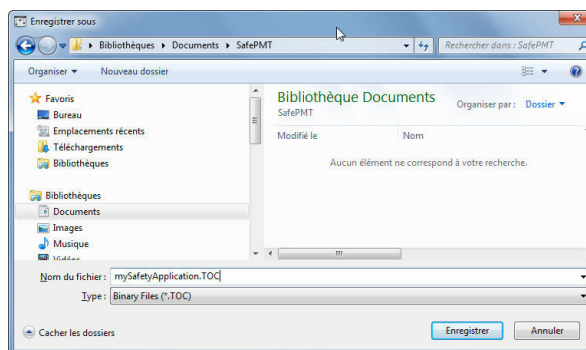


Sélectionner l'onglet Control et commencer le téléchargement de la configuration binaire :

Connection > Read > Configuration binary



La barre d'état indique l'avancement du téléchargement binaire. La sauvegarde binaire doit être enregistrée dans un fichier .TOC.





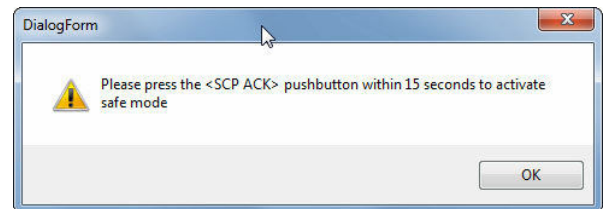
### 4.5.2 - RESTAURATION BINAIRE

Pour restaurer une sauvegarde binaire :

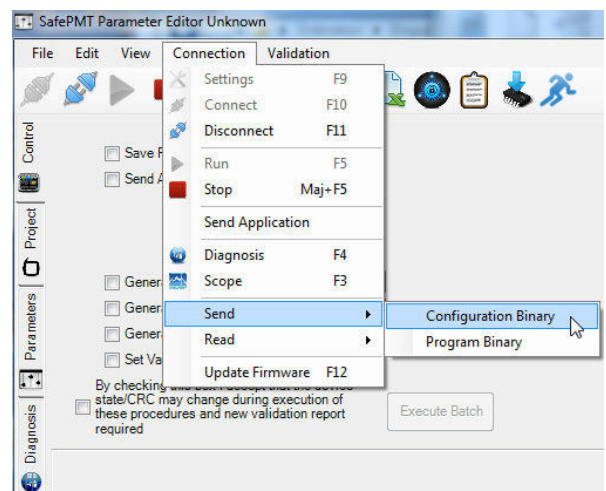
Se connecter au robot.



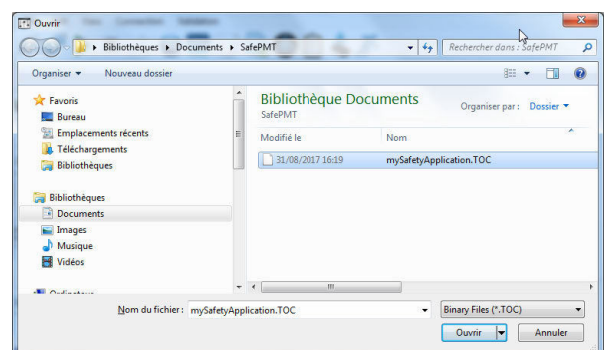
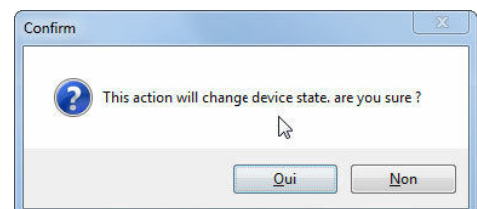
Confirmer la connexion sur le robot (« mode sécurisé ») : appuyer sur le bouton Update (SCP ACK) sur le tiroir central du CS9 pour s'assurer que la mise à jour est destinée au bon robot.



Sélectionner l'onglet Control et commencer le téléchargement de la configuration binaire :  
Connection > Send > Configuration binary



Sélectionner le fichier de sauvegarde binaire TOC à restaurer. La barre d'état indique l'avancement de la restauration binaire.



### 4.5.3 - VALIDATION DE LA RESTAURATION DE LA SAUVEGARDE

M0004687.1

Pour restaurer une configuration de sécurité à partir d'une sauvegarde du fichier source .pmt :

Sélectionner l'onglet **Diagnosis / System Info** (pour gagner du temps, ce choix peut être fait avant la connexion).

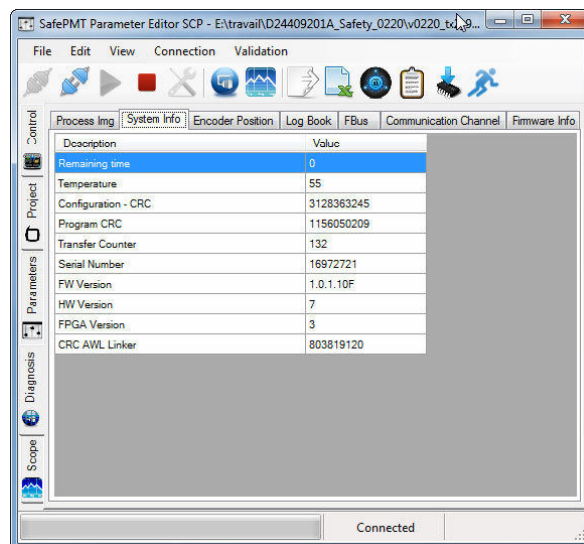
Diagnosis / System Info



Comparer :

- Configuration CRC.
- Program CRC.

aux mêmes paramètres sur la page 4 du rapport de validation.



Vérifier que le programme de sécurité fonctionne : les CRC affichées ne sont actualisées qu'au démarrage du programme.

Ces deux CRC de l'onglet System Info sont la « preuve » que la configuration de sécurité restaurée est une copie conforme de la configuration de sécurité d'origine : le fonctionnement peut reprendre sans qu'une nouvelle validation de sécurité soit nécessaire.

Les CRC s'affichent également dans la page Informations du SP2.

| INFORMATION           |                 |
|-----------------------|-----------------|
| REST_API Version      | s8.3.1cs9_BS885 |
| RSI Configuration CRC | 3128363245      |
| RSI FPGA              | 3               |
| RSI Firmware          | 1.0.1.10F       |
| RSI Hardware          | 7               |
| RSI Name              | SCP855          |
| RSI Program CRC       | 1156050209      |
| RSI S/N               | 16972721        |
| RSI Software          | 0.220           |



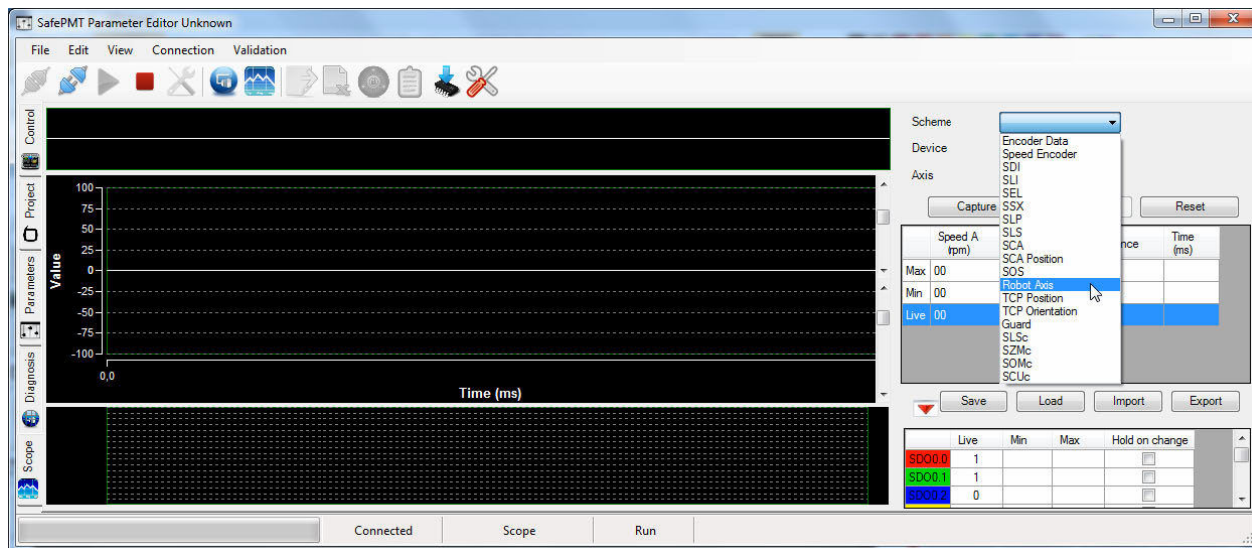
Pendant la production, on peut aussi vérifier que le programme de sécurité reste inchangé en lisant le compteur de transferts (accessible comme entrée analogique de RSI9), qui doit afficher la valeur donnée à la page 4 du rapport de validation, ou en vérifiant la CRC à l'aide des commandes **"getVersion"** (RSI Configuration CRC) et **"getVersion"** (RSI Program CRC) de VAL 3.

## 4.6 - MAINTENANCE

### 4.6.1 - DIAGNOSTICS

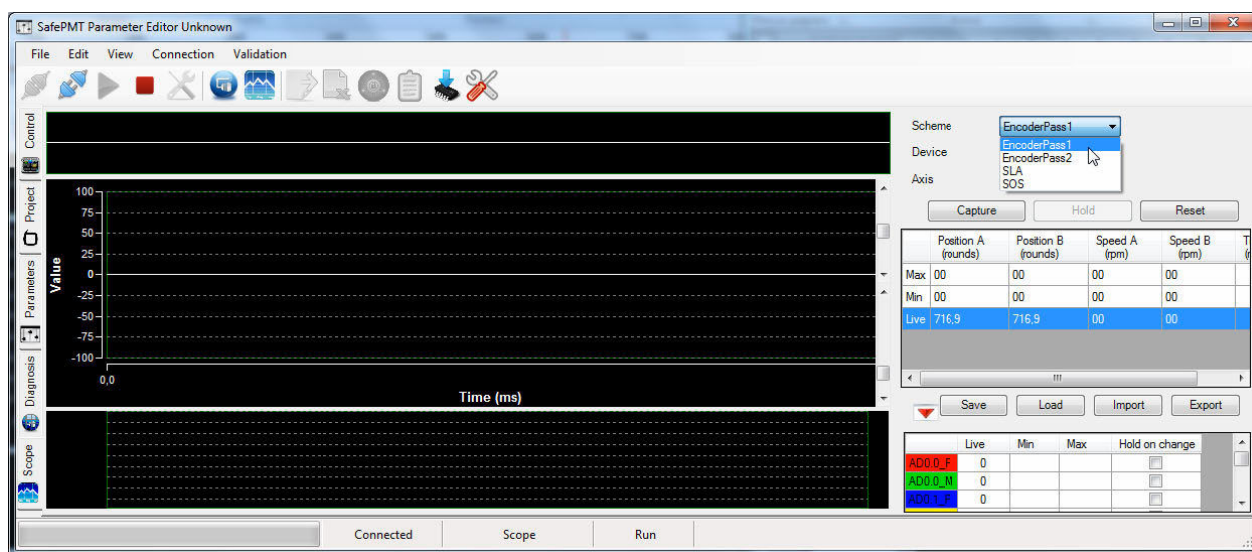
M0004688.1

L'onglet Scope peut être utilisé pour suivre l'état de différents éléments de sécurité lors de la connexion à la carte RS19 :



I0003954

ou à la carte DS19 :



I0003955

## 4.6.2 - MISE À JOUR DU FIRMWARE

M0004689.1

Pour mettre à jour le firmware sur les cartes RSI9 et DSI9, mettre d'abord à jour la carte DSI9, puis redémarrer SafePMT et mettre à jour la carte RSI9.

Vérifier que SafePMT est configuré pour la mise à jour du firmware. Le répertoire d'installation de SafePMT contient un fichier datas.dat et pas de fichier datar.dat.

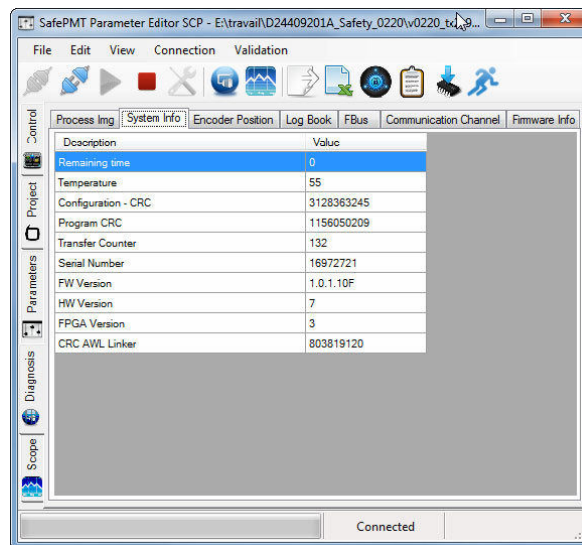
datas.dat / ~~datar.dat~~

Se connecter à la carte RSI9 (réglages par défaut) ou DSI9 (adresse ECAT:0:1002, voir le chapitre 4.1).



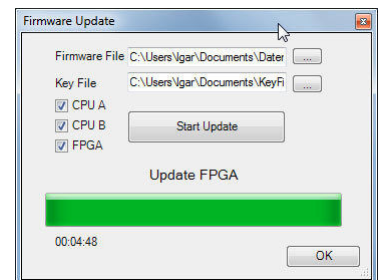
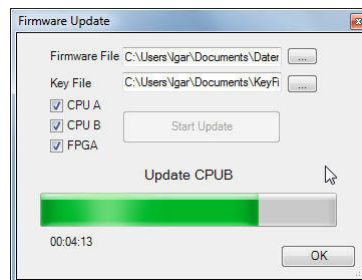
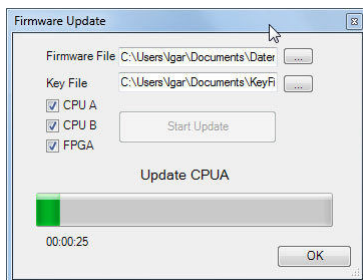
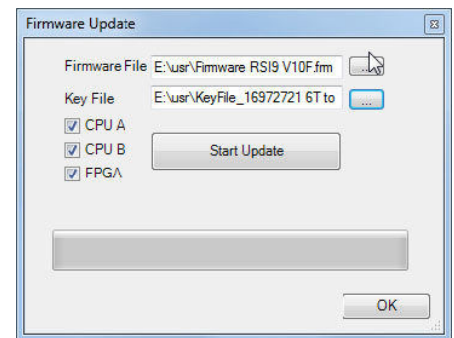
Diagnosis/System info

Noter le numéro de série de la carte RSI9 ou DSI9, qui apparaît également dans la page Information de SP2 et dans l'historique du robot.



Vérifier qu'aucun programme de VAL 3 n'est ouvert.

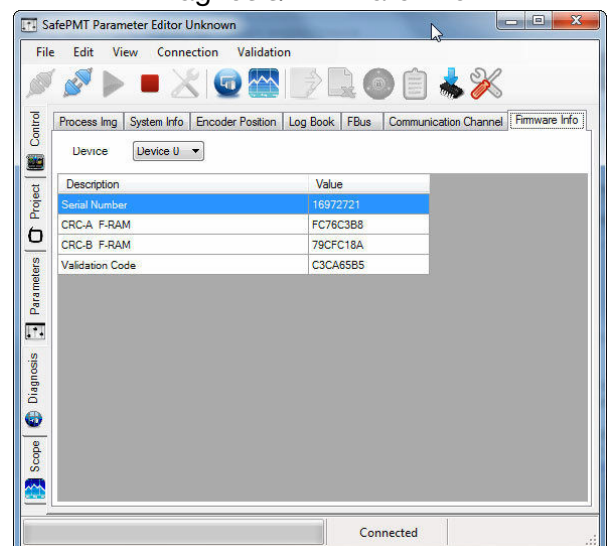
À l'aide du bouton « Firmware update », sélectionner le nouveau fichier de firmware et le fichier de clé correspondant au numéro de série, puis appuyer sur Start update. Selon les fichiers à mettre à jour, l'opération dure entre 5 et 15 minutes.



Redémarrer le contrôleur.  
(Pour la carte RSI9 uniquement, et selon la mise à jour du firmware). Au besoin, réinstaller le programme de sécurité en suivant la procédure de restauration (4.5) et redémarrer.

Vérifier la nouvelle version du firmware et rapporter le code de validation comme preuve de la mise à jour.

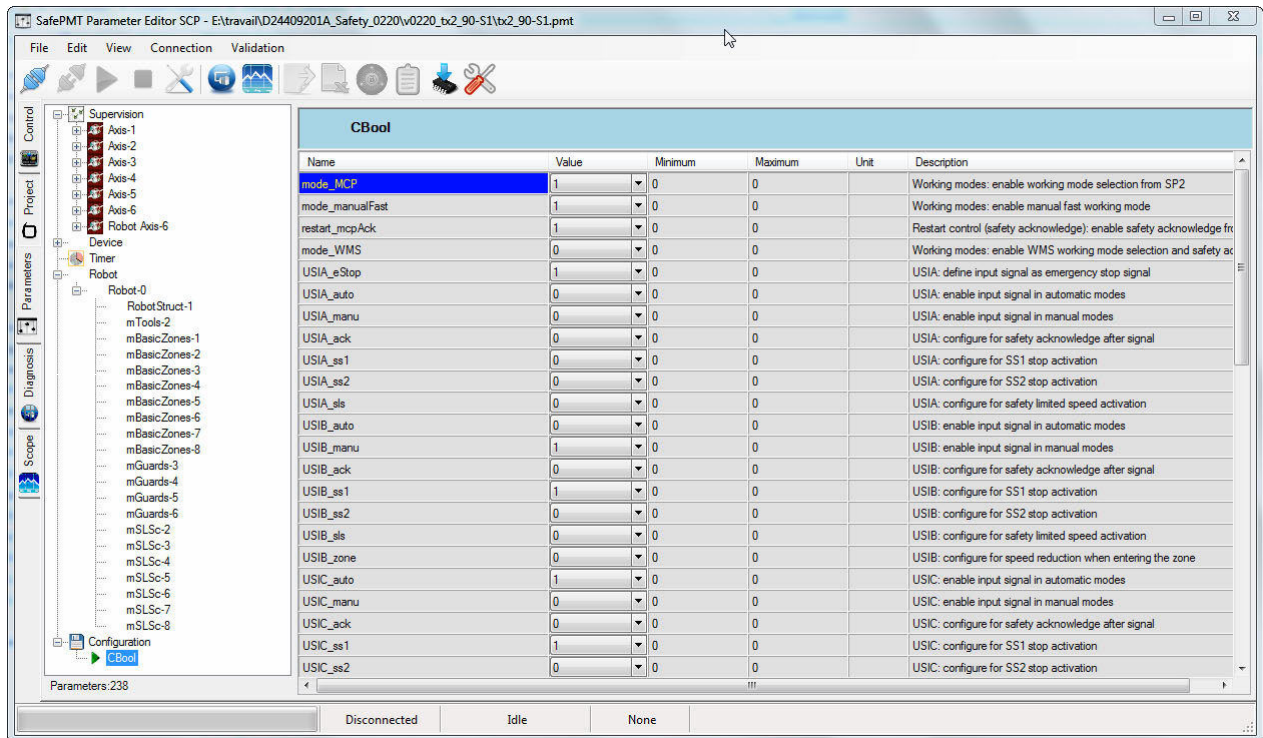
#### Diagnosis/Firmware info





# 5 - PARAMÈTRES DE SÉCURITÉ

Les paramètres de sécurité sont répertoriés dans l'onglet Parameters de SafePMT (voir chapitre 4.3).



10003963

Figure 5.1

Ils sont triés en 4 grandes catégories :

- Paramètres articulaires (dans Supervision / Axis-x).
- Valeurs de temporisation (dans Timer).
- Paramètres cartésiens (dans Robot/Robot- 0).
- Paramètres booléens (dans Configuration/CBool).

## 5.1 - (SAFECELL) ACTIVATION DE LA SURVEILLANCE DE SÉCURITÉ

### 5.1.1 - (SAFECELL+) SURVEILLANCE DE SÉCURITÉ DE SOS, SS2, SLSJ

M0004691.1



Ce paragraphe ne concerne que la version 1.001 du programme de sécurité et les anciennes versions de SafeCell+.

Les fonctions de sécurité SOS, SS2 et SLSj nécessitent que le retour codeur sûr fonctionne. Leur activation consiste à déclarer le retour du codeur sûr de la manière nécessaire.

| Type | Nom              | Valeurs | Description   |
|------|------------------|---------|---|
| Bool | safeEncoder_manu | 0       | Les fonctions de sécurité SOS, SS2 et SLSj sont en option en mode manuel. |
|      |                  | 1       | La fonction de sécurité SOS, SS2 ou SLSj est requise en mode manuel.      |



| Type | Nom              | Valeurs | Description   |
|------|------------------|---------|---|
| Bool | safeEncoder_auto | 0       | Les fonctions de sécurité SOS, SS2 et SLSj sont en option en mode automatique.            |
|      |                  | 1       | La fonction de sécurité SOS, SS2 ou SLSj est requise en mode automatique <sup>(1)</sup> . |

(1) Quand referencing\_auto est à 1, safeEncoder\_auto peut être mise soit à 0, soit à 1 (voir chapitre 5.1.2)

### 5.1.2 - (SAFECELL) SURVEILLANCE DE SÉCURITÉ DE SLP, SLSC, SZM



M0004692.1

Les fonctions de sécurité SLP, SLSc et SZM nécessitent un référencement sûr (voir chapitre 3.3.9). Leur activation consiste à déclarer le référencement de la manière requise et à définir les positions pour le référencement sûr.

Les fonctions de sécurité de limitation SLPc, SLSc et SZM nécessitent en outre la licence d'exécution SafeCELL+ sur le contrôleur.

| Type              | Nom                             | Valeurs | Description (voir chapitre 3.3.9)   |
|-------------------|---------------------------------|---------|---|
| Bool              | referencing_manu                | 0       | Les fonctions de sécurité SLP, SLSc et SZM sont en option en mode manuel.               |
|                   |                                 | 1       | Certaines des fonctions de sécurité SLP, SLSc et SZM sont requises en mode manuel.      |
| Bool              | referencing_auto                | 0       | Les fonctions de sécurité SLP, SLSc et SZM sont en option en mode automatique.          |
|                   |                                 | 1       | Certaines des fonctions de sécurité SLP, SLSc et SZM sont requises en mode automatique. |
| Bool              | safeEncoder_auto <sup>(1)</sup> | 0       | Vitesse réduite quand le référencement est perdu.                                       |
|                   |                                 | 1       | Arrêt de sécurité quand le référencement est perdu.                                     |
| Bool              | referencing_USID1               | 0       | Le capteur de référencement est câblé sur une entrée numérique CS9 ou via le bus FS.    |
|                   |                                 | 1       | Le capteur de référencement est câblé vers USID1 (J100 13–15).                          |
| Articulation SRX1 | refPos1_J1                      | ±360    | Coordonnées de la première position de référencement de l'articulation 1.               |
| Articulation SRX2 | refPos1_J2                      | ±360    | Coordonnées de la première position de référencement de l'articulation 2.               |
| Articulation SRX3 | refPos1_J3                      | ±360    | Coordonnées de la première position de référencement de l'articulation 3.               |
| Articulation SRX4 | refPos1_J4                      | ±360    | Coordonnées de la première position de référencement de l'articulation 4.               |
| Articulation SRX5 | refPos1_J5                      | ±360    | Coordonnées de la première position de référencement de l'articulation 5.               |



| Type                    | Nom   | Va-<br>leurs | Description (voir chapitre 3.3.9)   |
|-------------------------|---|--------------|---|
| Articula-<br>tion SRX6  | refPos1_J6<br> | ±360         | TX2-90/L/XL : Coordonnées de la première position de référencement de l'articulation 6.<br>TX2-40, TX2-60/L : Somme des coordonnées des articulations 5 et 6. |
| Articula-<br>tion SRX7  | refPos2_J1  | ±360         | Coordonnées de la deuxième position de référencement de l'articulation 1.   |
| Articula-<br>tion SRX8  | refPos2_J2  | ±360         | Coordonnées de la deuxième position de référencement de l'articulation 2.   |
| Articula-<br>tion SRX9  | refPos2_J3  | ±360         | Coordonnées de la deuxième position de référencement de l'articulation 3.   |
| Articula-<br>tion SRX10 | refPos2_J4  | ±360         | Coordonnées de la deuxième position de référencement de l'articulation 4.   |
| Articula-<br>tion SRX11 | refPos2_J5  | ±360         | Coordonnées de la deuxième position de référencement de l'articulation 5.   |
| Articula-<br>tion SRX12 | refPos2_J6<br> | ±360         | TX2-90/L/XL : Coordonnées de la deuxième position de référencement de l'articulation 6.<br>TX2-40, TX2-60/L : Somme des coordonnées des articulations 5 et 6. |

(1) Uniquement quand `referencing_auto` est à 1.

## 5.2 - (SAFECELL) FONCTIONS DE SÉCURITÉ D'ARRÊT

### 5.2.1 - (SAFECELL) ARRÊT D'URGENCE

M0004696.1

| Type | Nom        | Valeurs | Description (voir chapitre 3.3.3)   |
|------|------------|---------|---|
| Bool | USIA_eStop | 0       | USIA peut être configuré comme un arrêt de protection (si aucune interface WMS n'est utilisée). |
|      |            | 1       | (par défaut) USIA est un arrêt d'urgence non configurable.                                      |

Le paramètre `USIA_eStop` est un raccourci équivalent à la configuration de `USIA_manu`, `USIA_auto`, `USIA_ack` et `USIA_SS1` à 1.

`USIA_eStop` est ignoré (forcé à 1) quand le paramètre `mode_WMS` est à 1 (voir chapitre 5.4.1).

### 5.2.2 - BOUTON DE VALIDATION DU (SAFECELL)

M0005452.1

| Type | Nom          | Valeurs | Description (voir chapitre 3.3.4)  |
|------|--------------|---------|--|
| Bool | enabling_SS2 | 0       | Le dispositif d'activation déclenche un arrêt SS1 quand il est relâché dans les modes manuels. |
|      |              | 1       | Le dispositif d'activation déclenche un arrêt SS2 quand il est relâché dans les modes manuels. |

### 5.2.3 - (SAFECELL) ARRÊTS DE PROTECTION SS1/SS2

#### 5.2.3.1 - Tous arrêts

M0004697.1

| Type  | Nom         | Valeurs            | Description (voir chapitre 3.3.7)   |
|-------|-------------|--------------------|---|
| Timer | maxStopTime | 512 <sup>(1)</sup> | Temps d'arrêt (ms) quand un arrêt d'urgence SP2 ou un arrêt par le bouton d'activation est déclenché, temps maximal avant l'arrêt pour les arrêts USIx. |

(1) Le temps d'arrêt minimum varie de 64 à 144 ms selon les robots.

#### 5.2.3.2 - USIA

M0004698.1

| Type  | Nom              | Valeurs            | Description (voir chapitre 3.3.3)                                   |
|-------|------------------|--------------------|---|
| Bool  | USIA_auto        | 0 / 1              | USIA est inactif / actif dans les modes automatiques.               |
| Bool  | USIA_manu        | 0 / 1              | USIA est inactif / actif dans les modes manuels.                    |
| Bool  | USIA_ack         | 0                  | Pas d'acquittement de sécurité requis après l'activation d'USIA.    |
|       |                  | 1                  | Acquittement de sécurité requis après l'activation d'USIA.          |
| Bool  | USIA_SS1         | 0                  | USIA ne déclenche pas un arrêt SS1.                                 |
|       |                  | 1                  | USIA déclenche un arrêt SS1.  |
| Bool  | USIA_SS2         | 0                  | USIA ne déclenche pas un arrêt SS2.                                 |
|       |                  | 1                  | USIA déclenche un arrêt SS2 (si USIA_SS1 est à 0).                  |
| Timer | USIA_maxStopTime | 496 <sup>(1)</sup> | Temps d'arrêt (ms) quand USIA est déclenchée (voir chapitre 3.3.7). |

(1) Le temps d'arrêt minimum varie de 64 à 144 ms selon les robots.



La configuration d'USIA comme arrêt de protection est ignorée quand USIA\_eStop=1 ou mode\_WMS=1 (voir chapitre 5.2.1).

## 5.2.3.3 - USIB

M0004699.1

| Type  | Nom                   | Valeurs            | Description (voir chapitre 3.3.3)                                   |
|-------|-----------------------|--------------------|---|
| Bool  | USIB_auto             | 0 / 1              | USIB est inactif / actif dans les modes automatiques.               |
| Bool  | USIB_manu             | 0 / 1              | USIB est inactif / actif dans les modes manuels.                    |
| Bool  | USIB_ack              | 0                  | Pas d'acquiescement de sécurité requis après l'activation d'USIB.   |
|       |                       | 1                  | Acquiescement de sécurité requis après l'activation d'USIB.         |
| Bool  | USIB_SS1              | 0                  | USIB ne déclenche pas un arrêt SS1.                                 |
|       |                       | 1                  | USIB déclenche un arrêt SS1.  |
| Bool  | USIB_SS2              | 0                  | USIB ne déclenche pas un arrêt SS2.                                 |
|       |                       | 1                  | USIB déclenche un arrêt SS2 (si USIB_SS1 est à 0).                  |
| Bool  | USIB_zone (Safecell+) | 0                  | L'arrêt est déclenché quelle que soit la position du robot.         |
|       |                       | 1                  | L'arrêt est déclenché uniquement à l'intérieur de la zone USIB.     |
| Timer | USIB_maxStopTime      | 496 <sup>(1)</sup> | Temps d'arrêt (ms) quand USIB est déclenchée (voir chapitre 3.3.7). |

(1) Le temps d'arrêt minimum varie de 64 à 144 ms selon les robots.

## 5.2.3.4 - USIC

M0004700.1

| Type  | Nom                   | Valeurs            | Description (voir chapitre 3.3.3)                                   |
|-------|-----------------------|--------------------|---|
| Bool  | USIC_auto             | 0 / 1              | USIC est inactif / actif dans les modes automatiques.               |
| Bool  | USIC_manu             | 0 / 1              | USIC est inactif / actif dans les modes manuels.                    |
| Bool  | USIC_ack              | 0                  | Pas d'acquiescement de sécurité requis après l'activation d'USIC.   |
|       |                       | 1                  | Acquiescement de sécurité requis après l'activation d'USIC.         |
| Bool  | USIC_SS1              | 0                  | USIC ne déclenche pas un arrêt SS1.                                 |
|       |                       | 1                  | USIC déclenche un arrêt SS1.  |
| Bool  | USIC_SS2              | 0                  | USIC ne déclenche pas un arrêt SS2.                                 |
|       |                       | 1                  | USIC déclenche un arrêt SS2 (si USIC_SS1 est à 0).                  |
| Bool  | USIC_zone (Safecell+) | 0                  | L'arrêt est déclenché quelle que soit la position du robot.         |
|       |                       | 1                  | L'arrêt est déclenché uniquement à l'intérieur de la zone USIC.     |
| Timer | USIC_maxStopTime      | 496 <sup>(1)</sup> | Temps d'arrêt (ms) quand USIC est déclenchée (voir chapitre 3.3.7). |

(1) Le temps d'arrêt minimum varie de 64 à 144 ms selon les robots.

## 5.2.3.5 - USID

M0004701.1

| Type  | Nom              | Valeurs            | Description (voir chapitre 3.3.3)                                   |
|-------|------------------|--------------------|---|
| Bool  | USID_auto        | 0 / 1              | USID est inactif / actif dans les modes automatiques.               |
| Bool  | USID_manu        | 0 / 1              | USID est inactif / actif dans les modes manuels.                    |
| Bool  | USID_ack         | 0                  | Pas d'acquittement de sécurité requis après l'activation d'USID.    |
|       |                  | 1                  | Acquittement de sécurité requis après l'activation d'USID.          |
| Bool  | USID_SS1         | 0                  | USID ne déclenche pas un arrêt SS1.                                 |
|       |                  | 1                  | USID déclenche un arrêt SS1.  |
| Bool  | USID_SS2         | 0                  | USID ne déclenche pas un arrêt SS2.                                 |
|       |                  | 1                  | USID déclenche un arrêt SS2 (si USID_SS1 est à 0).                  |
| Timer | USID_maxStopTime | 496 <sup>(1)</sup> | Temps d'arrêt (ms) quand USID est déclenchée (voir chapitre 3.3.7). |

(1) Le temps d'arrêt minimum varie de 64 à 144 ms selon les robots.

## 5.3 - (SAFECELL) FONCTIONS DE SÉCURITÉ DE LIMITATION

### 5.3.1 - (SAFECELL) POSITION LIMITÉE DE SÉCURITÉ (SLP)

M0004702.1

| Type     | Nom                  | Valeurs               | Description (voir chapitre 3.3.8)                                    |
|----------|----------------------|-----------------------|--|
| Bool     | jointLimits_manu     | 0                     | Les limites SLP sont ignorées dans les modes manuels. <sup>(1)</sup> |
|          |                      | 1                     | Les limites SLP sont actives dans les modes manuels.                 |
| Axe-1SEL | jointLimits_minPosJ1 | ±400                  | Limite de position inférieure de l'axe 1 (°).                        |
|          | jointLimits_maxPosJ1 | ±400                  | Limite de position supérieure de l'axe 1 (°).                        |
|          | jointLimits_decelJ1  | 0-10000               | Décélération maximale pour arrêter le robot avant la limite.         |
| Axe-2SEL | jointLimits_minPosJ2 | ±400                  | Limite de position inférieure de l'axe 2 (°).                        |
|          | jointLimits_maxPosJ2 | ±400                  | Limite de position supérieure de l'axe 2 (°).                        |
|          | jointLimits_decelJ2  | 0-10000               | Décélération maximale pour arrêter le robot avant la limite.         |
| Axe-3SEL | jointLimits_minPosJ3 | ±400                  | Limite de position inférieure de l'axe 3 (°).                        |
|          | jointLimits_maxPosJ3 | ±400                  | Limite de position supérieure de l'axe 3 (°).                        |
|          | jointLimits_decelJ3  | 0-10000               | Décélération maximale pour arrêter le robot avant la limite.         |
| Axe-4SEL | jointLimits_minPosJ4 | ±400                  | Limite de position inférieure de l'axe 4 (°).                        |
|          | jointLimits_maxPosJ4 | ±400                  | Limite de position supérieure de l'axe 4 (°).                        |
| Axe-5SEL | jointLimits_minPosJ5 | ±400                  | Limite de position inférieure de l'axe 5 (°).                        |
|          | jointLimits_maxPosJ5 | ±400                  | Limite de position supérieure de l'axe 5 (°).                        |
| Axe-6SEL | jointLimits_minPosJ6 | ±10800 <sup>(2)</sup> | Limite de position inférieure de l'axe 6 (°).                        |
|          | jointLimits_maxPosJ6 | ±10800 <sup>(2)</sup> | Limite de position supérieure de l'axe 6 (°).                        |

(1) Les limites de position de sécurité sont toujours prises en compte par le contrôleur de mouvement pour les mouvements programmés, en mode manuel comme automatique. Les limites d'articulation en mode manuel, si elles sont activées, s'appliquent également aux déplacements manuels (jog).

(2) La valeur dépend du modèle de robot. Voir le mode d'emploi du bras.

### 5.3.2 - (SAFECELL) VITESSE LIMITÉE DE SÉCURITÉ (SLS)

M0005313.1

L'utilisation d'une vitesse cartésienne réduite nécessite la licence runtime SafeCell+. Le référencement sûr devrait être activé quand une limite de vitesse cartésienne de sécurité est utilisée (voir chapitre 5.1.2). La vitesse cartésienne est calculée aux points de contrôle (voir chapitre 5.3.4).

L'exactitude de la vitesse cartésienne sûre représente jusqu'à ±20% de la vitesse réelle ; elle dépend beaucoup de la configuration d'articulations du robot. Le contrôleur de mouvement du robot réduit automatiquement la vitesse de celui-ci afin qu'il ne dépasse pas 80% des limites de vitesse de sécurité configurées.

| Type  | Nom                           | Valeurs  | Description (voir chapitre 2.4.3)  |
|-------|-------------------------------|----------|--|
| Robot | maxCartVelManu<br>(SafeCell+) | 50 - 315 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans les modes manuels. |

## 5.3.2.1 - (SafeCell+) Modes manuels de SLS

M0005314.1

## 5.3.2.2 - SLS dans les modes automatiques

M0004703.1

| Type     | Nom                        | Valeurs  | Description (voir chapitre 2.4.3)   |
|----------|----------------------------|----------|---|
| Axe-xSLS | maxVelAuto_J1              | 10-10000 | Vitesse articulaire maximale sur l'axe 1 (°/s) dans les modes automatiques.                 |
|          | maxVelAuto_J2              | 10-10000 | Vitesse articulaire maximale sur l'axe 2 (°/s) dans les modes automatiques.                 |
|          | maxVelAuto_J3              | 10-10000 | Vitesse articulaire maximale sur l'axe 3 (°/s) dans les modes automatiques.                 |
|          | maxVelAuto_J4              | 10-10000 | Vitesse articulaire maximale sur l'axe 4 (°/s) dans les modes automatiques.                 |
|          | maxVelAuto_J5              | 10-10000 | Vitesse articulaire maximale sur l'axe 5 (°/s) dans les modes automatiques.                 |
|          | maxVelAuto_J6              | 10-10000 | Vitesse articulaire maximale sur l'axe 6 (°/s) dans les modes automatiques.                 |
| Robot    | maxCartVelAuto (SafeCell+) | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans les modes automatiques. |

## 5.3.2.3 - SLS USIA

| Type     | Nom                        | Valeurs  | Description  |
|----------|----------------------------|----------|--|
| Bool     | USIA_auto                  | 0 / 1    | USIA est inactif / actif dans les modes automatiques.                                    |
|          | USIA_manu                  | 0 / 1    | USIA est inactif / actif dans les modes manuels.   |
|          | USIA_ss1                   | 0        | USIA ne déclenche pas un arrêt sûr.  |
|          | USIA_ss2                   | 0        |  |
|          | USIA_sls                   | 1        | USIA déclenche une limite de vitesse globale.  |
| Timer    | USIA_maxStopTime           | 496      | Temps de décélération (ms) quand USIA est déclenchée.                                    |
| Axe-xSLS | USIA_maxVelJ1              | 10-10000 | Vitesse articulaire maximale sur l'axe 1 (°/s) quand USIA est déclenché.                 |
|          | USIA_maxVelJ2              | 10-10000 | Vitesse articulaire maximale sur l'axe 2 (°/s) quand USIA est déclenché.                 |
|          | USIA_maxVelJ3              | 10-10000 | Vitesse articulaire maximale sur l'axe 3 (°/s) quand USIA est déclenché.                 |
|          | USIA_maxVelJ4              | 10-10000 | Vitesse articulaire maximale sur l'axe 4 (°/s) quand USIA est déclenché.                 |
|          | USIA_maxVelJ5              | 10-10000 | Vitesse articulaire maximale sur l'axe 5 (°/s) quand USIA est déclenché.                 |
|          | USIA_maxVelJ6              | 10-10000 | Vitesse articulaire maximale sur l'axe 6 (°/s) quand USIA est déclenché.                 |
| Robot    | maxCartVelUSIA (SafeCell+) | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance quand USIA est déclenché. |



La configuration d'USIA comme SLS est ignorée quand USIA\_eStop=1 ou mode\_WMS=1 (voir chapitre 5.2.1).

## 5.3.2.4 - SLS USIB

M0004705.1

| Type         | Nom                           | Valeurs  | Description  |
|--------------|-------------------------------|----------|--|
| Bool         | USIB_auto                     | 0 / 1    | USIB est inactif / actif dans les modes automatiques.                                    |
|              | USIB_manu                     | 0 / 1    | USIB est inactif / actif dans les modes manuels.   |
|              | USIB_ss1                      | 0        | USIB ne déclenche pas un arrêt sûr.  |
|              | USIB_ss2                      | 0        |  |
|              | USIB_sls                      | 1        | USIB déclenche une limite de vitesse globale.  |
|              | USIB_zone<br>(SafeCell+)      | 0        | La limite de vitesse est déclenchée quelle que soit la position du robot.                |
|              |                               | 1        | La limite de vitesse est déclenchée uniquement à l'intérieur de la zone USIB.            |
| Timer        | USIB_maxStopTime              | 496      | Temps de décélération (ms) quand USIB est déclenchée.                                    |
| Axe-<br>xSLS | USIB_maxVelJ1                 | 10-10000 | Vitesse articulaire maximale sur l'axe 1 (°/s) quand USIB est déclenché.                 |
|              | USIB_maxVelJ2                 | 10-10000 | Vitesse articulaire maximale sur l'axe 2 (°/s) quand USIB est déclenché.                 |
|              | USIB_maxVelJ3                 | 10-10000 | Vitesse articulaire maximale sur l'axe 3 (°/s) quand USIB est déclenché.                 |
|              | USIB_maxVelJ4                 | 10-10000 | Vitesse articulaire maximale sur l'axe 4 (°/s) quand USIB est déclenché.                 |
|              | USIB_maxVelJ5                 | 10-10000 | Vitesse articulaire maximale sur l'axe 5 (°/s) quand USIB est déclenché.                 |
|              | USIB_maxVelJ6                 | 10-10000 | Vitesse articulaire maximale sur l'axe 6 (°/s) quand USIB est déclenché.                 |
| Robot        | maxCartVelUSIB<br>(SafeCell+) | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance quand USIB est déclenché. |



## 5.3.2.5 - SLS USIC

M0004706.1

| Type         | Nom                           | Valeurs  | Description  |
|--------------|-------------------------------|----------|--|
| Bool         | USIC_auto                     | 0 / 1    | USIC est inactif / actif dans les modes automatiques.                                    |
|              | USIC_manu                     | 0 / 1    | USIC est inactif / actif dans les modes manuels.   |
|              | USIC_ss1                      | 0        | USIC ne déclenche pas un arrêt sûr.  |
|              | USIC_ss2                      | 0        |  |
|              | USIC_sls                      | 1        | USIC déclenche une limite de vitesse globale.  |
|              | USIC_zone<br>(SafeCell+)      | 0        | La limite de vitesse est déclenchée quelle que soit la position du robot.                |
|              |                               | 1        | La limite de vitesse est déclenchée uniquement à l'intérieur de la zone USIC.            |
| Timer        | USIC_maxStopTime              | 496      | Temps de décélération (ms) quand USIC est déclenchée.                                    |
| Axe-<br>xSLS | USIC_maxVelJ1                 | 10-10000 | Vitesse articulaire maximale sur l'axe 1 (°/s) quand USIC est déclenché.                 |
|              | USIC_maxVelJ2                 | 10-10000 | Vitesse articulaire maximale sur l'axe 2 (°/s) quand USIC est déclenché.                 |
|              | USIC_maxVelJ3                 | 10-10000 | Vitesse articulaire maximale sur l'axe 3 (°/s) quand USIC est déclenché.                 |
|              | USIC_maxVelJ4                 | 10-10000 | Vitesse articulaire maximale sur l'axe 4 (°/s) quand USIC est déclenché.                 |
|              | USIC_maxVelJ5                 | 10-10000 | Vitesse articulaire maximale sur l'axe 5 (°/s) quand USIC est déclenché.                 |
|              | USIC_maxVelJ6                 | 10-10000 | Vitesse articulaire maximale sur l'axe 6 (°/s) quand USIC est déclenché.                 |
| Robot        | maxCartVelUSIC<br>(SafeCell+) | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance quand USIC est déclenché. |

## 5.3.2.6 - SLS USID

M0004707.1

| Type     | Nom                        | Valeurs  | Description  |
|----------|----------------------------|----------|--|
| Bool     | USID_auto                  | 0 / 1    | USID est inactif / actif dans les modes automatiques.                                    |
|          | USID_manu                  | 0 / 1    | USID est inactif / actif dans les modes manuels.   |
|          | USID_ss1                   | 0        | USID ne déclenche pas un arrêt sûr.  |
|          | USID_ss2                   | 0        |  |
|          | USID_sls                   | 1        | USID déclenche une limite de vitesse globale.  |
| Timer    | USID_maxStopTime           | 496      | Temps de décélération (ms) quand USID est déclenchée.                                    |
| Axe-xSLS | USID_maxVelJ1              | 10-10000 | Vitesse articulaire maximale sur l'axe 1 (°/s) quand USID est déclenché.                 |
|          | USID_maxVelJ2              | 10-10000 | Vitesse articulaire maximale sur l'axe 2 (°/s) quand USID est déclenché.                 |
|          | USID_maxVelJ3              | 10-10000 | Vitesse articulaire maximale sur l'axe 3 (°/s) quand USID est déclenché.                 |
|          | USID_maxVelJ4              | 10-10000 | Vitesse articulaire maximale sur l'axe 4 (°/s) quand USID est déclenché.                 |
|          | USID_maxVelJ5              | 10-10000 | Vitesse articulaire maximale sur l'axe 5 (°/s) quand USID est déclenché.                 |
|          | USID_maxVelJ6              | 10-10000 | Vitesse articulaire maximale sur l'axe 6 (°/s) quand USID est déclenché.                 |
| Robot    | maxCartVelUSID (SafeCell+) | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance quand USDI est déclenché. |

## 5.3.3 - (SAFECELL+) SURVEILLANCE DE LA ZONE SÛRE (SZM)

M0004708.1

Le programme de sécurité définit 4 zones sûres : les zones 1 et 2 sont toujours activées, tandis que 2 zones sûres sont liées à USIB et USIC et peuvent être activées ou désactivées à tout moment.

La géométrie des zones sûres permanentes 1 et 2 est définie par la combinaison de jusqu'à 3 volumes de base par zone ; la géométrie des zones sûres activables liées à USIB et USIC est définie par 1 volume de base par zone.

La zone est active soit à l'intérieur du volume défini, soit à l'extérieur. L'action dans la zone est déclenchée quand un point de contrôle (ou plusieurs) se trouve à l'intérieur de la zone.



Les paramètres zoneX\_noSpeedControl définissent les endroits où les zones ne sont PAS actives (voir chapitre 5.3.3.5). Quand zoneX\_noSpeedControl est 'Inside', la zone est active à l'extérieur du volume défini.

La vitesse cartésienne est calculée aux points de surveillance (voir chapitre 5.3.4).



Le contrôleur de mouvement ne tient pas compte des limites de zone sûres lors des grands mouvements des articulations (movej). Un grand mouvement d'articulation passant dans une zone sûre peut être accepté par le contrôleur de mouvements mais pas par le contrôleur de sécurité.

## 5.3.3.1 - Zone 1

| Type     | Nom                         | Valeurs  | Description  |
|----------|-----------------------------|----------|--|
| Bool     | zone1_manu                  | 0 / 1    | La zone 1 est inactive/active dans les modes manuels.                          |
|          | zone1_forbidden<br>(1.001+) | 0        | Une limite de vitesse est déclenchée dans la zone 1.                           |
|          |                             | 1        | Un arrêt SS1 est déclenché dans la zone 1.                                     |
| Axe-xSLS | zone1_maxVelJ1              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 1 dans la zone 1.           |
|          | zone1_maxVelJ2              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 2 dans la zone 1.           |
|          | zone1_maxVelJ3              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 3 dans la zone 1.           |
|          | zone1_maxVelJ4              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 4 dans la zone 1.           |
|          | zone1_maxVelJ5              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 5 dans la zone 1.           |
|          | zone1_maxVelJ6              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 6 dans la zone 1.           |
| Robot    | zone1_maxCartVel            | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans la zone 1. |
|          | zone1A_shape                |          | Définition du volume A pour la zone 1 (voir chapitre 5.3.3.5).                 |
|          | zone1A_noSpeedControl       |          |  |
|          | zone1A_X/Y/Z                |          |  |
|          | zone1A_p1/2/3/4             |          |  |
|          | zone1B_shape                |          | Définition du volume B pour la zone 1 (voir chapitre 5.3.3.5).                 |
|          | zone1B_noSpeedControl       |          |  |
|          | zone1B_X/Y/Z                |          |  |
|          | zone1B_p1/2/3/4             |          |  |
|          | zone1C_shape                |          | Définition du volume C pour la zone 1 (voir chapitre 5.3.3.5).                 |
|          | zone1C_noSpeedControl       |          |  |
|          | zone1C_X/Y/Z                |          |  |
|          | zone1C_p1/2/3/4             |          |  |



Les paramètres zone1X\_noSpeedControl doivent être les mêmes pour les volumes A, B et C.

## 5.3.3.2 - Zone 2

M0004710.1

| Type     | Nom                         | Valeurs  | Description  |
|----------|-----------------------------|----------|--|
| Bool     | zone2_manu                  | 0 / 1    | La zone 2 est inactive/active dans les modes manuels.                          |
|          | zone2_forbidden<br>(1.001+) | 0        | Une limite de vitesse est déclenchée dans la zone 2.                           |
|          |                             | 1        | Un arrêt SS1 est déclenché dans la zone 2.                                     |
| Axe-xSLS | zone2_maxVelJ1              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 1 dans la zone 2.           |
|          | zone2_maxVelJ2              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 2 dans la zone 2.           |
|          | zone2_maxVelJ3              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 3 dans la zone 2.           |
|          | zone2_maxVelJ4              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 4 dans la zone 2.           |
|          | zone2_maxVelJ5              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 5 dans la zone 2.           |
|          | zone2_maxVelJ6              | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 6 dans la zone 2.           |
| Robot    | zone2_maxCartVel            | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans la zone 2. |
|          | zone2A_shape                |          | Définition du volume A pour la zone 2 (voir chapitre 5.3.3.5).                 |
|          | zone2A_noSpeedControl       |          |  |
|          | zone2A_X/Y/Z                |          |  |
|          | zone2A_p1/2/3/4             |          |  |
|          | zone2B_shape                |          | Définition du volume B pour la zone 2 (voir chapitre 5.3.3.5).                 |
|          | zone2B_noSpeedControl       |          |  |
|          | zone2B_X/Y/Z                |          |  |
|          | zone2B_p1/2/3/4             |          |  |
|          | zone2C_shape                |          | Définition du volume C pour la zone 2 (voir chapitre 5.3.3.5).                 |
|          | zone2C_noSpeedControl       |          |  |
|          | zone2C_X/Y/Z                |          |  |
|          | zone2C_p1/2/3/4             |          |  |



Les paramètres zone2X\_noSpeedControl doivent être les mêmes pour les volumes A, B et C.

## 5.3.3.3 - Zone USIB

| Type     | Nom                     | Valeurs  | Description   |
|----------|-------------------------|----------|---|
| Bool     | USIB_auto               | 0 / 1    | USIB est inactif / actif dans les modes automatiques.                             |
|          | USIB_manu               | 0 / 1    | USIB est inactif / actif dans les modes manuels.                                  |
|          | USIB_ss1                | 0 / 1    | Action déclenchée par USIB : arrêt de sécurité ou limite de vitesse de sécurité.  |
|          | USIB_ss2                |          |   |
|          | USIB_sls                |          |   |
|          | USIB_zone               | 1        | L'action d'USIB n'est efficace qu'à l'intérieur de la zone USIB.                  |
| Axe-xSLS | USIB_maxVelJ1           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 1 dans la zone USIB.           |
|          | USIB_maxVelJ2           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 2 dans la zone USIB.           |
|          | USIB_maxVelJ3           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 3 dans la zone USIB.           |
|          | USIB_maxVelJ4           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 4 dans la zone USIB.           |
|          | USIB_maxVelJ5           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 5 dans la zone USIB.           |
|          | USIB_maxVelJ6           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 6 dans la zone USIB.           |
| Robot    | maxCartVelUSIB          | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans la zone USIB. |
|          | zoneUSIB_shape          |          | Définition du volume pour la zone USIB (voir chapitre 5.3.3.5).                   |
|          | zoneUSIB_noSpeedControl |          |   |
|          | zoneUSIB_X/Y/Z          |          |   |
|          | zoneUSIB_p1/2/3/4       |          |   |

## 5.3.3.4 - Zone USIC

M0004712.1

| Type     | Nom                     | Valeurs  | Description   |
|----------|-------------------------|----------|---|
| Bool     | USIC_auto               | 0 / 1    | USIC est inactif / actif dans les modes automatiques.                             |
|          | USIC_manu               | 0 / 1    | USIC est inactif / actif dans les modes manuels.                                  |
|          | USIC_ss1                | 0 / 1    | Action déclenchée par USIC : arrêt de sécurité ou limite de vitesse de sécurité.  |
|          | USIC_ss2                |          |   |
|          | USIC_sls                |          |   |
|          | USIC_zone               | 1        | L'action d'USIC n'est efficace qu'à l'intérieur de la zone USIC.                  |
| Axe-xSLS | USIC_maxVelJ1           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 1 dans la zone USIC.           |
|          | USIC_maxVelJ2           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 2 dans la zone USIC.           |
|          | USIC_maxVelJ3           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 3 dans la zone USIC.           |
|          | USIC_maxVelJ4           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 4 dans la zone USIC.           |
|          | USIC_maxVelJ5           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 5 dans la zone USIC.           |
|          | USIC_maxVelJ6           | 10-10000 | Vitesse maximale de l'articulation (°/s) sur l'axe 6 dans la zone USIC.           |
| Robot    | maxCartVelUSIC          | 10-10000 | Vitesse cartésienne maximale (mm/s) des points de surveillance dans la zone USIC. |
|          | zoneUSIC_shape          |          | Définition du volume pour la zone USIC (voir chapitre 5.3.3.5).                   |
|          | zoneUSIC_noSpeedControl |          |   |
|          | zoneUSIC_X/Y/Z          |          |   |
|          | zoneUSIC_p1/2/3/4       |          |   |

### 5.3.3.5 - Définition des volumes

Les coordonnées X, Y, Z de tous les volumes sont définies dans un référentiel commun. Par défaut, ce système de coordonnées correspond à celui du robot. Il est possible de le modifier à l'aide du paramètre de sécurité robotRz.

| Type                 | Nom             | Valeurs                         | Description   |
|----------------------|-----------------|---------------------------------|---|
| Robot                | shape           | Box / Cylinder / vertical plane | Définition de la forme du volume.   |
|                      | noSpeed-Control | Inside/outside                  | Côté de la forme où la vitesse n'est PAS limitée. Utiliser Inside Vplane pour un plan vertical <sup>(1)</sup> . |
|                      | X / Y / Z       | Box                             | Coordonnées du coin « inférieur gauche » du cube.   |
|                      | p1 / p2 / p3    |                                 | Dimension du cube sur les axes X / Y / Z.   |
|                      | X / Y / Z       | Cylinder                        | Coordonnées du centre de la base du cylindre.   |
|                      | p1              |                                 | Rayon de la base du cylindre.   |
|                      | p2              |                                 | Hauteur du cylindre.  |
|                      | p1 / p2         | Vertical plane                  | Coordonnées X,Y d'un premier point dans le plan vertical.   |
|                      | p3 / p4         |                                 | Coordonnées X,Y d'un deuxième point dans le plan vertical (même Z que le premier point).                        |
| RobotStruct du robot | robotRz         | ±360                            | Angle (°) entre les axes X du robot et les systèmes de coordonnées des volumes.                                 |

- (1) Pour les plans verticaux, le volume sans contrôle de vitesse est défini par l'ordre des points qui définissent le plan.



Pour les zones 1 et 2, les paramètres intérieurs/extérieurs doivent être les mêmes pour les 3 volumes qui définissent la zone. Il est possible de combiner des formes Box et Cylinder, mais vertical plane ne peut être combiné ni à Box ni à Cylinder.

## 5.3.4 - (SAFECELL+) POINTS DE SURVEILLANCE

M0004714.1

| Type          | Nom                                  | Valeurs | Description   |
|---------------|--------------------------------------|---------|---|
| Robot mTools  | tool1_X                              | ±10000  | Coordonnées du TCP par rapport à la bride (mm).<br>(1)  |
|               | tool1_Y                              |         |   |
|               | tool1_Z                              |         |   |
| Robot mGuards | Type                                 | Pos/Vel | Type de surveillance calculé avec le point : position, vitesse ou les deux.   |
|               | Enable                               | 0 / 1   | Désactivation/activation des calculs.   |
|               | tool1Point1_X                        | ±10000  | Coordonnées des points de surveillance par rapport à la bride (mm).   |
|               | tool1Point1_Y                        |         |   |
|               | tool1Point1_Z                        |         |   |
|               | tool1Point2_X                        |         |   |
|               | tool1Point2_Y                        |         |   |
|               | tool1Point2_Z                        |         |   |
|               | tool1Point3_X                        |         |   |
|               | tool1Point3_Y                        |         |   |
|               | tool1Point3_Z                        |         |   |
|               | tool1Point4_X                        |         |   |
|               | tool1Point4_Y                        |         |   |
|               | tool1Point4_Z                        |         |   |
| Robot mGuards | elbow_enable <sup>(2)</sup>          | 0 / 1   | Désactivation/activation des calculs.   |
|               | elbow_X                              | ±10000  | Coordonnées du point de surveillance par rapport à l'intersection des axes 3 et 4 (mm) (dans le référentiel World, quand le robot est dans la position à zéro). |
|               | elbow_Y                              | ±10000  |   |
|               | elbox_Z                              | ±10000  |   |
| Robot mSZMc   | zone1_axis3monitoring <sup>(2)</sup> | 0 / 1   | Désactivation/activation de la surveillance du coude dans la zone 1.  |
|               | zone2_axis3monitoring <sup>(2)</sup> | 0 / 1   | Désactivation/activation de la surveillance du coude dans la zone 2.  |
|               | zone3_axis3monitoring <sup>(2)</sup> | 0 / 1   | Désactivation/activation de la surveillance du coude dans la zone 3.  |
|               | zone4_axis3monitoring <sup>(2)</sup> | 0 / 1   | Désactivation/activation de la surveillance du coude dans la zone 4.  |

(1)



Le TCP défini par le VAL 3 peut être différent du TCP configuré dans la sécurité.

(2)



elbow\_enable doit être défini ou rafraîchi après tous les changements de l'un des paramètres zonex\_axis3monitoring.



## 5.4 - FONCTIONS DE SÉCURITÉ DE CONTRÔLE

### 5.4.1 - (INITIAL) INTERFACE WMS

M0004715.1

| Type | Nom      | Valeurs | Description   |
|------|----------|---------|---|
| Bool | mode_WMS | 0       | Le mode de marche est sélectionné selon mode_MCP et USIA est configurée selon les paramètres USIA_xxx.                    |
|      |          | 1       | Le mode de marche est sélectionné selon les entrées sûres J101 et USIA est configurée comme une entrée d'arrêt d'urgence. |

Le paramètre mode\_WMS est un raccourci qui fait passer en force mode\_MCP à 0 et USIA\_eStop à 1.

### 5.4.2 - (INITIAL) SÉLECTION DU MODE DE MARCHÉ

M0004716.1

| Type | Nom              | Valeurs | Description  |
|------|------------------|---------|--|
| Bool | mode_MCP         | 0       | Le mode de marche est sélectionné à partir des entrées sûres J101.                       |
|      |                  | 1       | Le mode de marche est sélectionné à partir de SRC (interface SP2 ou entrées numériques). |
| Bool | mode_manual-Fast | 0 / 1   | Le mode de marche manuel rapide est désactivé/activé.                                    |



Les paramètres mode\_MCP et mode\_manualFast sont ignorés (mis à 0 de force) quand mode\_WMS est réglé à 1.

### 5.4.3 - (INITIAL) CONTRÔLE DU REDÉMARRAGE (CONFIRMATION DE SÉCURITÉ/ RÉINITIALISATION MANUELLE)

M0004717.1

| Type  | Nom                | Valeurs  | Description  |
|-------|--------------------|----------|--|
| Bool  | restart_mcpAck     | 0        | La confirmation du redémarrage est déclenchée uniquement par un front descendant sur l'entrée sûre J101-4.   |
|       |                    | 1        | La confirmation du redémarrage est déclenchée par la sortie Qrestart de RSI9, un front descendant sur l'entrée sûre J101-4 ou l'interface de sécurité SP2. |
| Bool  | restart_enableAck  | 0 / 1    | Désactive/active la commande du redémarrage dans le contrôleur de sécurité du robot.   |
| Timer | ss2_restartTimeout | 0 – 24d  | Durée maximale de l'arrêt SS2 sans réinitialisation manuelle.  |
| Timer | ss2_restartWarning | 0s – 5s  | Délai avant le redémarrage après un arrêt SS2.   |
| Timer | ss2_restartSlow    | 0s – 10s | Délai avant le redémarrage à pleine vitesse après un arrêt SS2.  |



Les paramètres mode\_MCP et mode\_manualFast sont ignorés (mis à 0 de force) quand mode\_WMS est réglé à 1.

## 5.5 - ENTRÉES/SORTIES DE SÉCURITÉ

### 5.5.1 - (INITIAL) ENTRÉES/SORTIES SUR LE PROFIL ESCLAVE (FSOE)

M0005315.1

Le contenu du profil esclave dépend de la version du programme de sécurité (voir chapitre 3.3.3).

| Type | Nom              | Valeurs  | Description (voir chapitre 3.3.3)                       |
|------|------------------|----------|---|
| Bool | profile_activate | 0        | Le maître FSoE n'a pas le contrôle sûr du robot.        |
|      |                  | 1        | Le maître FSoE a le contrôle sûr du robot.              |
| FBus | profile_address  | 0..65535 | Adresse du FSoE sur la carte de sécurité du contrôleur. |

### 5.5.2 - (SAFECELL) USOA

M0004718.1

| Type | Nom               | Valeurs | Description                                       |
|------|-------------------|---------|---|
| Bool | USOA_VAL3         | 0 / 1   | VAL 3-OUT (voir les chapitres 3.2.5 et 3.3.6).    |
|      | USOA_SS2          |         | SS2-OUT (voir les chapitres 3.2.5 et 3.3.4.3).    |
|      | USOA_eStop        |         | ES-OUT (voir les chapitres 3.2.5 et 3.3.4.3).     |
|      | USOA_eStopWithAck |         | ES-RST-OUT (voir les chapitres 3.2.5 et 3.3.4.3). |

Quand toutes les configurations USOA sont à 0, USOA1 et USOA2 peuvent être entièrement contrôlées dans VAL 3 comme des sorties numériques non sûres.

### 5.5.3 - (SAFECELL) USOB

M0004719.1

| Type | Nom       | Valeurs | Description  |
|------|-----------|---------|--|
| Bool | USOB_VAL3 | 0 / 1   | VAL 3-OUT (voir les chapitres 3.2.5 et 3.3.6).   |
|      | USOB_SOS  |         | SOS-OUT (voir les chapitres 3.2.5 et 3.3.4.3).   |
|      | USOB_mode |         | MODE-OUT (voir chapitre 3.2.5).  |
|      | USOB_SLS  |         | SLSD-OUT (voir chapitre 3.2.5) :<br>USOB1 : 1 quand USID SLS est active<br>USOB2 : 1 quand USID SLS est inactive |

Quand toutes les configurations USOB sont à 0, USOB1 et USOB2 peuvent être entièrement contrôlées dans VAL 3 comme des sorties numériques non sûres.

### 5.5.4 - (SAFECELL) USOC

M0004720.1

| Type | Nom        | Valeurs | Description   |
|------|------------|---------|---|
| Bool | USOC_VAL3  | 0 / 1   | VAL 3-OUT (voir les chapitres 3.2.5 et 3.3.6).  |
|      | USOC_ack   |         | RST-OUT (voir chapitre 3.2.5).<br>USOC1 : 1 en attendant la confirmation de redémarrage<br>USOC2 : transmission du signal de confirmation |
|      | USOC_power |         | PWR-OUT état de l'alimentation (voir chapitre 3.2.5).   |
|      | USOC_SS2   |         | SS2-OUT (voir les chapitres 3.2.5 et 3.3.4.3).  |

Quand toutes les configurations USOC sont à 0, USOC1 et USOC2 peuvent être entièrement contrôlées dans VAL 3 comme des sorties numériques non sûres.

### 5.5.5 - (SAFECELL) CONTRÔLE SÛR DES ÉLECTROVANNES (SVC)

M0004695.1

| Type | Nom                | Valeurs | Description (voir chapitre 3.3.6)   |
|------|--------------------|---------|---|
| Bool | valves_safeControl | 0       | (par défaut) Les vannes sont toujours commandées par SRC.                     |
|      |                    | 1       | Les vannes sont commandées par SRC quand aucun arrêt de sécurité n'est actif. |

## 5.6 - (SAFECELL) FONCTIONS DE DIAGNOSTIC

### 5.6.1 - (SAFECELL) TEST DE RÉFÉRENCEMENT

M0004721.1

Le test de référencement suppose que la surveillance sûre de SLP, SLSc ou SZM soit activée (voir chapitre 5.1.2).

| Type  | Nom                 | Valeurs | Description (voir chapitre 3.3.9)   |
|-------|---------------------|---------|---|
| Bool  | referencing_timeout | 0 / 1   | Désactive/active le test régulier du référencement sûr.   |
| Timer | refWarningDelay     | 0 – 24d | Délai avant déclenchement de l'avertissement de dépassement du délai de test du référencement.              |
| Timer | refTimeoutDelay     | 0 – 24d | Délai avant arrêt ou réduction de la vitesse forcés du robot après l'avertissement de dépassement du délai. |

### 5.6.2 - (SAFECELL) ESSAI DES FREINS

M0004722.1

| Type  | Nom                    | Valeurs | Description (voir chapitre 3.3.10)   |
|-------|------------------------|---------|--|
| Bool  | brakeTest_manu         | 0       | L'essai des freins est en option en mode manuel.   |
|       |                        | 1       | En mode manuel, le robot est maintenu à l'arrêt quand les freins ne sont pas testés ou après l'expiration du délai d'essai des freins. |
| Bool  | brakeTest_auto         | 0       | L'essai des freins est en option en mode automatique.  |
|       |                        | 1       | La vitesse du robot est réduite de force en mode automatique quand les freins ne sont pas testés.                                      |
| Timer | brakeTestWarning-Delay | 0 – 24d | Délai avant déclenchement de l'avertissement de dépassement du délai d'essai des freins.   |
| Timer | brakeTestTimeout-Delay | 0 – 24d | Délai avant arrêt ou réduction de la vitesse forcés du robot après l'avertissement de dépassement du délai.                            |



## 6 - MISE EN SERVICE

La norme EN ISO 13849-2 définit la procédure de validation des systèmes de sécurité conçus conformément à EN ISO 13849-1. Le présent chapitre complète cette norme en détaillant les conditions spécifiques du robot qui doivent être validées et en indiquant la meilleure manière de procéder aux essais de validation sur le robot. L'annexe 7.1 propose une liste de vérifications de validation à utiliser à l'appui de la procédure de validation.

### 6.1 - INFORMATIONS POUR LA VALIDATION

M0004724.1

Comme le spécifie la norme EN ISO 13849-2, certaines informations sont nécessaires pour valider l'implémentation du concept de sécurité. Pour la validation de la sécurité du robot, les informations requises comprennent les spécifications et les descriptions de conception pour :

- L'ensemble des schémas électriques des interfaces de sécurité :  
L'alimentation électrique comportant les entrées et sorties de sécurité du robot doit être identifiée, avec les caractéristiques des signaux.
- Le mode de marche :  
Le dispositif qui définit le mode de marche du robot et les dispositifs qui utilisent ce mode de marche doivent être identifiés.
- La chaîne de contrôle du redémarrage :  
Les dispositifs qui émettent les signaux d'acquiescement du redémarrage au robot et ceux qui reçoivent un de ces signaux du robot doivent être identifiés.
- La chaîne d'arrêt d'urgence :  
Les dispositifs qui envoient les signaux d'arrêt d'urgence au robot et ceux qui reçoivent un de ces signaux du robot doivent être identifiés.
- Les arrêts de protection :  
Les dispositifs qui envoient les signaux d'arrêt de protection au robot et ceux qui reçoivent un de ces signaux du robot doivent être identifiés. Les caractéristiques de chaque signal d'arrêt de protection doivent être identifiées (SS1/SS2, contrôle du redémarrage, modes de marche d'activation).
- Les fonctions de sécurité de limitation (limites de position et de vitesse) :  
Les fonctions de surveillance de la position et de la vitesse doivent être décrites avec leur but, leurs signaux d'activation (le cas échéant) et leur effet.
- Les distances de séparation :  
Les distances de séparation entre le robot et les dispositifs de protection doivent être identifiées, avec le temps d'arrêt maximal du robot utilisé pour les calculer.
- L'espace de travail restreint :  
Les contraintes de l'espace de travail maximal du robot doivent être identifiées, avec le principe sur lequel elles se fondent : limites de position sûres, arrêts sur butées, solidité des barrières. Les différences entre les limites configurées du robot et les positions d'arrêt du robot dans le scénario le plus défavorable doivent être signalées. L'énergie maximale du robot supportée par les barrières utilisées comme limites de protection doit être spécifiée.

La validation se base également sur les paramètres de sécurité du robot, qui sont répertoriés dans le rapport de validation de la sécurité du robot de l'outil SafePMT (voir chapitre 4.4) ; il faut veiller à ce que le rapport de validation sur lequel se base l'application corresponde à la version de sécurité installée sur le robot : pour le vérifier, on peut comparer Program CRC et Configuration CRC (voir chapitre 4.5).

## 6.2 - VALIDATION DES ALIMENTATIONS ÉLECTRIQUES

M0004726.1

Il convient de veiller à ce que la détection des défauts des signaux de sécurité soit compatible avec le niveau de performances de sécurité visé (voir chapitre 3.3.2). Les courts-circuits entre les sorties sûres sont toujours détectés ; en revanche, leur détection entre les entrées sûres du robot dépend du programme de sécurité utilisé.

### ■ Sorties sûres :

Le dispositif connecté doit détecter un contact ouvert sur l'un des 2 signaux de sortie pour satisfaire aux exigences de sécurité de la catégorie 3.

### ■ Entrées sûres :

Si les courts-circuits entre des contacts des entrées ne sont pas détectés par un dispositif externe, il faut vérifier qu'ils le sont par la sécurité du robot (quand ces courts-circuits sont détectés, ceux au 24V ou 0V sont toujours détectés également).

## 6.3 - VALIDATION DES FONCTIONS DE SÉCURITÉ DE CONTRÔLE

### 6.3.1 - MODE DE MARCHÉ

M0004727.1

Le concept de sécurité doit définir l'interface qui contrôle le mode de marche du robot (SP2, WMS ou autre dispositif externe).

Le mode de marche peut être testé en vérifiant que le mode affiché sur SP2 correspond au mode sélectionné et que les modes de marche des différents dispositifs de la cellule concordent.

L'accessibilité de chaque mode de marche doit être vérifiée pour chaque profil d'utilisateur à accès restreint.

### 6.3.2 - CONTRÔLE DU REDÉMARRAGE

M0004728.1

Le concept de sécurité doit définir la nécessité d'une commande du redémarrage pour chaque arrêt sûr possible (voir les chapitres 3.3.4.1 et 3.3.5.1), la ou les interfaces à partir desquelles le signal de confirmation du redémarrage peut être déclenché et le chaînage du signal d'acquiescement du redémarrage entre les différents périphériques de la cellule.

La conformité de la commande du redémarrage au concept de sécurité doit être vérifiée pour :

- La commande du redémarrage après le reboot du contrôleur.
- La commande du redémarrage après le passage du mode de marche en automatique.
- La commande du redémarrage après les arrêts de sécurité, y compris les arrêts d'urgence.

## 6.4 - VALIDATION DES FONCTIONS DE SÉCURITÉ D'ARRÊT

### 6.4.1 - ARRÊTS D'URGENCE

M0004729.1

Il convient de vérifier que chaque arrêt d'urgence de la cellule entraîne un arrêt SS1 du robot avec une commande adéquate du redémarrage, quel que soit le mode de marche (manuel ou automatique). Les signaux d'arrêt d'urgence émis ou transmis par le robot (SP2, WMS, signal d'arrêt d'urgence sur USIA) doivent avoir l'effet attendu sur le reste de la cellule.

### 6.4.2 - ARRÊTS DE PROTECTION

M0004730.1

De la même manière que les arrêts d'urgence sont validés, chaque fonction d'arrêt sûr doit de préférence être validée en vérifiant que le comportement du robot est « correct » et que les signaux d'arrêt qu'il émet ou transmet ont l'effet attendu sur le reste de la cellule.

La définition du comportement « correct » pour les fonctions d'arrêt qui ne sont pas des arrêts d'urgence doit être donnée dans le concept de sécurité ; elle inclut la catégorie d'arrêt (SS1/SS2), les modes de marche d'activation (manuel ou automatique), la commande du redémarrage.

Le temps d'arrêt associé aux arrêts de protection doit être vérifié dans le cadre de la validation des distances de séparation.

### 6.4.3 - ARRÊT DES PÉRIPHÉRIQUES EXTERNES

M0004731.1

Quand le concept de sécurité l'exige, il faut vérifier que les périphériques contrôlés par les sorties de sécurité du robot sont inhibés quand le robot est en arrêt sûr :

- Electrovanes du robot (quand leur contrôle de sécurité est activé).
- Périphériques connectés aux sorties sûres USOA/USOB/USOC (quand la sortie est utilisée comme signal d'activation ou d'inhibition).

Quand une sortie de sécurité peut être commandée par SRC, elle peut être testée via un programme ou bien l'interface du pendant SP2, afin de vérifier que la commande n'a plus d'effet (donc est sûre) quand un arrêt de sécurité est actif.

Quand une sortie de sécurité est contrôlée par un état de sécurité du robot tel que SS2 ou SOS ou l'état d'énergie, le test peut vérifier si les dispositifs externes sont effectivement inhibés quand le robot est dans l'état de sécurité spécifié.

## 6.5 - VALIDATION DES DISTANCES DE SÉPARATION

M0004732.1

Les différentes distances de séparation doivent être validées d'abord en vérifiant que le calcul de la distance de séparation (selon EN ISO 13855 par exemple) utilise le temps d'arrêt indiqué par le rapport de validation, augmenté de 32 ms (voir chapitre 3.3.7). Il faut ensuite vérifier que le robot peut s'arrêter sans erreur, dans les conditions les plus difficiles des applications, comme le décrit par exemple l'annexe D de la norme EN ISO 13855.

## 6.6 - VALIDATION DES FONCTIONS DE SÉCURITÉ DE LIMITATION

M0004733.1

Le concept de sécurité doit identifier les fonctions de sécurité de limitation requises avec leur but (réduction du temps d'arrêt, des limites de l'espace de travail, de l'énergie du robot...), leurs conditions d'activation et leur effet sur le reste de l'équipement.

### 6.6.1 - ACTIVATION DE LA SURVEILLANCE SÛRE

M0004734.1

La surveillance sûre doit être activée de la manière définie dans le chapitre 5.1 pour activer les fonctions de sécurité de limitation.

Pour la version 1.000 de SafeCell+ et les versions antérieures uniquement : Les paramètres safeEncoder\_manu et safeEncoder\_auto peuvent être testés en désactivant le retour du codeur sûr et en utilisant la sortie RSI9 QnoSafePos : ceci doit contraindre le robot à un arrêt sûr.

Les paramètres de sécurité referencing\_manu et referencing\_auto peuvent être testés en réinitialisant le référencement sûr et en utilisant la sortie RSI QresetRef ; la vitesse doit alors être réduite (entrée Fast Speed de RSI9 = OFF) ou le robot arrêté, selon la configuration de sécurité et le mode de marche du robot.

|                  |                        |
|------------------|------------------------|
| safeEncoder_manu | Voir le chapitre 5.1.1 |
| safeEncoder_auto | Voir le chapitre 5.1.1 |

### 6.6.2 - ACTIVATION DES LIMITES DE SÉCURITÉ

M0004737.1

Il importe de vérifier que les limites de position et de vitesse sont activées de la manière définie dans le concept de sécurité :

- Avec le mode de marche (manuel ou automatique).
- Avec le signal d'activation USIA, USIB, USIC ou USID.

6.6.3 - POINTS DE SURVEILLANCE

M0004738.1

Les points de surveillance utilisés dans les calculs de limites pour les fonctions de sécurité SLPc et SLSc doivent être testés selon le concept de sécurité.

Les coordonnées du TCP et d'autres points peuvent être validées à l'aide des emplacements identifiés dans la cellule.

Les coordonnées X, Y, Z du TCP et des autres points peuvent ensuite être testées en amenant chacun de ces points dans une position cartésienne connue dans la cellule et en le comparant, à l'aide de la visualisation de SafePMT, aux coordonnées du TCP/guard dans SafePMT (voir chapitre 4.6.1). L'identifiant d'accès des 4 points de surveillance commence à 352 (350 est l'identifiant du TCP).

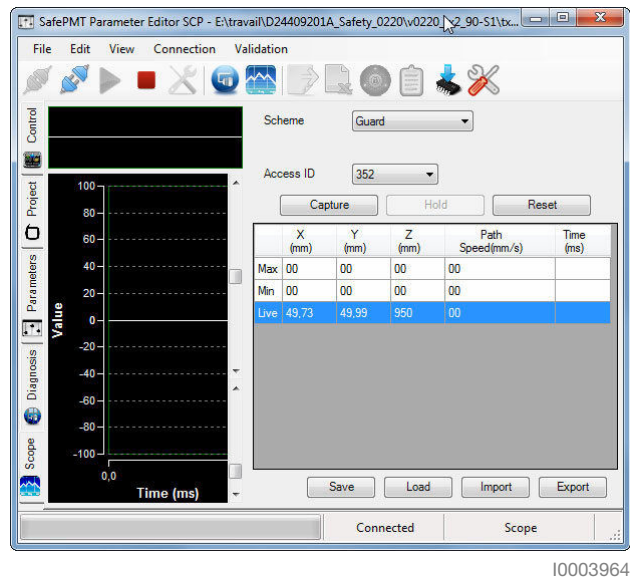


Figure 6.1

6.6.4 - LIMITES DE POSITION

M0004739.1

La surveillance de la position doit être validée d'abord en vérifiant que les limites de position correspondent à celles identifiées dans la disposition de la cellule. Chaque limite peut ensuite être testée en vérifiant le changement du retour de sécurité quand elle est dépassée. Afin d'éviter les arrêts sûrs à chaque fois qu'une limite est atteinte, il vaut mieux effectuer la validation en mode de maintenance (ou en mode manuel si la limite est désactivée en mode manuel).

- Le référencement sûr du robot doit être effectué (voir chapitre 3.3.9).
- Pour les limites des articulations, les positions maximale et minimale de l'articulation jointLimits\_minPosJx et jointLimits\_maxPosJx doivent être testées ; le retour est donnée par l'entrée numérique système lselOK RSI9 (ON dans les limites, OFF en dehors). Il faut vérifier, dans les modes manuels et automatiques, si la surveillance doit aussi être efficace en mode manuel (jointLimits\_manu=1).
- Les limites cartésiennes (zones sûres) peuvent être vérifiées avec un point de surveillance déjà validé (voir chapitre 5.3.4). Chaque paramètre définissant la zone doit ensuite être testé :
  - Cubes : coordonnées X/Y/Z minimum et maximum.
  - Cylindres : coordonnées sur Z minimum et maximum et points diamétralement opposés pour le rayon.
  - Plans verticaux : 2 points espacés.

Le retour est donné par l'entrée numérique lzoneX RSI9 (ON quand la surveillance de la vitesse de la zone est activée, OFF quand elle est désactivée). lzone3 et lzone4 correspondent aux zones associées à USIB et USIC, respectivement.

|                      |                        |
|----------------------|------------------------|
| jointLimits_minPosJx | Voir le chapitre 5.3.1 |
| jointLimits_maxPosJx | Voir le chapitre 5.3.1 |



jointLimits\_manu

Voir le chapitre 5.3.1

### 6.6.5 - LIMITES DE VITESSE

M0004741.1

La vérification des limites de vitesse se base sur les valeurs données dans le rapport de validation. Elle dépend du but de la limitation de vitesse : la vitesse utilisée pendant les tests doit être comparée aux limites de vitesse indiquées dans le rapport de validation.

- Les limites de vitesse utilisées pour réduire le temps d'arrêt sont testées avec les distances de séparation (voir chapitre 6.5).
- Les limites de vitesse utilisées pour réduire la distance d'arrêt dans le scénario le plus défavorable sont testées avec l'espace de travail restreint (voir chapitre 6.7).
- Les limites de vitesse utilisées pour réduire l'énergie maximale du robot sont testées avec l'espace de travail restreint (voir chapitre 6.7).

### 6.7 - VALIDATION DE L'ESPACE DE TRAVAIL RESTREINT

M0004743.1

Le test de l'espace de travail restreint doit être effectué avec des données de simulation conservatrices car les conditions d'essai dans la situation la plus défavorable ne peuvent pas être reproduites à la demande.

Les données de simulation décrites dans le chapitre 3.3.8 peuvent être vérifiées en comparant les paramètres de sécurité (vitesse et décélération maximales de l'articulation) aux valeurs du rapport de validation et en s'assurant que les données de la charge correspondent au scénario le plus défavorable.

Les limites de l'espace de travail restreint sont calculées par l'ajout de la distance maximale au-delà des limites par rapport aux limites du SLP. L'espace de travail restreint peut ensuite être validé en correspondance avec le concept de sécurité et sur site.

Quand l'espace de travail restreint est défini afin de protéger les personnes, un essai de frein régulier est activé de la manière décrite dans le chapitre 3.3.10.

### 6.8 - VALIDATION DES FONCTIONS DE SÉCURITÉ DES ENTRÉES/SORTIES

M0004744.1

La configuration correcte du profil esclave peut être testée en débranchant le câble Ethernet sur J207/208 ; cette déconnexion devrait imposer un arrêt SS1 au robot. L'utilisation du profil de sécurité est validée avec la validation des fonctions de sécurité de commande, d'arrêt et de limitation, activées via l'interface.

Les sorties de sécurité utilisées comme des signaux d'arrêt pour d'autres dispositifs sont validées à l'aide des fonctions de sécurité des sorties (voir chapitre 6.4) ; les sorties de sécurité utilisées pour le contrôle du mode de marche et la commande du redémarrage sont testées à l'aide des fonctions de sécurité de contrôle (voir chapitre 6.3).

Les autres fonctions de sécurité des sorties, par exemple SLSD-OUT, peuvent être testées en vérifiant l'impact sur les périphériques connectés dans les différents états de la sortie.

profile\_activate

Voir le chapitre 5.5.1

## 6.9 - VALIDATION DES FONCTIONS DE DIAGNOSTIC

### 6.9.1 - TEST DE RÉFÉRENCEMENT

M0004745.1

Le test de référencement doit être réalisé de la manière décrite au point 3.3.9.

Il peut être vérifié en imposant un nouveau test de référencement à l'aide de la sortie QforceRefTest RSI9.

L'indépendance entre les deux positions de référencement sûr doit être vérifiée, afin que si le premier référencement est effectué dans une position incorrecte (par ex. mauvaise configuration du bras), le référencement dans la deuxième position ne soit pas possible.

Des mesures sont prises pour empêcher le redémarrage à pleine vitesse après une collision du robot.

### 6.9.2 - ESSAI DES FREINS

M0004746.1

Pour des raisons de sécurité, les freins doivent être testés 100 fois plus souvent qu'ils sont utilisés. Nous recommandons un essai de frein toutes les 24h ; un essai de frein plus fréquent est requis si la cellule est régulièrement arrêtée et que le robot doit alors être arrêté sur ses freins. Le concept de sécurité doit définir la nécessité d'un essai de frein dans les modes manuels et automatiques et évaluer le risque d'arrêt du robot.

La conformité au concept de sécurité de l'activation de l'essai de frein (brakeTest\_auto, brakeTest\_manu) et de son intervalle (brakeTestTimeoutDelay) doit être vérifiée. Le paramètre brakeTestWarningDelay aide à empêcher une erreur de sécurité quand l'intervalle est dépassé : la différence entre brakeTestWarningDelay et brakeTestTimeoutDelay n'est pas importante pour la sécurité.

|                       |                        |
|-----------------------|------------------------|
| brakeTest_auto        | Voir le chapitre 5.6.2 |
| brakeTest_manu        | Voir le chapitre 5.6.2 |
| brakeTestTimeoutDelay | Voir le chapitre 5.6.2 |
| brakeTestWarningDelay | Voir le chapitre 5.6.2 |

## 6.10 - VALIDATION DES MESURES DE SÉCURITÉ

### 6.10.1 - ÉQUIPEMENT DE SÉCURITÉ

M0004747.1

Le concept de sécurité doit identifier l'équipement nécessaire en relation avec la sécurité et les mesures à prendre pour que le personnel concerné l'utilise correctement. Cet équipement peut comprendre :

- Le bouchon de maintenance, pour des opérations d'intégration et de maintenance plus sûres quand les dispositifs de protection de la cellule ne sont pas opérationnels ou doivent être désactivés.
- L'interface RBR, éventuellement avec une alimentation électrique TBTS/TBTP, afin de pouvoir libérer les freins quand le contrôleur ne fonctionne pas.
- Un emplacement pour ranger le SP2 s'il n'est pas connecté en permanence à un robot.

### 6.10.2 - AUTORISATION ET QUALIFICATION DE SÉCURITÉ

M0004748.1

Le concept de sécurité doit identifier les mesures permettant de contrôler l'accès aux opérations liées à la sécurité, par exemple :

- L'accès aux fichiers de la machine, notamment au programme de sécurité et à l'outil de configuration de la sécurité.
- Les profils d'utilisateur du robot, pour contrôler les opérations possibles sur l'interface SP2.
- Les opérations de maintenance nécessitant une qualification de sécurité (remplacement du contrôleur de sécurité).

### 6.10.3 - VALIDATION DES FICHIERS DE LA MACHINE

M0004749.1

Avec les informations de spécification et de conception, les fichiers de la machine doivent contenir les informations utilisées pour la validation, les rapports d'essais de validation et les fichiers requis pour la maintenance sûre de la machine.

- Le rapport de validation finale du robot doit être clairement identifié et ses CRCs et son compteur de mises à jour doivent correspondre aux CRCs et au compteur du robot à la fin de la phase de validation.
- Les fichiers de la machine doivent comprendre une archive du programme de sécurité et de l'outil de configuration de la sécurité.

### 6.11 - REMISE EN SERVICE

M0004750.1

Quand certains paramètres de sécurité doivent être changés pendant ou après une validation de sécurité, une nouvelle validation doit être effectuée ; cependant les tests déjà effectués et dont les résultats ne peuvent pas être affectés par le changement ne doivent cependant pas être refaits.

La description de chaque paramètre de sécurité doit être suffisamment claire pour évaluer l'effet des essais de validation ; en cas de doute, la fonction de sécurité correspondant au paramètre doit être entièrement testée à nouveau.

Après la remise en service, les fichiers de sécurité doivent contenir :

- Les différentes versions du rapport de validation du robot sur lesquelles les essais de validation se sont basés.
- La liste des paramètres modifiés entre chaque version du rapport de validation du robot et la suivante.
- La liste des essais de validation déclarés comme non influencés par le changement et qui n'ont donc pas été refaits.



## 7 - ANNEXES

### 7.1 - LISTE DE VÉRIFICATIONS POUR LA MISE EN SERVICE

M0004725.1

Informations pour la validation (voir chapitre 6.1) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité | Méthode |              |
|----------|--|--------------------------|---------|--------------|
|          |  |                          | Test    | Vérification |
| 6.1      | Le concept de sécurité définit le contrôle du mode de marche et de la commande du redémarrage, la chaîne d'arrêt d'urgence, les arrêts de protection, la fonction de surveillance de la position et de la vitesse avec les distances de séparation et l'espace de travail restreint. |                          |         | X            |
|          | Le Program CRC et la Configuration CRC du rapport de validation du robot utilisés pour la validation concordent avec le Program CRC de RSI et la Configuration CRC du robot.   |                          |         | X            |

Validation des alimentations électriques (voir chapitre 6.2) :

| Chapitre | Mesure applicable   | Paramètre(s) de sécurité | Méthode |              |
|----------|---|--------------------------|---------|--------------|
|          |   |                          | Test    | Vérification |
| 6.2      | Les contacts ouverts sur des sorties sûres sont détectés. |                          | X       | X            |
|          | Les courts-circuits sur des entrées sûres sont détectés.  |                          | X       | X            |

Validation des fonctions de sécurité de contrôle (voir chapitre 6.3) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité                        | Méthode |              |
|----------|--|---|---------|--------------|
|          |  |   | Test    | Vérification |
| 6.3.1    | Chaque mode de marche peut être sélectionné selon la définition donnée dans le concept de sécurité.  | mode_WMS, mode_MCP<br>mode_manualFast           | X       | X            |
|          | Le même mode de marche est partagé par les différents dispositifs qui l'utilisent.   | USOB_mode                                       | X       | X            |
| 6.3.2    | La commande du redémarrage du robot est configuré de la manière définie dans le concept de sécurité.   | restart_mcpAck<br>restart_enableAck<br>USOC_ack | X       | X            |
|          | Si elle est désactivée dans la sécurité du robot, la commande du redémarrage est implémentée ailleurs pour le redémarrage du contrôleur, le changement du mode de marche, les arrêts d'urgence et autres arrêts de protection pour lesquels elle est nécessaire. | restart_enableAck=0                             | X       | X            |

Validation des fonctions de sécurité d'arrêt (voir chapitre 6.4) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité  | Méthode |              |
|----------|--|---|---------|--------------|
|          |  |   | Test    | Vérification |
| 6.4.1    | Tous les arrêts d'urgence de la cellule entraînent un arrêt SS1 du robot avec commande du redémarrage pour les modes manuels et automatiques.  | USIA_eStop mode_WMS   | X       | X            |
|          | Le bouton d'arrêt d'urgence du MCP et tous les autres dispositifs d'arrêt d'urgence connectés au robot provoquent un arrêt SS0 ou SS1 d'autres équipements avec une commande du redémarrage. | USOA_eStop<br>USOA_eStopWithAck                                       | X       | X            |
| 6.4.2    | Tous les arrêts de protection de la cellule arrêtent le robot dans les conditions attendues.   | USlx_manu,<br>USlx_auto,<br>USlx_ack,<br>USlx_ss1=1<br>ou USlx_ss2=1  | X       | X            |
| 6.4.3    | Les sorties sûres USOA/USOB/USOC arrêtent les autres équipements conformément au concept de sécurité.  | USOA_SS2<br>USOC_SS2<br>USOC_power<br>USOx_VAL3<br>valves_safeControl | X       | X            |
|          | Si la SRC a le contrôle de USOA/USOB/USOC ou des électrovannes, celui-ci est désactivé lors des arrêts de protection conformément au concept de sécurité.                                    | USOx_VAL3<br>valves_safeControl                                       | X       | X            |

Validation des distances de séparation (voir chapitre 6.5) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité        | Méthode |              |
|----------|--|---------------------------------|---------|--------------|
|          |  |                                 | Test    | Vérification |
| 6.5      | Les distances de séparation identifiées dans le concept de sécurité sont calculées à partir du temps de réaction de la sécurité (voir chapitre 3.3.7). | maxStopTime<br>USlx_maxStopTime |         | X            |
|          | Avec un temps d'arrêt réduit, le robot peut s'arrêter sans erreur dans les situations les plus difficiles.   |                                 | X       |              |

Validation des fonctions de sécurité de limitation (voir chapitre 6.6) :

| Chapitre | Mesure applicable   | Paramètre(s) de sécurité  | Méthode |              |
|----------|---|---|---------|--------------|
|          |   |   | Test    | Vérification |
| 6.6.1    | La surveillance requise pour SOS, SS2 ou SLSj est activée selon la définition du concept de sécurité.   | safeEncoder_auto<br>safeEncoder_manu  | X       | X            |
|          | La surveillance requise pour SLP, SLSc ou SZM est activée selon la définition du concept de sécurité.   | referencing_auto<br>referencing_manu  | X       | X            |
|          | La perte de communication avec le FSoE maître, s'il y en a un, impose un arrêt SS1 au robot.  | profile_activate  | X       |              |
| 6.6.2    | Les surveillances de la position et de la vitesse sont activées avec les modes de marche et les entrées sûres définies dans le concept de sécurité.             | USIX_SLS, USIB_zone, USIC_zone, zone1_manu, zone2_manu, USIx_auto, USIx_manu  |         | X            |
| 5.3.4    | Les coordonnées du TCP et des points de surveillance correspondent à celles définies dans le concept de sécurité.   | tool1_X / Y / Z<br>tool1Point1_X / Y / Z<br>tool1Point2_X / Y / Z<br>tool1Point3_X / Y / Z<br>tool1Point4_X / Y / Z |         | X            |
|          | La position sûre calculée sur le TCP et au point de calcul correspond à une position connue dans la cellule.  |   | X       |              |
| 6.6.4    | Les limites minimum et maximum de l'articulation correspondent aux limites du concept de sécurité en mode manuel et automatique.                                | jointLimits_minPosJx<br>jointLimits_maxPosJx<br>jointLimits_manu  | X       | X            |
|          | Les limites de chaque volume de base (cube, cylindre, plan) correspondent à celles du concept de sécurité ; la surveillance est active du bon côté des limites. | zoneaB_X, zoneaB_Y, zoneaB_Z, zoneaB_p1, zoneaB_p2, zoneaB_p3, zoneaB_p4  | X       | X            |
| 6.6.5    | Les limites de vitesse correspondent à celles du concept de sécurité.   | maxCartVel_auto<br>zonex_maxCartVel<br>maxCartVel_USIx<br>maxVelAuto_Jx<br>zonei_maxVelJx<br>USIx_maxVelJx          |         | X            |
|          | L'énergie maximale du robot utilisée dans le concept de sécurité est calculée à partir des vitesses maximales des articulations.                                | maxVelAuto_Jx   |         | X            |

Validation de l'espace de travail restreint (voir chapitre 6.7) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité | Méthode |              |
|----------|--|--------------------------|---------|--------------|
|          |  |                          | Test    | Vérification |
| 6.7      | Les limites de l'espace de travail restreint ou de l'énergie du bras sont calculées à l'aide des paramètres corrects de sécurité et de charge. |                          |         | X            |
|          | Les limites de l'espace de travail restreint ou de l'énergie du bras correspondent à celles identifiées dans le concept de sécurité.           |                          |         | X            |
|          | Quand des limites restreintes sont définies, la réinitialisation de l'essai de frein contraint le robot à fonctionner à petite vitesse.        | brake-Test_auto          | X       | X            |

Validation des fonctions de sécurité des sorties (voir chapitre 6.8) :

| Chapitre | Mesure applicable   | Paramètre(s) de sécurité | Méthode |              |
|----------|---|--------------------------|---------|--------------|
|          |   |                          | Test    | Vérification |
| 6.8      | L'effet des autres fonctions de sécurité des sorties (qui ne sont pas déjà validées) est validé par rapport au concept de sécurité. | USOB_SLSD                | X       | X            |

Validation des fonctions de diagnostic (voir chapitre 6.9) :

| Chapitre | Mesure applicable   | Paramètre(s) de sécurité                                 | Méthode |              |
|----------|---|--|---------|--------------|
|          |   |  | Test    | Vérification |
| 6.9.1    | Les positions de référencement rendent le référencement impossible si la configuration du bras est incorrecte.                  | refPos1_Jx, refPos2_Jx                                   | X       | X            |
|          | L'activation du test de référencement et la limite de délai sont configurées de la manière définie dans le concept de sécurité. | referencingTimeout<br>refWarningDelay<br>refTimeoutDelay |         | X            |
|          | Des dispositions sont prises pour vérifier le référencement après une collision du robot.                                       |  |         | X            |
| 6.9.2    | L'essai de frein est activé afin d'éviter les risques liés aux freins, selon la définition du point 3.3.10.                     | brakeTest_auto<br>brakeTest_manu                         | X       |              |
|          | L'intervalle d'essai des freins est défini en fonction des risques, selon la définition du point 3.3.10.                        | brakeTestWarningDelay<br>brakeTestTimeoutDelay           |         | X            |



Validation des mesures de sécurité (voir chapitre 6.10) :

| Chapitre | Mesure applicable  | Paramètre(s) de sécurité | Méthode |              |
|----------|--|--------------------------|---------|--------------|
|          |  |                          | Test    | Vérification |
| 6.10.1   | Une interface de libération des freins (RBR) est disponible avec/sans alimentation 24 V externe, selon la définition du concept de sécurité.   |                          | X       |              |
|          | Un emplacement est défini pour ranger le SP2 s'il n'est pas connecté en permanence à un robot.   |                          |         |              |
|          | Un bouchon de maintenance est disponible pour les opérations d'intégration et de maintenance. Le personnel chargé de l'intégration et de la maintenance est informé de son intérêt afin de ne pas court-circuiter les signaux de sécurité. |                          | X       | X            |
| 6.10.2   | L'accès à l'outil de configuration de la sécurité est limité au personnel disposant des compétences adéquates.   |                          | X       | X            |
|          | Les profils d'utilisateur du robot sont définis de façon à adapter les droits d'accès aux utilisateurs.  |                          | X       | X            |
| 6.10.3   | Les fichiers de la machine contiennent le concept de sécurité, les rapports de validation du robot utilisés et les résultats d'essais.   |                          |         | X            |
|          | Le rapport de validation final du robot est clairement identifié, ses CRCs et son compteur de mises à jour doivent correspondre aux CRCs et au compteur du robot à la fin de la phase de validation.                                       |                          | X       | X            |
|          | Les fichiers de la machine comprennent une archive du programme de sécurité et de l'outil de configuration de la sécurité.   |                          |         | X            |
| 6.11     | Les fichiers de validation contiennent les différentes versions du rapport de validation du robot utilisées pour les essais, avec leurs différences, et la version utilisée comme référence pour chaque test de validation.                |                          |         | X            |

## 7.2 - RSI9 IOS

M0004735.1



Toutes les liaisons de RSI9 IOs commencent par Rsi9IO\.

### 7.2.1 - UTILISATEUR

M0004736.1

| Nom   | Liaison | Description (sorties)   |
|-------|---------|-------------------------|
| usiA1 | lusiA1  | État du signal J100-1.  |
| usiA2 | lusiA2  | État du signal J100-2.  |
| usiB1 | lusiB1  | État du signal J100-5.  |
| usiB2 | lusiB2  | État du signal J100-6.  |
| usiC1 | lusiC1  | État du signal J100-9.  |
| usiC2 | lusiC2  | État du signal J100-10. |
| usiD1 | lusiD1  | État du signal J100-13. |
| usiD2 | lusiD2  | État du signal J100-14. |

| Nom                 | Liaison         | Description (sorties)  |
|---------------------|-----------------|--|
| Power disabled      | Isto1           | <b>ON</b> : Bras hors tension ; <b>OFF</b> : Bras sous puissance.  |
| Safe Torque Off     | Isto2           | <b>ON</b> : STO activé ; <b>OFF</b> : STO désactivé.   |
| Ivalves             | Ivalves         | <b>ON</b> : Électrovannes commandées par VAL 3 ; <b>OFF</b> : les électrovannes sont inhibées par la sécurité. |
| usoA1 (J102-1)      | IusoA1          | État de la sortie sûre USOA1.  |
| usoA2 (J102-2)      | IusoA2          | État de la sortie sûre USOA2.  |
| usoB1 (J102-5)      | IusoB1          | État de la sortie sûre USOB1.  |
| usoB2 (J102-6)      | IusoB2          | État de la sortie sûre USOB2.  |
| usoC1 (J102-9)      | IusoC1          | État de la sortie sûre USOC1.  |
| usoC2 (J102-10)     | IusoC2          | État de la sortie sûre USOC2.  |
| Safe stop 1         | Iss1            | <b>ON</b> : Un arrêt sûr SS0 ou SS1 est actif.   |
| Safe stop 2         | Iss2            | <b>ON</b> : Un arrêt sûr est actif (SS0, SS1 ou SS2).  |
| Fast speed          | IfastSpeed      | <b>ON</b> : Vitesse rapide autorisée ; <b>OFF</b> : Vitesse lente uniquement.                                  |
| IsignalA            | IsignalA        | <b>ON</b> : La fonction de sécurité associée à USIA est activée.   |
| IsignalB            | IsignalB        | <b>ON</b> : La fonction de sécurité associée à USIB est activée.   |
| IsignalC            | IsignalC        | <b>ON</b> : La fonction de sécurité associée à USIC est activée.   |
| IsignalD            | IsignalD        | <b>ON</b> : La fonction de sécurité associée à USID est activée.   |
| Izone1              | Izone1          | <b>ON</b> : La limite de vitesse associée à la zone 1 est activée.   |
| Izone2              | Izone2          | <b>ON</b> : La limite de vitesse associée à la zone 2 est activée.   |
| Izone3              | Izone3          | <b>ON</b> : La limite de vitesse associée à la zone 3 est activée.   |
| Izone4              | Izone4          | <b>ON</b> : La limite de vitesse associée à la zone 4 est activée.   |
| Service mode        | IserviceMode    | <b>ON</b> : Le mode maintenance est actif.   |
| Waiting restart     | IwaitingRestart | <b>ON</b> : Un acquittement du redémarrage (réinitialisation manuelle) est attendue.                           |
| Enabling device     | IenablingDev    | <b>ON</b> : Le bouton d'activation est actionné et testé.  |
| MPC plug            | ImcpPlug        | <b>ON</b> : Le bouchon J103 MCP est en place.  |
| MCP removal         | ImcpRemoval     | <b>ON</b> : Demande de retrait du SP2.   |
| Referencing warning | IrefWarning     | <b>ON</b> : Le référencement doit être vérifié à nouveau.  |
| Brake test warning  | IbrakeTestWarn  | <b>ON</b> : Les freins doivent être essayés à nouveau.   |
| Brake test OK       | IbrakeTestOK    | <b>ON</b> : L'essai de frein en cours est réussi.  |

| Nom            | Liaison        | Description (sorties)                                     |
|----------------|----------------|---|
| Referencing OK | IreferencingOK | <b>ON</b> : L'essai de référencement en cours est réussi. |

| Nom            | Liaison       | Description (sorties)   |
|----------------|---------------|---|
| usoA1(J102-1)  | QusoA1        | Contrôle la sortie usoA1 (si elle est activée).   |
| usoA2(J102-2)  | QusoA2        | Contrôle la sortie usoA2 (si elle est activée).   |
| usoB1(J102-5)  | QusoB1        | Contrôle la sortie usoB1 (si elle est activée).   |
| usoB2(J102-6)  | QusoB2        | Contrôle la sortie usoB2 (si elle est activée).   |
| usoC1(J102-9)  | QusoC1        | Contrôle la sortie usoC1 (si elle est activée).   |
| usoC2(J102-10) | QusoC2        | Contrôle la sortie usoC2 (si elle est activée).   |
| Qrestart       | Qrestart      | Contrôle de l'acquittement du redémarrage du logiciel (si elle est activée).                                    |
| QmcpRemoval    | QmcpRemoval   | Signal de demande pour le remplacement du SP2 par son bouchon.  |
| QsosEnable     | QsosEnable    | Signal de demande pour relier le bouton d'activation du SP2 à un arrêt SS2 quand le bras est déjà sous tension. |
| QforceRefTest  | QforceRefTest | Réinitialise la vérification du référencement afin d'imposer un nouvel essai.                                   |
| QresetRef      | QresetRef     | Réinitialise le référencement sûr.  |

### 7.2.2 - SYSTÈME







M0004740.1

| Nom           | Liaison     | Description (sorties)  |
|---------------|-------------|--|
| Enabling 1    | Ienabling1  | État du signal J103-7.   |
| Enabling 2    | Ienabling2  | État du signal J103-2.   |
| Mcp eStop 1   | ImcpEstop1  | État du signal J103-5.   |
| Mcp eStop 2   | ImcpEstop2  | État du signal J103-3.   |
| WMS local     | IwmsAutoL   | État du signal J101-1.   |
| WMS remote    | IwmsAutoR   | État du signal J101-2.   |
| WMS manu      | IwmsManuS   | État du signal J101-3.   |
| WMS restart   | IwmsRestart | État du signal J101-4.   |
| Brake Control | Isbc        | <b>ON</b> : La fonction de sécurité SBC est active (freins serrés).  |
| Safe position | IsafePos    | <b>ON</b> : Le référencement sûr est défini (fonctions de sécurité SS2, SLP, SLS et SZM activées).                 |
| Safe velocity | IsafeVel    | <b>ON</b> : Pas de référencement sûr défini, retour du codeur OK (fonctions de sécurité SS2 et SLSj non activées). |
| Safe recovery | IsafeRec    | <b>ON</b> : Le référencement sûr doit être vérifié.  |

| Nom         | Liaison     | Description (sorties)   |
|-------------|-------------|---|
| QmcpRemoval | QmcpRemoval | Signal de demande pour le remplacement du SP2 par son bouchon.  |
| QsosEnable  | QsosEnable  | Signal de demande pour relier le bouton d'activation du SP2 à un arrêt SS2 quand le bras est déjà sous tension. |
| QnoSafePos  | QnoSafePos  | Ignorer les erreurs dans le retour du codeur sûr.   |
| QrefPos1    | QrefPos1    | Demande de définition du référencement sûr dans la première position de référencement.                          |
| QrefPos2    | QrefPos2    | Demande de test du référencement sûr dans la deuxième position de référencement.                                |

| Nom            | Liaison         | Description (entrées analogiques)   |
|----------------|-----------------|---|
| IBstatusSS1    | IBstatusSS1     | Code de l'arrêt SS1 actuel - 0 si pas d'arrêt SS1.  |
| IBdiagSS1      | IBdiagSS1       | Code de l'arrêt SS1 qui a coupé l'alimentation du bras (remis à 0 lors de la mise sous tension suivante du bras). |
| IBdiagAlarm    | IBdiagAlarm     | Code de l'alarme de sécurité actuelle. Un redémarrage est nécessaire pour la récupération.                        |
| Temperature    | IWtemperature   | Température de la carte RSI9 <sup>(1)</sup> .   |
| Status         | IBstatus        | État de la carte RSI.   |
| Error code     | IWerrorCode     | Code d'erreur pour la carte RSI.  |
| Upload counter | IWuploadCounter | Compteur de mises à jour du programme de sécurité RSI.  |

(1) La température de la carte ne doit pas dépasser 72°C.

| État de RSI |             | Description  |
|-------------|-------------|--|
| Code        | Nom         |  |
| 0           | NO_COMM     |  Pas de communication entre RSI9 et la SRC.   |
| 4           | RUNNING     |  RSI9 en fonctionnement.  |
| 5           | STOPPED     |  RSI9 arrêté à partir de l'interface SafePMT : redémarrer à partir de SafePMT.  |
| 6           | FATAL ERROR |  RSI9 arrêté avec code d'erreur : après avoir résolu la cause de l'erreur, redémarrer le contrôleur pour acquitter.                 |
| 7           | ALARM       |  RSI9 arrêté avec code d'erreur : après avoir résolu la cause de l'erreur, appuyer sur « Update » sur le contrôleur pour acquitter. |
| 8           | STANDALONE  |  RSI9 en mode autonome (DSI9 non utilisé pour la sécurité fonctionnelle).   |
| 1           | INIT_START  | États d'initialisation internes de RSI9.   |
| 2           | INIT_CHECK  |  |
| 3           | INIT_BUS    |  |

## 7.3 - ENTRÉES-SORTIES DE DSI9 (SYSTÈME)








Toutes les liaisons de DSI9 commencent par DsiI\O\

| Nom             | Liaison          | Description (sorties)                        |
|-----------------|------------------|--|
| DSI temperature | dsi_temp         | Température de la carte DSI9. <sup>(1)</sup> |
| Motor 1 temp.   | motorProbe1_temp | Température du moteur 1.                     |
| Motor 2 temp.   | motorProbe2_temp | Température du moteur 2.                     |
| Motor 3 temp.   | motorProbe3_temp | Température du moteur 3.                     |
| Motor 4 temp.   | motorProbe4_temp | Température du moteur 4.                     |
| Motor 5 temp.   | motorProbe5_temp | Température du moteur 5.                     |
| Motor 6 temp.   | motorProbe6_temp | Température du moteur 6.                     |
| Encoder 1 temp. | encoder1_temp    | Température du codeur 1. <sup>(2)</sup>      |
| Encoder 2 temp. | encoder2_temp    | Température du codeur 2. <sup>(2)</sup>      |
| Encoder 3 temp. | encoder3_temp    | Température du codeur 3. <sup>(2)</sup>      |
| Encoder 4 temp. | encoder4_temp    | Température du codeur 4. <sup>(2)</sup>      |
| Encoder 5 temp. | encoder5_temp    | Température du codeur 5. <sup>(2)</sup>      |
| Encoder 6 temp. | encoder6_temp    | Température du codeur 6. <sup>(2)</sup>      |
| DSI state       | dsi_state        | État de la carte DSI.                        |
| DSI error code  | dsi_errorCode    | Code d'erreur pour la carte DSI.             |

(1) La température de la carte doit se maintenir entre 0°C et 72°C.

(2) La température du codeur ne doit pas dépasser 110°C.

| État de DSI |             | Description  |
|-------------|-------------|--|
| Code        | Nom         |  |
| 0           | NO_COMM     |  Pas de communication entre DSI9 et la SRC.   |
| 4           | RUNNING     |  DSI9 en fonctionnement.  |
| 6           | FATAL ERROR |  DSI9 arrêté avec code d'erreur : après avoir résolu la cause de l'erreur, redémarrer le contrôleur pour acquitter.   |
| 7           | ALARM       |  DSI9 arrêté avec code d'erreur : après avoir résolu la cause de l'erreur, appuyer sur « Update » sur le contrôleur pour acquitter.                         |
| 8           | STANDALONE  |  DSI9 en mode autonome (pas de communication avec RSI9). Enlever ou éteindre l'interface RBR, puis appuyer sur « Update » sur le contrôleur pour acquitter. |
| 1           | INIT_SYNC   | États d'initialisation internes de DSI9.   |
| 2           | INIT_CHK1   |  |
| 3           | INIT_START  |  |
| 5           | INIT_CONFIG |  |
| 9           | INIT_ETH1   |  |
| 10          | INIT_CHK2   |  |
| 11          | INIT_ETH2   |  |

## 7.4 - VERSION DE SÉCURITÉ

### 7.4.1 - MICROGICIELS DE SÉCURITÉ

M0005455.1

Les versions de microgiciel des cartes de sécurité Rsi9 et Dsi9 doivent concorder, selon le tableau ci-dessous :

| Rsi9      | Dsi9     | SRC (TX2) | SRC (TS2) | SafePMT  |
|-----------|----------|-----------|-----------|----------|
| 2.0.0.3   | 1.0.0.4  | s8.9.1+   | s8.9.1+   | 3.0.0.28 |
| 1.0.0.10F | 0.1.1.36 | s8.5.1+   | s8.7+     | 3.0.0.28 |

Les versions du programme de sécurité prises en charge par chaque version du microgiciel Rsi9 sont détaillées dans les chapitres qui suivent.

## 7.4.2 - VERSIONS DE SÉCURITÉ INITIAL

M0005456.1

### Compatibilités

| Version | Famille | CRC        | SRC<br>Rsi9 1.0.1.10F | SRC<br>Rsi9 2.0.0.3    | SafePMT  |
|---------|---------|------------|-----------------------|------------------------|----------|
| 200.004 | TX2     | 1612935308 | s8.5.1+               | s8.9.1+                | 3.0.0.28 |
|         | TS2     | 4208504370 | s8.7+                 |                        |          |
| 200.003 | TX2     | 1429475567 | s8.5.1+               |                        |          |
|         | TS2     | 1493294710 | s8.7+                 |                        |          |
| 200.002 | TX2     | 4019834916 | s8.5.1+               |                        |          |
|         | TS2     | 666524696  | s8.7+                 |                        |          |
| 200.001 | TX2     | 1647715867 | s8.5.1+               |                        |          |
| 200.000 | TX2     | 2903133238 | s8.5.1+               | s8.9.1+ <sup>(1)</sup> |          |

(1) La procédure de changement de codeur n'est pas prise en charge.

### Modifications

| Version | Descriptif  |
|---------|---|
| 200.004 | <ul style="list-style-type: none"> <li>■ Prise en charge de l'option d'axe continu TX2 &amp; TS2.</li> <li>■ TS2 : possibilité d'ouvrir les axes 3 &amp; 4 ensemble.</li> </ul>                           |
| 200.003 | <ul style="list-style-type: none"> <li>■ Prise en charge du profil esclave FSoE (5.5.1) .</li> <li>■ TS2 : prévention de l'erreur de survitesse lors des déplacements manuels de l'axe 1 ou 2.</li> </ul> |
| 200.002 | <ul style="list-style-type: none"> <li>■ Limites de vitesse sûres en mode de desserrage manuel des freins.</li> </ul>   |
| 200.001 | <ul style="list-style-type: none"> <li>■ Prise en charge des bras TS2.</li> </ul>   |
| 200.001 | <ul style="list-style-type: none"> <li>■ Première version "Initial" pour les bras TX2.</li> </ul>   |

**Bras & CRCs**

| Bras  | Version | Programme CRC | Configuration de CRC par défaut avec contrôle des impulsions |            |
|---|---------|---------------|--|------------|
|   |         |               | Pas de WMS   | Avec WMS   |
| TS2-40-S1<br>TS2-60-S1<br>TS2-80-S1<br>TS2-100-S1 | 200.004 | 4208504370    | 488499114  | 3416178294 |
| TX2-40-S2   |         | 1612935308    | 2940407921   | 1340482888 |
| TX2-60-S1/S2                                      |         |               | 3668060093   | 973542020  |
| TX2-60L-S1/S2                                     |         |               | 1928736715   | 2454919922 |
| TX2-90-S1/S2                                      |         |               | 1782621793   | 2330301272 |
| TX2-90L-S1/S2                                     |         |               | 3317907796   | 627471469  |
| TX2-90XL-S1/S2                                    |         |               | 2364854685   | 1817306276 |
| TS2-40-S1   | 200.003 | 1493294710    | 1648789705   | 4120240026 |
| TS2-60-S1   |         |               | 1789654868   | 4252540935 |
| TS2-80-S1   |         |               | 2606539178   | 210761465  |
| TS2-100-S1  |         |               | 914342765  | 2712441918 |
| TX2-40-S2   |         | 1429475567    | 811592038  | 1319239951 |
| TX2-60-S1/S2                                      |         |               | 3937088386   | 2488720363 |
| TX2-60L-S1/S2                                     |         |               | 1124023284   | 1006818205 |
| TX2-90-S1/S2                                      |         |               | 3633777333   | 2792022748 |
| TX2-90L-S1/S2                                     |         |               | 1997860224   | 166266345  |
| TX2-90XL-S1/S2                                    |         |               | 1042513225   | 1088328992 |
| TS2-40-S1   |         | 666524696     | 396073434  | 2152255113 |
| TS2-60-S1   |         |               | 527885895  | 2292560148 |
| TS2-80-S1   |         |               | 468239288  | 2035476458 |
| TS2-100-S1  |         |               | 1134744190   | 3564209453 |
| TX2-40-S2   | 200.002 | 4019834916    | 2169669285   | 4289687244 |
| TX2-60-S1/S2                                      |         |               | 1875289694   | 289099319  |
| TX2-60L-S1/S2                                     |         |               | 3348278824   | 3111077441 |
| TX2-90-S1/S2                                      |         |               | 1576705897   | 587691776  |
| TX2-90L-S1/S2                                     |         |               | 4068046940   | 2357497909 |
| TX2-90XL-S1/S2                                    |         |               | 3142510741   | 3316842748 |



| Bras           | Version | Programme CRC | Configuration de CRC par défaut avec contrôle des impulsions |            |
|----------------|---------|---------------|--|------------|
|                |         |               | Pas de WMS   | Avec WMS   |
| TS2-40-S1      | 200.001 | 3812939765    | 3807570651   | 2496023991 |
| TS2-60-S1      |         |               | 3927938374   | 2620076586 |
| TS2-80-S1      |         |               | 468239288  | 1843160276 |
| TS2-100-S1     |         |               | 3066798463   | 3237938707 |
| TX2-40-S2      |         | 1647715867    | 549059902  | 1686896913 |
| TX2-60-S1/S2   |         |               | 1358388221   | 348301266  |
| TX2-60L-S1/S2  |         |               | 4171453323   | 3163991972 |
| TX2-90-S1/S2   |         |               | 2131283643   | 993866388  |
| TX2-90L-S1/S2  |         |               | 3498781070   | 2495534497 |
| TX2-90XL-S1/S2 |         |               | 2579282247   | 3716760936 |
| TX2-40-S2      | 200.000 | 2903133238    | 171545454  | 1666332692 |
| TX2-60-S1/S2   |         |               | 2727275322   | 3420799040 |
| TX2-60L-S1/S2  |         |               | 182117196  | 1672562742 |
| TX2-90-S1/S2   |         |               | 493151452  | 1947160486 |
| TX2-90L-S1/S2  |         |               | 3001484265   | 3683428499 |
| TX2-90XL-S1/S2 |         |               | 4224750368   | 2461743194 |

### 7.4.3 - VERSIONS DE SAFECELL

M0005459.1

#### Compatibilités

| Version | Famille | CRC        | SRC Rsi9 1.0.1.10F | SRC Rsi9 2.0.0.3 | SafePMT  |
|---------|---------|------------|--------------------|------------------|----------|
| 100.003 | TX2     | 1449620463 | s8.5.1+            | s8.9.1+          | 3.0.0.28 |

#### Modifications

| Version | Descriptif                                       |
|---------|--|
| 100.003 | ■ Première version "SafeCell" pour les bras TX2. |

#### Bras & CRCs

| Bras           | Version | Programme CRC | Configuration de CRC par défaut avec contrôle des impulsions |            |
|----------------|---------|---------------|--|------------|
|                |         |               | Pas de WMS   | Avec WMS   |
| TX2-40-S2      | 100.003 | 1449620463    | 4140896787   | 2284649082 |
| TX2-60-S1/S2   |         |               | 740673783  | 1389895838 |
| TX2-60L-S1/S2  |         |               | 2222047361   | 4203489512 |
| TX2-90-S1/S2   |         |               | 505016768  | 1625561513 |
| TX2-90L-S1/S2  |         |               | 2979665653   | 3479699100 |
| TX2-90XL-S1/S2 |         |               | 4172121660   | 2253418069 |

## 7.4.4 - VERSION SAFECCELL+

M0005460.1

## Compatibilités

| Version | Famille | CRC        | SRC<br>Rsi9 1.0.1.10F | SRC<br>Rsi9 2.0.0.3    | SafePMT  |
|---------|---------|------------|-----------------------|------------------------|----------|
| 1.003   | TX2     | 2396959198 | s8.3.1+               | s8.9.1+                | 3.0.0.28 |
| 1.001   | TX2     | 861061244  |                       |                        |          |
| 1.000   | TX2     | 2407622360 |                       |                        |          |
| 0.230   | TX2     | 2781859802 |                       | s8.9.1+ <sup>(1)</sup> |          |
| 0.220   | TX2     | 1156050209 |                       |                        |          |

(1) La procédure de changement de codeur n'est pas prise en charge.

## Modifications

| Ver-<br>sion | Descriptif  |
|--------------|---|
| 1.003        | <ul style="list-style-type: none"> <li>■ Arrêt configurable du dispositif d'activation : SS1 ou SS2 (voir chapitre 3.3.4.2).</li> <li>■ Vitesse cartésienne maximale en mode manuel configurable.</li> <li>■ Inhibition du référencement sûr quand l'option de référencement n'est pas activée.</li> <li>■ Prise en charge de l'activation à petite vitesse du profil esclave FSoE.</li> <li>■ Arrêt systématique du robot en cas de perte de la rétrosignalisation du codeur (voir chapitre 5.1.1).</li> </ul>   |
| 1.001        | <ul style="list-style-type: none"> <li>■ Limites de vitesse sûres en mode de desserrage manuel des freins.</li> <li>■ Inhibition du délai d'expiration de l'essai de frein quand l'essai de frein n'est pas activé.</li> <li>■ Inhibition de l'erreur de survitesse en cas de perte du référencement.</li> <li>■ Inhibition de l'erreur Starc quand un arrêt SS1 se produit avec le robot en arrêt SS2.</li> </ul>  |
| 1.000        | <ul style="list-style-type: none"> <li>■ Amélioration de la commande de redémarrage SS2 avec les signaux d'arrêt SS2 très courts.</li> <li>■ Retrait du MCP sans arrêt d'urgence limité désormais au seul mode à distance automatique.</li> <li>■ Possibilité de contraindre le robot à vitesse réduite après le délai d'expiration du référencement.</li> <li>■ Limites maximales des articulations sur l'axe 6 élargies.</li> <li>■ Inhibition de l'arrêt SS0 à l'expiration du délai de l'essai de frein ou de référencement.</li> </ul>   |
| 0.230        | <ul style="list-style-type: none"> <li>■ Réduction du temps d'arrêt minimum pour TX2-40, TX2-60 et TX2-60L.</li> <li>■ Commande de redémarrage pour les arrêts SS2 : temporisation du redémarrage, redémarrage lent, délai d'expiration de SS2.</li> <li>■ Prise en charge de la surveillance de la position du coude pour les zones sûres.</li> <li>■ Prise en charge de l'arrêt SS1 ou SS2 activable dans les zones sûres (USIB, USIC).</li> <li>■ Prise en charge du profil esclave FSoE.</li> <li>■ Prise en charge du mode d'économie d'énergie SRC.</li> <li>■ Prise en charge de l'alimentation électrique externe 24V avec maintien de la surveillance de l'arrêt d'urgence.</li> </ul> |
| 0.220        | <ul style="list-style-type: none"> <li>■ Première version "SafeCell+" pour les bras TX2.</li> </ul>   |

## Bras & CRCs

| Bras           | Version | Programme CRC | Configuration de CRC par défaut avec contrôle des impulsions |            |
|----------------|---------|---------------|--|------------|
|                |         |               | Pas de WMS   | Avec WMS   |
| TX2-40-S2      | 1.003   | 2396959198    | 903517955  | 1260879722 |
| TX2-60-S1/S2   |         |               | 4012789223   | 2446566798 |
| TX2-60L-S1/S2  |         |               | 1199195537   | 965193208  |
| TX2-90-S1/S2   |         |               | 3708974288   | 2750389433 |
| TX2-90L-S1/S2  |         |               | 1922143205   | 208436108  |
| TX2-90XL-S1/S2 |         |               | 1000735532   | 1163651909 |
| TX2-40-S2      | 1.001   | 861061244     | 1575518800   | 588606009  |
| TX2-60-S1/S2   |         |               | 2266781876   | 4192317661 |
| TX2-60L-S1/S2  |         |               | 793268418  | 1370863787 |
| TX2-90-S1/S2   |         |               | 3038798211   | 3420293610 |
| TX2-90L-S1/S2  |         |               | 446924470  | 1683910367 |
| TX2-90XL-S1/S2 |         |               | 1402214015   | 761921046  |
| TX2-40-S2      | 1.000   | 2407622360    | 3567416905   | 2425850470 |
| TX2-60-S1/S2   |         |               | 2766983306   | 3772329125 |
| TX2-60L-S1/S2  |         |               | 213440764  | 1217209555 |
| TX2-90-S1/S2   |         |               | 2333296076   | 3475421667 |
| TX2-90L-S1/S2  |         |               | 613458681  | 1621450454 |
| TX2-90XL-S1/S2 |         |               | 1839673904   | 697486879  |
| TX2-40-S2      | 0.230   | 2781859802    | 1764440967   | 756991912  |
| TX2-60-S1/S2   |         |               | 426089796  | 1565548907 |
| TX2-60L-S1/S2  |         |               | 2972816690   | 4110706973 |
| TX2-90-S1/S2   |         |               | 1269541703   | 262035304  |
| TX2-90L-S1/S2  |         |               | 3827846258   | 2686300253 |
| TX2-90XL-S1/S2 |         |               | 2904546491   | 3911852180 |
| TX2-40-S2      | 0.220   | 1156050209    | 4283227712   | 984236705  |
| TX2-60-S1/S2   |         |               | 2384480198   | 1271323431 |
| TX2-60L-S1/S2  |         |               | 645156784  | 3818050385 |
| TX2-90-S1/S2   |         |               | 3128363245   | 2140247052 |
| TX2-90L-S1/S2  |         |               | 368373720  | 3490870073 |
| TX2-90XL-S1/S2 |         |               | 1556315921   | 2569397232 |

## 7.5 - VERSIONS DE SAFECELL

M0005461.1

### Modifications

| Version        | Descriptif  |
|----------------|---|
| D.280.947.xx-D | ■ 3.2.5 : ajout du PFHd du bus de sécurité fonctionnelle (FSOE)   |
|                | ■ 3.3.5.1, 3.3.5.3 : amélioration de la documentation pour le WMS personnalisé par l'utilisateur ; ajout du mode de maintenance |
|                | ■ 3.3.7 : amélioration de la documentation ; éclaircissements sur le temps de réaction de FSoE                                  |
|                | ■ 3.3.8 : référence à l'outil BDC et procédure de test de la distance d'arrêt   |
|                | ■ 3.3.9 : actualisation de la description du référencement ; ajout du référencement_USID1                                       |
|                | ■ 3.3.10 : actualisation du comportement à l'expiration du délai d'essai de frein   |
|                | ■ 3.3.4.2, 5.2.2 : activation de la configuration du dispositif (activation_SS2)  |
|                | ■ 5.3.2 : ajout de maxCartVelManu, unités de vitesse  |
|                | ■ 5.3.3 : amélioration de la définition des zones et des points de surveillance ; ajout de robotRz                              |
|                | ■ 2.1.1, 2.1.4, 3.3.3, 5 : explicitation des différences entre les versions Initial, SafeCell et SafeCell+ du programme         |
|                | ■ 7.4 : actualisation & description complète des versions ; ajout des tableaux de compatibilité                                 |