

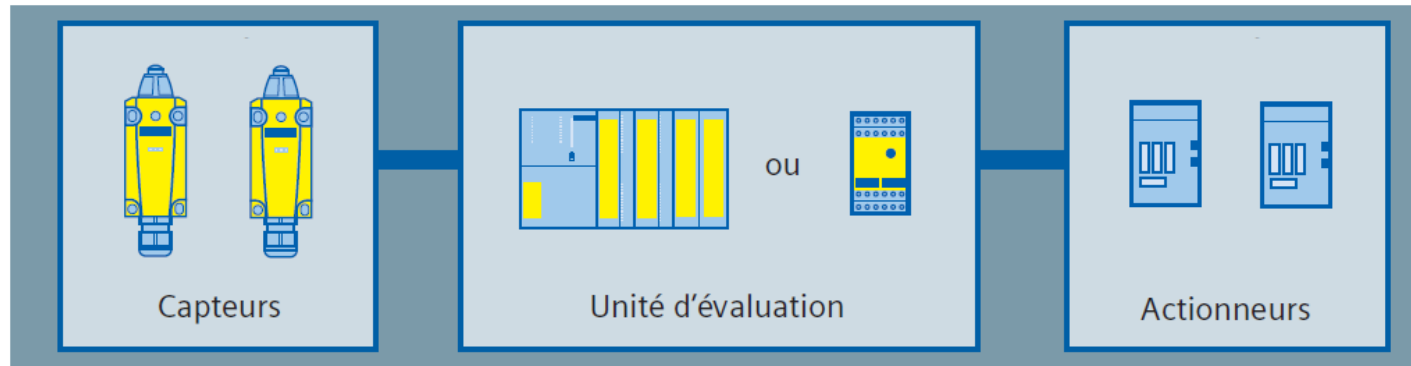
CHAPITRE 2

SOMMAIRE:

□	Présentation d'un système	<u>P 02.</u>
□	Modules d'entrées TOR Safety.....	<u>P 05.</u>
□	Raccordement module entrées TOR.....	<u>P 06.</u>
□	Modules de sorties TOR Safety.....	<u>P 12.</u>
□	Raccordement module sorties TOR.....	<u>P 13.</u>
□	Adresse PROFISAFE.....	<u>P 15.</u>
□	Spécificités des modules Safety	<u>P 18.</u>
□	Spécificités d'un programme Safety	<u>P 27.</u>
□	Langages CONT F et LOG F.....	<u>P 35.</u>
□	Les blocs programme Safety.....	<u>P 38.</u>
□	Protection d'accès.....	<u>P 49.</u>
□	Safety mode.....	<u>P 50.</u>
□	Comparaison.....	<u>P 51.</u>
□	Diagnostic.....	<u>P 52.</u>
□	Alarme de diagnostic.....	<u>P 55.</u>

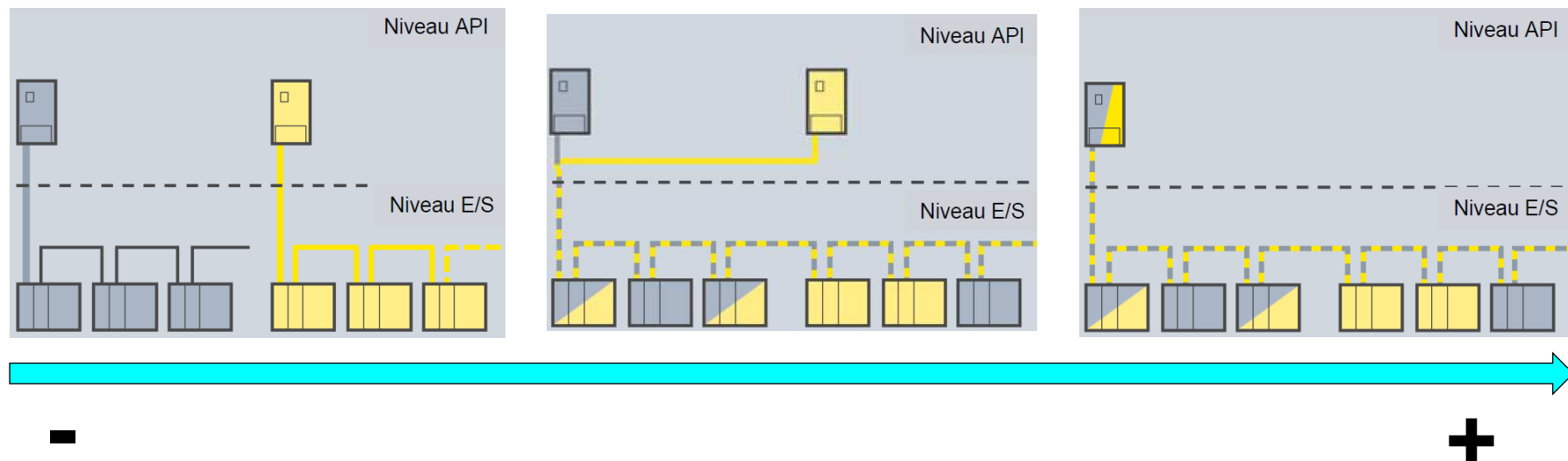
Structure d'une fonction de sécurité :

- Deux type de solutions pour traiter la fonction de sécurité d'un automatisme :



Automate Safety :

- Différents niveaux d'intégration de la fonction de sécurité :

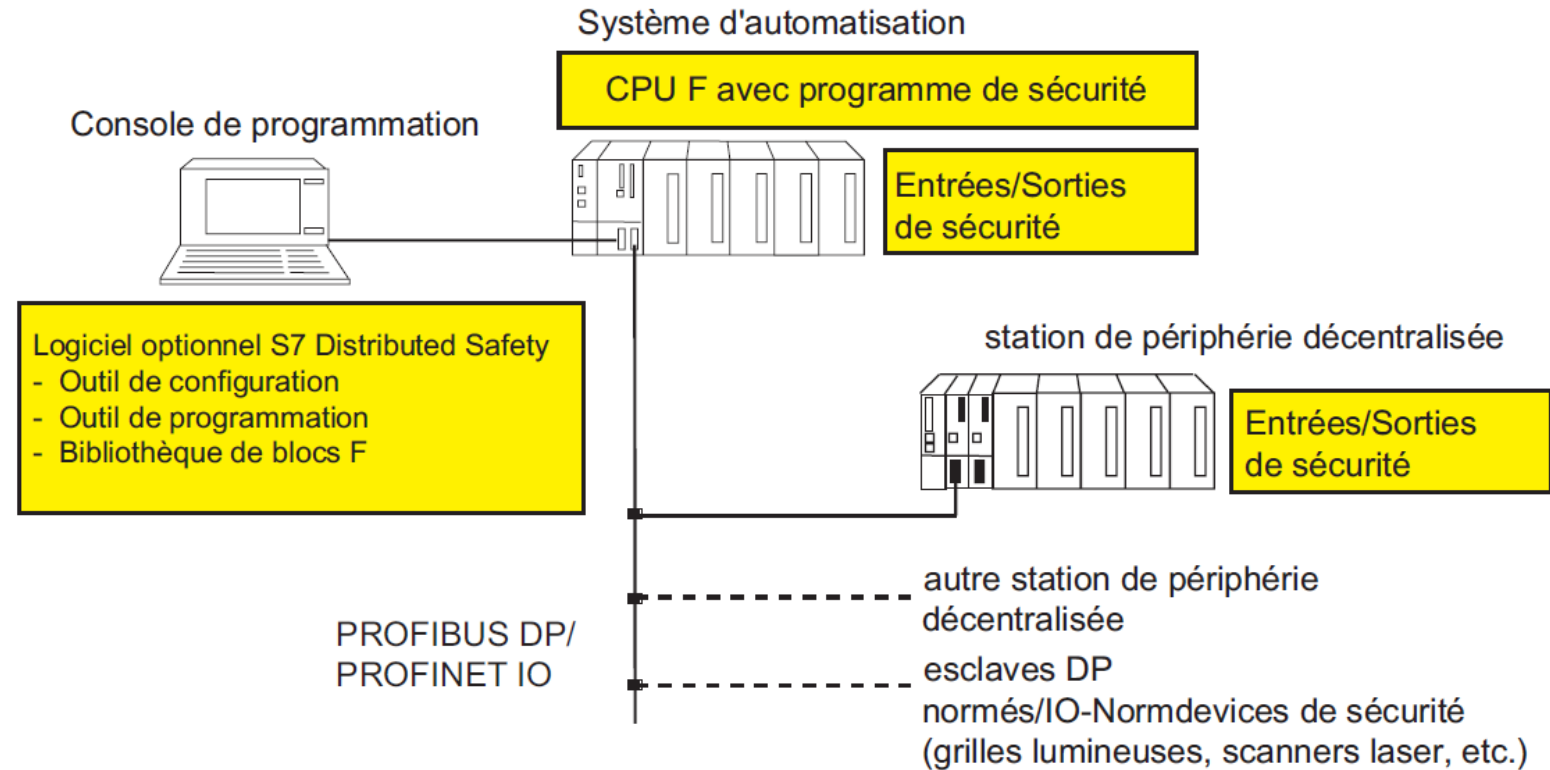


Automate Safety :

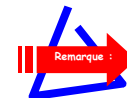
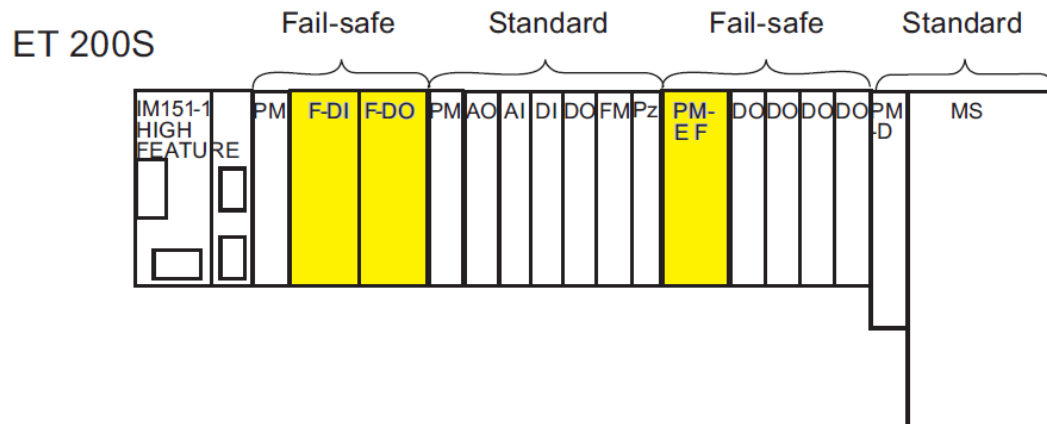
- Un automate de sécurité se caractérise par :
 - ❖ Un passage à une position de repli sure lors de la défaillance d'un de ses éléments (matériel et logiciel) :
 - ✓ La défaillance d'une entrée TOR se traduit par la mise à 0 du signal d'entrée,
 - ✓ Le débordement ou la défaillance (ex : rupture de fils si $< 1,18\text{mA}$) d'une entrée analogique se traduit par le forçage de la valeur à 0,
 - ✓ La défaillance d'une sortie TOR se traduit par la coupure d'énergie de cette voie.
 - ❖ Une structure redondante des principaux éléments (matériel et logiciel) : les automates de sécurité Siemens utilise la **redondance de traitement** avec un seul processeur.
 - ❖ Une série d'autotests destinés à vérifier l'absence de défaut latents (sur les micro-processeur, les mémoires RAM et EEPROM).
 - ❖ L'utilisation de cartes spécifiques de sécurité (ces cartes font du hand-shake avec la CPU).
- Les tensions des signaux des entrées TOR doivent respecter les seuils :

	Tension alimentation	Tensions d'entrée de changement d'état de l'automate		Courants d'entrée de changement d'état de l'automate	
		État 0	État 1	État 0	État 1
Valeurs ou limites conseillées	24 V c.c.	[-3 V, 5 V]	[15 V, 30 V]	< 2 mA	> 10 mA

Constitution :



PROFISAFE : protocole de communication sécurisé selon la norme CEI 61508.



2 possibilités pour des entrées /sorties de sécurité avec une station ET200S :

- Modules d'entrées/sorties de sécurité
- Modules d'entrées/sorties standards mais alimentés par un Power Module de sécurité

Vs1 et VS2 : alimentation interne nécessaire si on veut utiliser le test de court-circuit.

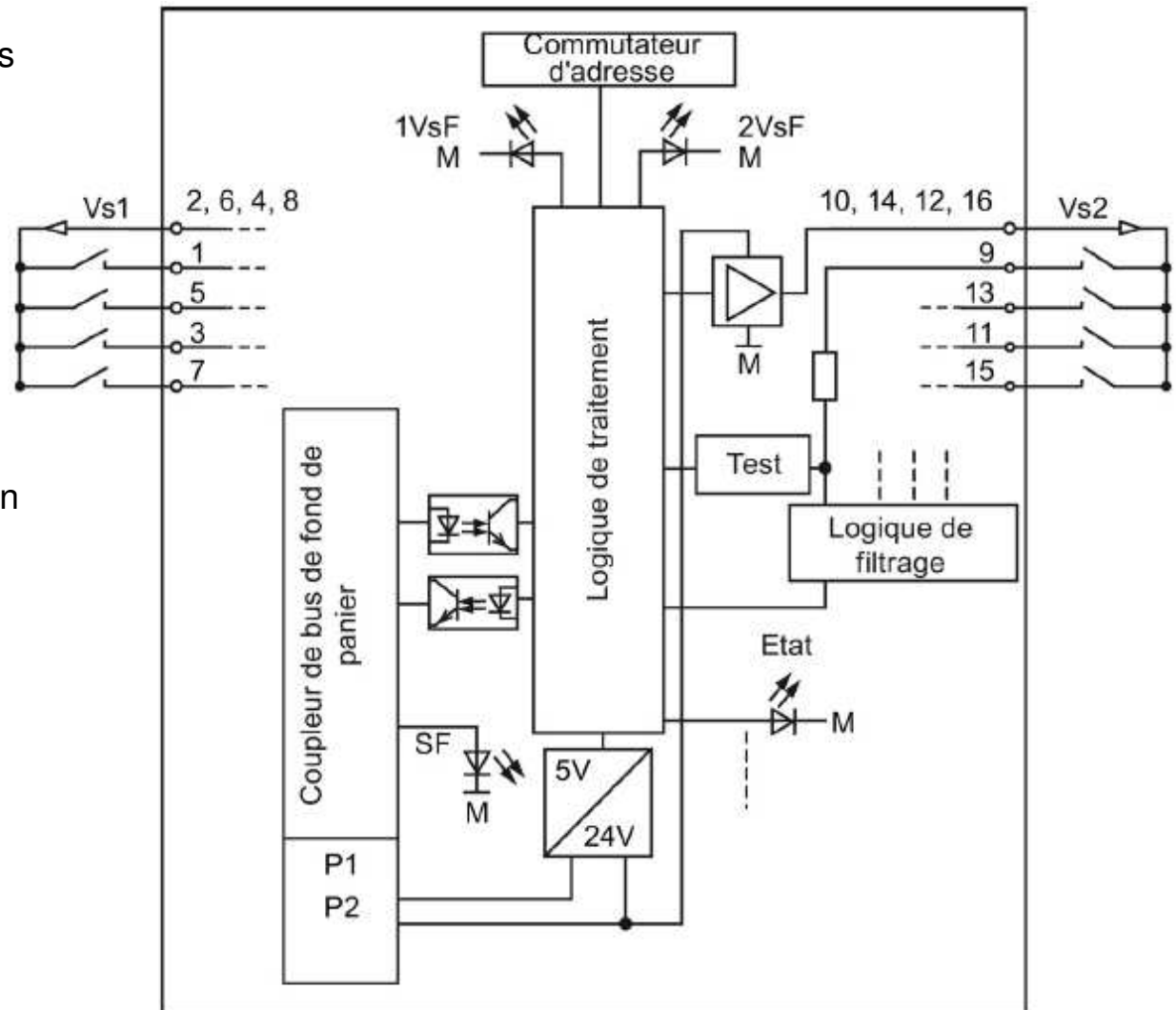
(utilisable uniquement pour des commutateurs simples, pas pour des capteurs ¾ fils).

Test de court-circuit :

- de l'entrée avec L+
- avec l'entrée d'une autre voie lorsque le signal est à 1
- de l'entrée avec l'alimentation capteur d'une autre voie
- de l'alimentation capteur avec l'alimentation capteur d'une autre voie

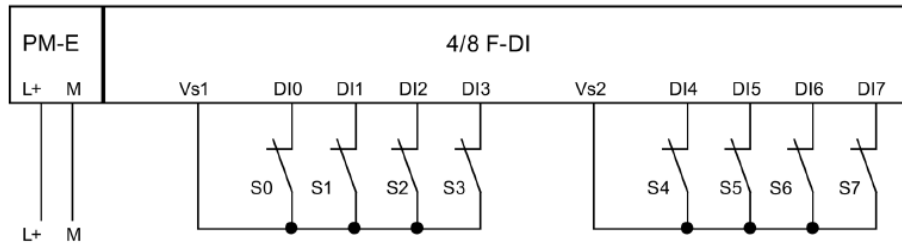


Structure interne à 2 voies :
2 processeurs intégrés se surveillent mutuellement et testent les circuits d'entrées et de sorties.

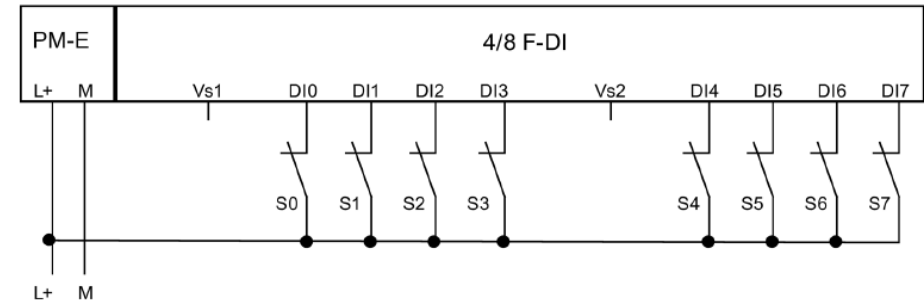




Un capteur sur une voie : 1oo1 - SIL2/Cat3/PLd

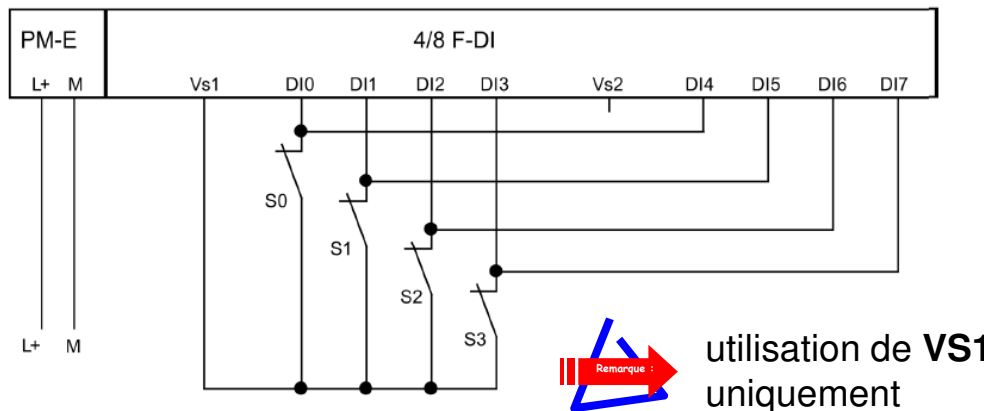


Alimentation interne avec ou sans test de court-circuit

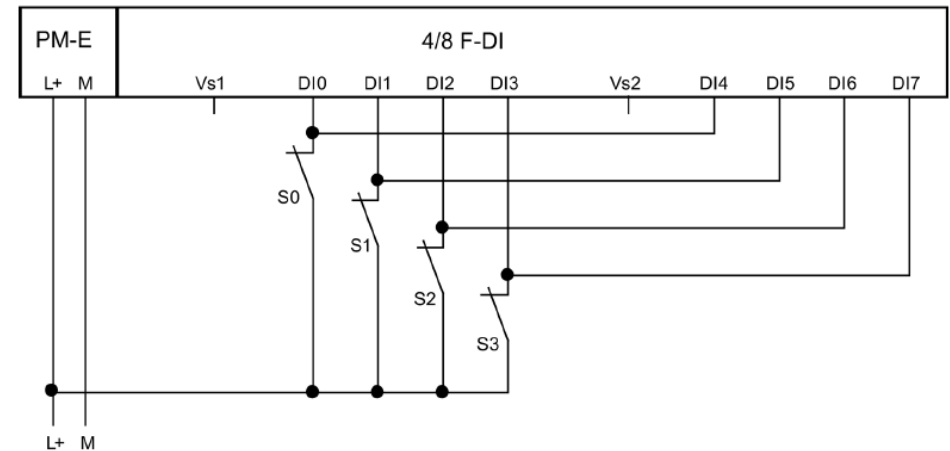


Alimentation externe

Un capteur sur une voie à deux entrées : 1oo2 - SIL3/Cat3/Plc

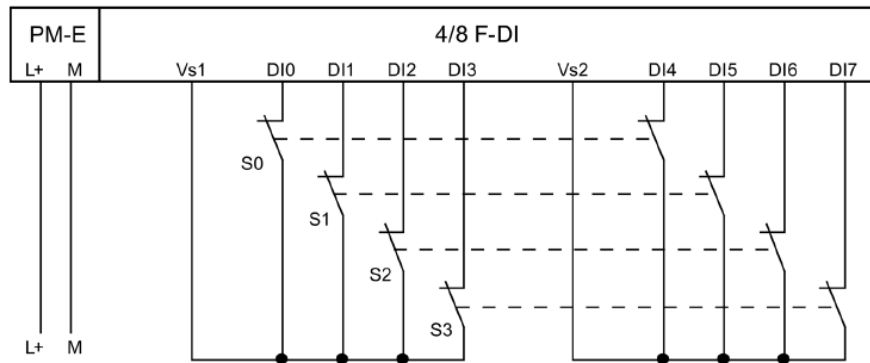


Alimentation interne avec ou sans test de court-circuit

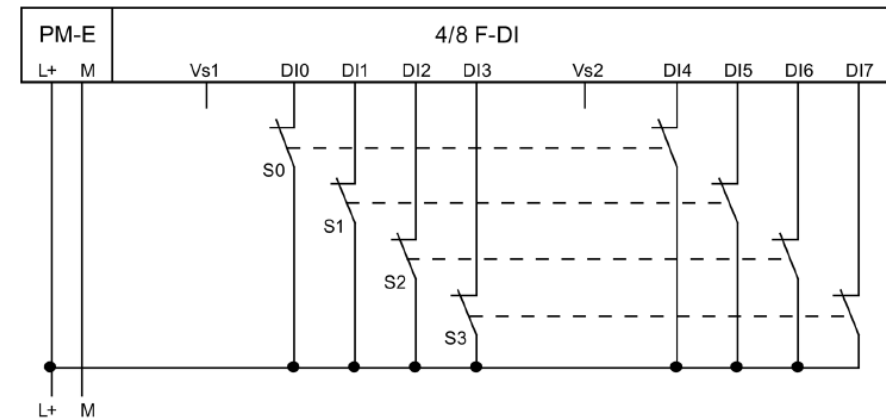


Alimentation externe

Un capteur à deux voies sur 2 voies : 1oo2 - SIL3/Cat3/PLe

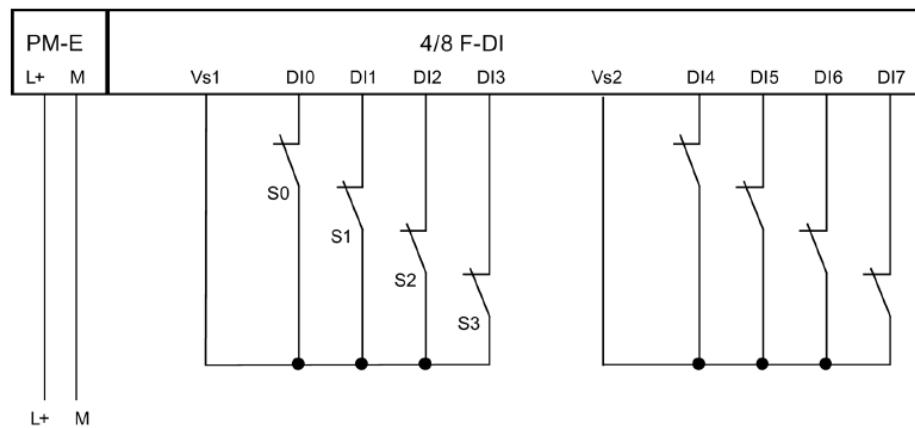


Alimentation interne sans test de court-circuit

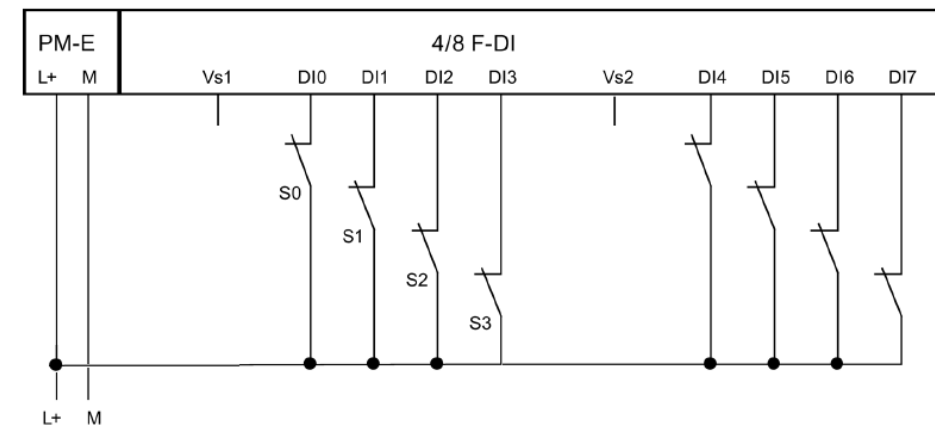


Alimentation externe

Deux capteurs à une voie sur 2 voies : 1oo2 - SIL3/Cat3/PLe

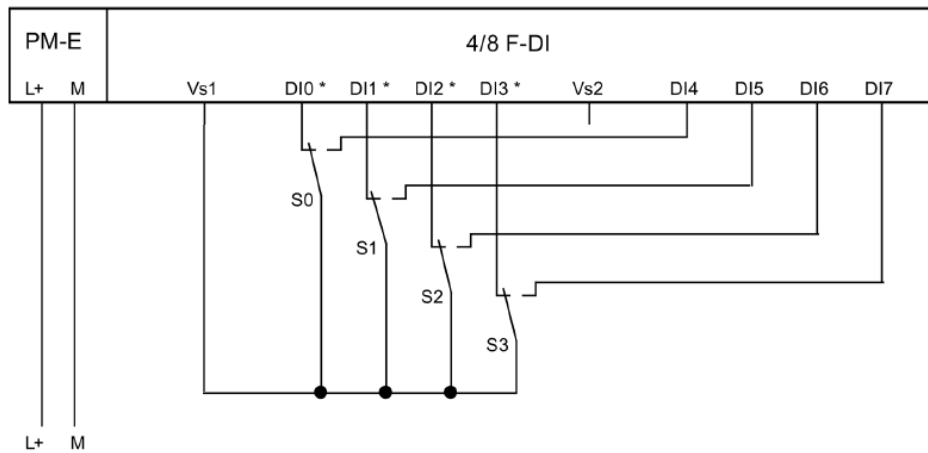


Alimentation interne sans test de court-circuit

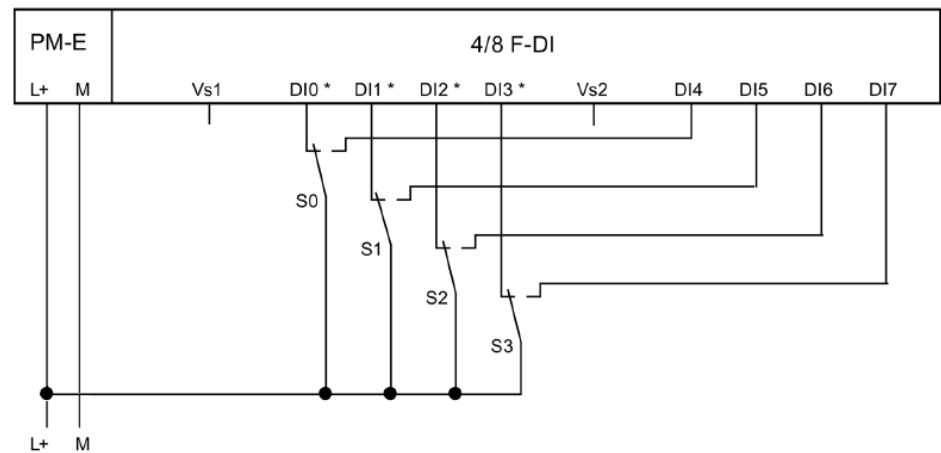


Alimentation externe

Un capteur antivalent sur 2 voies : 1oo2 - SIL3/Cat3/PLe

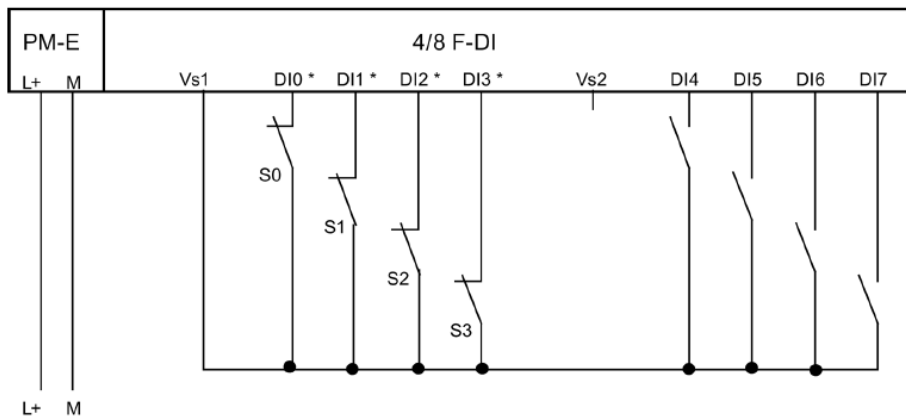


Alimentation interne sans test de court-circuit

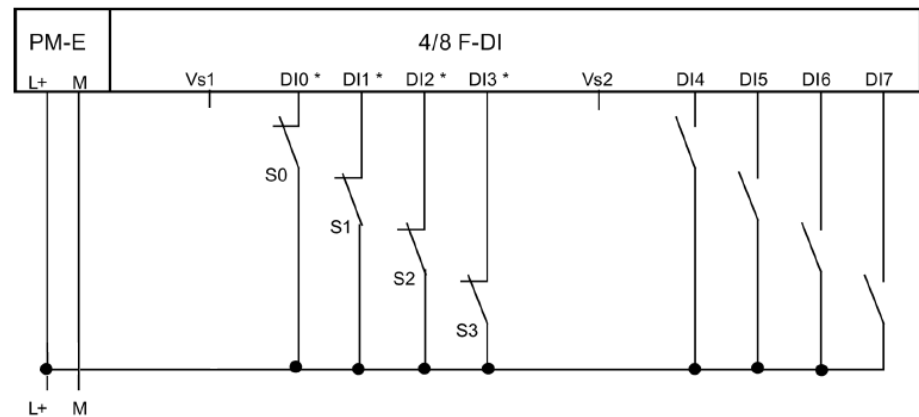


Alimentation externe

Deux capteurs antivalents à une voie sur 2 voies : 1oo2 - SIL3/Cat3/PLe

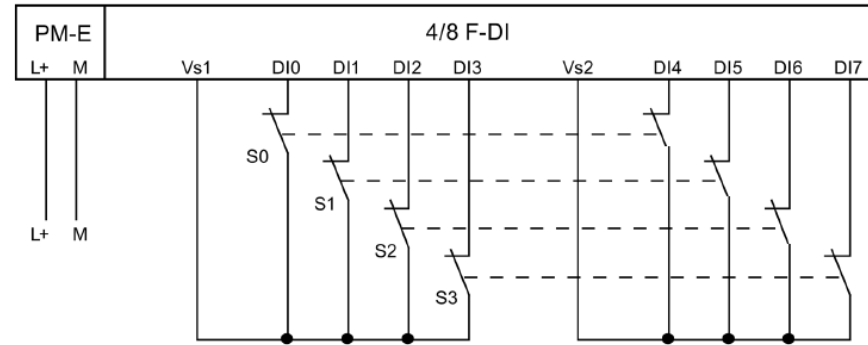


Alimentation interne sans test de court-circuit



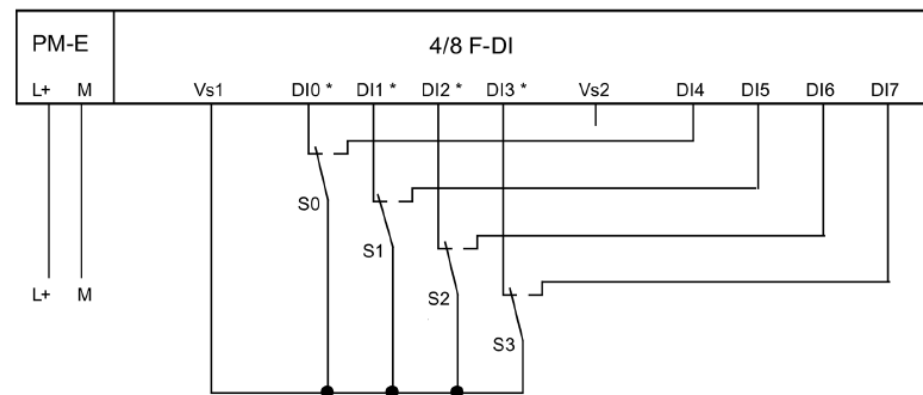
Alimentation externe

Un capteur à deux voies sur 2 voies : 1oo2 - SIL3/Cat4/PLe



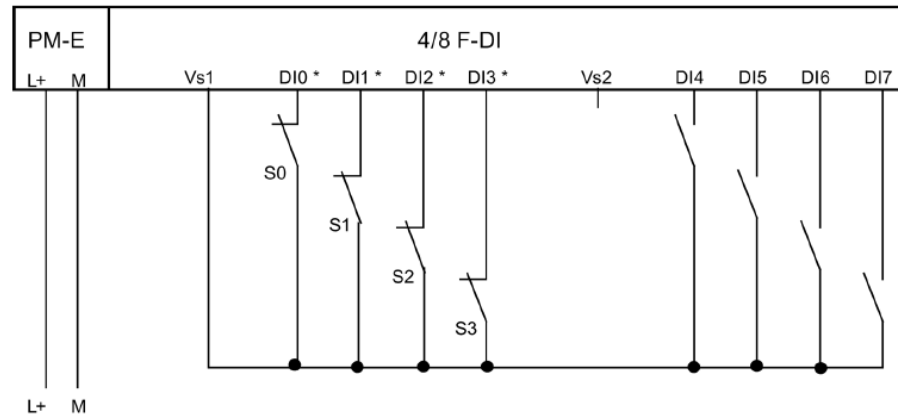
Alimentation interne avec test de court-circuit

Un capteur antivalent sur 2 voies : 1oo2 - SIL3/Cat4/PLe



Alimentation interne avec test de court-circuit

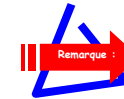
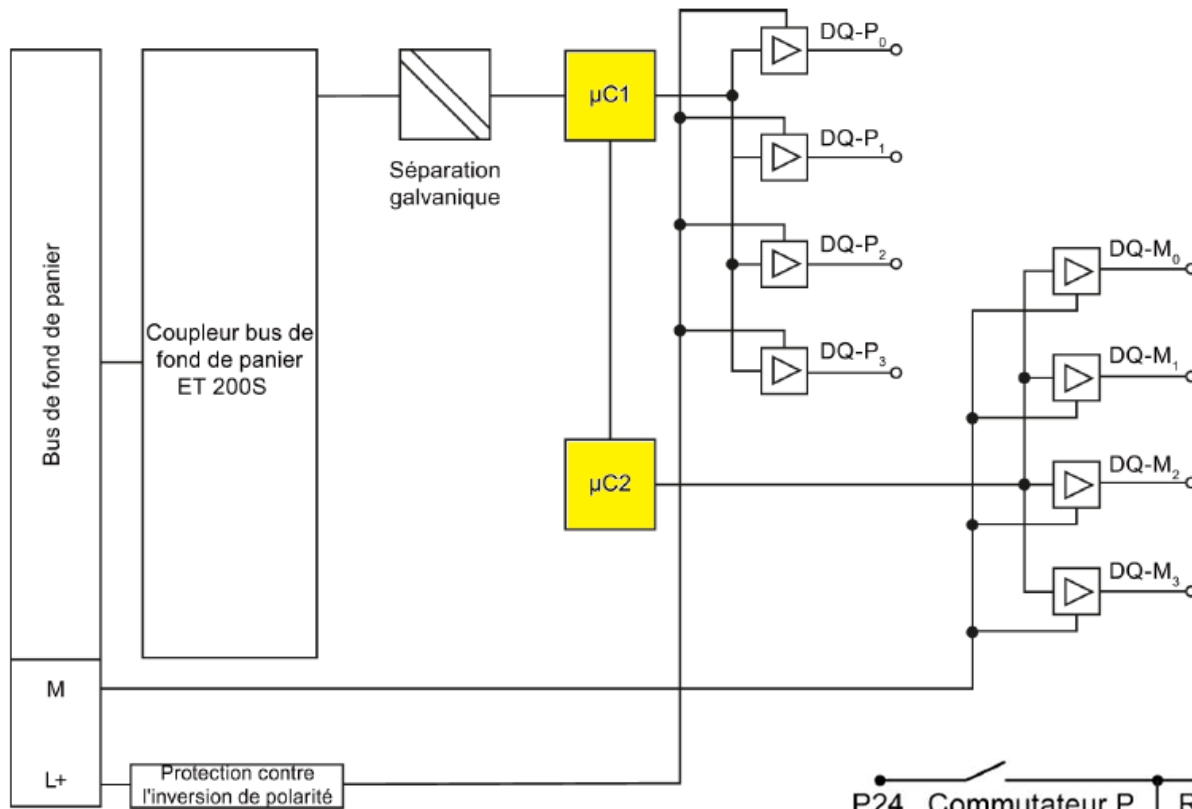
Deux capteurs antivalent sur 2 voies : 1oo2 - SIL3/Cat4/PLe



Alimentation interne avec test de court-circuit

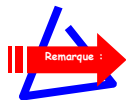
Spécificités des capteurs équivalent et antivalent :

- Utilisation de deux entrées TOR comme une seule entrée TOR.
- Affectation des paires d'entrées TOR :
 - DI 0 avec DI 4
 - DI 1 avec DI 5
 - DI 2 avec DI 6
 - DI 3 avec DI 7
- Les **voies de gauche** du module fournissent les **signaux utiles**.

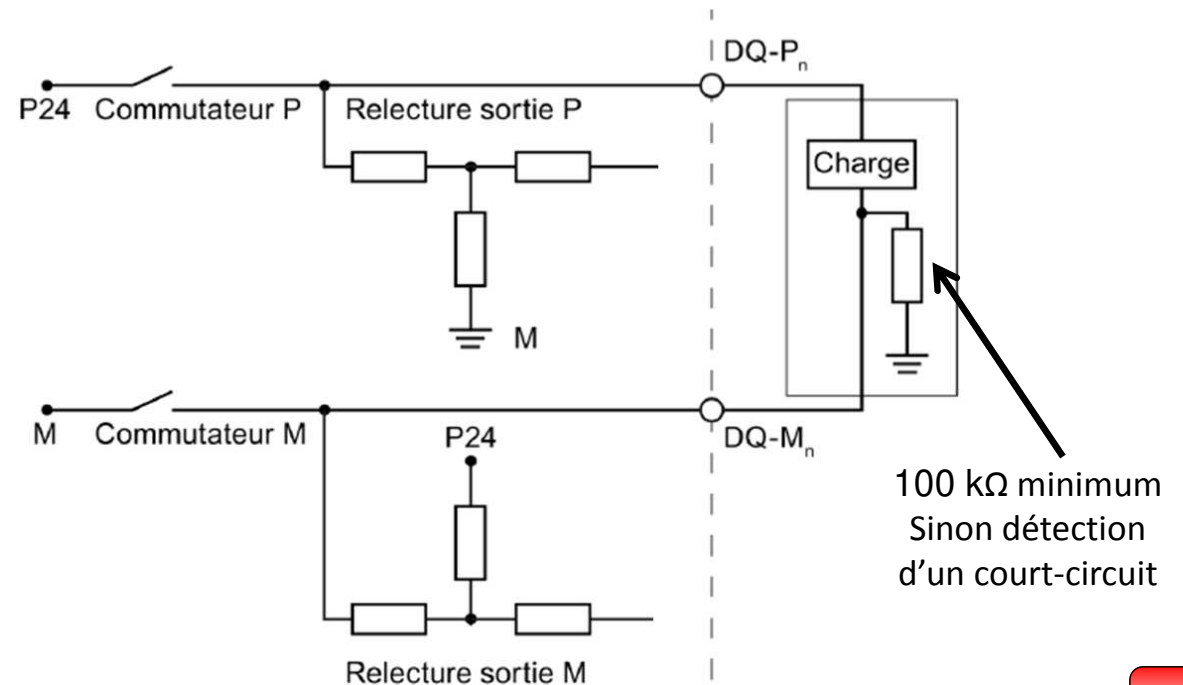


Chaque sortie est composée :

- d'un commutateur P
- d'un commutateur M.



Les cartes de sorties de sécurité coupent les bornes P et M.

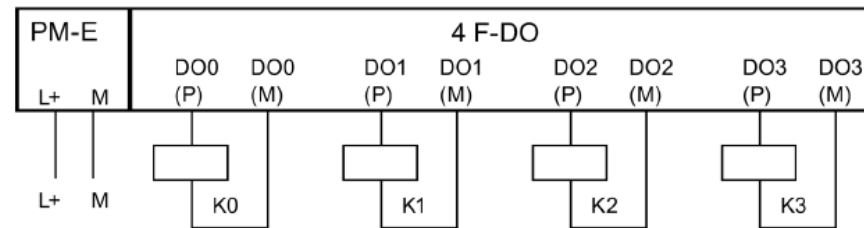




ET 200S/M F-DO	Cat.2	Cat.3/4	Cat.3/4
PM switching 			
PP switching 			

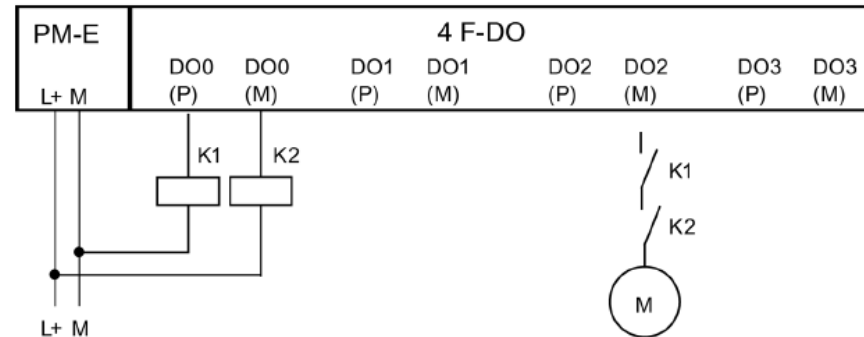
Une charge par sortie :

➤ SIL3/Cat4/PLe



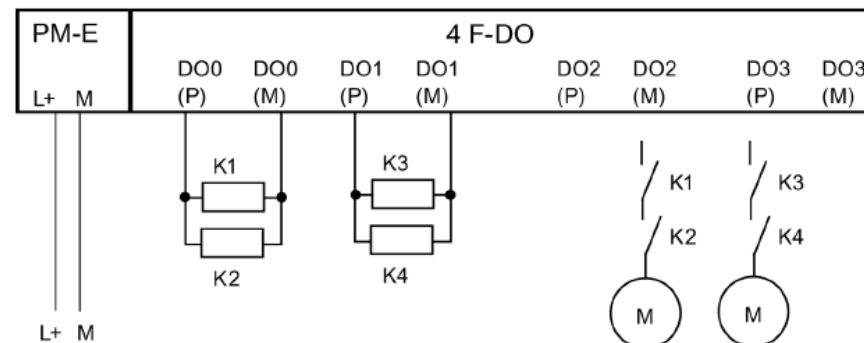
Une charge sur les bornes P et M d'une sortie :

➤ SIL3/Cat4/PLe



Deux charges en parallèle sur une sortie :

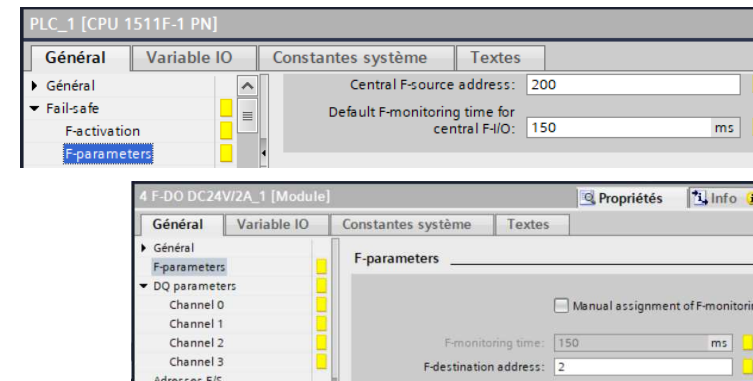
➤ SIL3/Cat4/PLe



Adresse PROFISAFE :

- Chaque module de sécurité possède sa propre adresse PROFIsafe.
- Elles sont attribuées automatiquement lors de la configuration matérielle.
- Les adresses PROFISAFE :

- **F-source address** pour la CPU,
- **F-destination address** pour les cartes Safety,



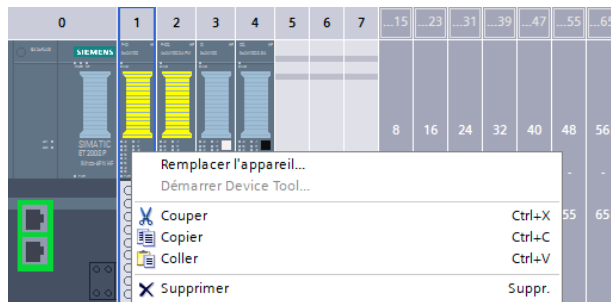
Module avec commutateur d'adresse PROFISAFE :

- Le commutateur d'adresse, positionné sur la partie gauche du module, doit être réglé **avant** l'installation du module.
- Plage d'adresse : entre 1 et 1022.

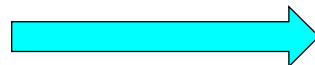


Module sans commutateur d'adresse PROFISAFE :

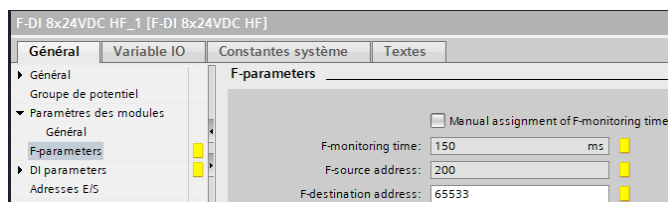
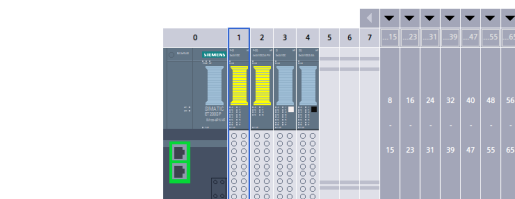
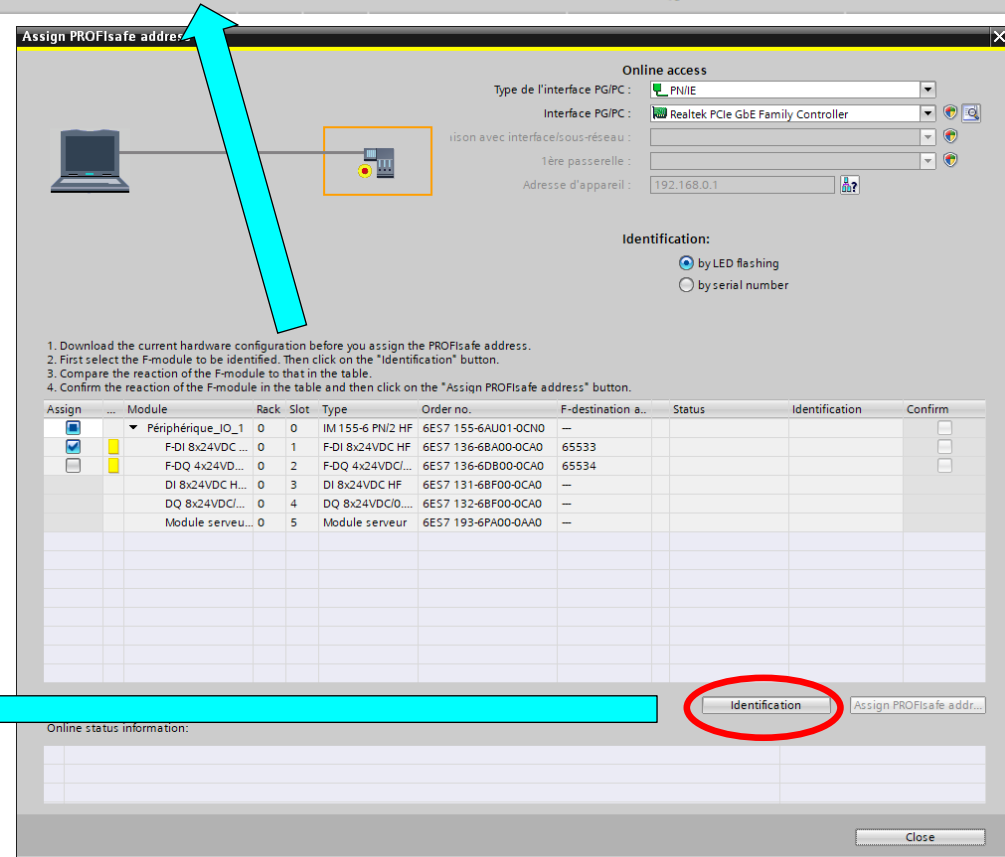
➤ **Avant** l'utilisation du module, son adresse doit être configurée :



Procédure



1. Download the current hardware configuration before you assign the PROFISafe address.
2. First select the F-module to be identified. Then click on the "Identification" button.
3. Compare the reaction of the F-module to that in the table.
4. Confirm the reaction of the F-module in the table and then click on the "Assign PROFISafe address" button.



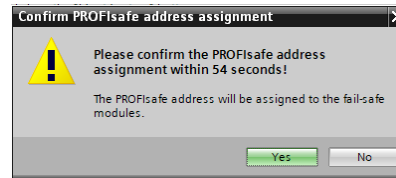
Assign	Module	Rack	Slot	Type	Order no.	F-destination a...	Status	Identification	Confirm
<input checked="" type="checkbox"/>	▼ Périphérique_IO_1	0	0	IM 155-6 PN/2 HF	6ES7 155-6AU01-0CN0	—			<input type="checkbox"/>
<input checked="" type="checkbox"/>	F-DI 8x24VDC ...	0	1	F-DI 8x24VDC HF	6ES7 136-6BA00-0CA0	65533	unassigned	LED flashing?	<input type="checkbox"/>
<input type="checkbox"/>	F-DQ 4x24VD...	0	2	F-DQ 4x24VDC/...	6ES7 136-6DB00-0CA0	65534			<input type="checkbox"/>
	DI 8x24VDC H...	0	3	DI 8x24VDC HF	6ES7 131-6BF00-0CA0	—			
	DQ 8x24VDC/...	0	4	DQ 8x24VDC/0...	6ES7 132-6BF00-0CA0	—			
	Module serveur...	0	5	Module serveur	6ES7 193-6PA00-0AA0	—			



La configuration doit d'abord être transférée dans la CPU avant l'assignation de l'adresse PROFISAFE.

- Les leds des entrées ou des sorties du module doivent clignoter. Il faut cocher la case "**Confirm**" avant de lancer la commande d'assignation.

Assign	...	Module	Rack	Slot	Type	Order no.	F-destination a...	Status	Identification	Confirm
<input type="checkbox"/>		▼ Périphérique_IO_1	0	0	IM 155-6 PN/2 HF	6ES7 155-6AU01-0CN0	—			<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>		F-DI 8x24VDC ...	0	1	F-DI 8x24VDC HF	6ES7 136-6BA00-0CA0	65533	! unassigned	LED flashing?	<input checked="" type="checkbox"/>
<input type="checkbox"/>		F-DQ 4x24VD...	0	2	F-DQ 4x24VDC/...	6ES7 136-6DB00-0CA0	65534			<input type="checkbox"/>
		DI 8x24VDC H...	0	3	DI 8x24VDC HF	6ES7 131-6BF00-0CA0	—			
		DQ 8x24VDC/...	0	4	DQ 8x24VDC/0....	6ES7 132-6BF00-0CA0	—			
		Module serveu...	0	5	Module serveur	6ES7 193-6PA00-0AA0	—			



Assign	...	Module	Rack	Slot	Type	Order no.	F-destination a...	Status	Identification	Confirm
<input type="checkbox"/>		▼ Périphérique_IO_1	0	0	IM 155-6 PN/2 HF	6ES7 155-6AU01-0CN0	—			<input type="checkbox"/>
		F-DI 8x24VDC ...	0	1	F-DI 8x24VDC HF	6ES7 136-6BA00-0CA0	65533	✓ assigned		
		F-DQ 4x24VD...	0	2	F-DQ 4x24VDC/...	6ES7 136-6DB00-0CA0	65534	✓ assigned		
		DI 8x24VDC H...	0	3	DI 8x24VDC HF	6ES7 131-6BF00-0CA0	—			
		DQ 8x24VDC/...	0	4	DQ 8x24VDC/0....	6ES7 132-6BF00-0CA0	—			
		Module serveu...	0	5	Module serveur	6ES7 193-6PA00-0AA0	—			

Remplacement d'un module d'entrées/sorties :

- Remplacement possible d'un module F par un module ayant un numéro de référence **plus** élevé.
- Le remplacement d'un module F durant le fonctionnement provoque une erreur de communication dans la CPU-F.

Maintenance préventive :

- La probabilité de défaillance d'un composant homologué du système Safety impose de tester ce composant dans un intervalle de 10 ans (valeur à vérifier dans la documentation constructeur).
- Le test des composantes électroniques complexes étant difficile à réaliser, celui-ci se traduit généralement par le remplacement du composant par un neuf.
- En général, un intervalle de test plus court est nécessaire pour les capteurs et les actionneurs.

Caractéristiques d'un module F :



Les modules Safety ne peuvent être utilisés qu'en mode Safety !

- Les modules possèdent une structure à 2 canaux :
2 processeurs intégrés se surveillent mutuellement et testent automatiquement les circuits d'E/S.
- En cas **d'erreur**, un module F est commuté vers un **état de sécurité**.
- Accès à la périphérie F :
 - Utilisation de la Mémoire Image (MIE et MIS),
 - Accès "direct" à la mémoire interdit,
 - Le programme standard peut accéder à **l'état** des Entrées/Sorties **F** (**utilisation obligatoire du DB**).
 - La commande des sorties **F** est n'autorisé qu'à un groupe d'exécution F.
- Rafraichissement :
 - de la MIE avant le début du traitement du groupe d'exécution F,
 - de la MIS après le traitement du groupe d'exécution F.
- Exploitation **1oo2** des capteurs (1 capteur bicanal ou 2 capteurs monocanal) :
seule la première entrée utilisée est accessible au programme Safety.

Exemple : Channel 0,4 ➔ seule l'entrée 0 est accessible par le programme.

- Périphérie F : utilisation d'une zone MIE et MIS plus grande que celle nécessaire à l'état des entrées et des sorties de sécurité → données nécessaires pour la gestion de la communication ProfiSafe.

Module F	Octets occupés dans la CPU F :	
	dans la zone des entrées	dans la zone des sorties
PM-E F pm DC24V PROFIsafe	x + 0 à x + 4	x + 0 à x + 4
PM-E F pp DC24V PROFIsafe	x + 0 à x + 4	x + 0 à x + 4
PM-D F DC24V PROFIsafe	x + 0 à x + 4	x + 0 à x + 4
4/8 F-DI DC24V PROFIsafe	x + 0 à x + 5	x + 0 à x + 3
4 F-DI/3 F-DO DC24V PROFIsafe	x + 0 à x + 6	x + 0 à x + 4
4 F-DO DC24V/2A PROFIsafe	x + 0 à x + 4	x + 0 à x + 4
1 F-RO DC24V/AC24..230V/5A	x.0 et x.1	—

x = adresse de début du module

- Exemple pour un module 4/8 F-DI DC24V PROFIsafe :

	7	6	5	4	3	2	1	0
x + 0	DI ₇	DI ₆	DI ₅	DI ₄	DI ₃	DI ₂	DI ₁	DI ₀
x + 1	Etat de la valeur pour DI ₇	Etat de la valeur pour DI ₆	Etat de la valeur pour DI ₅	Etat de la valeur pour DI ₄	Etat de la valeur pour DI ₃	Etat de la valeur pour DI ₂	Etat de la valeur pour DI ₁	Etat de la valeur pour DI ₀

← Etat de l'entrée

← Etat de la valeur (cpu 1200 et 1500) :

1 : valeur de process valide

0 : valeur de remplacement ou voie désactivée

Passivation d'un module F :

- L'activation de la fonction de sécurité (**passivation** du module) sur les modules F entraîne l'utilisation de **valeurs de remplacement** (état de sécurité) à la place des valeurs de processus.
- La passivation d'une voie ou d'une carte se fait lors :
 - ❖ du démarrage du système F,
 - ❖ d'une erreur de communication entre la CPU F et le module F (hand-shake),
 - ❖ d'une erreur du périphérique F ou d'une voie,
 - ❖ de l'écriture de la variable PASS_ON à 1 dans le DB de la périphérie F,
 - ❖ de l'arrêt de la CPU F.
- Utilisation d'une valeur de remplacement : valeur écrite dans la MIE pour une carte d'entrée (**0**).
valeur transmise à la carte pour une carte de sorties (**0**).
- Après l'apparition d'un défaut sur une voie, la réaction du module est paramétrable :
 - ❖ Passivation de la voie
 - ❖ Passivation du module F

Behavior after channel fault:	Passivate channel
	Passivate the entire module
	Passivate channel

Réintégration d'un module F :

- La réintégration entraîne la commutation des valeurs de remplacement (état de sécurité) aux valeurs de processus.
- La réintégration peut être :
 - ❖ Automatique (dès que le défaut a disparu) :
 - variable ACK_NEC = 0 du DB du module F
 - ❖ Manuelle (nécessite un acquittement opérateur) :
 - variable ACK_NEC = 1 du DB du module F
 - front montant de la variable ACK_REI du DB du module F

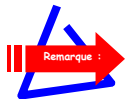
Test des modules de sorties F :

- Les sorties sont testées à intervalles réguliers (toutes les 15 minutes environ) ⇔ vérification que les sorties ne restent pas bloquées :
 - ❖ désactivation brève (< 1ms) par le module des sorties activées,
 - ❖ activation brève (< 1ms) par le module des sorties désactivées.

Paramétrage d'un module d'entrées F :

Paramétrage carte

Adresse cible
PROFIsafe



Source = CPU
Cible = carte F

Les voies non utilisées
doivent être
désactivées !

Paramétrage voie

Paramétrage d'un module de sorties F :

Paramétrage carte

Adresse cible
PROFIsafe

4 F-DO DC24V/2A_1 [Module]

Propriétés Info Diagnostic

Général Variable IO Constantes système Textes

F-parameters

Manual assignment of F-monitoring time

F-monitoring time: 150 ms

F-destination address: 2

DIP-switch setting (9.....0): 0000000010

F-parameter signature (without addresses): 33196

Behavior after channel fault: Passivate channel

F-I/O DB manual number assignment

F-I/O DB-number: 8002

F-I/O DB-name: F00008_4F-DODC24V/2A_1

Les voies non utilisées
doivent être
désactivées !

Paramétrage voie

4 F-DO DC24V/2A_1 [Module]

Propriétés Info Diagnostic

Général Variable IO Constantes système Textes

Channel 0

Activated

Diagnosis: Wire break

Readback time: 1 ms

DB F de périphérie :

- Un **DB F** est généré automatiquement pour chaque module de périphérie F lors de la compilation de la configuration matérielle.
- Pendant les opérations système, la CPU F lit et écrit des données dans ce DB.
- L'accès en écriture aux variables du DB est réservé au seul groupe d'exécution concerné.
- L'accès en lecture est autorisé pour le programme standard.

Passivation complète
d'un module de la périphérie F

ACK_NEC = 0
Réintégration automatique

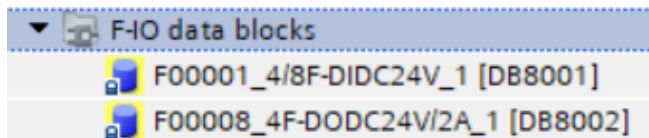
Variable	Type de données	Fonction	Valeur par défaut
PASS_ON	BOOL	1=active la passivation	0
ACK_NEC	BOOL	1=acquittement pour la réintégration requis après erreurs de périphérie F/voie	1
ACK_REI	BOOL	1=acquittement de réintégration	0
IPAR_EN	BOOL	Variable pour le reparamétrage d'esclaves DP normés/IO-Normdevices de sécurité ou pour SM 336 ; AI F 6 x 0/4 ... 20 mA HART pour la validation de la communication HART.	0

INPUT

ACK_REQ = 1
Acquittement utilisateur nécessaire

PASS_OUT	BOOL	Sortie de passivation*	1
QBAD	BOOL	1=Mise à disposition des valeurs de remplacement*	1
ACK_REQ	BOOL	1=requête d'acquittement de réintégration	0
IPAR_OK	BOOL	Variable pour le reparamétrage d'esclaves DP normés/IO-Normdevices de sécurité ou pour SM 336 ; AI F 6 x 0/4 ... 20 mA HART pour la validation de la communication HART.	0
DIAG	BYTE	Information de maintenance	
QBAD_I_xx	BOOL	1=Mise à disposition des valeurs de remplacement sur la voie d'entrée xx	1
QBAD_O_xx	BOOL	1=Mise à disposition des valeurs de remplacement sur la voie de sortie xx	1

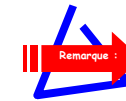
OUTPUT



Indication des voies
d'entrées/sorties passivées

Détail de la donnée DIAG du DB de périphérie :

- Mise à disposition d'informations pour la maintenance :



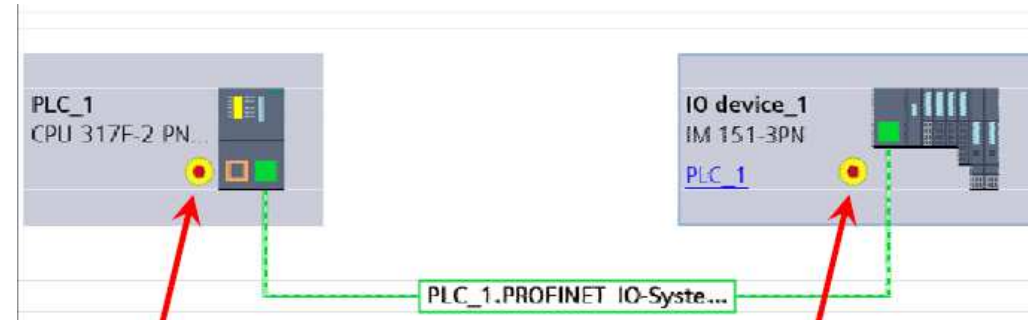
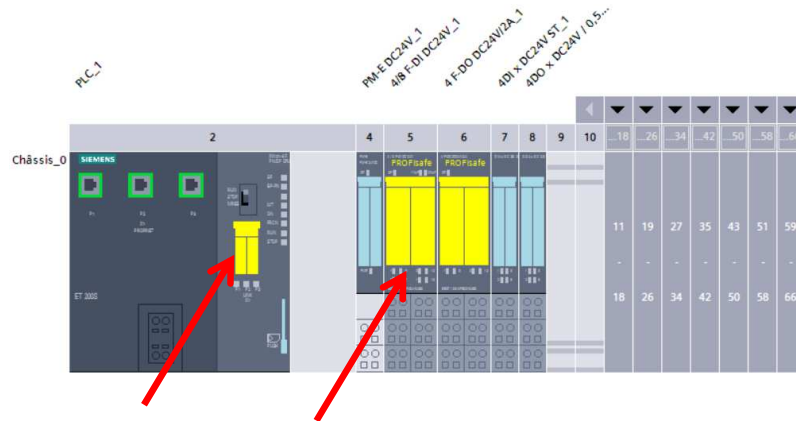
Ces informations restent disponibles jusqu'à la réintégration du module.

N° de bit	Occupation	Origine possible de l'erreur	Remède
Bit 0	Détection de timeout de la périphérie F	Liaison PROFIBUS/PROFINET entre CPU F et périphérie F en dérangement. La valeur paramétrée dans <i>HW Config</i> pour le temps de surveillance de la périphérie F est trop faible. La périphérie F contient des données de paramétrage invalides.	<ul style="list-style-type: none"> Contrôlez la liaison PROFIBUS/PROFINET et vérifiez l'absence de sources de perturbation externes. Contrôlez le paramétrage de la périphérie F <i>dans HW Config</i>. Augmentez si nécessaire la valeur du temps de surveillance. Compilez de nouveau la configuration matérielle et rechargez-la dans la CPU F. Compilez une nouvelle fois le programme de sécurité. Contrôlez le tampon de diagnostic de la périphérie F. Mettez la périphérie F hors tension puis à nouveau sous tension.
		erreur interne de la périphérie F	Echangez la périphérie F
		ou erreur interne de la CPU F	Remplacez la CPU F
Bit 1	Détection d'une erreur de périphérie F/voie de la périphérie F	voir <i>Manuels de la périphérie F</i>	voir <i>Manuels de la périphérie F</i>
Bit 2	Détection d'une erreur de CRC/numéro de séquence de la périphérie F	Voir la description du bit 0	Voir la description du bit 0
Bit 3	Réserve	-	-
Bit 4	Détection de timeout du système F	Voir la description du bit 0	Voir la description du bit 0
Bit 5	Détection d'erreur de numéro de séquence du système F	Voir la description du bit 0	Voir la description du bit 0
Bit 6	Détection d'une erreur de CRC du système F	Voir la description du bit 0	Voir la description du bit 0
Bit 7	Réserve	-	-

Reconnaissance d'un système Safety :

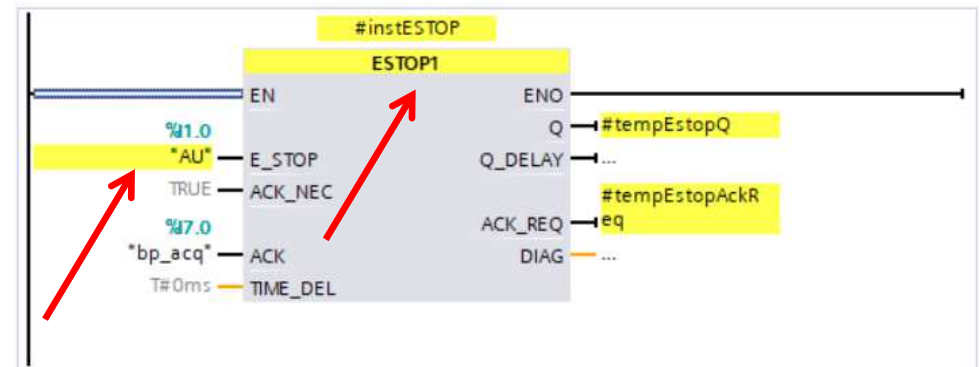
➤ Les constituants matériels :

- Les CPUs
- Les cartes d'entrées/sorties



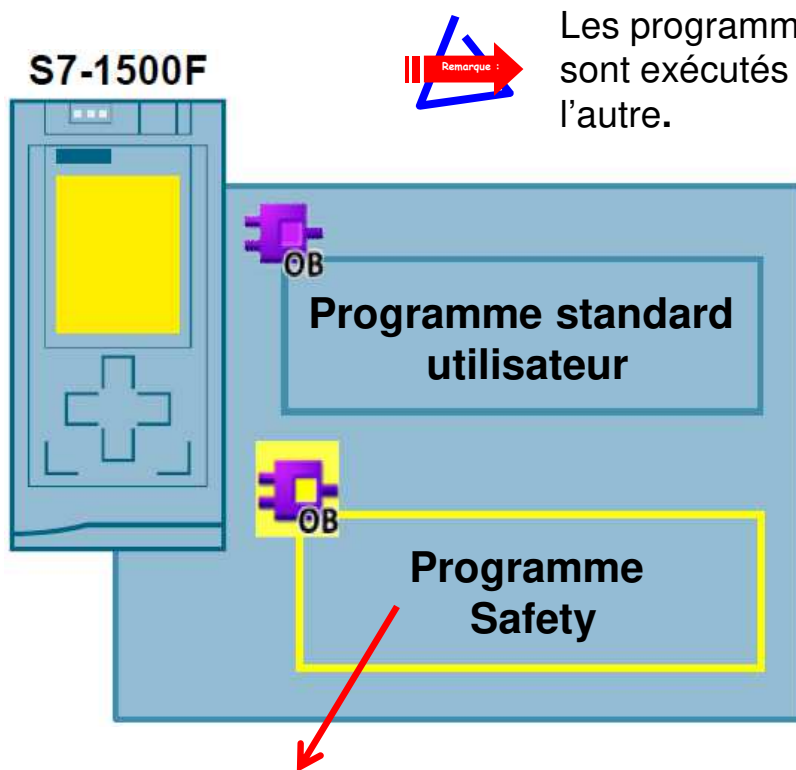
➤ Les éléments logiciels :

- les blocs programme
- les variables



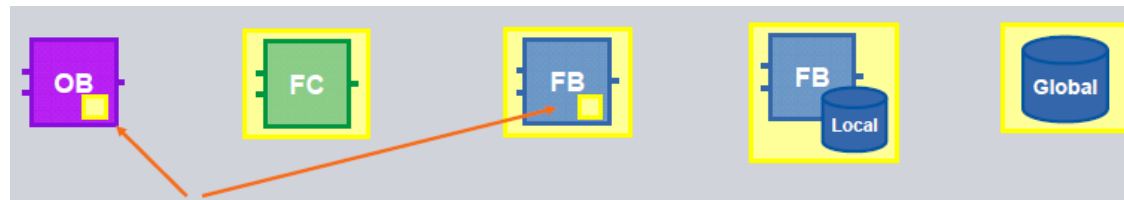
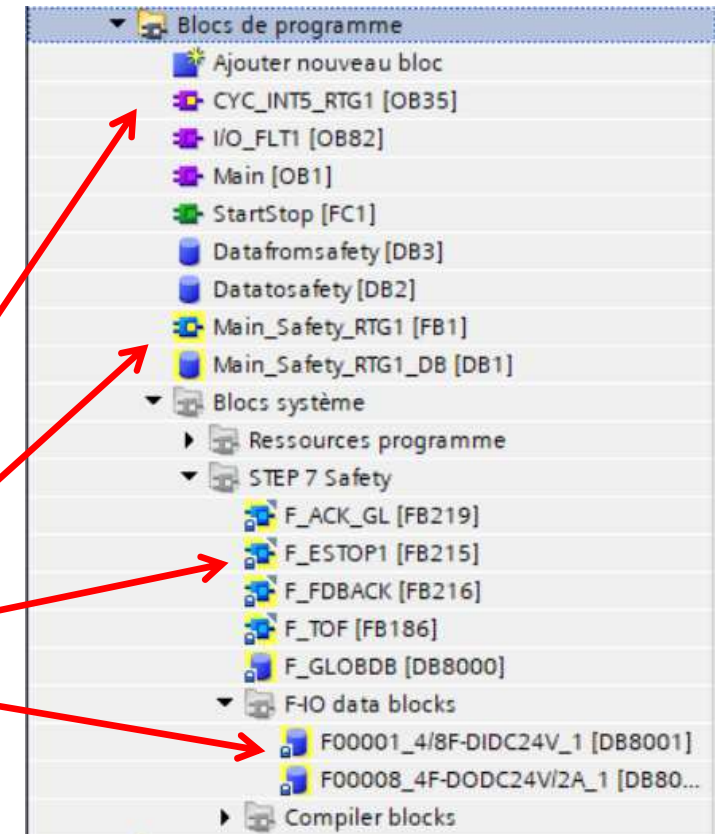
	Nom	Type de données	Adresse
1	bp_acq	Bool	%I7.0
2	bp_start	Bool	%I7.1
3	bp_stop	Bool	%I7.2
4	ret_contacteurs	Bool	%I7.3
5	AU	Bool	%I1.0
6	Cd_contacteurs	Bool	%Q8.0

Programmes automatés :



- Un programme de sécurité écrit par le concepteur.
- Un programme de sécurité diversifié créé par la CPU.
- Les deux programmes de sécurité sont exécutés l'un après l'autre et leurs résultats sont comparés.

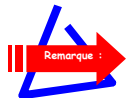
Blocs F



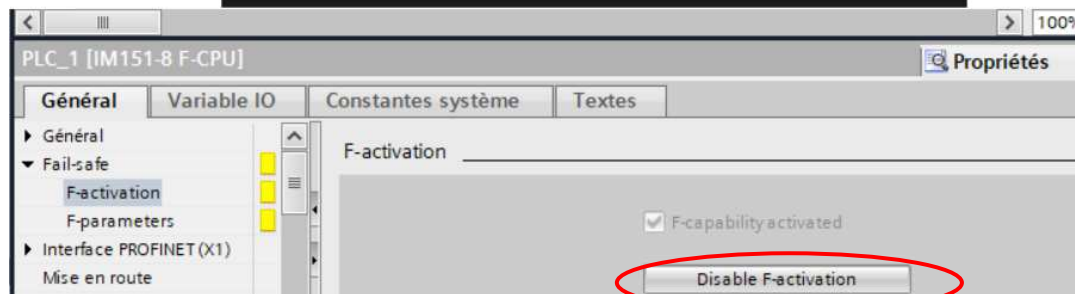
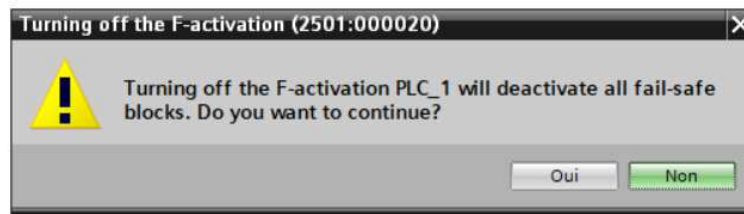
Blocs créés automatiquement pour la gestion d'un groupe d'exécution (RTG)

Constitution d'un programme Safety :

- **Blocs F utilisateurs** programmés en langage **CONT F** ou **LOG F** (pas de langage List).
- **Blocs F de fonctions Safety** provenant des instructions de base et de communication :
- Le programme Safety est complété automatiquement par des blocs pour des mesures de contrôle de défaillance.



La désélection des fonctions de sécurité de l'automate entraîne la désactivation de tout les blocs de sécurité.



Instructions		
Options		
> Favoris		
▼ Instructions de base		
Nom	Description	Version
▶ General		
▶ Bit logic operations		
▼ Safety functions		V1.6
ESTOP1	Emergency STOP up t...	V1.4
TWO_HAND	Two-hand monitoring	V1.0
TWO_H_EN	Two-hand monitorin...	V1.2
MUTING	Muting	V1.0
MUT_P	Parallel muting	V1.3
EV1oo2DI	1oo2 evaluation with ...	V1.2
FDBACK	Feedback monitoring	V1.4
SFDOOR	Safety door monitoring	V1.2
ACK_GL	Global acknowledgm...	V1.2
▶ Timer operations		V1.6
▶ Counter operations		V1.6
▶ Comparator operati...		
▶ Math functions		
▶ Move operations		V1.6
▶ Conversion operati...		V1.6
▶ Program control op...		
▶ Word logic operatio...		
▶ Shift and rotate		V1.6
▶ Operate		V1.6
▶ ETC Additional instructi...		

Signature du programme :



- Doit correspondre à l'annexe 1 du rapport du certificat.

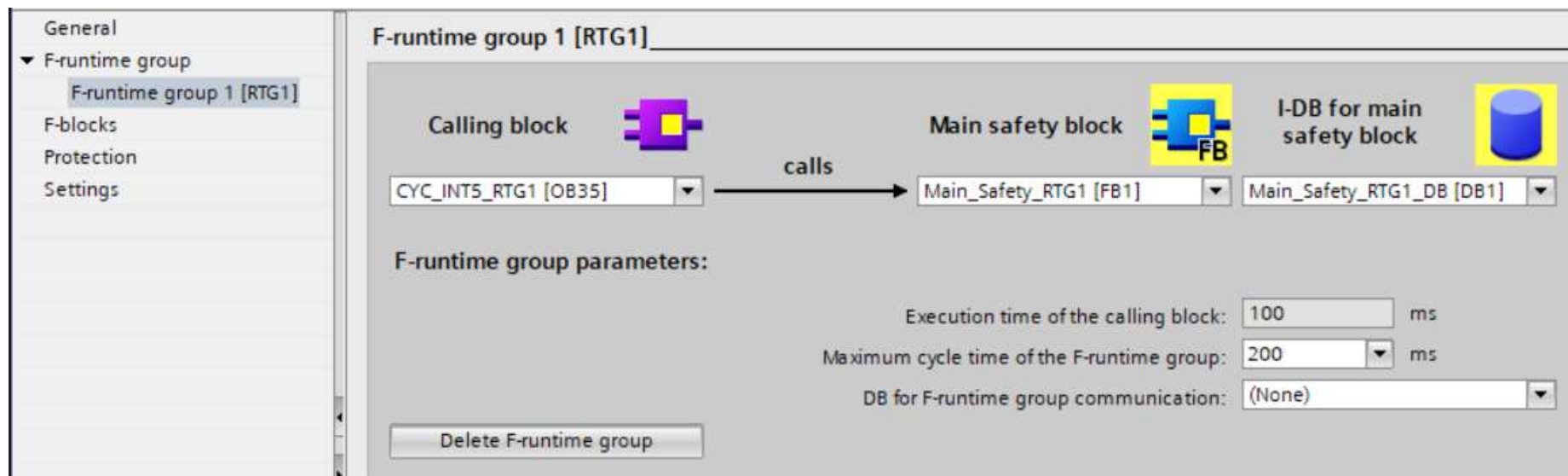
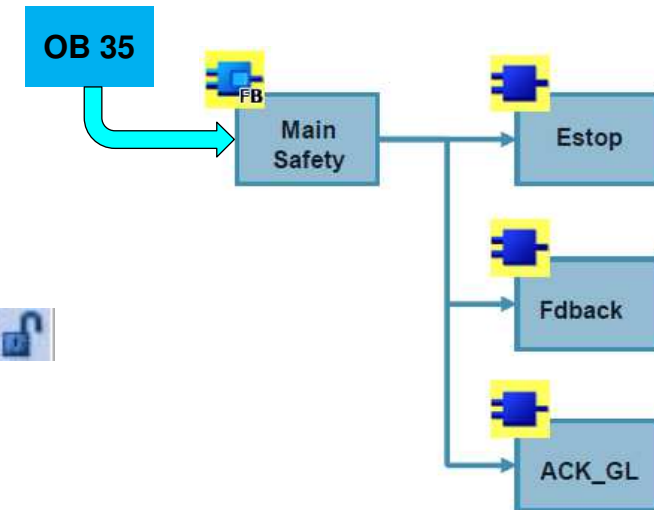
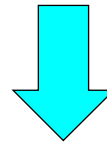
Description	Offline signature	Time stamp
Collective F-signature	5FA36E89	18/12/2024 13:25:27 (UTC +1:00)

Blocs du programme de sécurité :

Description	Used and compiled	Function in safety program	Offline signature	Time stamp
Blocs de programme				
Main_Safety_RTG1 [FB1]	Yes	F-FB	0x30BC	18/12/2024 13:2...
Main_Safety_RTG1_DB [DB1]	Yes	I-DB for F-FB	0x26AE	17/12/2024 10:2...
Blocs système				
STEP 7 Safety				
F_ACK_GL [FB219]	Yes	F-Application Block	0x8B12	20/07/2011 19:4...
F_ESTOP1 [FB215]	Yes	F-Application Block	0x4E49	20/07/2011 19:4...
F_FDBACK [FB216]	Yes	F-Application Block	0x8395	20/07/2011 19:4...
F_SFDOOR [FB217]	Yes	F-Application Block	0x86DA	20/07/2011 19:4...
F_TOF [FB186]	Yes	F-Application Block	0x14B4	20/07/2011 19:4...
ACK_GL_DB [DB6]	Yes	I-DB for F-Application Block	0xF2DE	17/12/2024 14:2...
ESTOP1_DB [DB4]	Yes	I-DB for F-Application Block	0x038A	17/12/2024 14:4...
FDBACK_DB [DB5]	Yes	I-DB for F-Application Block	0x7649	17/12/2024 14:4...
F_GLOBDB [DB8000]	Yes	F-shared DB	0xA99E	18/12/2024 13:2...
SFDOOR_DB_1 [DB8]	Yes	I-DB for F-Application Block	0x76E6	18/12/2024 11:4...
Compiler blocks				
F-I/O data blocks				
F00001_4/8F-DIDC24V_1 ...	Yes	F-I/O DB	0xF2E5	18/12/2024 11:4...
F00007_4F-DODC24V/2A...	Yes	F-I/O DB	0x87AA	17/12/2024 14:4...

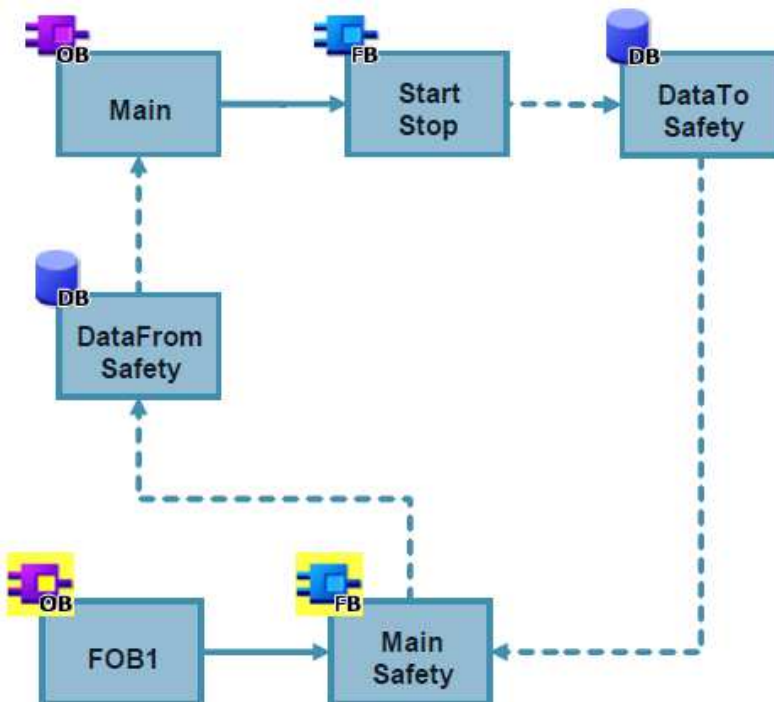
Les groupes d'exécution F (Run Time Groupe) :

- Un programme de sécurité est composé d'un ou de deux "groupes d'exécution F" :
 - ➔ gestion simplifiées des fonctions de sécurité du process,
 - ➔ boucles de sécurité avec des temps de réaction différents.
- Éléments de base d'un groupe d'exécution :



Echanges entre les programmes standard et Safety :

	Pour le programme Standard		Pour le programme Safety	
	Accès en lecture	Accès en écriture	Accès en lecture	Accès en écriture
Elément d'un DB	autorisé	autorisé	Accès en lecture ou accès en écriture	
Elément d'un DB_F	autorisé	non autorisé	autorisé	autorisé
Mémento	autorisé	autorisé	Accès en lecture ou accès en écriture	
MIE	autorisé	autorisé	autorisé	non autorisé
MIS	autorisé	autorisé	non autorisé	autorisé
MIE_F	autorisé	non autorisé	autorisé	non autorisé
MIS_F	autorisé	non autorisé	non autorisé	autorisé

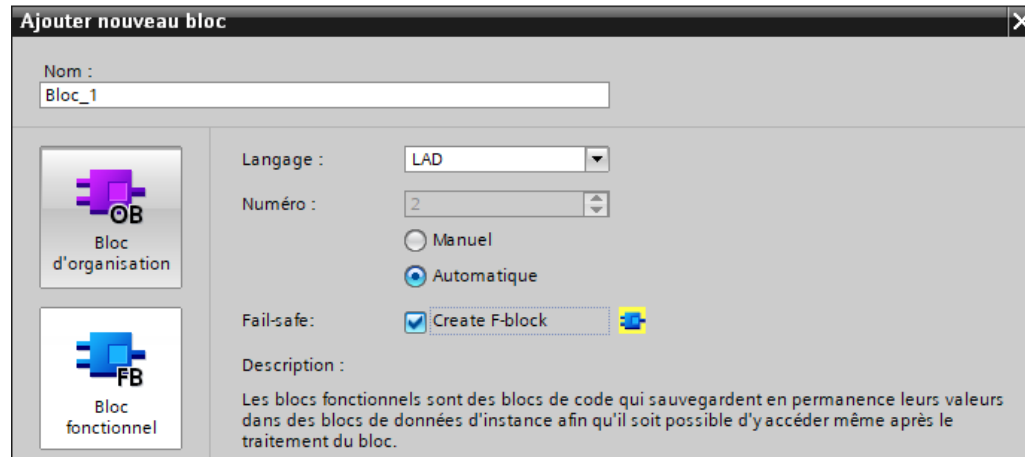


Pour l'échange d'informations entre les programmes Standard et Safety, la **solution recommandée** est l'utilisation de deux DB :

- un DB global **DataToSafety** qui procure au programme Safety les signaux de contrôle.
- un DB global **DataFromSafety** qui procure au programme standard des informations de diagnostic

Caractéristiques des programmes standard et Safety :

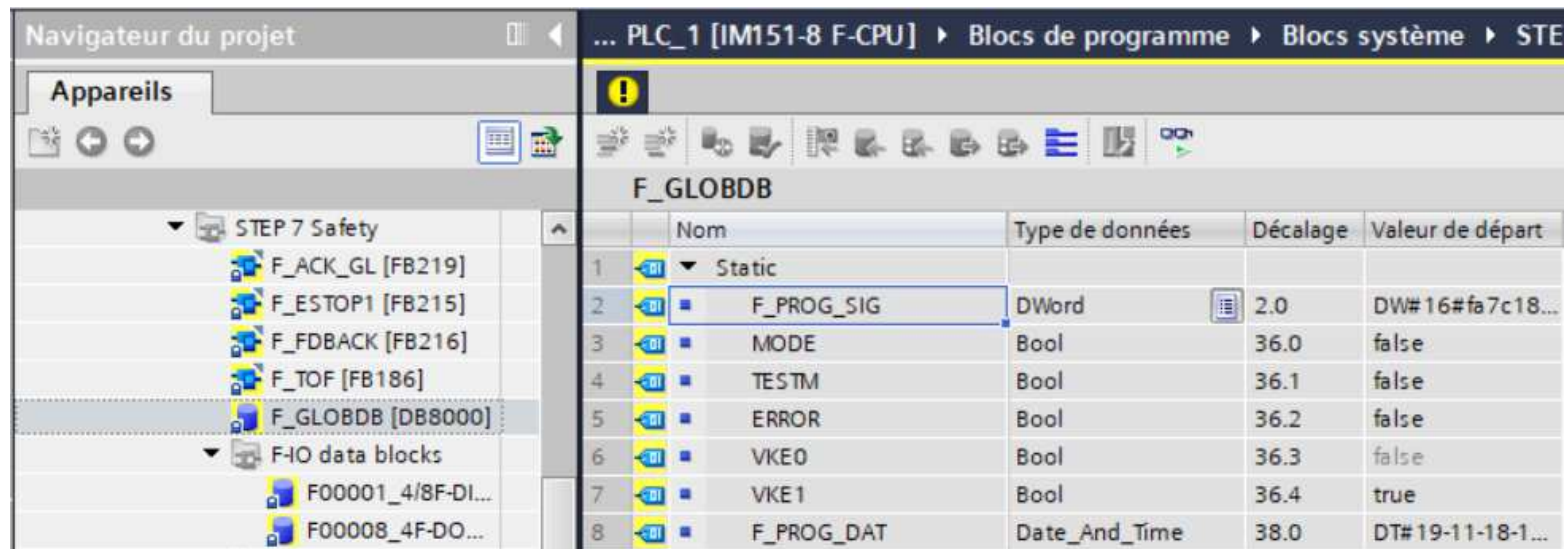
- Les blocs FC, FB et DB peuvent être créés en tant que :
 - Bloc utilisateur standard,
 - Bloc Safety.



- Les fonctions et les blocs fonctionnels créés comme **bloc Safety** ne peuvent être appelés que dans un **groupe d'exécution**.
- Les blocs de données créés comme bloc Safety peuvent être lu par le programme standard utilisateur mais ne peuvent être modifiés que par le programme Safety.
- L'accès aux voies d'un module Safety ne peut se faire que dans un groupe d'exécution.
- En mode Safety, le forçage de données du programme Safety n'est pas autorisé.
- Si le logiciel Safety n'est pas installé, seule la lecture des blocs Safety est autorisé, mais leur modification est interdite.

DB global F associé à un groupe d'exécution :

➤ F_DBGLOB :



	Nom	Type de données	Décalage	Valeur de départ
1	Static			
2	F_PROG_SIG	DWord	2.0	DW#16#fa7c18...
3	MODE	Bool	36.0	false
4	TESTM	Bool	36.1	false
5	ERROR	Bool	36.2	false
6	VKE0	Bool	36.3	false
7	VKE1	Bool	36.4	true
8	F_PROG_DAT	Date_And_Time	38.0	DT#19-11-18-1...

➤ Le programme utilisateur peut accéder à ces variables qui fournissent des **informations** sur l'état du projet Safety :

- Variable **MODE** : mode de sécurité activé (false) / désactivé (true)
- Variable **ERROR** : erreur lors du traitement du programme de sécurité
- Variable **F_PROG_SIG** : signature globale du programme de sécurité
- Variable **F_PROG_DAT** : date de compilation du programme de sécurité

- Le programme de sécurité est écrit en langage CONT F ou LOG F.
- Les langages CONT F et LOG F sont très proches des langages CONT et LOG hormis un certain nombre de restrictions.
- Restrictions des formats : seuls les formats **BOOL**, **INT**, **DINT**, **WORD** et **TIME** sont autorisés.
- Constantes booléennes 0 et 1 ➔ variables **VKE0** et **VKE1** du **DB global F**.
- Opérations :

Opération		Fonction	Description
LOG F	CONT F		
>=1	-	Opération binaire	Combinaison OU
&	-	Opération binaire	Combinaison ET
XOR	-	Opération binaire	Combinaison OU EXCLUSIF
---	-	Opération binaire	Activation entrée binaire
---o	-	Opération binaire	Négation entrée binaire
=	-	Opération binaire	Affectation
-	--- ---	Opération binaire	Contact à fermeture
-	--- / ---	Opération binaire	Contact à ouverture
-	--- NOT ---	Opération binaire	Inversion du résultat de l'opération binaire
-	---()	Opération binaire	Bobinage de sortie
#	---(#)--	Opération binaire	Connecteur
S	---(S)	Opération binaire	Mise à 1 de la sortie
R	---(R)	Opération binaire	Mise à 0 de la sortie
SR	SR	Opération binaire	Mise à 1/mise à 0 de la bascule
RS	RS	Opération binaire	Mise à 0/mise à 1 de la bascule



Ne pas utiliser l'instruction Set pour les sorties F (passivation).

➤ Opérations :

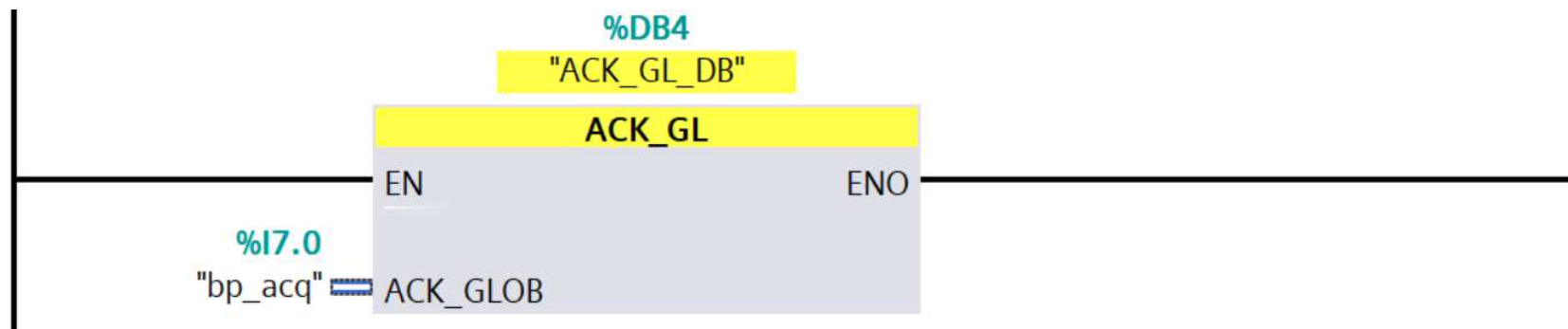
Opération		Fonction	Description
LOG F	CONT F		
N	---(N)---	Opération binaire	Détection de front descendant
NEG	NEG	Opération binaire	Détection de front descendant de signal
P	---(P)---	Opération binaire	Détection de front montant
POS	POS	Opération binaire	Détection de front montant de signal
WAND_W	WAND_W	Opération sur mot	Combinaisons ET à 16 bits
WOR_W	WOR_W	Opération sur mot	Combinaisons OU à 16 bits
WXOR_W	WXOR_W	Opération sur mot	Combinaisons OU EXCLUSIF à 16 bits
ADD_I	ADD_I	Fonction virgule fixe	Addition d'entiers (16 bits)
DIV_I	DIV_I	Fonction virgule fixe	Division d'entiers (16 bits)
MUL_I	MUL_I	Fonction virgule fixe	Multiplication d'entiers (16 bits)
SUB_I	SUB_I	Fonction virgule fixe	Soustraction d'entiers (16 bits)
CMP ? I	CMP ? I	Comparateur	Comparaison d'entiers (16 bits) (CMP==I, CMP<>I, CMP>I, CMP<I, CMP>=I, CMP<=I)
NEG_I	NEG_I	Convertisseur	Générer complément à deux de l'entier de 16 bits
OPN	---(OPN)	Appel de DB	Ouverture d'un bloc de données
MOVE	MOVE	Décalage	Transfert d'une valeur
CALL_FC (FC appelé comme boîte)	CALL_FC (FC appelé comme boîte)	Gestion d'exécution de programme	Appel inconditionnel de FC F (EN = 1, pas de connexion de EN !)

➤ Opérations :

Opération		Fonction	Description
LOG F	CONT F		
CALL_FB (FB appelé comme boîte)	CALL_FB (FB appelé comme boîte)	Gestion d'exécution de programme	Appel inconditionnel de FB F (EN = 1, pas de connexion de EN !)
vRET	---(RET)	Gestion d'exécution de programme	Retour (quitter le bloc)
appel d'instances multiples	appel d'instances multiples	Gestion d'exécution de programme	appel d'instances multiples
JMP	---(JMP)	Opération de saut	Saut absolu dans le bloc Saut dans le bloc si 1 (conditionné)
JMPN	---(JMPN)	Opération de saut	Saut dans le bloc si 0 (conditionné)
OV	OV --- ---	Bit du mot d'état	Exploitation du bit d'erreur débordement (bit OV dans le mot d'état)

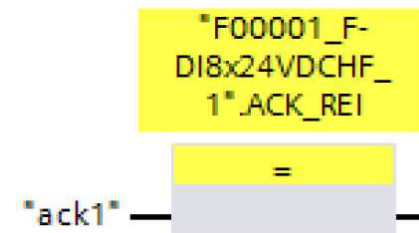
Bloc Global Acknowledge : acquittement (ACK) global (GL)

- Ce bloc génère un **acquiescement simultané** de tous les modules Safety qui ont été passivés (discordance d'une voie, erreur d'un module), afin de les réintégrer dans le système comme modules opérationnels.
- Il évite de redémarrer la CPU après une erreur Safety.

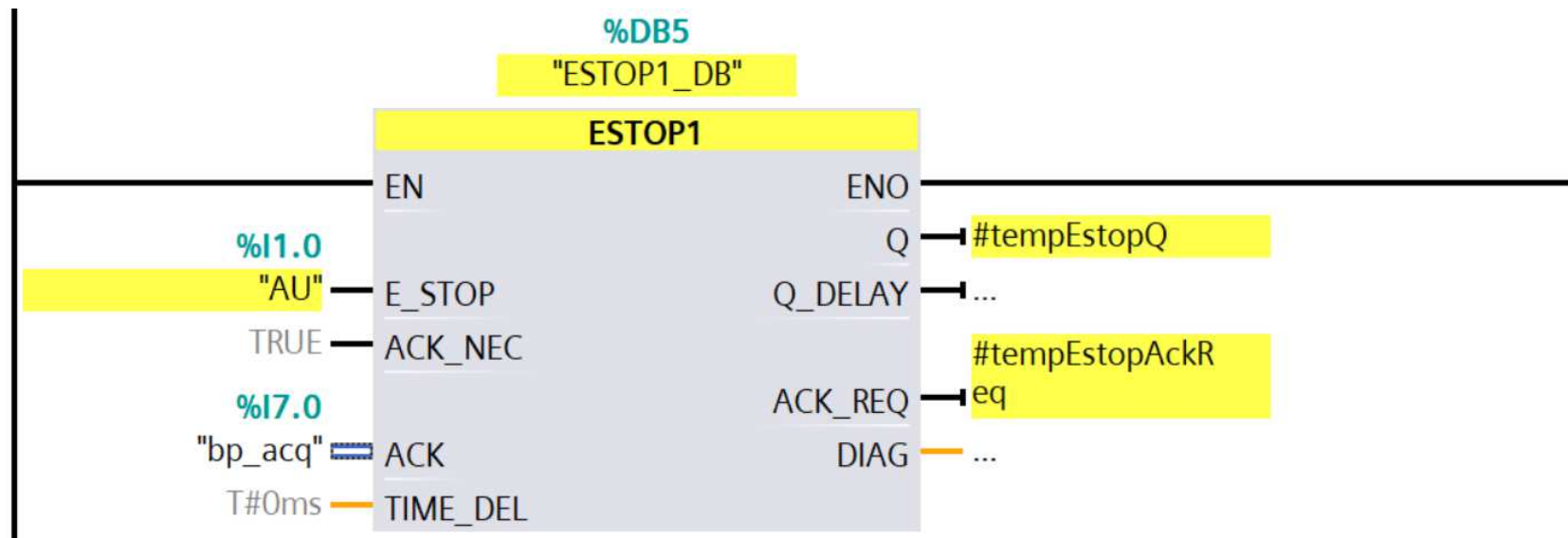


✓ **ACK_GLOB** = acquittement par front montant

- La réintégration séparée d'un module Safety se fait à l'aide de la variable **"ACK_REI"** du bloc de données du module Safety :



Bloc ESTOP1 : réalisation d'un arrêt d'urgence (catégories 0 et 1) avec acquittement.



- ✓ **E_STOP** : arrêt d'urgence
- ✓ **ACK_NEC** : acquittement = 0 → automatique,
= 1 → par front montant
- ✓ **ACK** : acquittement
- ✓ **TIME_DEL** : temps de retard entre perte de l'AU
et changement d'état de Q_DELAY
- ✓ **Q** : arrêt de type 0 (coupure de la puissance)
= 0 → dès que l'arrêt d'urgence est actionné
= 1 → si E_STOP = 1 et acquittement effectué
- ✓ **Q_DELAY** : arrêt de type 1
= 0 après écoulement de TIME_DEL
- ✓ **ACK_REQ** : signalisation "acquittement nécessaire"
- ✓ **DIAG** : information non sécurisée relative aux erreurs



Un module d'entrées TOR F-DI surveille les deux canaux d'un arrêt d'urgence (catégories 3 et 4) contre les défauts :

- discordance entre les deux voies de l'arrêt d'urgence,
- croisement entre les deux voies de l'arrêt d'urgence.

Info DIAG du Bloc ESTOP1 :

N° de bit	Occupation	Origine possible de l'erreur	Solution
Bit 0	Temps de retard TIM_DEL paramétré incorrect	Temps de retard paramétré < 0	Paramétrer un temps de retard > 0
Bit 1	Réserve	-	-
Bit 2	Réserve	-	-
Bit 3	Réserve	-	-
Bit 4	Acquittement impossible, car l'arrêt d'urgence est encore actif	Bouton d'arrêt d'urgence verrouillé	Déverrouiller le bouton d'arrêt d'urgence
		Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F du bouton d'arrêt d'urgence	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
		Bouton d'arrêt d'urgence défectueux	Vérifier le bouton d'arrêt d'urgence
		Erreur de câblage	Vérifier le câblage du bouton d'arrêt d'urgence
Bit 5	en cas d'absence de validation : l'entrée ACK est à l'état 1 en permanence	Touche d'acquittement défectueuse	Vérifier le bouton d'acquittement
		Erreur de câblage	Vérifier le câblage du bouton d'acquittement vérifier
Bit 6	Acquittement nécessaire (= état de ACK_REQ)	-	-
Bit 7	Etat de la sortie Q	-	-

Bloc TWO H EN : surveillance de commande bimanuelle (H) avec validation (EN)



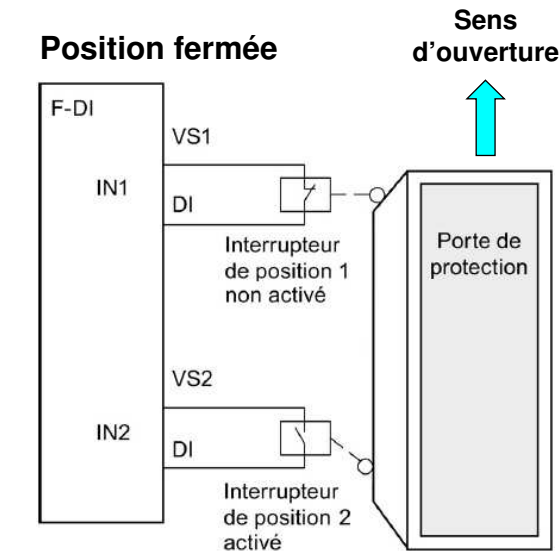
- ✓ **IN1** : Bouton poussoir 1
- ✓ **IN2** : Bouton poussoir 2
- ✓ **ENABLE** : Entrée de validation
- ✓ **DISCTIME** : temps de discordance (0..500ms)

- ✓ **Q** : validation
= 1 dès que IN1 et IN2 passent à 1 dans un temps inférieur à DISCTIME et ENABLE à 1
= 0 dès que IN1 ou IN2 ou ENABLE passe à 0
- ✓ **DIAG** : information non sécurisée relative aux erreurs

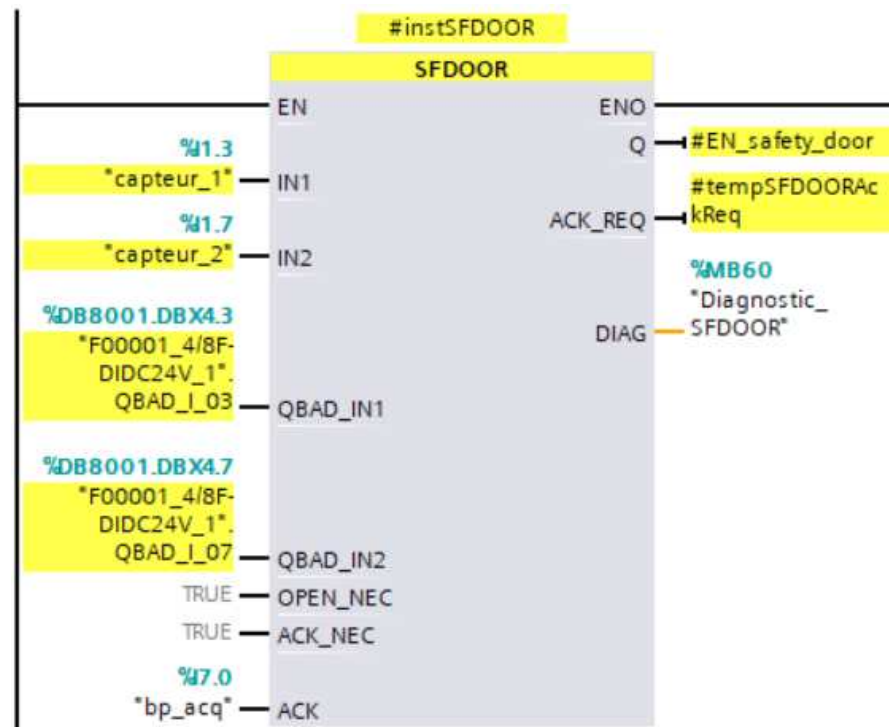
Info DIAG du Bloc TWO H EN :

N° de bit	Occupation	Origine possible de l'erreur	Solution
Bit 0	temps de discordance DISCTIME paramétré incorrect	Temps de discordance paramétré < 0 ou > 500 s	Paramétrer un temps de discordance entre 0 et 500 s
Bit 1	Temps de discordance écoulé	Temps de discordance trop petit	Augmenter le cas échéant le temps de discordance
		Boutons-poussoirs n'ont pas été activés durant le temps de discordance	Relâchez les boutons-poussoir et les activer durant le temps de discordance
		Erreur de câblage	Vérifier le câblage des boutons-poussoirs
		Bouton-poussoir défectueux	Vérifiez le bouton-poussoir
		Les boutons-poussoirs sont câblés sur différentes périphéries F et il y a une erreur de périphérie F, une erreur de voie ou une erreur de communication ou encore une passivation par PASS_ON sur une périphérie F	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 2	Réserve	-	-
Bit 3	Réserve	-	-
Bit 4	Ordre d'activation erroné	Un bouton-poussoir n'a pas été relâché	Relâchez les boutons-poussoir et les activer durant le temps de discordance
		Bouton-poussoir défectueux	Vérifiez le bouton-poussoir
Bit 5	Validation ENABLE non activée	Validation ENABLE = 0	Mettre la validation ENABLE = 1, relâchez le bouton-poussoir et l'activer durant le temps de discordance
Bit 6	Réserve	-	-
Bit 7	Etat de la sortie Q	-	-

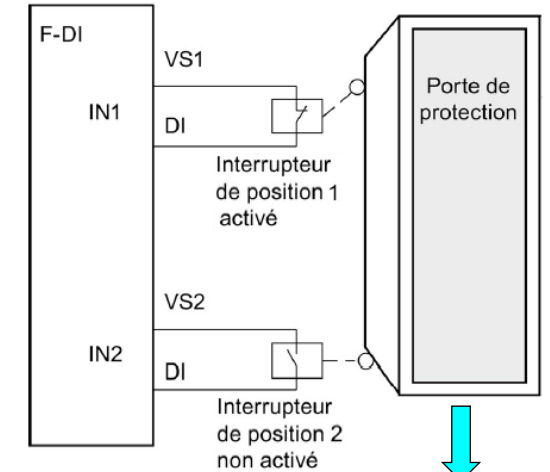
Bloc SFDOOR : surveillance de la porte de protection



Interrupteur de position 2 placé de sorte qu'il soit actionné lorsque la porte est fermée



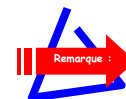
Position ouverte



Interrupteur de position 1 placé de sorte qu'il soit actionné lorsque la porte

- ✓ **IN1** : fin de course 1
- ✓ **IN2** : fin de course 2
- ✓ **QBAD_INI1** : signal QBAD voie IN1 de la carte F_DI (permet de distinguer si l'entrée est à 0 :
* Fin de course non activé,
* Entrée passivée)
- ✓ **QBAD_INI2** : signal QBAD voie IN2 de la carte F_DI
- ✓ **OPEN_NEC** : = 1 → ouverture requise au démarrage
- ✓ **ACK_NEC** : acquittement = 0 → automatique,
= 1 → par front montant
- ✓ **ACK** : acquittement

- ✓ **Q** : validation
= 1 porte de protection fermée
= 0 dès que IN1 **ou** IN2 passe à 0
- ✓ **ACK_REQ** : signalisation "acquiescement nécessaire"
- ✓ **DIAG** : information non sécurisée relative aux erreurs

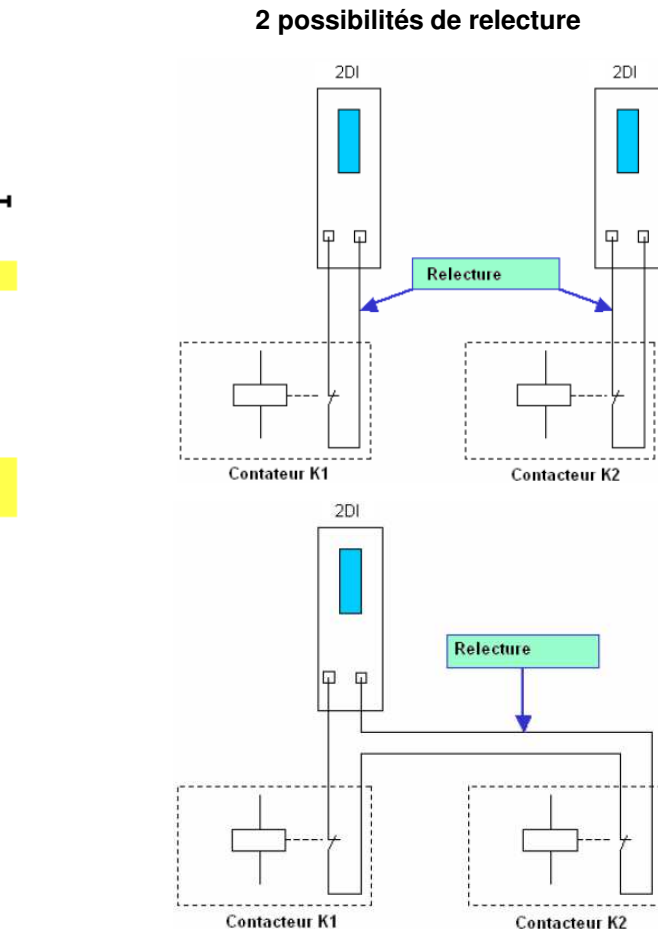
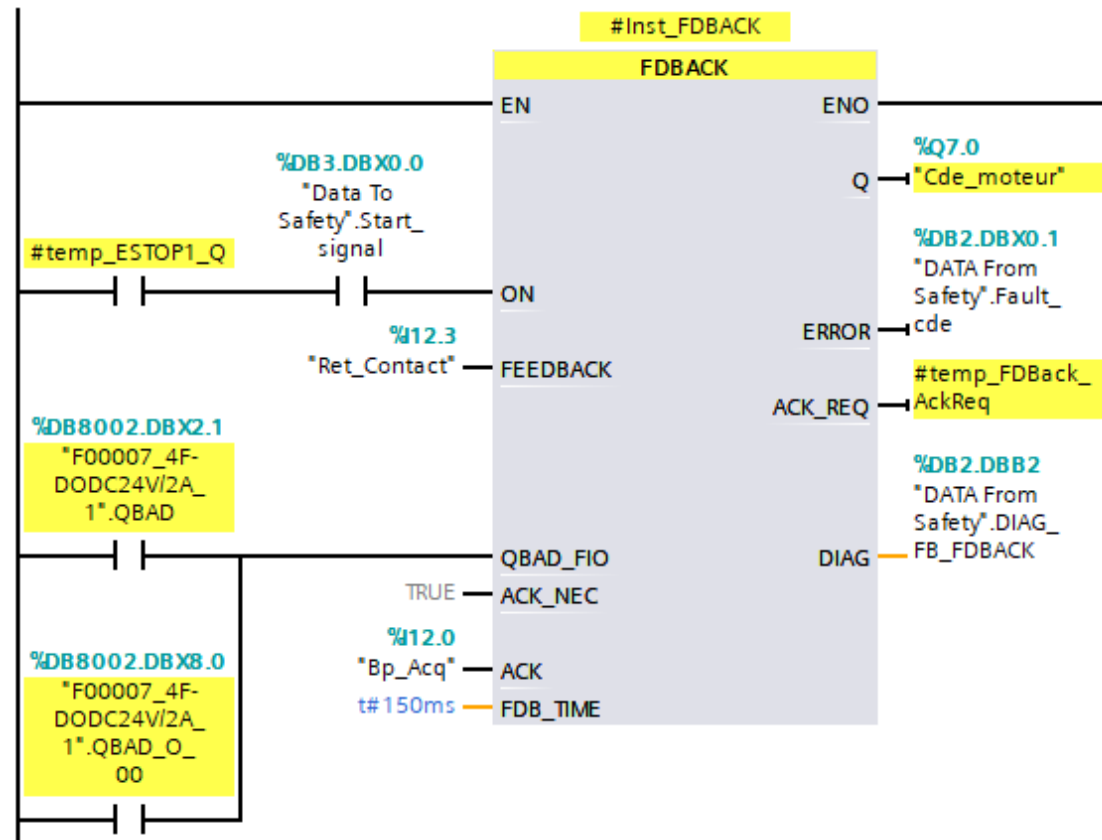


Le signal Q ne pourra repasser à 1 que si les deux entrées IN 1 et IN2 sont passées à zéro (porte suffisamment ouverte) avant la fermeture de la porte.

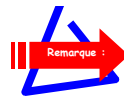
Info DIAG du Bloc SFDOOR :

N° de bit	Occupation	Origine possible de l'erreur	Solution
Bit 0	Réserve	-	-
Bit 1	Etat de signal 0 des deux entrées IN1 et IN2 manquant	Après démarrage du système F, la porte de protection n'a pas été ouverte entièrement avec OPEN_NEC = 1	Ouvrir entièrement la porte de protection
		La porte de protection n'a pas été ouverte entièrement	Ouvrir entièrement la porte de protection
		Erreur de câblage	Vérifier le câblage des commutateurs de positionnement
		Commutateurs de positionnement défectueux	Vérifier les commutateurs de positionnement
		Commutateurs de positionnement mal réglés	Régler correctement les commutateurs de positionnement
Bit 2	Etat de signal 1 des deux entrées IN1 et IN2 manquant	La porte de protection n'a pas été fermée	Fermer la porte de protection
		Erreur de câblage	Vérifier le câblage des commutateurs de positionnement
		Commutateurs de positionnement défectueux	Vérifier les commutateurs de positionnement
		Commutateurs de positionnement mal réglés	Régler correctement les commutateurs de positionnement
Bit 3	QBAD_IN1 et/ou QBAD_IN2 = 1	Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F/voie de IN1 et/ou IN2	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 4	Réserve	-	-
Bit 5	en cas d'absence de validation : l'entrée ACK est à l'état 1 en permanence	Touche d'acquiescement défectueuse	Vérifier le bouton d'acquiescement
		Erreur de câblage	Vérifier le câblage du bouton d'acquiescement
Bit 6	Acquiescement nécessaire (= état de ACK_REQ)	-	-
Bit 7	Etat de la sortie Q	-	-

Bloc FDBACK : surveillance de boucles de retour



- ✓ **ON** : activation de la sortie
- ✓ **FEEDBACK** : lecture du retour
- ✓ **QBAD_FIO** : état de la périphérie
- ✓ **ACK_NEC** : acquittement = 0 → automatique, = 1 → par front montant
- ✓ **ACK** : acquittement
- ✓ **FDB_TIME** : temps de lecture maximum toléré du retour
- ✓ **Q** : sortie
= 1 dès que ON passe à 1
= 0 dès que ON passe à 0 ou ERREUR passe à 1
- ✓ **ERROR** : erreur de lecture du retour
- ✓ **ACK_REQ** : signalisation "acquittement nécessaire"
- ✓ **DIAG** : information non sécurisée relative aux erreurs

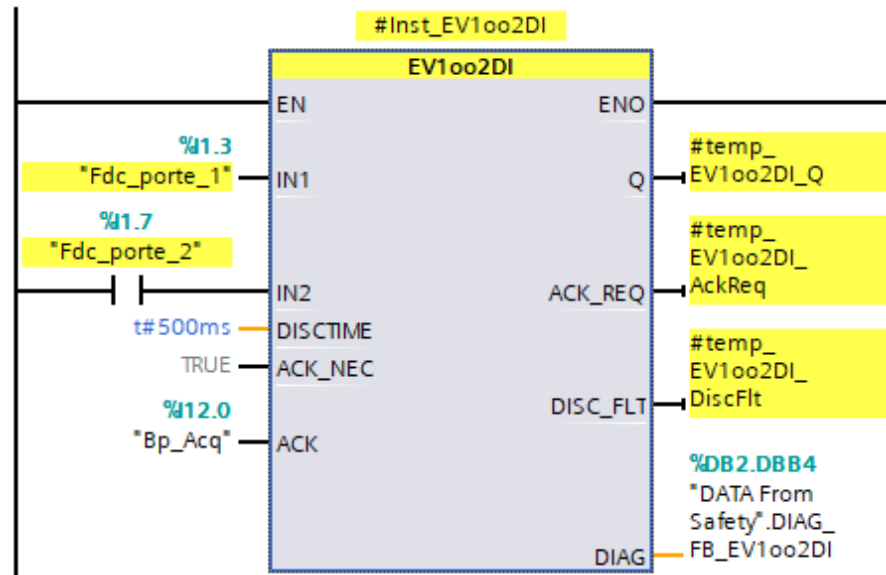


La sortie Q doit correspondre à l'état inversé de l'entrée FEEDBACK

Infos DIAG du bloc FDBACK :

N° de bit	Occupation	Origine possible de l'erreur	Solution
Bit 0	Erreur de lecture de retour ou temps de lecture de retour paramétré incorrect (= état de ERROR)	Temps de lecture de retour paramétré < 0	Paramétrer un temps de lecture de retour > 0
		Temps de lecture de retour trop petit	Augmenter le cas échéant le temps de lecture de retour
		Erreur de câblage	Vérifier le câblage de l'actionneur et du contact de lecture de retour
		Actionneur ou contact de lecture de retour défectueux	Vérifier l'actionneur et le contact de lecture de retour
		Erreur de périphérie ou de voie de l'entrée de lecture de retour	Vérifier la périphérie
Bit 1	Passivation de la périphérie F/voie commandée par la sortie Q (= état de QBAD_FIO)	Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 2	après l'erreur de lecture de retour : l'entrée de lecture de retour a en permanence l'état de signal 0	Erreur de périphérie ou de voie de l'entrée de lecture de retour	Vérifier la périphérie
		Contact de lecture de retour défectueux	Vérifier le contact de lecture de retour
		Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F de l'entrée de lecture de retour	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 3	Réserve	-	-
Bit 4	Réserve	-	-
Bit 5	lors d'une erreur de lecture de retour : l'entrée ACK est à l'état 1 en permanence	Touche d'acquiescement défectueuse	Vérifier le bouton d'acquiescement
		Erreur de câblage	Vérifier le câblage du bouton d'acquiescement
Bit 6	Acquiescement nécessaire (= état de ACK_REQ)	-	-
Bit 7	Etat de la sortie Q	-	-

Bloc VE1oo2DI : exploitation 1oo2 de deux capteurs monocanal avec analyse de discordance



- ✓ **IN1** : capteur 1 à évalué
- ✓ **IN2** : capteur 2 à évalué
- ✓ **DISCTIME** : temps avant évaluation de la divergence
- ✓ **ACK_NEC** : acquittement = 0 → automatique,
= 1 → par front montant
- ✓ **ACK** : acquittement
- ✓ **Q** : sortie
= 1 si IN1 et IN2 sont à 1 et DISC_FLT = 0
- ✓ **ACK_REQ** : signalisation "acquittement nécessaire"
- ✓ **DISC_FLT** : défaut "divergence entre IN1 et IN2"
= 1 si états de IN1 et IN2 différents après écoulement de DISCTIME
- ✓ **DIAG** : information non sécurisée relative aux erreurs

Infos DIAG du bloc FDBACK :

N° de bit	Occupation	Origine possible de l'erreur	Solution
Bit 0	Erreur de lecture de retour ou temps de lecture de retour paramétré incorrect (= état de ERROR)	Temps de lecture de retour paramétré < 0	Paramétrer un temps de lecture de retour > 0
		Temps de lecture de retour trop petit	Augmenter le cas échéant le temps de lecture de retour
		Erreur de câblage	Vérifier le câblage de l'actionneur et du contact de lecture de retour
		Actionneur ou contact de lecture de retour défectueux	Vérifier l'actionneur et le contact de lecture de retour
		Erreur de périphérie ou de voie de l'entrée de lecture de retour	Vérifier la périphérie
Bit 1	Passivation de la périphérie F/voie commandée par la sortie Q (= état de QBAD_FIO)	Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 2	après l'erreur de lecture de retour : l'entrée de lecture de retour a en permanence l'état de signal 0	Erreur de périphérie ou de voie de l'entrée de lecture de retour	Vérifier la périphérie
		Contact de lecture de retour défectueux	Vérifier le contact de lecture de retour
		Erreur de périphérie F, erreur de voie ou erreur de communication ou encore passivation par PASS_ON de la périphérie F de l'entrée de lecture de retour	Voir la variable DIAG, bits 0 à 6 au chapitre "DB de périphérie F".
Bit 3	Réserve	-	-
Bit 4	Réserve	-	-
Bit 5	lors d'une erreur de lecture de retour : l'entrée ACK est à l'état 1 en permanence	Touche d'acquiescement défectueuse	Vérifier le bouton d'acquiescement
		Erreur de câblage	Vérifier le câblage du bouton d'acquiescement
Bit 6	Acquiescement nécessaire (= état de ACK_REQ)	-	-
Bit 7	Etat de la sortie Q	-	-

➤ Deux mots de passe pour accéder au système Safety :

- Mot de passe pour le **chargement** de la CPU F
➔ menu Protection des propriétés de la CPU.



Le chargement d'un bloc du programme standard ne nécessite pas de mot de passe

Constantes système | Textes

Protection

Niveau d'accès

Sélectionnez le niveau d'accès pour l'API.

Niveau d'accès	IHM	Lire	Ecrire	De sécurité	Mot de pass
<input type="radio"/> Accès complet, y compris failsafe (pas d..	✓	✓	✓	✓	
<input checked="" type="radio"/> Accès complet (pas de protection)	✓	✓	✓		
<input type="radio"/> Accès en lecture	✓	✓			
<input type="radio"/> Accès IHM	✓				
<input type="radio"/> Aucun accès (protection complète)					

Accès complet (pas de protection) :
Les utilisateurs de TIA Portal obtiendront l'accès aux fonctions standard.
Les applications IHM peuvent accéder à toutes les fonctions (failsafe et standard).

Mot de passe obligatoire :
Pour un accès supplémentaire aux fonctions failsafe, l'utilisateur de TIA Portal doit saisir le mot de passe pour "Accès complet, y compris failsafe".

Constantes système | Textes

Protection

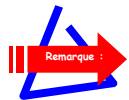
IM151

☐ Pas de protection
☐ Lecture seule
☐ Protection en écriture et en lecture
☒ Protection en écriture pour blocs de sécurité
☐ Modifiable par mot de passe

Mot de passe pour accès en lecture/écriture

Mot de passe:

Confirmer le mot de passe:



Le chargement de l'ensemble des blocs programmes nécessite l'arrêt de la CPU.
Le chargement d'un bloc se fait normalement si l'arrêt de la CPU est demandé, autrement TIA demande de désactiver le mode Safety !

- Mot de passe pour la **modification** du programme Safety

Arrêter tout

Charger la sélection

Download selection

☐ Disable

☐ Confirm

Projet_safety

- Ajouter un appareil
- Appareils & Réseaux
- PLC_1 [IM151-8 F-CPU]
 - Configuration des appareils
 - En ligne & Diagnostic
 - Safety Administration

General

- F-runtime group
 - F-runtime group 1 [RTG1]
 - F-blocks
 - Protection
 - Settings

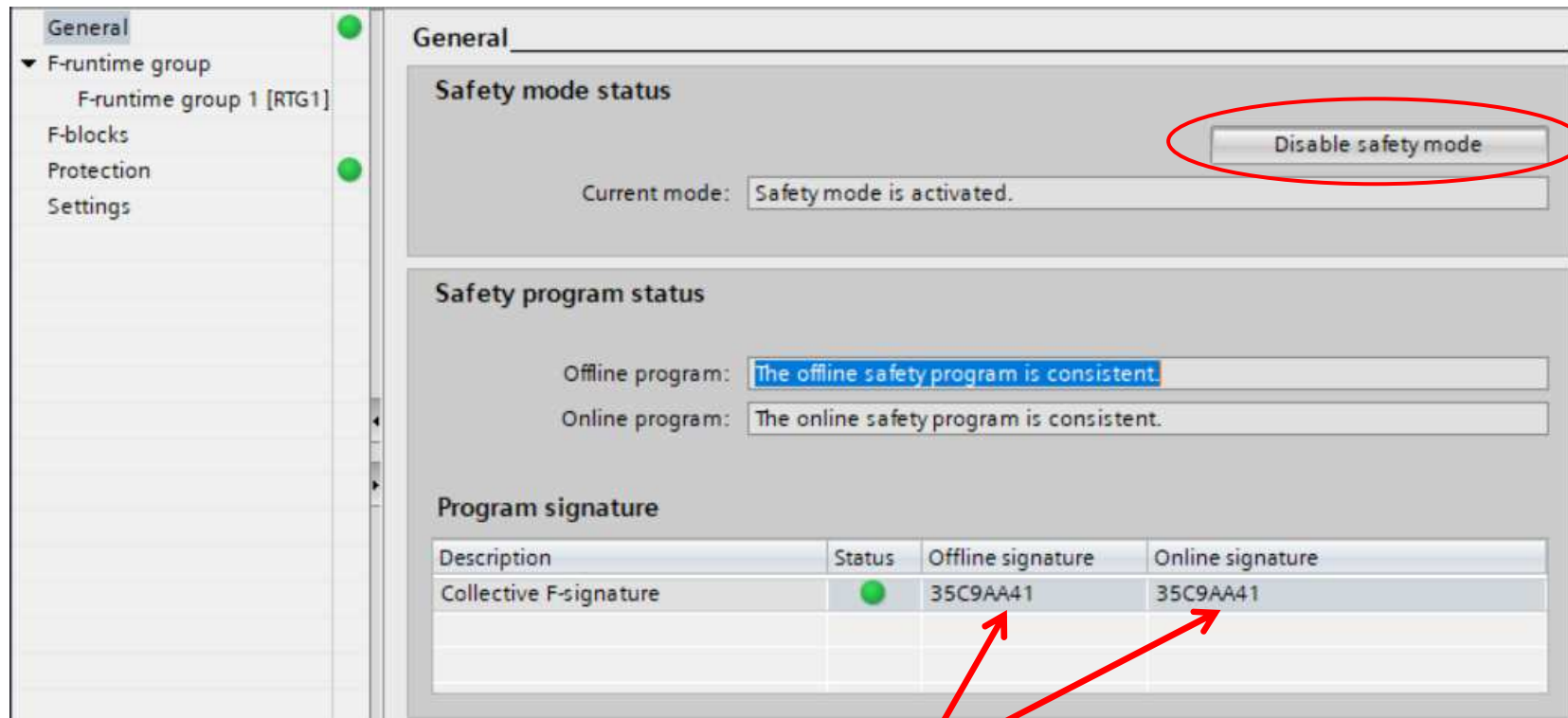
Offline safety program protection

Password for modifying safety program:

Password:

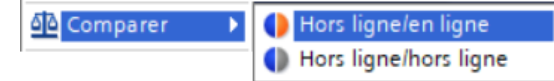
Log off Change

- En fonctionnement **normal**, le programme de sécurité s'exécute dans la CPU F en **mode Safety** : toutes les mesures de suppression d'erreurs sont activées.
- Le chargement de modifications du programme Safety en mode RUN nécessite la désactivation du mode de Safety. Cette désactivation doit être réservée uniquement pour la mise au point du programme → **la sécurité de l'installation doit être assurée par d'autres mesures d'organisation.**
- La réactivation du mode Safety se fait par une commutation STOP/RUN de la CPU F.



Programmes Safety dans le projet et dans la CPU F identiques.

- Comparaison entre le programme de la CPU F et celui du projet :



Editeur de comparaison en ligne

Projet_safety: PLC_1							*Online PLC*						
Nom	Adresse	Type	Interface horodatage	Code horodatage	Signature	Etat	Action	Nom	Adresse	Type	Interface horodatage	Code horodatage	Signature
PLC_1								PLC_1					
Blocs de progra...													
Main [OB1]	OB1	OB	03/08/2007 - 18:55:...	14/11/2019 - 23:...	0x6A84			OB1 [OB1]	OB1	OB	03/08/2007 - 18:55:...	14/11/2019 - 23:...	0x6A84
CYC_INT5_RT...	OB35	OB	03/08/2007 - 18:55:...	13/11/2019 - 23:...	0xCA89			OB35 [OB35]	OB35	OB	03/08/2007 - 18:55:...	13/11/2019 - 23:...	0xCA89
I/O_FLT1 [OB...	OB82	OB	03/08/2007 - 18:55:...	14/11/2019 - 22:...	0x75F4			OB82 [OB82]	OB82	OB	03/08/2007 - 18:55:...	14/11/2019 - 22:...	0x75F4
StartStop [FC1]	FC1	FC	14/11/2019 - 17:57:...	14/11/2019 - 18:...	0xDFF7			FC1 [FC1]	FC1	FC	14/11/2019 - 17:57:...	14/11/2019 - 18:...	0xDFF7
Datafromsaf...	DB3	DB	14/11/2019 - 17:55:...	14/11/2019 - 17:...	0x6A19			DB3 [DB3]	DB3	DB	14/11/2019 - 17:55:...	14/11/2019 - 17:...	0x6A19
Datatosafety...	DB2	DB	14/11/2019 - 17:51:...	14/11/2019 - 17:...	0x6A19			DB2 [DB2]	DB2	DB	14/11/2019 - 17:51:...	14/11/2019 - 17:...	0x6A19
Main_Safety...	FB1	FB	13/11/2019 - 23:14:...	25/11/2019 - 19:...	0xF8BA			FB1 [FB1]	FB1	FB	13/11/2019 - 23:14:...	24/11/2019 - 21:...	0xEE59
Main_Safety...	DB1	DB	13/11/2019 - 23:14:...	13/11/2019 - 23:...	0x019C			DB1 [DB1]	DB1	DB	13/11/2019 - 23:14:...	13/11/2019 - 23:...	0x019C
Blocs système													
STEP 7 Sa...													
F_ACK...	FB219	FB	24/10/2006 - 11:35:...	20/07/2011 - 19:...	0x8B12			F_ACK_GL [FB219]	FB219	FB	24/10/2006 - 11:35:...	20/07/2011 - 19:...	n.a.
F_EST...	FB215	FB	01/12/2010 - 17:49:...	20/07/2011 - 19:...	0x4E49			F_ESTOP1 [FB215]	FB215	FB	01/12/2010 - 17:49:...	20/07/2011 - 19:...	n.a.
F_FDB...	FB216	FB	01/12/2010 - 17:49:...	20/07/2011 - 19:...	0x8395			F_FDBACK [FB216]	FB216	FB	01/12/2010 - 17:49:...	20/07/2011 - 19:...	n.a.
F_TOF...	FB186	FB	05/03/2004 - 16:47:...	20/07/2011 - 19:...	0x1484			F_TOF [FB186]	FB186	FB	05/03/2004 - 16:47:...	20/07/2011 - 19:...	n.a.
F_GL...	DB8000	DB	25/11/2019 - 19:34:...	25/11/2019 - 19:...	0x4D55			DB8000 [DB8000]	DB8000	DB	24/11/2019 - 21:48:...	24/11/2019 - 21:...	0x60F0
FIO d...													

Résultat de la comparaison : Le code diffère.

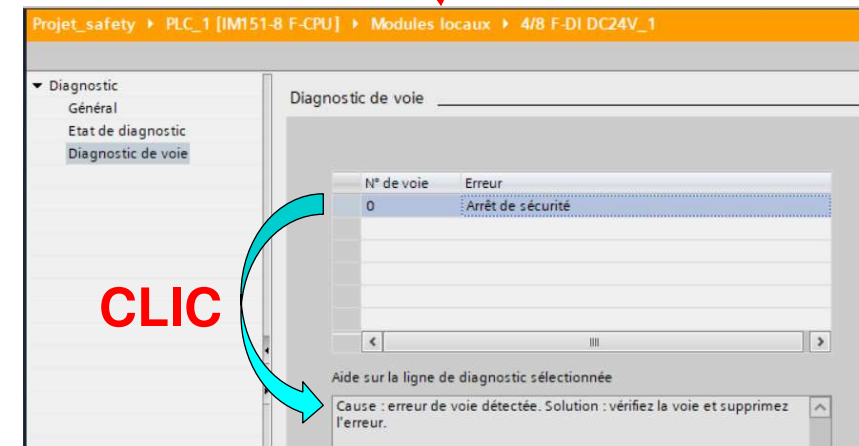
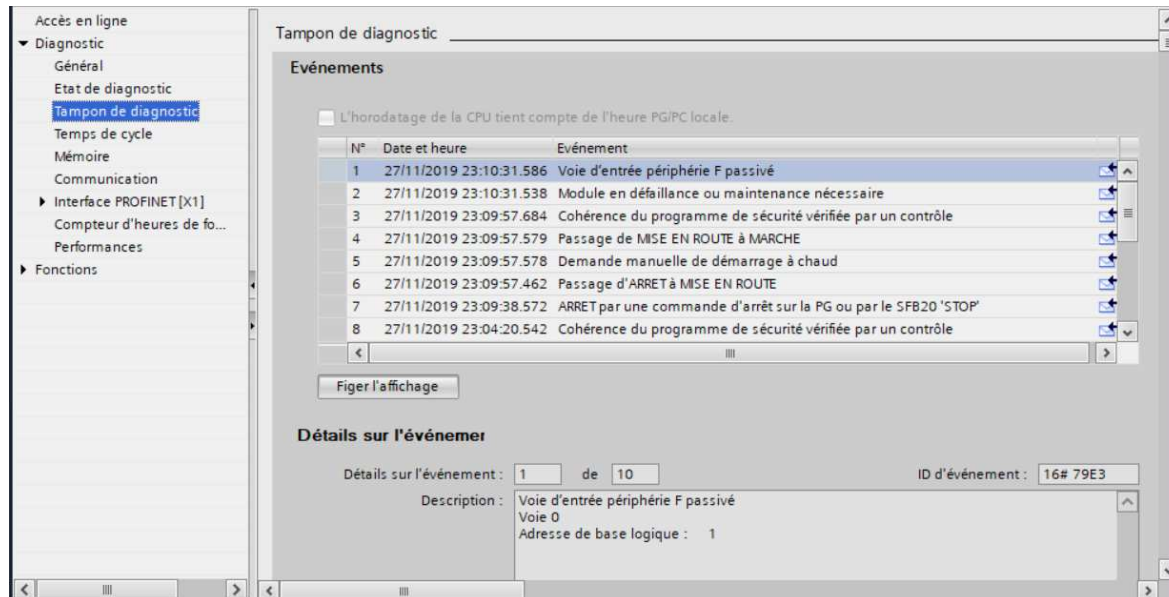
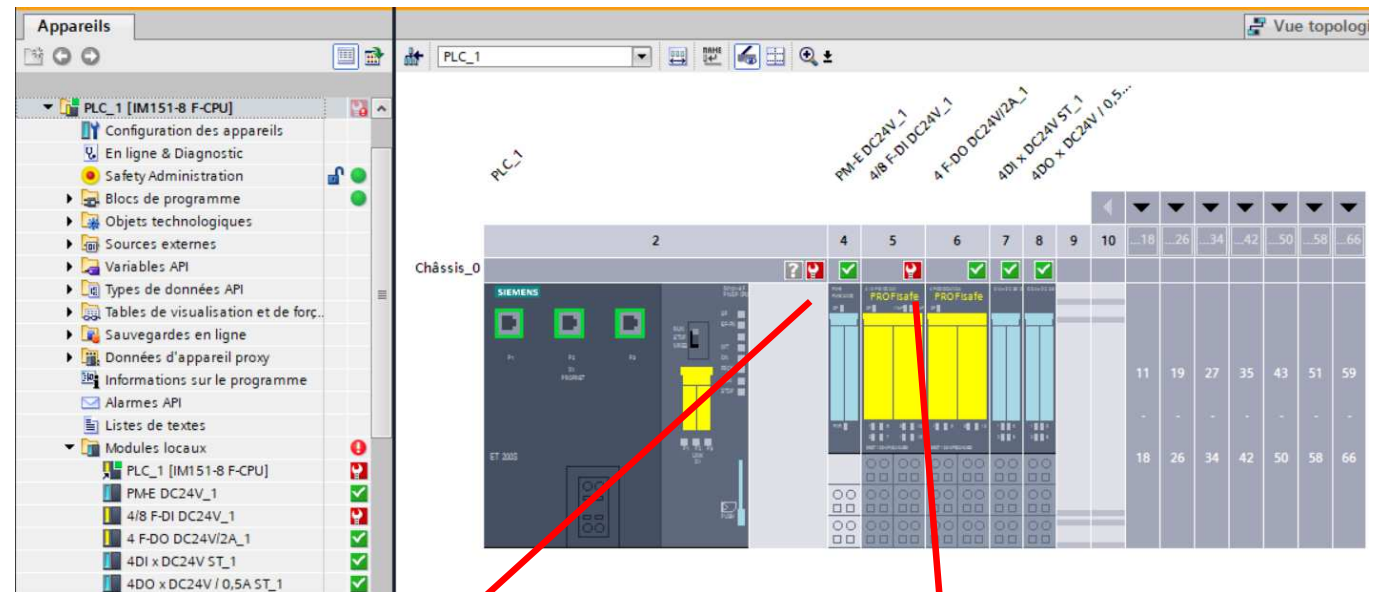
Main_Safety_RTG1 [FB1]		FB1 [FB1]	
Adresse:	FB1		FB1
Type:	FB		FB
Interface horodatage:	13/11/2019 - 23:14:36.923		13/11/2019 - 23:14:36.923
Code horodatage:	25/11/2019 - 19:34:17.158		24/11/2019 - 21:48:15.758
Horodatage de la dernièr...	n.a.		n.a.
Signature:	0xF8BA		0xEE59

Leds d'erreur :

- Led **SF** (erreur groupée) :
 - **s'allume** aussitôt que le module F déclenche une fonction de diagnostic.
(ex. : voies en double canal et différences entre les deux canaux).
 - **clignote** lorsqu'une erreur a disparu, mais qu'elle n'a pas encore été acquittée.
- Leds **VsF**, **1VsF** et **2VsF** :
 - Uniquement sur les cartes d'entrées Safety.
 - Erreur d'alimentation interne pour les capteurs.



Diagnostic matériel :



Bloc de données associé au module :

Projet_safety ▶ PLC_1 [IM151-8 F-CPU] ▶ Blocs de programme ▶ Blocs système ▶ STEP 7 Safety ▶ F-IO data blocks ▶ F00001_4/8F-DIDC24V_1 [DB8001]

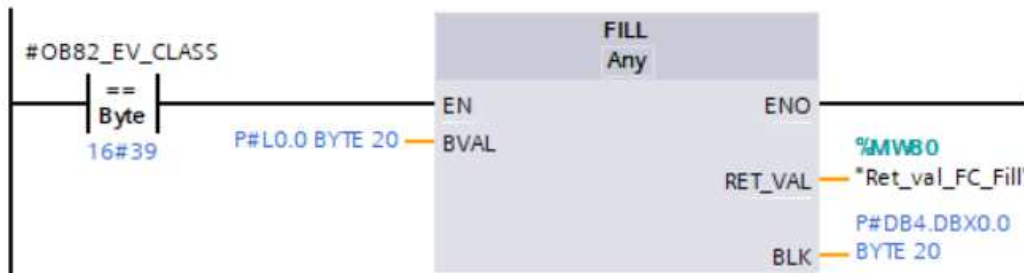
F00001_4/8F-DIDC24V_1

	Nom	Type de données	Décalage	Valeur de départ	Valeur de visualisati.	Rémanence	Visible da...	Valeur de ..	Commentaire
6	▼ Output					<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7	PASS_OUT	Bool	2.0	TRUE	TRUE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=PASSIVATION OUTPUT
8	QBAD	Bool	2.1	TRUE	TRUE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=FAIL-SAFE VALUES ARE OUTPUT
9	ACK_REQ	Bool	2.2	false	FALSE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=ACKNOWLEDGEMENT REQUEST
10	IPAR_OK	Bool	2.3	false	FALSE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=NEW I-PARAMETER VALUES ASSIGNED
11	DIAG	Byte	3.0	16#0	16#02	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DIAGNOSTIC INFORMATION
12	QBAD_I_00	Bool	4.0	TRUE	TRUE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=FAIL-SAFE VALUE IS OUTPUT AT INPUT CHA...
13	QBAD_I_01	Bool	4.1	TRUE	FALSE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=FAIL-SAFE VALUE IS OUTPUT AT INPUT CHA...
14	QBAD_I_02	Bool	4.2	TRUE	FALSE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=FAIL-SAFE VALUE IS OUTPUT AT INPUT CHA...
15	QBAD_I_03	Bool	4.3	TRUE	FALSE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1=FAIL-SAFE VALUE IS OUTPUT AT INPUT CHA...

- En cas d'erreur, les cartes d'entrées et de sorties safety émettent une alarme de diagnostic.
- Lorsqu'une alarme de diagnostic est détectée par le système, deux cas se présentent :
 - Pas d'OB de réaction dans la CPU ➔ S7 300 / S7 400 : arrêt de la CPU avec led "SF" allumée, S7 1200 / S7 1500 : erreur ignorée.
 - OB de réaction (**OB82**) dans la CPU ➔ l'OB est exécuté, et la led "SF" reste allumée.

Exemple de traitement
avec une CPU S7-300 :

I/O_FLT1				
	Nom	Type de données	Décalage	Commentaire
1	Temp			
2	OB82_EV_CLASS	Byte	0.0	16#39, Event class 3, Entering event state, Internal fa.
3	OB82_FLT_ID	Byte	1.0	16#XX, Fault identification code
4	OB82_PRIORITY	Byte	2.0	Priority of OB Execution
5	OB82_OB_NUMBR	Byte	3.0	82 (Organization block 82, OB82)
6	OB82_RESERVED_1	Byte	4.0	Reserved for system
7	OB82_IO_FLAG	Byte	5.0	Input (01010100), Output (01010101)
8	OB82_MDL_ADDR	Word	6.0	Base address of module with fault
9	OB82_MDL_DEFECT	Bool	8.0	Module defective
10	OB82_INT_FAULT	Bool	8.1	Internal fault
11	OB82_EXT_FAULT	Bool	8.2	External fault
12	OB82_PNT_INFO	Bool	8.3	Point information



DB alarme diag				
	Nom	Type de données	Décalage	Valeur de visu..
1	Static			
2	OB82_EV_CLASS	Byte	0.0	16#39
3	OB82_FLT_ID	Byte	1.0	16#42
4	OB82_PRIORITY	Byte	2.0	16#1A
5	OB82_OB_NUMBR	Byte	3.0	16#52
6	OB82_RESERVED_1	Byte	4.0	16#C5
7	OB82_IO_FLAG	Byte	5.0	16#54
8	OB82_MDL_ADDR	Word	6.0	16#0008
9	OB82_MDL_DEFECT	Bool	8.0	TRUE
10	OB82_INT_FAULT	Bool	8.1	FALSE
11	OB82_EXT_FAULT	Bool	8.2	TRUE
12	OB82_PNT_INFO	Bool	8.3	TRUE