SPECIFICATIONS DU PROTOCOLE DE COMMUNICATION

CLEARSY
Safety Solutions Designer

SATURN

Code arbre technique	C
Code dictionnaire	D411-A
Edition	04
Révision	02
Nombre total de pages	
Etat	Référence

SATURN

CONTACT@CLEARSY.COM

	RÉDACTION	VÉRIFICATION	ACCEPTATION
FONCTION	Resp Réseau et conception	Expert	Chef de projet
NOM	D. Rambaud & M. Comptier	P Sauvage	Sebastien Agostini
DATE	07/11/2016	07/11/2016	07/11/2016
SIGNATURE			

Mises à jour et suivi d'évolution

ED	REV	DATE DE MODIFICATION	AUTEUR	ORIGINE DE LA MODIFICATION
00	01	16/09/13	D. Rambaud	Premier Draft, document de travail
01	00	11/02/2014	S. Agostini	Mises à jour du protocole sur la partie sécuritaire et reprogrammation
02	00	22/05/2014	D. Rambaud	Différenciation des champs SEC et SEQ. Ajout de précisions sur l'utilisation de ces champs.
03	00	04/06/2014	M.Comptier	Mise à jour des registres OUT_REP et CONF
03	01	07/07/2014	M.Comptier	Mise à jour du registre VER sur 2 octets et correction de la structure des trames de lecture non sécuritaires
03	02	08/07/2014	M.Comptier	Mise à jour format trame de réponse non sécuritaire
03	03	15/07/2014	M.Comptier	Mise à jour code du registre TYP pour différentier les cartes d'entrées des cartes sorties
03	04	18/07/2014	D. Rambaud	Complément de l'exigence CON-PRO-0060 et rajout de l'exigence CON-PRO-0065
03	05	29/07/2014	S. Agostini	Ajout de précision sur certaines exigences
03	06	14/08/2014	M.Comptier	Modifications suite aux FFT1, 2 et 3
03	07	03/09/2014	S. Agostini	Suppression d'un TBD dans § III.2.2.7 (définition champs SEC)
03	08	05/09/2014	D. Rambaud	Rajout du code TYP pour les SIO0 (§III.3)
03	09	22/09/2014	M.Comptier	MAJ suite aux FFT 5 et 6 créées lors des tests sur SO2 version 0.4 + ajout de la partie dynamique du réseau
03	10	24/10/2014	M.Comptier	Ajout d'une trame de vérification des invariants
03	11	30/10/2014	M.Comptier	Prise en compte FFT 8
03	12	15/01/15	S. Agostini	Suppression de l'allocation des exigences 2040 & 2050 au pic
03	13	12/02/2015	M.Comptier	Prise en compte FFT n°17
03	14	23/02/2015	M.Comptier	Prise en compte FFT n°18,19 et 20
03	15	07/09/2015	D. Rambaud	Nettoyage typo
04	00	01/08/2015	S. Agostini	Mise ajour des tags des exigences pour compatibilité Reqtify + Prise en compte fiche de relecture BLD

1 GENERALITES

1.1 OBJET DU DOCUMENT

Ce document constitue la spécification détaillée du protocole utilisé sur le réseau SATURN. Il définit les formats de trames échangées, les règles que doivent respecter les agents connectés sur le bus, ainsi que les règles d'implémentation.

1.2 GLOSSAIRE

Agent	Tout équipement connecté sur le réseau
Client	Ou réseau client. Système utilisateur du service SATURN.
concentrateur	Agent particulier capable d'administrer le réseau SATURN. Un concentrateur peut être en mode actif, passif ou passant.
Image du procédé	Etat des entrées/sorties de tous les MIO, stocké dans un concentrateur.
MIO	Agent esclave du réseau offrant au système ses fonctionnalités d'entrée/sortie. On qualifie de MIO sécuritaire les module SI2 SO2 CO2 SI4 SO4 et CO4

1.3 DOCUMENTATION

1.3.1 Documents applicables

RÉFÉRENCE	DÉSIGNATION	ORIGINE	VERSION
D411	Spécifications fonctionnelles et techniques	CLEARSY - Axseam	1.4
EN 50 129	Applications ferroviaires Systèmes de signalisation, de télécommunications et de traitement, Systèmes électroniques de sécurité pour la signalisation	EN	Mai 2003

1.3.2 Documents de référence

RÉFÉRENCE	DÉSIGNATION	VERSION
EN 50159-1	Applications ferroviaires Systèmes de signalisation, de télécommunications et de traitement Communication de sécurité sur des systèmes de transmission fermés	Aout 2001

1.4 CONVENTIONS

1.4.1 Notations numériques

Dans ce document les notations suivantes sont utilisées pour les nombres.

- Notation hexadécimale : le nombre est suivi d'un 'h' (ex : 12AEh)
- Notation binaire : le nombre est suivi d'un 'b' (Ex : 101101b)
- Notation décimale : le nombre est soit suivi d'un 'd' soit n'est pas suffixé (Ex : 158d ou 158)

Pour les notations hexadécimales et binaires, le MSB est toujours le plus à gauche.

1.4.2 Notations des exigences

Les exigences décrites dans ce document respectent le format suivant :

CON-PRO-xxxx

Texte de l'exigence

Couverture :

[Justification : Ce champ optionnel apporte des précisions sur l'origine de l'exigence]

[Sécurité] : Ce champ optionnel indique, s'il est présent, que l'exigence intervient dans une fonction de sécurité du système.

2 DESCRIPTION GENERALE

2.1 TOPOLOGIE DU RÉSEAU

Le protocole décrit dans ce document est destiné à être implémenté sur le réseau de communication du système SATURN qui a la topologie suivante :

- Le réseau est câblé en daisy-chain

Le réseau est constitué de segments de bus indépendants. Chaque segment relie point à point 2 agents. Chaque agent a donc 2 ports de communication qui le relient à 2 autres agents. Le réseau est rebouclé sur lui-même en anneau (le dernier agent est relié au premier).

- Les agents connectés sur le réseau sont de 3 types

  - Les concentrateurs sont les administrateurs du réseau. Il peut y avoir sur le même réseau de 1 à 8 concentrateurs. A un instant donné, il ne peut y'avoir qu'un seul concentrateur actif sur le réseau, les autres concentrateurs étant passifs.

  - Les MIO sont les esclaves du réseau. Il peut y avoir sur le même réseau entre 1 et 128 MIO. D'un point de vue communication, tous les MIO ont le même mode de fonctionnement. En revanche, les MIO peuvent implémenter des fonctions métiers différentes (entrées/sorties discrètes, analogiques, interfaces CAN, …).

  - Les modules d'alimentation. Ils fournissent l'énergie aux autres agents du réseau à partir de l'alimentation train BT. Ceux sont des agents communicants au même titre que les MIO et s'insèrent donc dans l'anneau de communication. Les modules d'alimentation peuvent être vus comme des MIO particuliers, non sécuritaires.

- Le système SATURN est destiné à s'interfacer avec un système utilisateur de ses services appelé client ou réseau client. Les concentrateurs assurent l'interface avec le client.
- Le système SATURN supporte sur le même anneau de communication des agents sécuritaires (SIL2 ou SIL4) et non sécuritaires (SIL0).

2.2 IDENTIFICATION DES AGENTS

Afin d'être compatible des exigences de sécurité tout en limitant la bande passante nécessaire aux communications sur l'anneau, les agents utilisent 4 identifiants de communication différents :

- L'identifiant MAC est un identifiant unique codé sur 64 bits et protégé par un CRC 8 bits. Il est attaché à un connecteur de train et l'identifie de façon unique. L'identifiant MAC est donc représentatif de la position d'un agent dans le train et non de l'agent lui-même. Seuls les agents sécuritaires utilisent l'identifiant MAC.

- L'identifiant sécuritaire (SID) est un identifiant unique sur 24 bits, attribué à chaque agent sécuritaire par le concentrateur actif à chaque démarrage du système. L'attribution se fait en fonction de l'identifiant MAC, à partir d'une trame de communication spécifique. L'association entre un identifiant MAC et un identifiant sécuritaire fait partie des IDS du concentrateur, définis à l'installation du système. Cet identifiant sécuritaire est utilisé pour identifier l'agent source et l'agent destination lors de communications sécuritaires. Seuls les agents sécuritaires utilisent un identifiant sécuritaire.

- L'identifiant de transport (TID) est un identifiant unique sur 8 bits et attribué à chaque agent par le concentrateur actif à chaque démarrage du système. L'identifiant de transport est utilisé par la couche transport du protocole pour router les trames de communication vers son destinataire. Tous les agents, sécuritaires ou non, utilisent un identifiant de transport.

- L'identifiant interne (IID) est un numéro unique codé sur 64 bits qui identifie un agent particulier (ce numéro peut être vu comme le numéro de série d'un agent). L'identifiant IID est donc représentatif d'un agent particulier et non de sa position dans le train. Cet identifiant est utilisé par le concentrateur pour détecter le remplacement d'un agent (action de maintenance ou de malveillance), et pour attribuer à chaque agent son identifiant de transport.

L'identifiant de transport (TID) peut prendre les valeurs suivantes :
- Entre **01h et 8Eh** pour identifier un MIO, (les valeurs **7Dh** et **7Eh** sont interdites),
- **F0h** pour identifier le concentrateur actif,

A la mise sous tension, un MIO prend par défaut le TID provisoire **8Fh**, un concentrateur passif prend le TID provisoire **8Fh**. Le TID **FFh** est utilisé pour l'envoi d'un message en mode broadcast. Lors du démarrage du système, le concentrateur actif fourni un TID à chaque agent du réseau excepté aux autres concentrateurs présents sur le réseau qui prendront le TID 0xF0 au démarrage du LANSCAN.

De même, à la mise sous tension, les MIO et les concentrateurs sécuritaires passifs prennent par défaut le SID provisoire **FFFFFFh.** Lors du démarrage du système, le concentrateur actif fourni un SID à chaque agent sécuritaire du réseau.

Note: Les TID et SID pourraient être des IDS de chaque agent, mais afin de ne pas avoir à différencier les agents en production et faciliter la maintenance à chaud du système, il est décidé de les attribuer à chaque agent au démarrage du système.

2.3 PRINCIPE DES ECHANGES

Le protocole de communication SATURN s'appuie sur un échange de trames de communication entre les différents agents connectés sur le bus.
Le protocole supporte 6 formats de trame :
- La trame de synchronisation,
- Les trames de communication,
- La trame d'attribution de TID,
- La trame d'attribution de SID,
- La trame d'acquittement d'attribution de SID.
- La trame de vérification des invariants
- La trame de reprogrammation d'un agent sur le réseau

Un concentrateur peut être en mode actif, passif ou passant. En mode actif, un concentrateur peut émettre des trames de requête, de synchronisation et d'attribution des SID et TID. En mode passif, un concentrateur espionne toute l'activité du réseau sans intervenir. Le mode passant correspond à un mode dégradé où le concentrateur n'est plus pleinement opérationnel mais ferme tout de même l'anneau de communication. A un instant donné, il ne peut y'avoir qu'un seul concentrateur en mode actif sur le réseau.

De même un MIO peut être en mode passif en fonctionnement nominal ou en mode passant en cas de panne ou défaut.

2.3.1 Les trames de communication

Les trames de communication peuvent être de 2 sortes :

- Les trames de requêtes,
- Les trames de réponse,

Les trames de requête sont toujours à l'initiative du concentrateur actif et sont utilisées pour réaliser 2 types d'actions :

- Une requête d'écriture permet à un concentrateur d'écrire une ou plusieurs valeurs à partir d'une adresse donnée, dans la mémoire du destinataire de la trame,
- Une requête de lecture permet à un concentrateur de demander au destinataire de la trame de renvoyer une ou plusieurs valeurs stockées dans sa mémoire à partir d'une adresse donnée.

Les trames de réponse sont utilisées par l'agent destinataire d'une requête pour répondre à une requête de lecture ou à une trame de synchronisation.

Les trames de communication peuvent être au format sécuritaire ou non, selon si elles sont émises ou à destination d'un agent SIL0 ou SIL2 / SIL4.

2.3.2 La trame de synchronisation

La trame de synchronisation est utilisée pour envoyer un signal de synchronisation à tous les agents du bus. Elle est émise périodiquement en mode broadcast par le concentrateur actif. Elle est utilisée par tous les agents du réseau (MIO, module d'alimentation et concentrateurs passifs) pour synchroniser leurs horloges et compteurs de séquence internes. La trame de synchronisation est également un indicateur périodique de présence d'un concentrateur actif sur le réseau. En cas d'absence de trame de synchronisation, les MIO doivent se mettre en mode de repli.
Sur réception d'une trame de synchronisation, chaque agent du réseau doit émettre une trame de réponse qui contient les informations sur l'état de ses entrées et sorties. La trame de synchronisation peut donc être également vue comme une requête de lecture générale envoyée à tous les agents.
La trame de synchronisation a un format sécuritaire (i.e. elle possède les éléments nécessaires à l'authentification sécuritaire de la trame). Cependant, un agent non sécuritaire peut utiliser le contenu non sécuritaire de cette trame pour se synchroniser et émettre une trame de réponse.

2.3.3 La trame d'attribution du TID

La trame d'attribution du TID permet au concentrateur actif d'attribuer un TID aux différents agents du bus (Module d'alimentation, MIO et concentrateurs passifs). La trame d'attribution du TID utilise l'identifiant interne IID pour attribuer le bon TID au bon module.
Cette trame a un format non sécuritaire.

2.3.4 La trame d'attribution du SID

La trame d'attribution du SID permet au concentrateur actif d'attribuer un SID aux différents agents sécuritaires du bus (MIO et concentrateurs passifs). La trame d'attribution du SID utilise l'identifiant MAC pour attribuer le bon SID au bon module.

Cette trame a un format sécuritaire.

2.3.5 La trame d'acquittement d'attribution du SID

La trame d'acquittement d'attribution du SID permet à un agent de confirmer la bonne prise en compte du SID qui lui a été attribué. Lorsque le concentrateur actif émet une trame d'attribution du SID, il attend en retour une trame d'acquittement d'attribution de SID. Si la trame de retour n'est pas reçue dans le délai imparti, ou bien si ses données ne sont pas conformes, le concentrateur actif doit déclarer une erreur et placer le réseau dans un mode restrictif.
Cette trame a un format sécuritaire.

2.3.6 La trame de reprogrammation

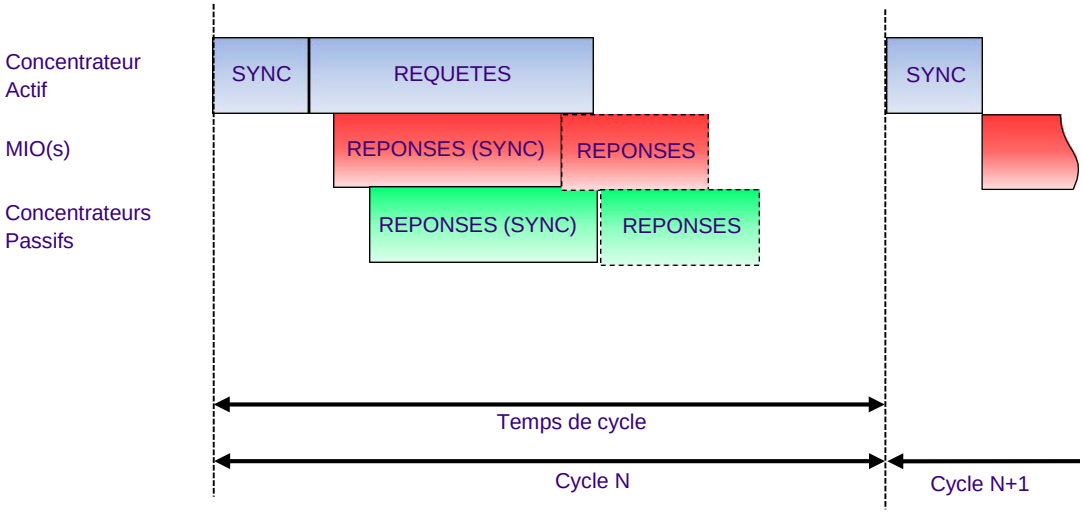
La trame de reprogrammation permet à l'utilisateur de mettre à jour le logiciel et/ou les IDS d'un agent sur les réseaux. Cette trame est issue du concentrateur actif et peut être à destination d'équipement sécuritaire, c'est pourquoi elles peuvent être au format sécuritaire ou non, selon si elles sont émises ou à destination d'un agent SIL0 ou SIL2 / SIL4. A ce stade les trames de reprogrammation SIL4 ne sont pas implémentées.
Cette fonctionnalité n'est pas implémentée dans la version actuelle de SATURN SIL4.

2.3.7 La trame de vérification des invariants

Cette trame permet à un concentrateur actif de vérifier les invariants des autres concentrateurs présents sur le réseau individuellement. Cette trame est envoyée lors du LANSCAN ou d'une récupération à chaud d'un concentrateur. Puisque tous les concentrateurs possèdent la même configuration (correspondant à l'image du réseau), le concentrateur actif envoie cette trame avec le CRC de ses invariants de configuration et le CRC de sa logique booléenne. Lorsqu'un agent passant reçoit cette trame il vérifie les 2 CRC avec ses CRC à lui et reste en mode « passant » si ces derniers sont différents.

2.3.8 Le cycle de communication

Le cycle de communication SATURN respecte 2 phases distinctes. La durée d'un cycle (ou temps de cycle) est constante, mais la durée des 2 phases peut être variable d'un cycle à l'autre.
Le cycle de communication se représente ainsi :



Le cycle est initié par le concentrateur actif qui émet une trame de synchronisation (SYNC). Les MIO et les concentrateurs passifs émettent alors leur trame de réponse à la trame de synchronisation. Dans le même temps, et à la suite de la trame de synchronisation, le concentrateur actif émet vers les MIO et les concentrateurs passifs des trames de requête (typiquement, des trames d'écritures pour mettre à jour les sorties des MIO et des trames de lecture pour remonter des statuts particuliers). Les MIO et les concentrateurs passifs émettent leurs trames de réponse selon la nature des requêtes. Le bus est alors inutilisé jusqu'au début du cycle suivant.
La topologie en anneau daisy chain implique que chaque agent doit recopier toute trame incidente sur un port de communication, sur l'autre port. Afin d'éviter la propagation infinie d'une trame, l'anneau doit être ouvert en un point, c'est-à-dire qu'un des agents ne doit pas recopier les trames incidentes. L'anneau est toujours ouvert au niveau du concentrateur en mode actif.
Le réseau SATURN utilise 2 paramètres temporels fixés par l'installateur du système en fonction du nombre d'agents du réseau, du volume des données à échanger à chaque cycle, du débit brut de communication limité par la distance maximale entre 2 agents, et des performances attendues :

- Le temps de cycle TCYC est utilisé par les concentrateurs pour administrer le réseau, et de façon générale par tous les agents pour diagnostiquer d'éventuels problèmes de communication.
- Le temps de propagation TPROP caractérise le temps nécessaire à une trame pour faire tout le tour de l'anneau, lorsqu'il n'y a pas de contention (i.e. lorsque la trame circule seule sur l'anneau). Ce paramètre est utilisé par les concentrateurs pour déterminer si un agent répond à une requête dans le temps imparti.

2.3.9 Gestion des concentrateurs

A tout instant, il ne peut y avoir sur le réseau privé qu'un seul concentrateur actif. Afin de faire cohabiter plusieurs concentrateurs sur le même réseau, chaque concentrateur doit se voir attribuer à l'installation du système un numéro de priorité qui définit l'ordre de prise en main du réseau. Le concentrateur configuré avec le niveau de priorité le plus élevé est le concentrateur actif au démarrage du système. Les autres concentrateurs doivent être passifs. Tous les concentrateurs doivent partager la même configuration du système (topologie du réseau, temps de cycle, SID, …).
Le numéro d'ordre ou priorité d'un concentrateur est donné par son SID. Le SID 11EE01 correspond au numéro d'ordre 1 et est le plus prioritaire. A contrario, le SID 887708 correspond au numéro d'ordre 8 et est le moins prioritaire. Le tableau suivant donne le rapport priorité / SID :

SID	PRIORITE
11EE11	1
22DD22	2
33CC33	3
44BB44	4
55AA55	5
669966	6
778877	7
887788	8

A la mise sous tension, chaque concentrateur doit espionner l'état du réseau durant l'équivalent de 5 temps de cycle pour détecter une éventuelle activité, signe qu'un autre concentrateur est actif sur le réseau. Si aucune trame n'est détectée, chaque concentrateur continue d'espionner le réseau

durant un laps de temps proportionnel à son ordre de priorité. Si aucune activité n'est détectée durant ce laps de temps, le concentrateur devient concentrateur actif.
En fonctionnement normal, chaque concentrateur passif espionne les trames de synchronisation émises par le concentrateur actif. En cas d'absence de trame de synchronisation durant un nombre de cycle proportionnel à l'ordre de priorité du concentrateur, le concentrateur passe d'actif à passif.
Lorsqu'un concentrateur passe actif, que ce soit à la mise sous tension, ou bien sur détection d'une absence de trame de synchronisation, il doit reconfigurer les autres agents du réseau, notamment avec l'attribution des TID et SID.

Lorsqu'un concentrateur actif détecte une trame de synchronisation dont il n'est pas l'émetteur, il doit passer immédiatement en mode passif.

Le nombre de temps de cycle que doit attendre un concentrateur avant de passer actif doit pouvoir être paramétrable (dans IDS) afin de pouvoir gérer la priorité des concentrateurs (pour le cas où il y aurait concentrateur passif sur le réseau).

3 SPECIFICATION DE TAILLEE DU PROTOCOLE

3.1 MAPPING MEMOIRE

CON-PRO-3000

Toutes les données d'un agent accessible sur le bus (MIO, module d'alimentation ou concentrateur passif) doivent être vues comme une mémoire organisée en 256 mots de 8 bits.
Le mapping mémoire implémenté par les agents doit respecter l'organisation suivante

Couverture :

ADRESSE	NOM DE LA ZONE	TAILLE EN OCTETS	ACCES (R/W)	VALEUR A LA MISE SOUS TENSION	COMMENTAIRE
FFh 80h	Zone métier à disposition de l'application de l'agent. Le mapping de cette zone est figé pour une valeur du champ TYP C'est-à-dire que cette zone mémoire est organisée différemment en fonction du type de module.				
7Fh 26h	Zone réservée	92	R/W	FFh	Zone réservée pour des extensions futures
25h	CONF	1	R/W	00h	Configuration du fonctionnement de l'agent (Cf. Ci-dessous)
24h	CPT_FOR	1	R/W	00h	Compteur de trames non supportées par l'agent
23h	CPT_SYNC	1	R/W	00h	Compteur d'absence de trame de synchronisation.
22h	CPT_TOAC2	1	R/W	00h	Compteur d'absence d'activité sur le port 2
21h	CPT_TOAC1	1	R/W	00h	Compteur d'absence d'activité sur le port 1
20h	CPT_SEQ	1	R/W	00h	Compteur d'erreur de séquence sur le champ SEQ ou CYC d'une trame sécuritaire
1Fh	CPT_TOCO2	1	R/W	00h	Compteur d'absence de commande sur le port 2
1Eh	CPT_TOCO1	1	R/W	00h	Compteur d'absence de commande sur le port 1

ADRESSE	NOM DE LA ZONE	TAILLE EN OCTETS	ACCES (R/W)	VALEUR A LA MISE SOUS TENSION	COMMENTAIRE
1Dh	SZ_REF	1	R/W	XX11	Taille en octets de la zone mémoire à transmettre dans une réponse à une trame de synchronisation
1Ch	AD_REF	1	R/W	XX11	Adresse de la zone mémoire à transmettre dans une trame de réponse à une trame de synchronisation
1Bh	CNF_CYC2	1	R/W	02h	Nombre de cycles de communication sans trame de synchronisation avant de passer en mode repli. 00 : Réservé
1Ah	CNF_REP2	1	R/W	05h	Nombre de cycles de communication sans commande sécuritaire avant de passer en mode repli. 00 : Réservé
19h	STATUT	1	R	00h	Statut de l'agent (cf. Ci-dessous)
18h	TCYC	1	R/W	FFh	Temps de cycle en ms. Ne doit pas être égale à 0 (contrainte concentrateur)
17h	OUT_REP	1	R/W	AAh	Commande de sortie de repli de l'agent
16h 14h	MSB SID LSB	3	R	FFFFFFh	SID de l'agent. Ne peut être modifié que par une commande de type attribution de SID
13h	TID	1	R	8Fh	TID de l'agent. Ne peut être modifié que par une commande de type attribution de TID. La valeur au reset dépend du type d'agent (concentrateur ou module).
12h 11h	VER	2	R	VER	VER[0] : Version du firmware PIC32 de l'agent découpée en 2 zones de 4 bits : [b7 b6 b5 b4].[b3 b2 b1 b0] VER[1] : Version du firmware FPGA de l'agent découpée en 2 zones de 4 bits : [b7 b6 b5 b4].[b3 b2 b1 b0]

ADRESSE	NOM DE LA ZONE	TAILLE EN OCTETS	ACCES (R/W)	VALEUR A LA MISE SOUS TENSION	COMMENTAIRE
10h	TYP	1	R	TYP	Type de l'agent. Ce code indique la nature et la fonction réalisée par l'agent. 00h : Concentrateur non sécuritaire 80h : Concentrateur sécuritaire SIL2 01h : Module d'alimentation 02h : MIO SI0 03h : MIO SO0 04h : MIO SIO0 05h à 7Fh : MIO non sécuritaire 81h : MIO SI2 82h : MIO SO2 83h : MIO SI4 84h : MIO SO4 85h : Concentrateur sécuritaire SIL4 86h à FFh : MIO sécuritaire
0Fh 08h	MSB IID LSB	8	R	IID	Identifiant IID de l'agent
07h 00h	MSB MAC LSB	8	R	MAC	Identifiant MAC de l'agent. Pour un agent non sécuritaire, ce champ vaut toujours : FFFFFFFFh

Tableau 1 – Structure du mapping mémoire d'un agent

[1] La valeur d'initialisation de ces champs à la mise sous tension est laissée libre au concepteur du module

[2] Ce registre n'est inutilisé que pour les MIO et module d'alimentation. Pour les concentrateurs, ce registre vaut toujours FFh.

REGISTRE CONF (ADRESSE 25H)							
-	-	-	-	R/W-0	R/W-0	R/W-0	R/W-0
Réservé	Réservé	Réservé	Réservé	ENR	ENTX	CPY2	CPY1
bit 7							bit 0

bit 7-4 Réservé

bit 3 **ENR :** Autorise l'émission de la trame de réponse automatique (implémenté uniquement pour les MIO non sécuritaires et les modules d'alimentation. Sans effet pour les concentrateurs)

0 = Emission de la trame automatique sur réception d'une synchro non autorisée

1 = Emission de la trame automatique autorisée

bit 2 **ENTX :** Autorise l'émission de trames sur le réseau

0 = Emission de trames autorisée

1 = Emission de trames autorisée non autorisée

bit 1 **CPY2 :** Autorisation de recopie du port RX2 sur TX1

0 = La recopie est interdite

1 = La recopie est autorisée

bit 0 **CPY1 :** Autorisation de recopie du port RX1 sur TX2

0 = La recopie est interdite

1 = La recopie est autorisée

REGISTRE STATUT (ADRESSE 19H) BITS ACTIFS A 1							
R-1	R-0	R-0	R-0	R-0	R-0	R-0	R-0
REP	PTS	BFO	NTS	NA2	NA1	ESE	CNR

bit 7 bit 0

Les bits du registre de statut sont actifs à '1' et sont automatiquement mis à 0 sur une lecture.

bit 7 **REP :** Pour un MIO sécuritaire, indique que le module est en repli.
Pour un concentrateur, indique que le module est passant.

bit 6 **PTS :** Indique sur quel port a été reçu la requête qui a engendré la réponse qui contient l'octet STATUT (0 -> port 1, 1 -> port 2)

bit 5 **BFO :** Format de trame non supporté ou bien débordement du buffer de réception sur un des 2 ports.

bit 4 **NTS :** Pas de trame de synchronisation détectée depuis TCYC

bit 3 **NA2 :** Pas d'activité détectée sur le port 2 depuis au moins TCYC

bit 2 **NA1 :** Pas d'activité détectée sur le port 1 depuis au moins TCYC

bit 1 **ESE :** Au moins un numéro de séquence (SEQ ou CYC) était erroné (non implémenté pour les modules non sécuritaires)

bit 0 **CNR :** Une trame n'a pas été reçue sur les 2 ports

[Sécurité]

3.2 FORMAT DES TRAMES

Les trames échangées par le protocole SATURN implémentent 3 couches du modèles OSI :

- Couche 1 : PHY
- Couche 2 : Transport,
- Couche 7 : Application.

Les trames peuvent être de 11 formats :

- Trame de synchronisation (sécuritaire),
- Trame de requête sécuritaire,
- Trame de requête non sécuritaire,
- Trame de réponse sécuritaire,
- Trame de réponse non sécuritaire,
- Trame d'attribution de TID (non sécuritaire),
- Trame d'attribution de SID (sécuritaire),
- Trame d'acquittement d'attribution de SID (sécuritaire),
- Trame de vérification des invariants (sécuritaire),
- Trame de reprogrammation (non sécuritaire),
- Trame de reprogrammation (sécuritaire).

Les couches 1 et 2 sont identiques pour les 8 types de trames. La différence se fait au niveau du format de la couche applicative (couche 7). Ainsi, seule la couche applicative implémente des mécanismes qui participent aux fonctions de sécurité.

3.2.1 Couches PHY et Transport

Le protocole de communication SATURN s'implémente sur un support physique de type RS485.
La couche Physique des trames SATURN doit être conforme au standard EIA-485 (i.e. RS485) et doit supporter un débit brut de 12Mbits/s en Full-Duplex.
Les trames SATURN doivent être émises octet par octet. Un octet doit être transmis avec 1 bit de START, 1 bit de STOP, sans PARITE, le LSB (bit de poids faible) en premier.
Les octets d'une même trame doivent être émis consécutivement. Le délai inter-octet ne doit jamais excéder la durée de 1 bit.
Justification : L'objectif est d'optimiser l'utilisation du bus et de faciliter la détection de l'espace inter-trame.

CON-PRO-2030

Les champs d'octets qui constituent les trames SATURN doivent prendre les valeurs suivantes.

Couverture :

<table>
<tr><th>NOM DU CHAMP</th><th>LONGUEUR EN OCTET(S)</th><th>SIGNIFICATION</th></tr>
<tr><td>Fanion de Début</td><td>1</td><td>Ce champ vaut toujours 7Eh</td></tr>
<tr><td>Adresse</td><td>1</td><td>Ce champ identifie le TID du ou des destinataires du message :
<table>
<tr><th>VALEUR</th><th>SIGNIFICATION</th></tr>
<tr><td>De 01h à 8Fh</td><td>TID d'un MIO en particulier (7Dh et 7Eh réservées)</td></tr>
<tr><td>8Fh</td><td>Tout MOI dont le TID n'a pas encore été configuré par le concentrateur actif ou tout concentrateur passif avant le début du LANSCAN.</td></tr>
<tr><td>90h</td><td>Tous les MOI connectés sur le bus (Broadcast MIO)</td></tr>
<tr><td>F0h</td><td>Tous les concentrateurs sur le réseau (Broadcast concentrateur)</td></tr>
<tr><td>De F1h à F8h</td><td>TID d'un concentrateur en particulier</td></tr>
<tr><td>FFh</td><td>Tous les agents connectés sur le bus (MIO et concentrateur)</td></tr>
<tr><td>Autres valeurs</td><td>Réservées</td></tr>
</table></td></tr>
<tr><td>Données Applicatives</td><td>4 à 269</td><td>Ce champ respecte le format défini au §Erreur ! Source du renvoi introuvable.</td></tr>
<tr><td>FCS</td><td>2</td><td>Le champ Frame Check Sequence est un CRC calculé sur la base de tous les champs de la trame compris entre les 2 Fanions hormis le stuffing, à partir du polynôme : x16+x12+x5+1</td></tr>
</table>

Fanion de Fin	1	Ce champ vaut toujours 7Eh

Tableau 2 – Définition des champs d'une trame RS485

CON-PRO-2040

En émission, tout octet des champs Données Applicatives et FCS ayant pour valeur :
- 7Eh doit être remplacé par les 2 octets 7Dh 5Eh,
- 7Dh doit être remplacé par les 2 octets 7Dh 5Dh.

Couverture :

Justification : Ce mécanisme de stuffing permet d'utiliser le fanion 7Eh comme délimiteur de début et de fin de trame.

CON-PRO-2050

En réception, toute séquence de 2 octets ayant pour valeur :
- 7Dh 5Eh doit être interprétée comme l'octet 7Eh,
- 7Dh 5Dh doit être interprétée comme l'octet 7Dh.

Couverture :

Justification : Ce mécanisme de stuffing permet d'utiliser le fanion 7Eh comme délimiteur de début et de fin de trame.

3.2.2 Couche Applicative

La couche applicative permet de véhiculer 9 formats de trames. La différence de format se fait au niveau du champ TYP, selon le tableau suivant.

VALEUR DU CHAMP TYP	SIGNIFICATION
00h	Trame de synchronisation
07h	Trame de requête sécuritaire
08h	Trame de requête non sécuritaire
70h	Trame de réponse sécuritaire
80h	Trame de réponse non sécuritaire
3Ch	Trame d'attribution du TID
C3h	Trame d'attribution du SID
33h	Trame d'acquittement d'attribution de SID
B4h	Trame de vérification des invariants
A6	Trame de reprogrammation sécuritaire
6A	Trame de reprogrammation non sécuritaire

Tableau 3 – Définition du champ de différenciation des formats de trame

3.2.2.1 Trame de synchronisation

La trame de synchronisation est destinée à tous les agents du réseau et doit donc être émise en mode broadcast (champ adresse de la couche transport fixé à **FFh**).

CON-PRO-2200

Les champs d'octets qui constituent les Données Applicatives d'une trame de synchronisation doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de synchronisation. Il vaut toujours : **00h**
SRC	1	3	Ce champ donne le SID de l'émetteur du message. Il doit être différent de 0xFFFFFF pour que la trame soit acceptée et doit correspondre à un des huit possibles SID récupéré lors de la trame d'attribution des SID.
CYC	4	1	Ce champ est un compteur qui identifie le numéro de cycle de communication du concentrateur actif. (Pour information : En fonctionnement nominal ce champ est incrémenté de 1 par rapport à la trame de synchronisation du cycle précédent.)
CRC	5	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : x16+ x15+x12+ x7+x6+ x4+ x3+1

Tableau 4 – Définition des champs des données applicatives de la trame de synchronisation

[Sécurité]

3.2.2.2 Trame de requête sécuritaire

CON-PRO-2210

Les champs d'octets qui constituent les Données Applicatives d'une trame de requête sécuritaire doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête sécuritaire. Il vaut toujours : **07h**
DEST	1	3	Ce champ identifie le SID du destinataire du message
SRC	4	3	Ce champ identifie le SID de l'émetteur du message. Il doit être différent de 0xFFFFFF pour que la trame soit acceptée et doit correspondre à un des huit possibles SID récupéré lors de la trame d'attribution des SID.
CYC	7	1	Ce champ identifie le compteur de cycle de communication interne de l'agent émetteur. En fonctionnement normal, il reprend le champ CYC de la trame de synchronisation précédente.
SEQ	8	1	Ce champ identifie le numéro de séquence du message pour le couple émetteur/destinataire concerné. Il est égal au complément à 1 du champ CYC incrémenté de 1 pour la première requête du cycle puis incrémenté à chaque nouvelle requête du cycle.
COM	9	1	Type de requête : 77h : Ecriture de DATL octets à partir de l'adresse ADD 88h : Lecture de DATL octets à partir de l'adresse ADD Autres valeurs réservées.
DATL	10	1	Longueur en octets des données à écrire ou lire.
ADD	11	1	Indique la première adresse dans la base de registre de l'agent destinataire concerné par l'action de lecture/écriture.
DATA	12	DATL	Présent si COM vaut **77h** (écriture). Données à écrire à partir de l'adresse ADD de la base de registre de l'agent destinataire. Vide si COM vaut 88h (lecture)
CRC	12+DATL	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^{7}+x^{6}+ x^{4}+ x^{3}+1$

Tableau 5 - Définition des champs des données applicatives de la trame de requête sécuritaire

3.2.2.3 Trame de requête non sécuritaire

CON-PRO-2220

Les champs d'octets qui constituent les Données Applicatives d'une trame de requête non sécuritaire doivent prendre les valeurs suivantes :

Couverture :

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête non sécuritaire. Il vaut toujours : 08h
SRC	1	1	Ce champ identifie le TID de l'émetteur du message
COM	2	1	Type de requête : 01h : Ecriture de DATL octets à partir de l'adresse ADD 02h : Lecture de DATL octets à partir de l'adresse ADD Autres valeurs réservées.
DATL	3	1	Longueur en octets des données à écrire ou lire.
ADD	4	1	Indique la première adresse dans la base de registre de l'agent destinataire concernée par l'action de lecture/écriture.
DATA	5	DATL	Présent si COM vaut 01h (écriture). Données à écrire à partir de l'adresse ADD de la base de registre de l'agent destinataire. Vide si COM vaut 02h (lecture)

Tableau 6 - Définition des champs des données applicatives de la trame de requête non sécuritaire

3.2.2.4 Trame de réponse sécuritaire

CON-PRO-2230

Les champs d'octets qui constituent les Données Applicatives d'une trame de réponse sécuritaire doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de réponse sécuritaire. Il vaut toujours : **70h**
DEST	1	3	Ce champ identifie le SID du destinataire du message (i.e SID concentrateur actif).
SRC	4	3	Ce champ identifie le SID de l'émetteur du message.
CYC	7	1	Ce champ identifie le compteur de cycle de communication interne de l'agent émetteur. En fonctionnement normal, il reprend le champ CYC de la trame de synchronisation précédente.
SEQ	8	1	Ce champ identifie le numéro de séquence du message pour le couple émetteur/destinataire concerné. Pour une réponse à une requête, il doit prendre la valeur du champ SEQ de la trame de requête à laquelle il répond augmenté de 1. Pour une réponse à une trame de synchronisation, il doit prendre le complément à 1 du champ CYC.
COM	9	1	Type de réponse : - 07h : Réponse à une trame de synchronisation - 70h : Réponse à une requête de lecture - AAh : Erreur lors de la réponse à une trame de synchronisation (mauvais champs SZ_REF et AD_REF) - 55h : Erreur lors de la réponse à une requête de lecture (mauvais champs DATL et ADD) Autres valeurs réservées.
DATL	10	1	Longueur en octets du champ DATA. - Reprend le champ DATL de la requête de lecture s'il s'agit d'une réponse à une requête de lecture (COM = 70h). - Reprend le registre SZ_REF de l'agent (cf. §**Erreur ! Source du renvoi introuvable.**) dans le cas d'une réponse à une trame de synchronisation (COM = 07h)

ADD	11	1	Adresse dans la base de registre où ont été lue les DATL données. Reprend le champ ADD de la requête de lecture s'il s'agit d'une réponse à une requête de lecture (COM = 70h). Reprend le registre AD_REF de l'agent (cf. §Erreur ! Source du renvoi introuvable.) dans le cas d'une réponse à une trame de synchronisation (COM = 07h)
DATA	12	DATL	DATL données lues dans la base de registre de l'agent à partir de l'adresse ADD. Vide si COM = AAh ou 55h
STAT	12+DATL	1	Ce champ reprend l'octet de statut du module émetteur de la réponse (cf. §Erreur ! Source du renvoi introuvable.)
CRC	13+DATL	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : x16+ x15+x12+ x7+x6+ x4+ x3+1

Tableau 7 - Définition des champs des données applicatives de la trame de réponse sécuritaire

[Sécurité]

3.2.2.5 Trame de réponse non sécuritaire

CON-PRO-2240

Les champs d'octets qui constituent les Données Applicatives d'une trame de réponse non sécuritaire doivent prendre les valeurs suivantes :

Couverture :

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de réponse non sécuritaire. Il vaut toujours : 80h
SRC	1	1	Ce champ identifie le TID de l'émetteur du message
COM	2	1	Type de réponse : 01h : Réponse à une trame de synchronisation 02h : Réponse à une requête de lecture AAh : Erreur lors de la réponse à une trame de synchronisation (mauvais champs SZ_REF et AD_REF) 55h : Erreur lors de la réponse à une requête de lecture (mauvais champs DATL et ADD) Autres valeurs réservées.
DATL	3	1	Longueur en octets du champ DATA. Reprend le champ DATL de la requête de lecture s'il s'agit d'une réponse à une requête de lecture (COM = 02h). Reprend le registre SZ_REF de l'agent (cf. §Erreur ! Source du renvoi introuvable.) dans le cas d'une réponse à une trame de synchronisation (COM = 01h)
ADD	4	1	Adresse dans la base de registre où ont été lue les DATL données. Reprend le champ ADD de la requête de lecture s'il s'agit d'une réponse à une requête de lecture (COM = 02h). Reprend le registre AD_REF de l'agent (cf. §Erreur ! Source du renvoi introuvable.) dans le cas d'une réponse à une trame de synchronisation (COM = 01h)
DATA	5	DATL (+1 si COM = 01h)	DATL données lues dans la base de registre de l'agent à partir de l'adresse ADD. Si COM = 01h : Octet de statut du module émetteur de la réponse est rajouté en position 6+DATL Vide si COM = AAh ou 55h

Tableau 8 - Définition des champs des données applicatives de la trame de réponse non sécuritaire

3.2.2.6 Trame d'attribution de TID

La trame d'attribution de TID doit être routée vers tous les agents et doit donc être émise en mode broadcast.

CON-PRO-2250

Les champs d'octets qui constituent les Données Applicatives d'une trame d'attribution de TID doivent prendre les valeurs suivantes :

Couverture :

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame d'attribution de TID. Il vaut toujours : **3Ch**
SRC	1	1	Ce champ identifie le TID de l'émetteur du message
IID	2	8	Identifiant IID de l'agent destinataire de la trame.
TID	10	1	TID que doit prendre le destinataire du message.

Tableau 9 - Définition des champs des données applicatives de la trame d'attribution de TID

3.2.2.7 Trame d'attribution de SID d'un module SIL2

CON-PRO-2260

Les champs d'octets qui constituent les Données Applicatives d'une trame d'attribution de SID doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête sécuritaire. Il vaut toujours : **C3h**
SRC	1	3	Ce champ identifie le SID de l'émetteur du message. Il doit être différent de 0xFFFFFF pour que la trame soit acceptée
SEC	4	4	Ce champ identifie de façon unique la trame d'attribution de SID.
MAC	8	8	Ce champ identifie le MAC de l'agent destinataire du message.
SID	16	3	Ce champ donne le SID que l'agent destinataire de la trame doit utiliser. Il doit être différent de 0xFFFFFF pour que la trame puisse être acceptée
CRC	19	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^{7}+x^{6}+ x^{4}+ x^{3}+1$

Tableau 10 - Définition des champs des données applicatives de la trame d'attribution du SID

[Sécurité]

3.2.2.8 Trame d'attribution de SID d'un module SIL4

Il faut avoir les moyens de garantir qu'un module SIL4 ne puisse recevoir de SID que d'un CO4 (et pas d'un CO2).
Pour cela on définit un format de trame supplémentaire qui sera inconnu des modules SIL2 :

CON-PRO-2261

Couverture : EXI.C_D401_58

Les champs d'octets qui constituent les Données Applicatives d'une trame d'attribution de SID doivent prendre les valeurs suivantes :

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame d'affectation de SID SIL4. Il vaut toujours : **BCh**
SRC1	1	3	Ce champ identifie le SID de l'émetteur du message. Il doit être différent de 0xFFFFFF pour que la trame soit acceptée
SEC	4	4	Ce champ identifie de façon unique la trame d'attribution de SID.
MAC	8	8	Ce champ identifie le MAC de l'agent destinataire du message.
SIDµ1	16	3	Ce champ donne le SID que l'agent destinataire de la trame doit utiliser. Il doit être différent de 0xFFFFFF pour que la trame puisse être acceptée
SIDµ2	19	3	Ce champ donne le SID que l'agent destinataire de la trame doit utiliser. Il doit être différent de 0xFFFFFF pour que la trame puisse être acceptée
SRC2	22	3	Ce champ identifie le SID du second µC de l'émetteur du message (forcément un double cœur car SIL4). Il doit être différent de 0xFFFFFF pour que la trame soit acceptée
CRC	25	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^7+x^6+ x^4+ x^3+1$

Cette trame permet d'affecter les 2 SID de l'agent SIL4 (SIDµ1 & SIDµ2). De plus elle permet à l'agent destination de connaitre les 2 SID du concentrateur sources de ce message (SRC1 & SRC2).

3.2.2.9 Trame d'acquittement d'attribution de SID

CON-PRO-2270

Les champs d'octets qui constituent les Données Applicatives d'une trame d'acquittement d'attribution de SID doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête sécuritaire. Il vaut toujours : **33h**
SRC	1	3	Ce champ identifie le SID de l'émetteur du message.
DST	4	3	Ce champ identifie le SID du destinataire du message (i.e. SID du concentrateur actif qui a émis la trame d'attribution de SID à laquelle on répond). Il doit être différent de 0xFFFFFF pour que la trame soit acceptée et doit correspondre à un des huit possibles SID récupéré lors de la trame d'attribution des SID.
SEC	7	4	Ce champ reprend le champ SEC de la trame d'attribution de SID à laquelle cette trame répond.
MAC	11	8	Ce champ identifie le MAC de l'agent émetteur du message.
CRC	19	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^{7}+x^{6}+ x^{4}+ x^{3}+1$

Tableau 11 - Définition des champs des données applicatives de la trame d'acquittement d'attribution du SID

[Sécurité]

3.2.2.10 Trame de vérification des invariants

CON-PRO-3010

Les champs d'octets qui constituent les Données Applicatives d'une trame de vérification des invariants doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête sécuritaire. Il vaut toujours : **B4h**
DEST	1	3	Ce champ identifie le SID du destinataire du message
SRC	4	3	Ce champ identifie le SID de l'émetteur du message. Il doit être différent de 0xFFFFFF pour que la trame soit acceptée et doit correspondre à un des huit possibles SID récupéré lors de la trame d'attribution des SID.
CYC	7	1	Ce champ identifie le compteur de cycle de communication interne de l'agent émetteur. En fonctionnement normal, il reprend le champ CYC de la trame de synchronisation précédente.
SEQ	8	1	Ce champ identifie le numéro de séquence du message pour le couple émetteur/destinataire concerné. Il est égal au complément à 1 du champ CYC incrémenté de 1 pour la première requête du cycle puis incrémenté à chaque nouvelle requête du cycle.
DATA	9	4	Les 2 premiers octets représentent le CRC des invariants de configuration Les 2 derniers représentent le CRC de la fonction de logique booléenne
CRC	13	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^7+x^6+ x^4+ x^3+1$

Tableau 12 - Définition des champs des données applicatives de la trame de requête sécuritaire

[Sécurité]

Remarque : La fonction de vérification des invariants gère le champ SEQ de la même manière que les trames de requêtes sécuritaires.

3.2.2.11 Trame de reprogrammation sécuritaire

CON-PRO-2280

Les champs d'octets qui constituent les Données Applicatives d'une trame de reprogrammation doivent prendre les valeurs suivantes :

Couverture : EXI.C_D401_58

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête sécuritaire. Il vaut toujours : **A6h**
SRC	1	3	Ce champ identifie le TID de l'émetteur du message
DST	4	3	Ce champ identifie le SID du destinataire du message
SEC	7	4	Ce champ reprend le champ SEC de la trame d'attribution de SID à laquelle cette trame répond.
SEQ	11	1	Ce champ identifie le numéro de séquence du message pour le couple émetteur/destinataire concerné. Il est égal au complément à 1 du champ CYC pour la première requête du cycle puis incrémenté à chaque nouvelle requête du cycle.
DAT	12	N	Donnée de reprogrammation
DATL	12+N	1	Longueur en octets des données : Valeur de N
CRC	13+N	2	Le champ CRC 16 bits est calculé sur la base de tous les champs précédents à partir du polynôme : $x^{16}+ x^{15}+x^{12}+ x^7+x^6+ x^4+ x^3+1$

Tableau 13 - Définition des champs des données applicatives de la trame de reprogrammation sécuritaire

3.2.2.12 Trame de reprogrammation non sécuritaire

CON-PRO-2290

Les champs d'octets qui constituent lesDonnées Applicativesd'une trame de reprogrammation non sécuritaire doivent prendre les valeurs suivantes :

Couverture :

NOM DU CHAMP	POSITION	LONGUEUR (OCTET)	SIGNIFICATION
TYP	0	1	Ce champ identifie le type de trame de requête non sécuritaire. Il vaut toujours : **6Ah**
SRC	1	1	Ce champ identifie le TID de l'émetteur du message
DAT	12	N	Donnée de reprogrammation
DATL	12+N	1	Longueur en octets des données : Valeur de N

Tableau 14 - Définition des champs des données applicatives de la trame de reprogrammation non sécuritaire

3.3 COMPORTEMENT DES AGENTS

Cette section décrit les contraintes d'implémentation que doivent respecter les différents agents du bus (MIO, module d'alimentation ou Concentrateur passifs) pour garantir un bon fonctionnement du protocole.
Le terme 'Agent passif' désigne un agent autre que le concentrateur actif (i.e. un MIO, un module d'alimentation ou bien un concentrateur passif).

3.3.1 Fonctionnement général des agents

CON-PRO-0010

Sur réception d'une trame d'attribution de TID, un agent passif (hormis concentrateur) doit comparer le champ IID contenu dans la trame à son propre identifiant IID. En cas d'égalité, l'agent doit s'attribuer le TID passé en paramètre dans la trame.

Couverture :

[Sécurité]

CON-PRO-0020

Sur réception d'une trame d'attribution de SID, un agent passif sécuritaire (hormis concentrateur) doit comparer le champ MAC contenu dans la trame à son propre identifiant MAC. En cas d'égalité, l'agent doit s'attribuer le SID passé en paramètre dans la trame, doit mémoriser le SID du concentrateur actif, et doit émettre sa trame d'acquittement d'attribution de SID.

Couverture :

[Sécurité]

CON-PRO-0021

Un agent passif (hormis concentrateur) doit pouvoir mémoriser jusqu'à 8 SID de concentrateur. L'agent accepte un premier SID concentrateur contenu dans la trame d'attribution de SID si le SID qui lui est attribué est différent de 0xFFFFFF.
Un agent acceptera ensuite jusqu'à 8 SID concentrateur récupérés dans les trames d'attribution de SID si le SID qui lui est attribué est identique à son SID valide envoyé par le premier concentrateur.
Dans tous les cas une trame d'attribution de SID n'est acceptée que si le SID de l'émetteur (concentrateur) est aussi différent de 0xFFFFFF.

Couverture :

[Sécurité]

CON-PRO-0022

Un concentrateur doit pouvoir mémoriser jusqu'à 8 SID de concentrateur. Ces informations doivent être stockées dans ses invariants de configuration.

Couverture :

[Sécurité]

CON-PRO-0030

Sur réception d'une trame de synchronisation, un agent passif doit mettre à jour son compteur de cycle et si l'agent est autre qu'un concentrateur doit émettre une trame de réponse dont le contenu est paramétrable à partir de registres spécifiques.

Couverture :

[Sécurité]

CON-PRO-0040

Sur réception d'une requête de lecture, un agent passif doit émettre une et une seule trame de réponse (sur ses 2 ports de communication).

Couverture :

CON-PRO-0050

A réception d'une trame, un agent doit vérifier l'intégrité de la trame en recalculant le(s) champ(s) FCS de la couche transport. En cas d'erreur, la trame correspondante doit être ignorée et les statuts correspondants mis à jour.

Couverture :

Note : Cette action intervient au niveau de la couche transport du protocole et n'est donc pas sécuritaire. De plus, elle n'affecte pas la fonction de recopie d'une trame d'un port sur l'autre (une trame incidente est recopiée même si elle est erronée).

CON-PRO-0060

Si un agent reçoit plusieurs trames de synchronisation ou de requêtes sécuritaires valides identiques dans un même cycle, seule la première trame doit être prise en compte et les suivantes doivent être ignorées.

Couverture :

[Sécurité]

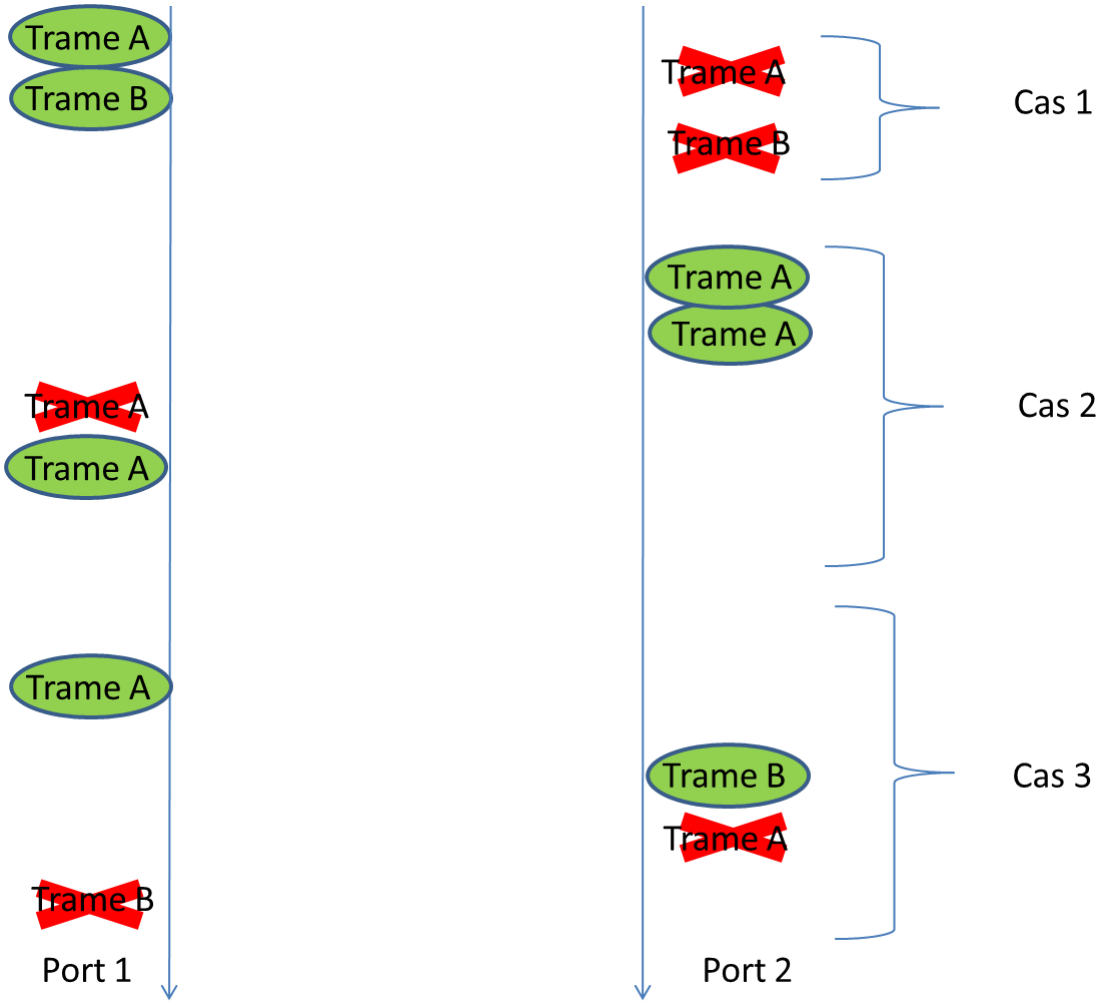
Note : Ce mécanisme n'est pas sécuritaire pour le CO car géré par le FPGA.

CON-PRO-0065

Si un agent reçoit la même trame valide sur ses 2 ports, seule la première trame doit être prise en compte et la suivante doit être ignorée. Attention, une même trame valide reçue sur le même port plusieurs fois doit être traitée à chaque fois.

Couverture :

Le logiciel doit donc respecter les 3 cas illustrés dans le schéma ci-dessous :



Note : Ce mécanisme n'est pas sécuritaire pour le CO car géré par le FPGA.

CON-PRO-0070

L'émission d'une trame ne doit pas corrompre les autres trames qui circulent déjà sur l'anneau (i.e. une trame ne doit pas être émise au milieu d'une autre, et doit respecter l'éventuel délai inter-trame).

Couverture :

Note : Ceci implique qu'un agent souhaitant émettre une trame alors qu'il est en train d'en recopier une autre doit attendre la fin de la trame incidente avant d'émettre à son tour.

CON-PRO-0080

Lorsqu'un agent émet une trame (conçue par lui-même), il doit l'émettre sur ses 2 ports de communication.

Couverture :

Note : L'émission sur les 2 ports n'est pas nécessairement simultanée puisqu'un port peut être occupé à recopier une trame incidente. Dans ce cas, l'émission se fera immédiatement si le port est libre, et retardée de la durée de la trame recopiée si le port est occupé.

CON-PRO-0090

La réception par un agent d'un format de trame qu'il ne supporte pas doit être prévue et ne pas remettre en cause le fonctionnement de cet agent. Il doit ignorer la trame.

Couverture :

[Sécurité]

CON-PRO-0100

Chaque agent passif doit recopier sur un port toute trame incidente sur l'autre port (si elle ne lui est pas destinée), sans contrôle d'intégrité. Cette recopie ne doit pas introduire un délai entre la trame incidente et la trame recopiée de plus de Tcop.

Couverture :

Note : Le temps Tcop est un paramètre intrinsèque de l'agent. Il doit être défini à la conception de l'agent et documenté pour pouvoir dimensionner les échanges sur le bus. Ce paramètre influe directement sur les performances du réseau. Il est recommandé qu'il n'excède pas quelques centaines de ns.

CON-PRO-0110

Le mécanisme de recopie d'un agent doit pouvoir être commandé par un bit spécifique du registre de configuration. Par défaut, le mécanisme de recopie est inhibé à la mise sous tension de l'agent.

Couverture :

Note : Ce mécanisme n'est pas sécuritaire.

Justification : Ce mécanisme a pour but de pouvoir isoler un agent qui saturerait le bus en inhibant le mécanisme de copie de ses voisins. L'inhibition au démarrage permet au concentrateur actif de faire une énumération des agents sur le bus et de déterminer leur position logique sur l'anneau en les activant un par un.

CON-PRO-0120

Lorsqu'un agent passif est en train d'émettre une trame, il doit stocker toute trame incidente sur un port pour pouvoir la recopier telle quelle sur l'autre port à l'issue de sa propre émission.

Couverture :

CON-PRO-0130

Un agent passif en mode RUN doit s'assurer de la validité des trames de synchronisation qu'il voit passer. Le délai entre 2 trames de synchronisation valides doit être compris entre (N+0.8)xTCYC et (N+1.2)xTCYC, N étant un entier quelconque. Une trame de synchronisation reçue en dehors de cette fenêtre doit être considérée non valide et doit être ignorée.

Couverture :

Justification : La périodicité d'émission des trames de synchronisation est de TCYC. Du fait des contentions sur le réseau, le délai de réception par un MIO entre 2 trames de synchronisation consécutives est de TCYC±20%. La fenêtre de réception entre 2 trames de synchronisation non nécessairement consécutives est donc de NxTCYC±20%xTCYC.

[Sécurité]

CON-PRO-0140

Un agent sécuritaire doit implémenter un compteur CYC 8 codé sur bits de cycle de communication interne. Ce compteur doit être positionné à la valeur contenu dans les trames de synchronisation reçue par l'agent lorsque ce dernier est en mode REPLI puis incrémenté à chaque cycle de communication lorsque l'agent n'est plus en repli. L'agent doit utiliser le paramètre TCYC pour identifier la fin d'un cycle de communication, et doit se recaler temporellement sur réception d'une trame de synchronisation valide. Au démarrage de la carte cette variable doit être égale à 0x00.

Couverture : Exi.C_D213.commFPGARep1 , Exi.C_D213.commFPGARep3 , Exi.C_D213.commFPGADelaisTransmission , Exi.C_D213.conceptionProtocole2 , Exi.C22_D560.SI4.1

Note : Ce compteur est utilisé pour dater les communications avec une précision de 1 cycle.

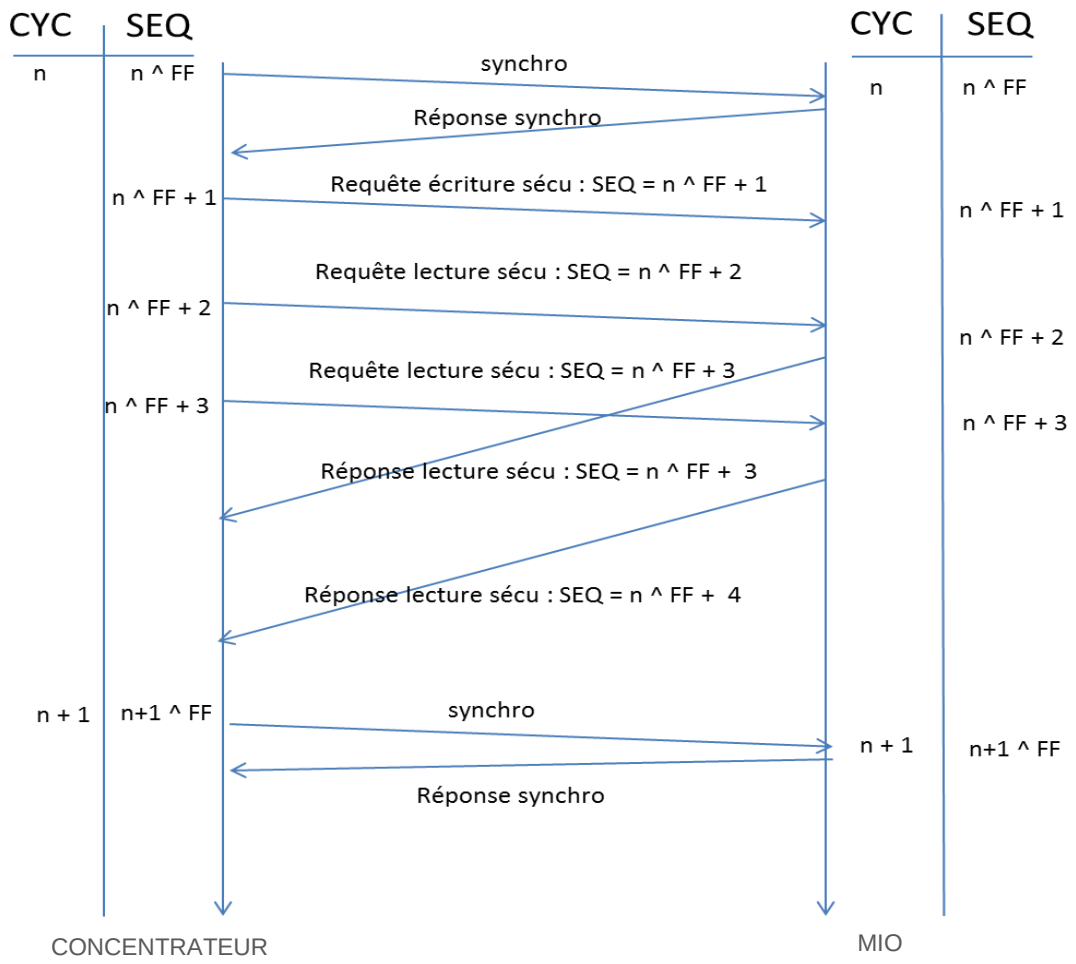
[Sécurité]

CON-PRO-0150

Un agent sécuritaire doit implémenter un compteur SEQ 8 bits de trame de communication pour chaque agent avec lequel il peut dialoguer. Ce compteur est initialisé avec le complément à 1 du numéro de cycle courant (CYC) à chaque réception d'une trame de synchronisation et au démarrage de la carte. L'agent doit ensuite vérifier que chaque requête sécuritaire valide le concernant possède son champ SEQ incrémenté de 1 et doit l'incrémenter de 1. Si la requête est une requête de lecture, la trame de réponse doit avoir son champ SEQ au compteur SEQ interne de l'agent incrémenté de 1.

Couverture : Exi.C_D213.commFPGARep1 , Exi.C_D213.commFPGARep3 , Exi.C_D213.commFPGADelaisTransmission , Exi.C_D213.conceptionProtocole2 , Exi.C22_D560.SI4.1

Le schéma ci-dessous illustre cette exigence :



Justification : Ce compteur est utilisé pour garantir le séquencement des requêtes/réponses sécuritaire à l'intérieur d'un cycle de communication.

[Sécurité]

CON-PRO-0160

Sur réception d'une trame de requête (hormis concentrateur) ou de réponse au format sécuritaire, un agent SIL2 ou SIL4 doit vérifier les champs suivants : SID de l'émetteur : il doit correspondre à un des 8 SID du concentrateur actif mémorisé lors de l'attribution du SID si l'agent est un MIO (les MIO n'envoyant pas de requête), sinon il doit correspondre au SID du MIO émetteur SID du destinataire : il doit correspondre à son propre SID celui-ci devant être différent de 0xFFFFFF, CYC : ce champ doit être égal au numéro de cycle en cours et confirmé par la trame de synchronisation reçue en début de cycle, (datation de donnée) SEQ : ce champ doit être égal au compteur SEQ interne de l'agent destinataire incrémenté de 1 pour une trame de requête reçue, et doit être égal au champ SEQ de la trame de requête qui a engendrée la trame de réponse incrémenté de 1 pour une trame de réponse

CRC : ce champ doit être égal au CRC recalculé par l'agent destinataire de la trame. En cas d'inégalité sur un de ces champs, la trame correspondante doit être ignorée par l'agent destinataire (i.e. il doit considérer que la trame n'a pas été reçue). Si l'inégalité porte sur un des champs CYC, SEQ ou CRC, l'évènement correspondant doit être enregistré (cf.§III.3.6).

Couverture : Exi.C_D213.commFPGARep1 , Exi.C_D213.commFPGARep3 , Exi.C_D213.commFPGAIntegrite1 , Exi.C_D213.commFPGADelaisTransmission , Exi.C_D213.conceptionProtocole2 , Exi.C22_D560.SI4.1 , Exi.C22_D560.SI4.2

[Sécurité]

CON-PRO-0161

Sur réception d'une trame sécuritaire un agent SIL2 ou SIL4 doit vérifier le champ suivant : CRC : ce champ doit être égal au CRC recalculé par l'agent destinataire de la trame. En cas d'inégalité, la trame correspondante doit être ignorée par l'agent destinataire (i.e. il doit considérer que la trame n'a pas été reçue et l'évènement doit être enregistré (cf. §III.3.6).

Couverture : Exi.C_D213.commFPGAIntegrite1 ,

Exi.C22_D560.SI4.2

[Sécurité]

3.3.2 Fonctionnement des MIO et module d'alimentation

Chaque MIO ou module d'alimentation implémente une partie métier et une partie communication. La partie métier lui est propre et dépend de la fonction à réaliser. La partie communication doit être commune à tous les types de module pour garantir un bon fonctionnement du réseau.
Cette section ne traite que de la partie communication des modules.
Dans cette section, le terme module désigne indifféremment un MIO ou bien un module d'alimentation.

CON-PRO-0300

Un module doit supporter 2 modes de fonctionnement : - Mode RUN, - Mode REPLI.

Couverture :

[Sécurité]

Le mode **RUN** se définit par un état synchronisé et fonctionnel sur le réseau. C'est le mode de fonctionnement nominal en l'absence de défaut mettant en cause la sécurité. Un module en mode RUN est synchronisé à un ou plusieurs CO c'est-à-dire qu'il reçoit périodiquement (en fonction du paramètre TCYC) des trames de synchronisation et peut répondre sur le réseau. Un module ne peut passer en mode RUN (après une mise sous tension) que s'il a était configuré par un CO.
Le mode REPLIS est par opposition au mode RUN le mode sécuritaire dans lequel le module n'émet pas de trame soit parce qu'il n'est pas synchronisé à un CO soit car il est en défaut.

CON-PRO-0310

A la mise sous tension, chaque module doit prendre le TID par défaut **8Fh.**

Couverture :

CON-PRO-0320

A la mise sous tension, chaque module sécuritaire doit prendre le SID par défaut **FFFFFFh.** indiquant qu'il n'a pas encore été configuré.

Couverture :

[Sécurité]

CON-PRO-0330

A la mise sous tension, un module doit être un mode REPLI jusqu'à ce qu'il reçoive l'ordre du concentrateur actif de passer en mode RUN.

Couverture :

[Sécurité]

CON-PRO-0340

Pour passer du mode REPLI au mode RUN, un module doit recevoir dans l'ordre :

- Un ordre de sorti du mode repli du concentrateur actif
- Une trame de synchronisation valide

Couverture :

Note : Un ordre de sortie du mode de repli (implémenté uniquement pour les MIO sécuritaires. Sans effet pour les concentrateurs) est réalisée par une requête sécuritaire sur le booléen sécuritaire OUT_REP (STRUE = 0x55 et SFALSE = 0xAA).

[Sécurité]

CON-PRO-0350

En mode REPLI, les entrées sorties d'un module doivent être dans un état restrictif (état sécuritaire).

Couverture : Exi.C_D213.SO4commFPGAPasMessage

[Sécurité]

CON-PRO-0360

Lorsque les conditions suivantes sont remplies simultanément:

- Réception d'une trame de synchronisation en dehors de la fenêtre de réception autorisée sur un des ports,
- Absence de réception de trame de synchronisation valide sur l'autre port sur la durée du cycle en cours,

le module doit passer en mode repli.

Couverture :

[Sécurité]

CON-PRO-0370

Un module en mode RUN doit vérifier que le champ CYC des trames de synchronisation est conforme à son compteur de cycle interne. En cas d'erreur, il doit ignorer la trame correspondante, et passer en mode repli.

Couverture :

[Sécurité]

CON-PRO-0380

Lorsqu'un module ne reçoit pas de trame de synchronisation valide durant un nombre de cycles de communication configurable par registre (CNF_CYC), il doit passer en mode REPLI.

Couverture : Exi.C_D213.SO4commFPGAPasMessage, Exi.C22_D212.valeurEntreeAbsenceMessage

Note : Le module doit utiliser le paramètre TCYC pour compter les cycles sans trame de synchronisation.

[Sécurité]

CON-PRO-0390

Lorsqu'un module possédant des sorties ne reçoit pas de trame de requête de mise à jour de ses sorties durant un nombre de cycles configurable par registre (CNF_REQ), il doit passer en mode REPLI.

Couverture : Exi.C_D213.SO4commFPGAPasMessage

Justification : On ne peut pas se baser uniquement sur la réception des trames de synchronisation pour passer en mode repli car il faut considérer le cas où la couche transport (i.e. le FPGA fournirait au PIC les trames de synchro et pas les trames de requête).

[Sécurité]

CON-PRO-0400

Lorsqu'il émet une trame de réponse à une requête (sécuritaire ou non), un module doit fixer le TID du destinataire à F0h (multicast vers tous les concentrateurs du réseau).

Couverture :

3.3.3 Fonctionnement des concentrateurs

CON-PRO-0600

Un concentrateur doit supporter 3 modes de fonctionnement :
- Mode actif,
- Mode passif,
- Mode repli.

Couverture :

[Sécurité]

CON-PRO-0610

Un concentrateur doit maintenir en permanence une image des entrées/sorties des MIO (on parle d'image du procédé). Cette image doit être mise à jour en fonction :
- Des requêtes du client,
- Des trames de réponse émises par les MIO,
- Des trames de requête émises par l'éventuel autre concentrateur.

Couverture :

[Sécurité]

CON-PRO-0620

Un concentrateur doit mettre à disposition du client les informations suivantes :
- L'image du procédé et de ses statuts
- L'état de ses statuts internes
- S'il est actif ou passif
- L'état du réseau (agents absents ou intrus, anneau de communication ouvert ou dégradé, …)

Couverture :

[Sécurité]

CON-PRO-0640

Le concentrateur actif doit émettre une trame de synchronisation en broadcast au début de chaque cycle de communication.

Couverture :

[Sécurité]

CON-PRO-0650

Suite à l'émission de la trame de synchronisation, le concentrateur actif doit émettre des trames de requête pour mettre à jour toutes les sorties des MIO en fonction de son image du procédé.

Couverture :

Note : Cette action doit être effectuée même si l'état des sorties n'a pas évolué par rapport au cycle précédent.

[Sécurité]

CON-PRO-0660

A la mise sous tension, le concentrateur actif doit prendre le TID **F0h**.

Couverture :

CON-PRO-0670

A la mise sous tension, les concentrateurs passifs doivent prendre le TID par défaut **8Fh**.

Couverture :

CON-PRO-0680

A la mise sous tension, les concentrateurs doivent prendre le SID qui est donné par la configuration système.

Couverture :

CON-PRO-0690

Un concentrateur passif doit passer passant s'il reçoit plus de trois trames de synchronisation hors fenêtre consécutivement.

Couverture :

[Sécurité]

CON-PRO-0700

Il ne doit y avoir qu'un seul concentrateur actif à la fois sur le réseau. Les concentrateurs se servent de leur numéro d'ordre donné par le SID afin de déterminer à quel moment ils doivent devenir actifs.

Couverture :

Justification : la différence de traitement en fonction du numéro d'ordre a pour but d'éviter que plusieurs concentrateurs passifs ne décident de devenir actif en même temps.

[Sécurité]

CON-PRO-0730

Si le concentrateur actif est actif depuis au moins un cycle TCYC et qu'il reçoit une trame de synchronisation dont il n'est pas l'émetteur, il doit passer immédiatement passif.

Couverture :

Justification : Durant le cycle où un concentrateur passif devient actif, 2 trames de synchronisation d'origines différentes peuvent cohabiter sur le réseau. Le passage d'actif à passif sur réception d'une trame de synchronisation d'origine différente ne doit donc se faire que si le concentrateur est actif depuis au moins un cycle complet.

[Sécurité]

CON-PRO-0740

Un concentrateur doit être en mode repli (ou passant) au démarrage. Un concentrateur ne peut passer hors repli que si :

- Le concentrateur est le concentrateur primaire ou le concentrateur le plus prioritaire qui réalise le LANSCAN.
- Le concentrateur reçoit une trame de vérification des invariants qui confirme la validité de ses invariants.

=> Le concentrateur devient alors passif

Couverture :

[Sécurité]

CON-PRO-0750

Un concentrateur en mode repli (ou passant) ne valide une trame de vérification des invariants que si :

- Les 2 premiers octets du champ DATA correspondent au CRC de ses invariants de configuration
- Les 2 derniers octets du champ DATA correspondent au CRC de sa logique booléenne.

Couverture :

[Sécurité]

3.3.4 Configuration

CON-PRO-1000

Lors de l'installation du système, chaque concentrateur doit être configuré avec un numéro d'ordre de prise de contrôle sur le réseau privé. Ce numéro s'établit de 1 à N avec N le nombre de concentrateurs dans le réseau.

Couverture :

[Sécurité]

CON-PRO-1010

Chaque concentrateur doit sauvegarder dans une mémoire non volatile (IDS) la configuration du réseau :

- Temps de cycle TCYC applicable au réseau,
- Nombre d'agents,
- Pour chaque agent (y compris les autres concentrateurs du système):
  => Identifiant MAC de l'agent (pour les modules sécuritaires),
  => Identifiant SID de l'agent (pour les modules sécuritaires),
  => Identifiant IID de l'agent,
  => Identifiant TID de l'agent,
  => Type d'agent (fonction métier + niveau de sécurité),
  => Nombre de trames de synchronisation manquantes avant de passer en repli (paramètre CNF_CYC)
  => Nombre de trames de requête manquantes avant de passer en repli (paramètre CNF_REQ)
  => Données de configuration fonctionnelle du MIO (paramètres liés à sa partie métier).

L'intégrité de la mémoire de stockage de la configuration doit être assurée par un CRC CCITT-32.

Couverture :

[Sécurité]

CON-PRO-1030

En régime établi, chaque concentrateur doit vérifier à chaque cycle de communication, que le réseau est toujours conforme à sa configuration (nombre d'agents, type TID et SID des agents connectés). En cas d'incohérence, le client doit en être informé.

Couverture :

[Sécurité]

CON-PRO-1040

En régime établi, si un concentrateur perd la communication avec un MIO, il doit l'interroger périodiquement (chaque cycle système) pour détecter un éventuel rétablissement de la communication. Lorsque la communication est rétablie, si ce MIO est conforme (en termes de type et de MAC), le concentrateur doit le reconfigurer (notamment le sortir du mode de repli) avant de pouvoir lui envoyer à nouveau des requêtes au cycle suivant.

Couverture :

Justification : Ce mécanisme permet de changer un MIO à chaud et assure qu'une commande ne sera pas envoyée à tort à un agent qui n'est pas censé la recevoir.

3.3.5 Mise sous tension

CON-PRO-1200

A sa mise sous tension, chaque concentrateur doit vérifier l'intégrité de sa mémoire de stockage de la configuration. Si la mémoire est corrompue, le concentrateur concerné doit passer en mode passant. Le concentrateur ne peut sortir du mode passant que par un redémarrage.

Couverture :

Justification : le mode passant permet d'augmenter la disponibilité du système en cas de problème de configuration du réseau.

[Sécurité]

CON-PRO-1210

A sa mise sous tension, chaque concentrateur doit vérifier auprès du concentrateur maître que sa configuration est la bonne. En cas d'incohérence, il doit rester en mode passant.

Couverture :

Justification : ce mécanisme est important en cas de maintenance et de remplacement d'un concentrateur pour assurer que le système ne démarre pas avec 2 concentrateurs configurés différemment, ou bien avec une configuration qui ne correspond pas au réseau.

CON-PRO-1220

A la mise sous tension, tout concentrateur doit respecter une temporisation équivalente à N*1s (avec N correspond à son numéro d'ordre donné par son SID). Durant cette temporisation :

- S'il reçoit une trame valide (i.e dont le champs FCS, Frame Check Sequence transport est valide), il poursuit immédiatement sa séquence de démarrage en mode passif, sans attendre la fin de la temporisation.

S'il ne reçoit aucune trame valide, il se met en mode actif et gère le LANSCAN

Couverture :

Justification : ce mécanisme permet à un concentrateur de démarrer dans un réseau déjà actif sans le perturber, et permet d'ordonnancer le démarrage simultané de plusieurs concentrateurs.

CON-PRO-1230

Le concentrateur ayant démarré en mode actif doit vérifier que le réseau est conforme à sa configuration (nombre d'agents, type, MAC et IID). Il doit signaler toute incohérence au client.

Couverture :

[Sécurité]

CON-PRO-1240

Le concentrateur ayant démarré en mode actif doit configurer les autres agents du système (TID, SID, paramètre TCYC, paramètres CNF_CYC et CNF_REQ, données de configuration fonctionnelles).

Couverture :

[Sécurité]

CON-PRO-1250

Lorsque le concentrateur actif configure le SID des agents sécuritaires, il doit : Emettre une trame d'attribution de SID Attendre la trame d'acquittement d'attribution de SID qui doit arriver en moins de TCYC (dans le cycle courant). Si la trame d'acquittement ne lui parvient pas dans le temps imparti, ou bien si les données qu'elle contient ne sont pas conformes aux valeurs attendues, l'agent concerné est déclaré absent et ne doit pas être utilisé par la suite.

Couverture :

[Sécurité]

3.3.6 Monitoring

Dans ce chapitre, le terme « réception de trame » sous-entend réception d'une trame valide, dont le(s) champ(s) FCS est (sont) correct(s). Pour les trames de synchronisation, valide sous-entend également 'reçue dans la bonne fenêtre temporelle'.
Les fonctions décrites ici sont optionnelles et participent au diagnostic permanent du réseau. Elles ne participent pas aux fonctions sécuritaires du système.
Dans cette chapitre, le terme module désigne indifféremment un MIO ou bien un module d'alimentation.

CON-PRO-1400

Sur réception d'une trame dont il ne supporte pas le format un agent doit incrémenter un compteur interne 8 bits correspondant à cet évènement et positionner à 1 le flag de statut correspondant (bit BFO « Format de trame non supporté ou bien débordement du buffer» de son registre interne Statut).

Couverture :

3.3.6.1 Module

CON-PRO-1410

Un module doit vérifier que chaque trame de requête, d'attribution de TID ou SID, et de synchronisation qui lui est adressée est reçue sur ses 2 ports. Si un port ne reçoit pas la trame dans le temps imparti (TCYC défini par registre), le module doit incrémenter un compteur interne 8 bits correspondant au port défaillant, et positionner à 1 le flag de statut correspondant (bit CNR « Une trame n'a pas été reçue sur les 2 ports » de son registre interne Statut).

Couverture :

CON-PRO-1420

Un module doit vérifier que les champs SEQ et CYC des requêtes sécuritaires qui lui sont adressées est conforme aux règles définies au §Erreur ! Source du renvoi introuvable. En cas d'erreur, il doit incrémenter un compteur d'erreur interne 8 bits et positionner à 1 le flag de statut correspondant (bit ESE,»SEQ OU CYC ERRONÉ» de son registre interne Statut).

Couverture :

CON-PRO-1430

Un module doit vérifier qu'il reçoit au moins une trame sur chacun de ses ports à chaque cycle. En cas de silence sur une période supérieure au TCYC+20% défini par registre, le module doit incrémenter un compteur interne 8 bits correspondant au port défaillant, et positionner à 1 le flag de statut correspondant (bits NA1 et NA2 de son registre interne Statut cf CON-PRO-3000).

Couverture :

CON-PRO-1440

Un module doit vérifier qu'il reçoit périodiquement (à chaque cycle) une trame de synchronisation sur au moins un port de communication. En cas d'absence de trame de synchronisation valide, le module doit incrémenter un compteur interne 8 bits, et positionner à 1 le flag de statut correspondant (bit NTS, «Pas de trame de synchronisation détectée depuis TCYC » de son registre interne Statut).

Couverture :

CON-PRO-1450

Chaque compteur de statut géré par un module doit être incrémenté, s'il est inférieur à 255, sur détection de l'évènement correspondant. Les compteurs de statut ne peuvent être remis à 0 que par une commande d'écriture à l'adresse correspondante.
Chaque compteur de statut doit être à 0 à la mise sous tension du module.

Couverture :

3.3.6.2 Concentrateur

CON-PRO-1460

Un concentrateur doit vérifier que chaque trame est reçue sur ses 2 ports. Si un port ne reçoit pas la seconde trame dans le temps imparti (TCYC défini par registre), le concentrateur doit incrémenter un compteur interne 8 bits correspondant au port défaillant (CPT_TOCOx), et positionner à 1 le flag de statut correspondant (bit CNR « Une trame n'a pas été reçue sur les 2 ports » de son registre interne Statut).

Couverture :

CON-PRO-1470

Un concentrateur doit vérifier que le champ SEQ et CYC de toutes les trames qu'il voit passer est conforme aux règles définies au **§Erreur ! Source du renvoi introuvable.** En cas d'erreur, il doit incrémenter un compteur d'erreur interne 8 bits (CPT_SEQ) et positionner à 1 le flag de statut correspondant (bit ESE,»SEQ OU CYC ERRONÉ» de son registre interne Statut).

Couverture :

CON-PRO-1480

Le concentrateur en mode passif doit vérifier que le champ CYC des trames de synchronisation est conforme à son compteur interne de cycle de communication. En cas d'erreur, il doit incrémenter un compteur d'erreur interne 8 bits (CPT_SEQ) et positionner à 1 le flag de statut correspondant (bit ESE,»SEQ OU CYC ERRONÉ» de son registre interne Statut).

Couverture :

CON-PRO-1490

Un concentrateur doit vérifier qu'il reçoit au moins une trame sur chacun de ses ports à chaque cycle. En cas de silence sur une période supérieure au TCYC+20% défini par registre, le concentrateur doit incrémenter un compteur interne 8 bits correspondant au port défaillant, et positionner à 1 le flag de statut correspondant (bits NA1 et NA2 de son registre interne Statut cf CON-PRO-3000).

Couverture :

CON-PRO-1500

Un concentrateur doit vérifier qu'il reçoit périodiquement (à chaque cycle) une trame de synchronisation sur au moins un port de communication. En cas d'absence de trame de synchronisation valide, le concentrateur doit incrémenter un compteur interne 8 bits, et positionner à 1 le flag de statut correspondant (bit NTS, «Pas de trame de synchronisation détectée depuis TCYC » de son registre interne Statut).

Couverture :

Note : L'exigence s'applique également au concentrateur en mode actif (émetteur de la trame de synchronisation) qui doit vérifier que la trame de synchronisation lui revient bien dans le délai imparti.

CON-PRO-1510

Chaque compteur de statut géré par un concentrateur doit être incrémenté, s'il est inférieur à 255, sur détection de l'évènement correspondant. Les compteurs de statut ne peuvent être remis à 0 que par une commande spécifique du client.
Chaque compteur de statut doit être à 0 à la mise sous tension du concentrateur.

Couverture :

4 SPECIFICATION DYNAMIQUE DU RESEAU

4.1 CONFIGURATION DU SYSTEME AU DEMARRAGE : LAN SCAN

Au démarrage, la vérification du réseau doit permettre de confirmer que le réseau privé connecté au concentrateur est conforme à la configuration enregistrée.
Dans un premier temps, le concentrateur doit s'assurer que l'autobaudrate des MIO s'est bien calé sur le baudrate attendu et stocké dans le fichier de configuration. Pour cela, le PIC peut demander l'émission de caractères de contrôle à partir du bit SPHY du registre de contrôle.
Par défaut, lorsqu'un MIO démarre, les recopies d'un port sur l'autre sont autorisées. L'algorithme de LAN SCAN peut donc être le suivant

- Configuration du registre CONFIG_RP du concentrateur en mode Actif et avec le baudrate du FPGA donné par le fichier de Configuration
- Configuration du registre de contrôle du FPGA concentrateur avec la valeur 00h:
    - Copies interdites
    - Mode normal
    - FIFO Tx pas en reset
- Emission 8 fois des caractères de contrôle (bit SPHY du registre CONTROL)
- Emission d'une trame de commande en broadcast qui interdit la recopie dans tous les MIO (mise à '0' des bits '0' et '1' du registre CONF de tous les MIO)

A ce stade, le concentrateur ne voit que les 2 MIO qui sont de part et d'autre. (Car la recopie par les agents d'une trame d'un port sur l'autre est désactivée. Les messages ne peuvent donc atteindre que les agents de part et d'autre du CO).

Tant que l'on n'a pas découvert complètement le réseau :

- Lecture en mode broadcast des 8 octets de l'IID de chaque MIO
- Récupération en principe de deux réponses :
    - Erreur 1 : On ne reçoit qu'une réponse, un agent est défaillant ou le réseau est ouvert d'un coté
    - Erreur 2 : Aucune réponse n'est reçue : Le réseau est ouvert des deux côtés et les agents sont notés en défaut.
    - Erreur 3 : L'IID reçue est différent de celui décrit dans la configuration. La découverte du réseau n'est pas bloquée et on stocke ce nouvel IID.
- Envoie du TID de l'agent
- Envoie du SID de l'agent si l'agent est sécuritaire.
- Lecture du champ TYP avec les TID et SID donnés précédemment.
- Vérification des types :
- Si un type n'est pas correct l'agent est mis en défaut.
- Envoie de la configuration des agents (TCYC, CNF_CYC, CNF_REQ (pour les agents sécuritaires, AD_REF et SZ_REF) + configuration des entrées pour les modules SIO0 + la trame de vérification des invariants pour les modules concentrateurs (avec un champ CYC à 0).
- Envoi de l'autorisation de recopie

L'algorithme se poursuit jusqu'à ce qu'on ait découvert tous les modules attendus. A la fin de l'algorithme, il faut s'assurer qu'une trame fait tout le tour de l'anneau (i.e. qu'une trame émise par le concentrateur revient bien sur ces 2 ports) pour s'assurer que l'anneau n'est pas ouvert au milieu de l'anneau.

Plusieurs cas particuliers sont en prendre en compte :

- L'anneau est ouvert à un endroit l'algorithme trouvera à chaque cycle qu'un seul nouveau module au lieu de 2. On note la coupure et on poursuit l'algorithme jusqu'à découvrir tous les modules
- L'anneau est ouvert à 2 endroits, l'algorithme ne trouvera plus de nouveaux modules alors qu'il lui en manque. L'algorithme doit donc s'arrêter là en notant tous les agents non configurés en défaut.
- Lorsqu'un agent est mis en défaut, on arrête sa configuration.

4.2 FONCTIONNEMENT PERMANENT

Suite au démarrage le logiciel PIC du concentrateur doit effectuer périodiquement les opérations suivantes :

- Emission de la trame de synchro
- Emission des requêtes de sorties de repli pour les agents configurés (pas en défaut) mais n'étant pas sortie de repli (récupération à chaud par exemple, les agents ont été configurés configuré au cycle précédent)
- Emission des requêtes de pilotage des sorties à partir de l'image réseau qu'il gère (modules sécuritaires et non sécuritaires)
- Emission des requêtes spécifiques pour analyser le réseau
- Réception des trames émises par les modules
- Gestion des requêtes clients
- Gestion des informations passerelle
- Gestion de l'image du réseau

Dans le même temps, la passerelle analyse tout le trafic pour pouvoir en diagnostiquer l'état. Le PIC concentrateur se servira des trames de réponse à la synchronisation pour déceler la perte d'un agent. Un agent sera noté « en défaut » s'il ne répond pas pendant CNF_CYC cycle consécutif aux trames de synchronisation.

4.3 RECUPERATION DES AGENTS A CHAUD

Lorsque des agents sont en défaut (détectés lors du LANSCAN ou par non réponse aux trames de synchronisation), le concentrateur va tenter de récupérer l'agent. A chaque cycle système une étape décrite ci-dessous est réalisée :

- Emission d'une trame de commande à tous les agents n'ayant pas de TID qui interdit la recopie (mise à '0' des bits '0' et '1' du registre CONF)
- Lecture des 8 octets de l'IID à tous les agents n'ayant pas de TID
- Récupération en principe de deux réponses
- Envoie du TID de l'agent
- Envoie du SID de l'agent si l'agent est sécuritaire.
- Lecture du champ TYP avec les TID et SID donnés précédemment.
- Vérification des types :
    - Si un type n'est pas correct l'agent reste en défaut.

- Envoie de la configuration des agents (TCYC, CNF_CYC, CNF_REQ (pour les agents sécuritaires, AD_REF et SZ_REF) + configuration des entrées pour les modules SIO0 + la trame de vérification des invariants pour les modules concentrateurs.
  Envoi de l'autorisation de recopie

Plusieurs cas particuliers sont en prendre en compte :

- Si l'agent ne répond pas à la trame de lecture de l'IID, la récupération continuera puisque l'agent a pu être perdu sans que la carte ait été débranchée et de ce fait le TID est déjà configuré.
- Le concentrateur pourra récupérer deux agents en même temps.

5 ANNEXE 1 – VENTILATION DES EXIGENCES POUR SIO

	FPGA	PIC	SECURITE
CON-PRO-0010		X	
CON-PRO-0020		X	X
CON-PRO-0021		X	X
CON-PRO-0030		X	X
CON-PRO-0040		X	
CON-PRO-0050	X		
CON-PRO-0060		X	X
CON-PRO-0065		X	
CON-PRO-0070	X		
CON-PRO-0080	X		
CON-PRO-0090	X	X	X
CON-PRO-0100	X		
CON-PRO-0110	X		
CON-PRO-0120	X		
CON-PRO-0130		X	X
CON-PRO-0140		X	X
CON-PRO-0150		X	X
CON-PRO-0160		X	X
CON-PRO-0300		X	X
CON-PRO-0310	X		
CON-PRO-0320		X	X
CON-PRO-0330		X	X
CON-PRO-0340		X	X

CON-PRO-0350		X	X
CON-PRO-0360		X	X
CON-PRO-0370		X	X
CON-PRO-0380		X	X
CON-PRO-0390		X	X
CON-PRO-0400	X		
CON-PRO-1400		X	
CON-PRO-1410		X	
CON-PRO-1420		X	
CON-PRO-1430		X	
CON-PRO-1440		X	
CON-PRO-1450		X	
CON-PRO-2040	X		
CON-PRO-2050	X		
CON-PRO-2200		X	X
CON-PRO-2210		X	X
CON-PRO-2220		X	
CON-PRO-2230		X	X
CON-PRO-2240	X	X	X
CON-PRO-2250	X	X	X
CON-PRO-2260		X	X
CON-PRO-2270		X	X
CON-PRO-2280		X	
CON-PRO-2290		X	
CON-PRO-3000		X	X
CON-PRO-3010		X	X

6 ANNEXE 2 – VENTILATION DES EXIGENCES POUR CO2

	FPGA	PIC	SECURITE
CON-PRO-0022		X	X
CON-PRO-0030		X	X
CON-PRO-0040		X	
CON-PRO-0050	X		
CON-PRO-0060	X		
CON-PRO-0065	X		
CON-PRO-0070	X		
CON-PRO-0080	X		
CON-PRO-0090	X	X	X
CON-PRO-0100	X		
CON-PRO-0110	X		
CON-PRO-0120	X		
CON-PRO-0130		X	X
CON-PRO-0140		X	X
CON-PRO-0150		X	X
CON-PRO-0600		X	X
CON-PRO-0610		X	X
CON-PRO-0620		X	X
CON-PRO-0640		X	X
CON-PRO-0650		X	X
CON-PRO-0660		X	X
CON-PRO-0670		X	X
CON-PRO-0680		X	X

CON-PRO-0690		X	X
CON-PRO-0700		X	X
CON-PRO-0730		X	X
CON-PRO-0740		X	X
CON-PRO-0750		X	X
CON-PRO-1000		X	X
CON-PRO-1010		X	X
CON-PRO-1030		X	X
CON-PRO-1040		X	X
CON-PRO-1200		X	X
CON-PRO-1210		X	X
CON-PRO-1220		X	X
CON-PRO-1230		X	X
CON-PRO-1240		X	X
CON-PRO-1250		X	X
CON-PRO-1400		X	
CON-PRO-1460	X	X	
CON-PRO-1470		X	
CON-PRO-1480		X	
CON-PRO-1490	X	X	
CON-PRO-1500		X	
CON-PRO-1510		X	
CON-PRO-2030	X	X	
CON-PRO-2040	X		
CON-PRO-2050	X		
CON-PRO-2200		X	X
CON-PRO-2210		X	X

CON-PRO-2220		X	
CON-PRO-2230		X	X
CON-PRO-2240		X	
CON-PRO-2250		X	
CON-PRO-2260		X	X
CON-PRO-2270		X	X
CON-PRO-2280		X	
CON-PRO-2290		X	
CON-PRO-3010		X	X

CLEARSY
Safety Solutions Designer

contact@clearsy.com
www.clearsy.com

320 Avenue Archimède
Les Pléiades III Bat A
13100 Aix-en-Provence - France

Tél. +33 (0)4 42 37 12 70

Fax. +33 (0)4 42 37 12 61