
# Améliorations TCP/IP

Document 26-867 | Version FRA05 | 2019-02-13

0

0

## 0.1 Historique du document

| Version | Date | Changements | Remarques |
|---|---|---|---|
| pFR01 | 2010-06-07 | - | Traduction de l'anglais |
| FR01 | 2010-08-25 | Chapitre 2<br>Chapitre 8.1 | - retravaillée<br>- élargi |
| FR02 | 2011-08-26 | Couverture<br>Ch4.4.4 | - éliminé PCD2.M480 et PCS1<br>- nouvel avertissement |
| FR03 | 2012-11-23 | Chapitre 1 et 4 | Modification |
| FR04 | 2013-11-08 | - | Nouveau logo et<br>nouveau nom de l'entreprise |
| FRA05 | 2019-02-13 | Chapitre A | Nouveau numéro de téléphone<br>(À partir du 15 février 2015) |

## 0.2 Marques déposées

Saia PCD® et Saia PG5® sont des marques déposées de Saia-Burgess Controls AG.

Les modifications techniques dépendent de l'état de la technologie.



Publié en Suisse.

# 1 Introduction



Ce manuel traite les protocoles IP prise en charge de systèmes Saia PCD®. Chaque protocole est expliqué et traité à l'aide d'une exemples de configuration.

En plus des protocoles abordés dans ce guide les protocoles additionnels suivants sont supportés du serveur d'automatisation au niveau du firmware:

| | | |
|---|---|---|
| HTTP | manuel | 26/790 |
| FTP | manuel | 26/855 |
| Modbus TCP, UDP | manuel | 26/866 |
| BACnet / IP | manuel | 26/849 |
| LON / IP | manuel | 26/883 |

## 1.1 Modèle de référence OSI

Le modèle de couches ISO/OSI suivant représente les protocoles IP pris en charge par les contrôleurs Saia PCD®. Les protocoles mis en évidence en couleur sont nouveaux et seront pris en charge par les versions actuelles du microprogramme des UC PCD3 et PCD2.M5.

<table>
<tr><td colspan="2"></td><td colspan="7">Programme utilisateur<br>Biblioth. BF</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">Application</td><td rowspan="2">Ser-<br>veur<br>HTTP/<br>FTP</td><td></td><td colspan="5">Listes d'instructions, instructions CSF</td></tr>
<tr><td>DHCP<br>DNS<br>SNTP<br>SNMP</td><td>BACnet</td><td>SMTP<br>E-mail</td><td>S-Bus</td><td>Mo-<br>dbus</td><td>Mode<br>de<br>don-<br>nées<br>ou-<br>vert</td></tr>
<tr><td>6</td><td>Session</td><td colspan="7" rowspan="2">Non utilisée</td></tr>
<tr><td>5</td><td>Présenta-<br>tion</td></tr>
<tr><td>4</td><td>Transport</td><td colspan="7">TCP, UDP</td></tr>
<tr><td>3</td><td>Réseau</td><td colspan="7">IP</td></tr>
<tr><td>2</td><td>Liaison de<br>données</td><td colspan="4">Ethernet</td><td colspan="3">PPP</td></tr>
<tr><td>1</td><td>Physique</td><td colspan="4">IEEE802.3</td><td colspan="3">RS-232,<br>modem</td></tr>
</table>

## 1.2 Configuration minimale requise

| Modèle de Saia PCD® | Version matérielle | Version Firmware |
|---|---|---|
| PCD3.Mxxx0 | ≥D | 1.14.23 |
| PCD3.M3120, M3020 | ≥E48 | 1.14.23 |
| PCD2.M5xx0 | A (pas de réstriction) | 1.14.23 |
| PCD1.M2120 | A (pas de réstriction) | 1.14.23 |
| PCD2.M480 | non pris en charge | |
| PCD3.M2x30 (WAC, Compact) | A (pas de réstriction) | |

Version 2.0 du Saia PG5® avec configurateur matériel

## 1.3 Abréviations

**TCP:** **Transfer Control Protocol**

**IP:** **Internet Protocol**

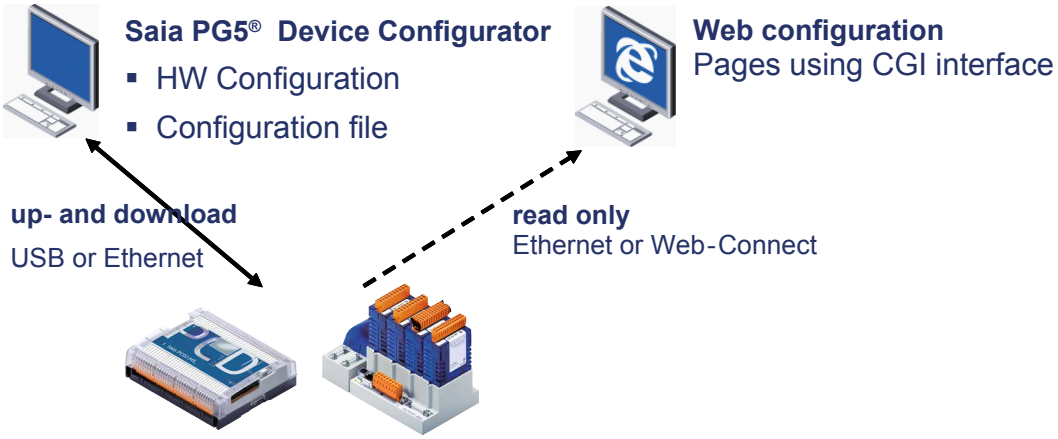
**UDP:** **User Datagram Protocol**

# 2 Utilisation des fichiers de configuration

## 2.1 Généralités

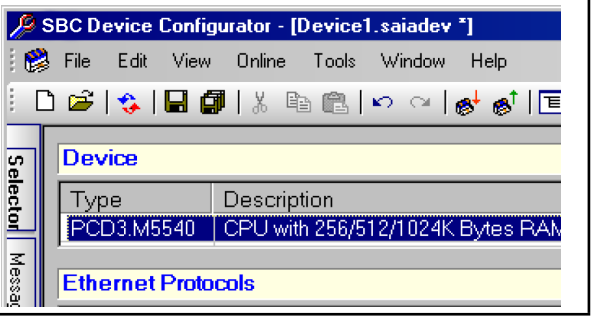


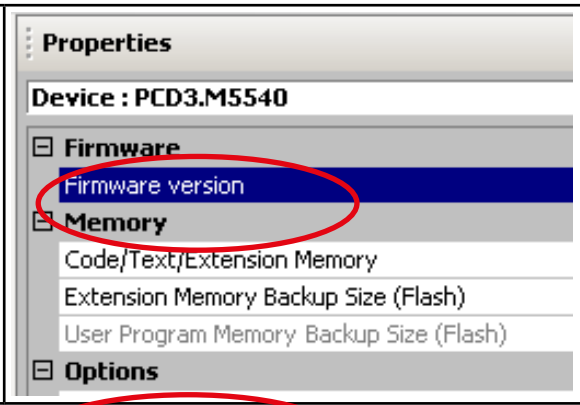
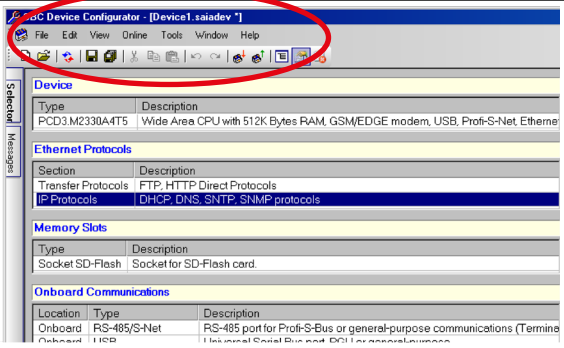
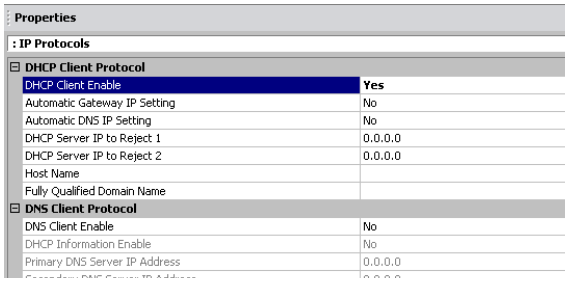
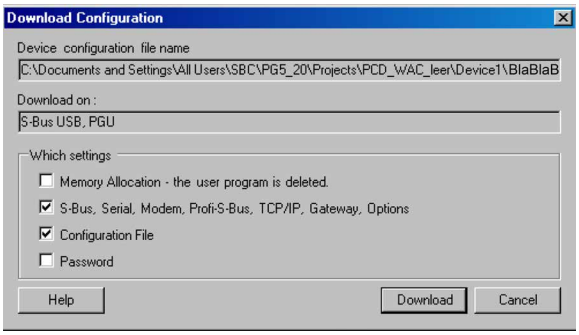
Tous les protocoles TCP/IP sont configurés à l'aide du configurateur matériel «Device Configurator» du Saia PG5® 2.0. Tous les paramètres de configuration sont enregistrés dans un fichier de configuration PCD.SCFG qui est stocké dans le dossier du projet Saia PG5®. Le téléchargement réalisé à l'aide du configurateur matériel inclut la configuration matérielle et le téléchargement du fichier de configuration vers le système PLC.




Saia PCD® System with NT-OS

## 2.2 Configurateur matériel pour SNTP, SNMP, DHCP et DNS

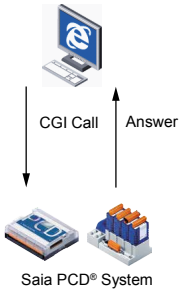
| | | |
|---|---|---|
| ① | Lancez le configurateur matériel. |  |
| ② | Sélectionnez le type d'UC. |  |

| | | |
|---|---|---|
| ③ | Sélectionnez la version du microprogramme. Pour utiliser les nouvelles améliorations apportées pour IP, vous devez disposer au moins de la version 1.14.xx du microprogramme. |  |
| ④ | Sélectionnez le protocole IP. |  |
| ⑤ | Chaque protocole IP peut être activé séparément. |  |
|  | Enregistrer : Enregistre la configuration PCD.SCFG dans le dossier du projet de l'UC. | |
|  | Télécharger vers le système : Télécharge la configuration matérielle et le fichier de configuration du protocole IP (PCD.SCFG en option) vers le système Saia PCD®. Le téléchargement de la configuration du périphérique comprend par défaut :<br>- La configuration matérielle<br>- Le fichier de configuration PCD.SCFG (en option) |  |
| | Sur le Saia PCD®, le fichier sera stocké dans le dossier de configuration (PLC_SYS) | Veuillez noter que ce dossier n'est pas accessible par l'utilisateur. |
|  | Télécharger depuis le système : Télécharge la configuration matérielle et le fichier de configuration du protocole IP (PCD.SCFG) depuis le système Saia PCD®. | |

## 2.3 Diagnostic Web via l'interface CGI

La plupart des paramètres de configuration peuvent être visualisés à l'aide de l'interface CGI.






## 2.4 Programmation avancée

En ce qui concerne la programmation avancée à l'aide d'instructions CSF, veuillez vous reporter à la bibliothèque de fonctions du système et aux documents d'aide que vous trouverez dans la version 2.0 du Saia PG5®.

# 3 PPP (protocole point à point)

## 3.1 Introduction

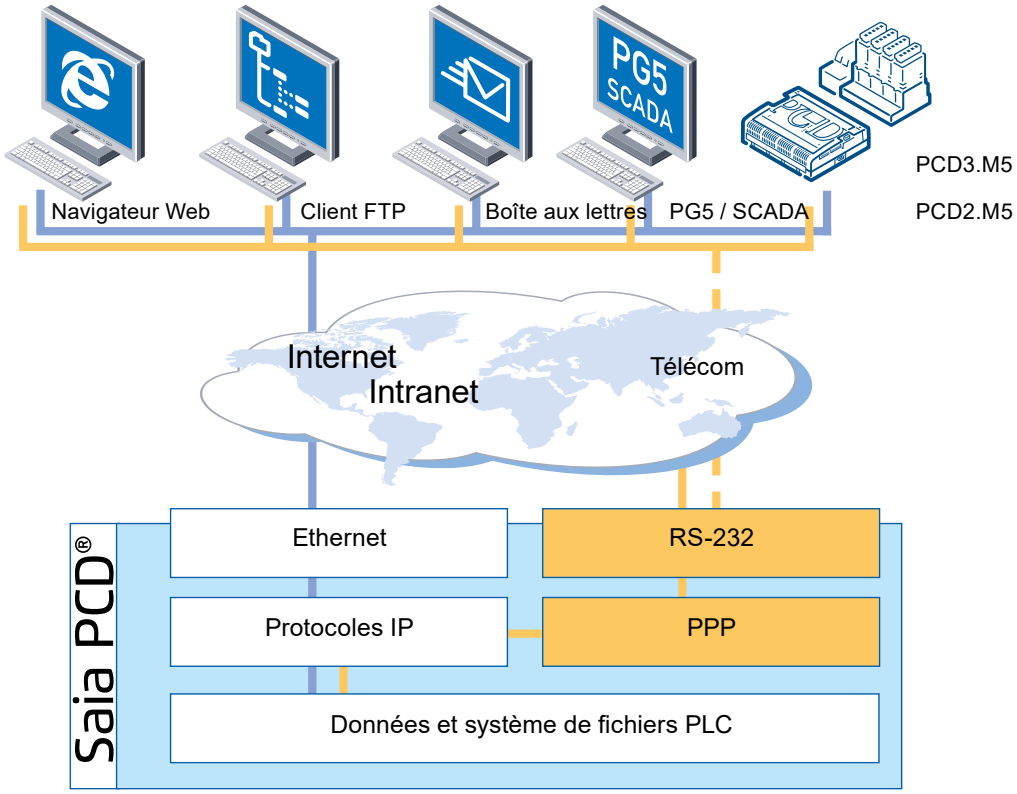
Il s'agit d'un protocole qui établit une communication entre deux points (emplacements). PPP est principalement utilisé pour transporter le protocole TCP/IP sur une ligne série ou une connexion par modem.



PPP fonctionne dans les deux couches inférieures du modèle ISO/OSI et permet les mêmes fonctions qu'une connexion Ethernet.

Le protocole CHAP (Challenge Handshake Authentication Protocol) a été introduit afin de répondre aux besoins grandissants en matière de sécurité établis pour la numérotation dans les réseaux d'entreprise ou les installations comprenant des tâches critiques. Contrairement au protocole PAP (Password Authentication Protocol), le mot de passe transmis avec celui-ci est chiffré.

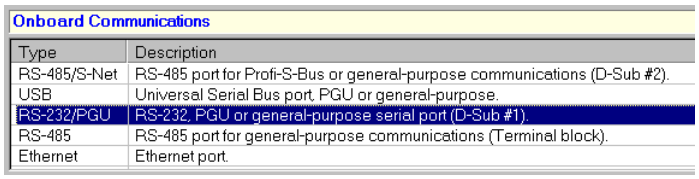
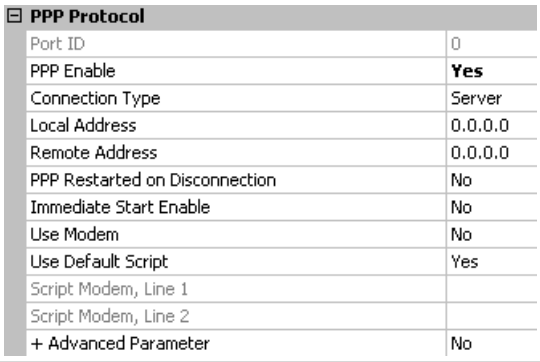
Les serveurs Web et FTP sont accessibles, même avec des dispositifs meilleur marché ne disposant pas de connexion Ethernet. Ces serveurs peut être intégrés dans des environnements IP via des ports série. Les modems raccordés au port série de ces appareils peuvent être utilisés directement pour la connexion à Internet ou Intranet. Les navigateurs Web standard peuvent être utilisés avec tous les contrôleurs Saia PCD®, sans logiciel supplémentaire. Les contrôleurs Saia PCD® peuvent désormais également être connectés directement à l'aide de méthodes de communication modernes telles que les réseaux GPRS et UMTS.




En créant une connexion PPP, la passerelle par défaut sera définie comme PPP. Ainsi seulement PPP est pris en compte pour les connexions à l'extérieur du réseau local. (et il n'est plus possible de communiquer par l'intermédiaire de la passerelle par défaut de l'interface Ethernet, tandis que les PPP est actif).

Lorsque vous utilisez le protocole DHCP sur l'interface Ethernet en parallèle avec une configuration de PPP, la configuration DHCP « Automatique passerelle IP paramètre » dans le Configurateur de périphérique doit être définie sur « No ». Dans cette constellation (tout en fonctionnant sans le PPP) sera communiquée uniquement sur le réseau local.

## 3.2 Activation de PPP

| | |
|---|---|
| Il est possible d'activer PPP sur toutes les interfaces RS-232 pouvant exécuter l'établissement d'une liaison RS-232 complète. |  |
| Configurez « PPP Enable » sur « Yes ».<br>PPP est lancé immédiament après le téléchargement de la configuration. Il est possible de contrôler PPP à l'aide de boîtes de fonctions ou d'instructions CSF. |  |





Lancement et arrêt de PPP

L'état de PPP peut être contrôlé à tout moment par le programme utilisateur à l'aide de boîtes de fonctions ou d'instructions CSF.

Toutes les bibliothèques CSF PPP sont décrites dans le PG5 2.0.

## 3.3 Types de connexion et paramètres associés

Veuillez lire la note d'application des améliorations TCP/IP pour obtenir de plusamples détails. Elle est peut être téléchargée sur le site de support du PCD.



### 3.3.1 Connexion directe par câble

Les paramètres les plus importants pour ce type de connexion sont :

- Définit quel périphérique est le client / serveur. Le serveur déterminera l'adresse IP (locale et à distance), les champs peuvent ne pas être remplis pour le client.
- Le paramètre UseModem doit être configuré sur 0.
- Il est possible de définir n'importe quel script. Si l'un des périphériques est un PC fonctionnant sous Windows®, le script par défaut peut être utilisé du côté du Saia PCD®.
- Les paramètres CheckDCD, DTRPulse et DCDTimeout doivent être configurés sur 0.
- Le paramètre EnaEReq doit être défini avec les paramètres ERTInterval et ERNumber pour réaliser des contrôles d'anomalies pour la connexion. En cas de problèmes de connexion, la connexion PPP sera fermée et relancée en fonction des paramètres spécifiés.

### 3.3.2 Connexion par modem

Les paramètres les plus importants pour ce type de connexion sont :

- Définit quel périphérique est le client / serveur. Le serveur déterminera l'adresse IP (locale et à distance), les champs peuvent ne pas être remplis pour le client.
- Le paramètre UseModem doit être configuré sur 1. Ceci permet de contrôler les signaux DSR/DCD dès l'établissement de la connexion. Dès que l'un des signaux est interrompu, la connexion est fermée et relancée en fonction des paramètres spécifiés.
- Les lignes de script du modem définiront les commandes AT* permettant de configurer le modem et d'initier la connexion par modem. Le modem peut être configuré en mode réponse automatique (temps indéterminé avant l'établissement de la connexion) ou peut initier la séquence de numérotation.
- Le paramètre CheckDCD doit être configuré sur 1 avec le paramètre DCDTimeout. Ceci permet de contrôler le signal DCD une fois que le script du modem a été lu.
- Le paramètre DTRPulse doit être configuré sur 1. S'il est correctement initialisé, le modem sera réinitialisé si le DTR reste en niveau bas logique pendant une période définie. Le modem élèvera également le signal DSR dès que le signal DTR sera à nouveau au niveau haut.
- Il n'est pas utile de configurer les paramètres EnaEReq, ERTInterval et ERNumber.

### 3.3.3 Connexion sans fil avec PPP comme serveur

Les paramètres les plus importants pour ce type de connexion, par ex. PPP sur Bluetooth, sont identiques aux paramètres des connexions par modem.

La seule exception est le paramètre DTRpulse qui doit être configuré sur 0. Le dispositif Bluetooth est automatiquement réinitialisé au cours de la séquence de démarrage.



Il est possible de définir n'importe quel script, comme pour les paramètres de connexion directe.

Il est à noter que le dispositif Bluetooth doit être configuré séparément dans son propre fichier de configuration. Le mode Point d'extrémité doit être sélectionné. Il est possible de définir une connexion sécurisée (utilisant un code PIN) ou l'adresse du partenaire Bluetooth à distance.

### 3.3.4 Connexion sans fil avec PPP comme client

Les paramètres les plus importants pour ce type de connexion, par ex. PPP sur Bluetooth, sont identiques aux paramètres des connexions par modem.

L'une des exceptions est le paramètre DTRpulse qui doit être configuré sur 0. Le dispositif Bluetooth est automatiquement réinitialisé au cours de la séquence de démarrage.

La seconde exception est le paramètre CheckDCD qui doit être configuré sur 2 pour permettre au script PPP d'être lu lorsque le dispositif est réellement connecté au partenaire à distance.

Il est possible de définir n'importe quel script, comme pour les paramètres de connexion directe.

Il est à noter que le dispositif Bluetooth doit être configuré séparément dans son propre fichier de configuration. Le mode de connexion doit être sélectionné, ainsi que l'adresse du partenaire Bluetooth à distance. Il est possible de définir une autre connexion sécurisée (utilisant un code PIN, par ex.).

### 3.3.5 Traitement de l’authentification

PPP définit deux modes d’authentification : l’identification des homologues et l’authentification locale. Il est possible de les activer toutes les deux simultanément ou une à la fois ou de n’en activer aucune.

# 4 DHCP et DNS

## 4.1 DHCP - Dynamic Host Configuration Protocol

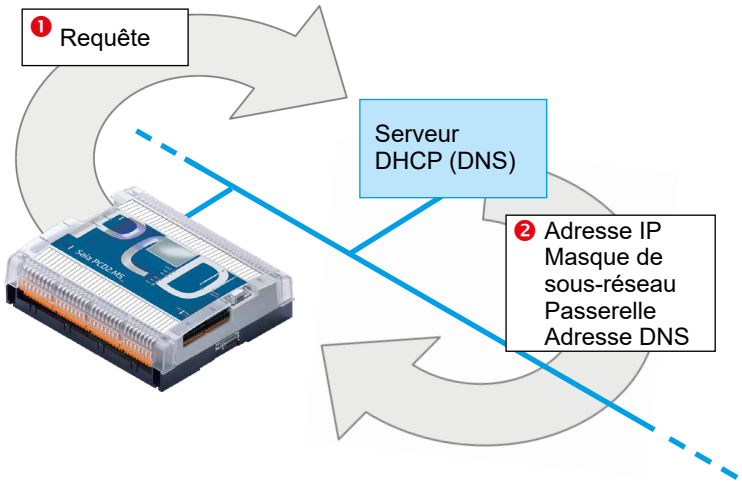
Il s'agit d'un protocole destiné à la configuration automatique de la communication IP. Il n'est plus nécessaire de consacrer beaucoup de temps à saisir manuellement les paramètres de communication. Ils sont attribués directement à partir d'un serveur central. Après une requête, un client DHCP reçoit automatiquement l'adresse IP, le masque de sous-réseau, la passerelle et l'adresse DNS.



Les périphériques sont automatiquement intégrés dans les réseaux existants. Un seul paramètre doit être configuré manuellement sur le périphérique client : celui indiquant à ce dernier de recevoir automatiquement sa configuration d'un serveur DHCP.

Les périphériques peuvent être intégrés dans des réseaux existants sans que les paramètres de ces derniers ne soient connus. Il devient également plus facile d'accroître la disponibilité des périphériques et cela simplifie la gestion des adresses utilisées. Les péripériques peuvent être remplacés par du personnel de service, même si celui-ci n'a pas d'expérience technique ou ne connaît pas précisément les données.

La création de réseaux de plus grande taille devient un jeu d'enfant. Des réseaux de n'importe quelle taille peuvent être créés en attribuant de manière optimale les adresses IP. Il est possible de connecter directement des périphériques directement, même à des réseaux en constante expansion, sans clarification importante.




Les paramètres IP, qui sont envoyés par le serveur DHCP, sont utilisé par le serveur DHCP pendant un temps spécifique. Après ce temps, une nouvelle adresse va âtre demandée par le serveur (généralement le serveur fournit de nouveau la même adresse.)

## 4.2 DNS - Domain Name System

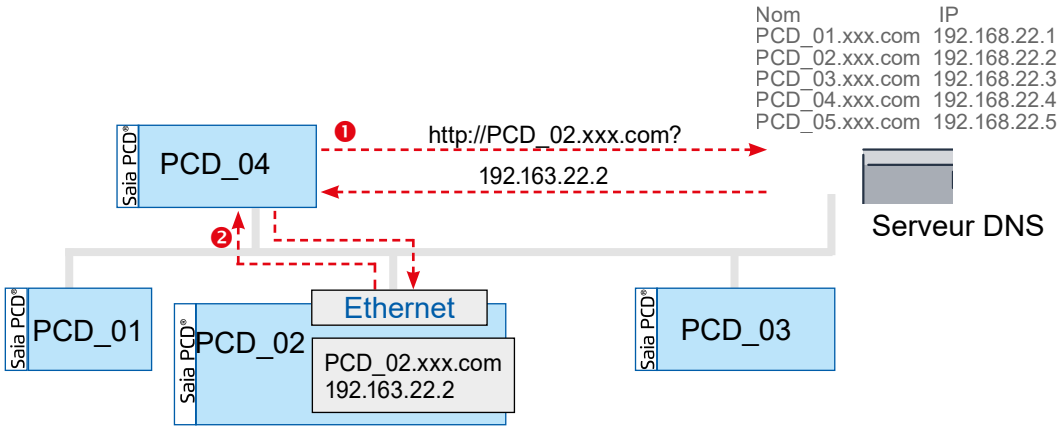
Accès aux contrôleurs grâce à l'attribution de noms d'hôte fixes. Il n'est pas nécessaire de connaître l'adresse IP du contrôleur de destination pour établir une communication entre deux contrôleurs. Le nom d'hôte suffit. Ce dernier peut être utilisé pour demander l'adresse IP à partir d'un serveur DNS.

Les périphériques n'utilisent plus d'adresses IP anonymes contenant peu d'informations. La structure et la disponibilité des réseaux individuels sont définies une fois et n'ont pas besoin d'être adaptés en fonction des changements apportés aux adresses IP disponibles. Les contrôleurs sont fournis préconfigurés et programmés. Les adresses IP sont uniquement transférées sur site et ne sont en général pas connues.



Les utilisateurs sur site n'ont besoin de connaître que les noms conviviaux des périphériques. Les systèmes sont par conséquent simplifiés et leur utilisation devient plus intuitive. Les noms d'hôte peuvent contenir des informations pertinentes et utiles, telles que l'emplacement ou la fonction du périphérique. Ils deviennent ainsi beaucoup plus intelligibles que les adresses IP. La documentation des réseaux comprenant de multiples poste peut être affichée plus clairement.

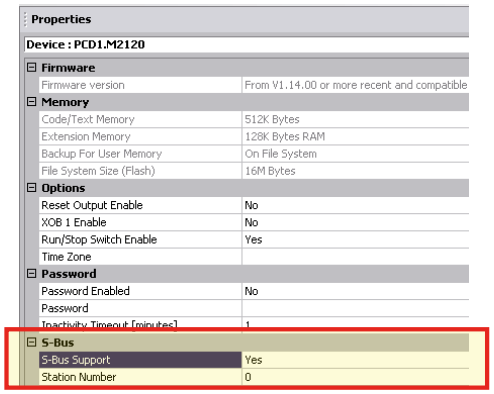
Il est possible de créer des réseaux relativement grands ou petits accessibles régulièrement depuis des emplacements différents. Les topologies de ces réseaux peuvent être ajustées en fonction des circonstances, sans que la disponibilité des postes ne soit restreinte. L'utilisation du nom des postes peut être maintenue pour le monde extérieur.



## 4.3 Activation de DHCP

### 4.3.1 Activation de la prise en charge de S-Bus

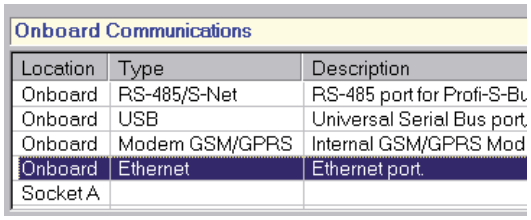
Il est nécessaire d'activer la prise en charge de S-Bus pour pouvoir utiliser n'importe quelle fonctionnalité IP sur un Saia PCD®.




4

### 4.3.2 Utilisation d'adresses IP fixes

Pour activer l'utilisation d'adresses IP fixes, il est nécessaire d'activer TCP/IP dans les paramètres de communications Ethernet embarquées :

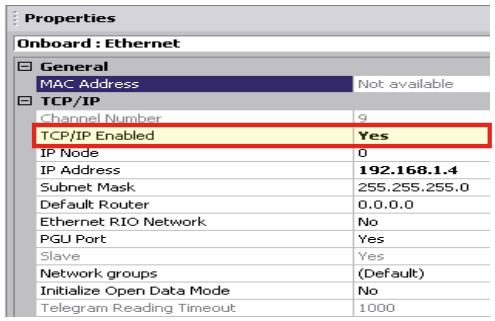



Changez « TCP/IP Enabled » en « Yes »

La passerelle maître n'est disponible que si des adresses IP fixes sont utilisées.

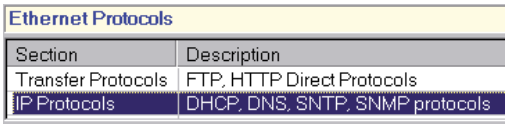
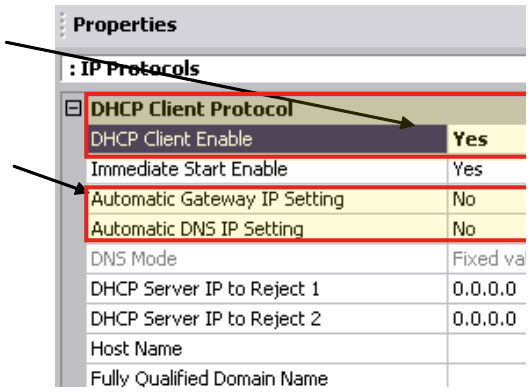
Si DHCP est activé, l'adresse IP statique est définie à 0.0.0.0 par le dispositif configurateur de la version PG5 2.0 SP2.

Si une nouvelle adresse IP en temps réel est écrit (au moyen d'une boîte de fonctions), cette adresse IP est utilisée. Des firmware 1.16.27, l'adresse IP doit être écraser à 0.0.0.0 par le programme utilisateur ou le périphérique configurateur.



### 4.3.3 Adressage IP dynamique

Ai-je besoin d'activer l'Ethernet embarqué ?

| | |
|---|---|
| Vous devez activer DHCP pour utiliser l'adressage IP dynamique.<br>TCP/IP enabled ➔ No |  |
| Au démarrage, le Saia PCD® recherche les paramètres du serveur DHCP à l'aide de commandes de diffusion générale.<br><br>Si vous utilisez un réseau comportant des routeurs, il peut être utile d'activer les paramètres Passerelle automatique et DNS. |  |

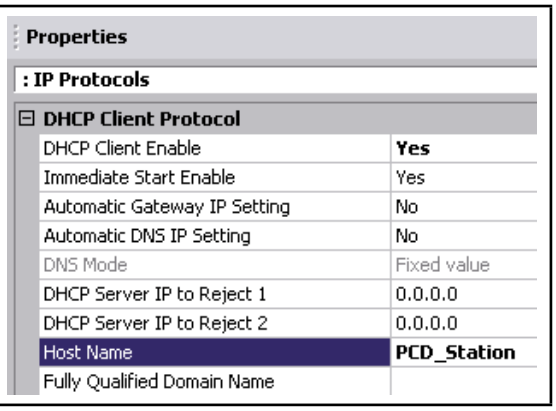
### 4.3.4 Vérification de la configuration IP avec Web-Connect

Comment puis-je vérifier la configuration IP reçue ? Une possibilité est d'utiliser Web-Connect et la commande de diagnostic Web sur l'interface CGI :

| | |
|---|---|
| 1. | Ouvrez le poste USB (par ex. Poste_USB) avec Web-Connect (cf. manuel de Web-Connect) |
| 2. | Connectez le Saia PCD® au PC à l'aide d'un câble USB |
| 3. | Ouvrez Internet Explorer et tapez la commande suivante :<br>http://localhost/station_USB/cgi-bin/readVal.exe?SYS-DHCP.AssignedIPAddr |
| 4. | La valeur retournée indiquera l'adresse IP reçue par le serveur DHCP. |

## 4.4 Utilisation de noms d'hôte et activation de DNS

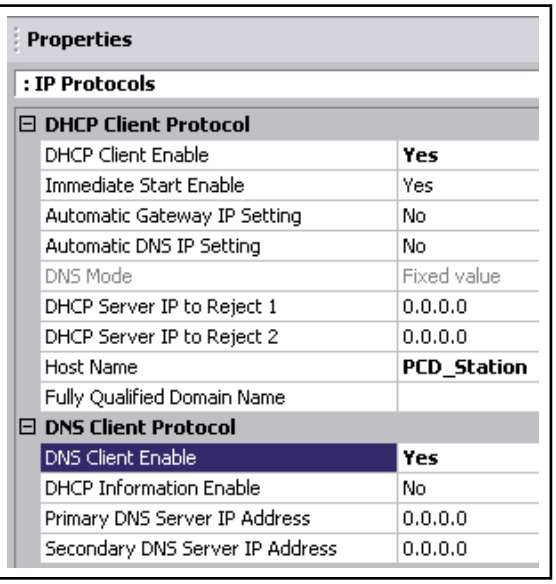
### 4.4.1 Attribution d'un nom d'hôte au Saia PCD®

| | |
|---|---|
| Vous devez définir un nom d'hôte pour accéder au Saia PCD® à l'aide de son nom. |  |

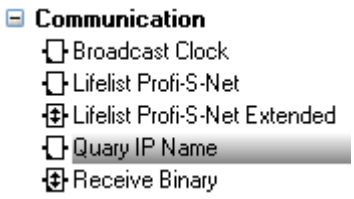
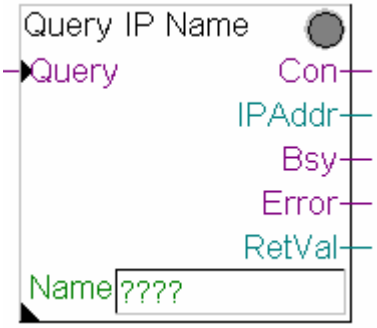


### 4.4.2 Utilisation de la résolution des noms DNS

Communication par nom d'hôte

| | |
|---|---|
| Activez le DNS<br><br>Définissez l'adresse IP du serveur DNS |  |

### 4.4.3 Utilisation de la résolution des noms avec des boîtes de fonctions

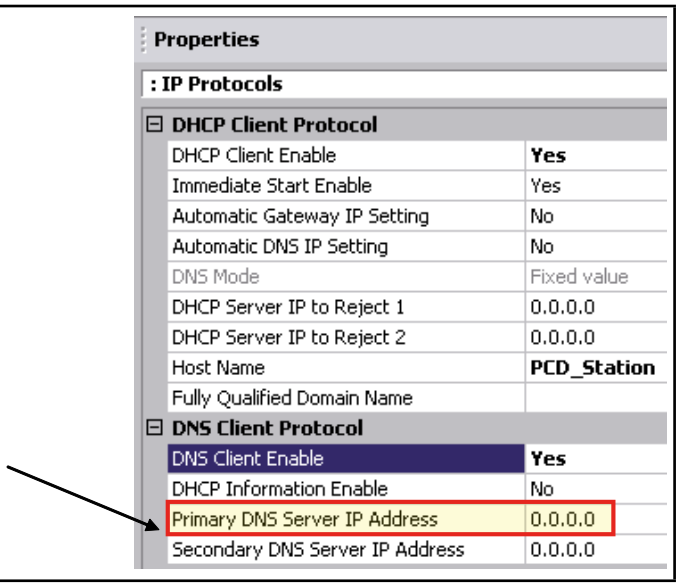
| | |
|---|---|
| Bibliothèque de boîtes de fonctions de communication |  |
| Cette boîte de fonctions émet une requête DNS afin d'obtenir l'adresse IP en fonction d'un nom d'hôte donné.<br><br>Le DNS doit être activé pour utiliser la boîte de fonctions « Query IP Name ». |  |

Cette boîte de fonction est exécutée par un transitoire positif sur l'entrée. L'adresse IP retournée peut être utilisée pour d'autres boîtes de fonctions utilisant des adresses IP

Appeler plusieurs « query F-Box » dans le même temps, ne fonctionne que si toutes les boîtes (F-Box) sont dans le même fichier-Fupla

### 4.4.4 Utilisation de la résolution des noms avec un routeur

La configuration du contrôleur Saia PCD® a besoin de l'adresse IP du routeur pour utiliser la résolution des noms DNS passant par le routeur.



## 4.5 Utilisation d'instructions CSF

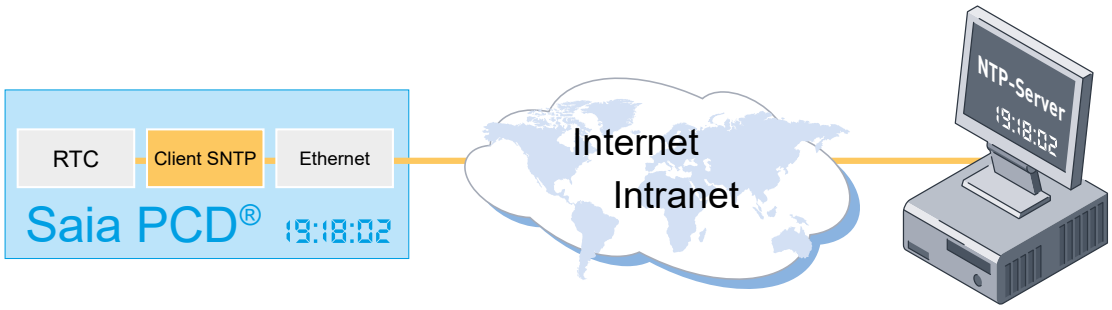
| | |
|---|---|
| S.DNS.QueryByName | Cette instruction CSF émet une requête DNS afin d'obtenir une adresse IP en fonction d'un nom d'hôte donné. |
| S.DNS.QueryByAddr | Cette instruction CSF émet une requête DNS afin d'obtenir un nom d'hôte en fonction d'une adresse IP donnée. |

Les détails sont décrits dans l'aide en ligne des bibliothèques PG5 2.0.

# 5 SNTP – Simple Network Time Protocol

## 5.1 Introduction

Le Simple Network Time Protocol est une norme permettant de synchroniser plusieurs appareils dans des réseaux IP. Ce protocole permet à des serveurs se trouvant sur Internet ou Intranet de transmettre l'heure réelle. Deux modes sont disponibles : diffusion individuelle point à point (le client SNTP initie une requête de temps) ou diffusion générale point à multipoint (les informations relatives à l'heure sont envoyées simultanément à tous les clients par un serveur NTP). La précision de l'heure obtenue avec la diffusion individuelle est d'environ 500 ms et avec la diffusion générale de 1 s. Des algorithmes intelligents garantissent que les différents temps d'exécution sont compensés par un réseau.
La synchronisation est réalisée pour plusieurs postes de réseau à la fois. Les horloges internes des postes de réseau individuels sont synchronisées de manière centrale à partir d'un serveur d'horloge. Une source de synchronisation unique dans le réseau suffit pour synchroniser automatiquement tous les autres périphériques. Etant donné que le protocole est une élément fixe du microprogramme des Saia PCD®, il peut être utilisé avec rapidité et simplicité.
La synchronisation des horloges internes devient un jeu d'enfant. Le personnel sur site n'a pas besoin de s'occuper de chaque poste du réseau. Des événements tels que le passage de l'heure d'été à l'heure d'hiver ont lieu automatiquement et simultanément sur tous les postes du réseau. Le protocole peut être utilisé sur des réseaux de grande taille pour synchroniser plusieurs postes de sorte que les événements enregistrés puissent également être stockés par ordre chronologique.



## 5.2 Activation de SNTP

Pour utiliser SNTP, configurez « SNTP Enable » sur « Yes ». Le serveur SNTP (ou NTP) peut être spécifié à l'aide de son adresse IP ou de son nom d'hôte.

| SNTP Protocol | |
|---|---|
| SNTP Enable | **Yes** |
| SNTP Mode | Use NTP server list |
| Immediate Start Enable | **Yes** |
| Start Delay | 0 |
| Maximum Delta Clock | 2000 |
| Server NTP 1 | 0.0.0.0 |
| Server NTP 2 | 0.0.0.0 |
| Time Zone | CET-01,CEST-02,M3.5.0/2,M10.5.0/2 |



Si Enable = 1, par défaut, une requête est effectuée avec le protocole SNTP environ toutes les 10 (+/- 0,5) secondes. L'intervalle des requêtes peut être modifié.

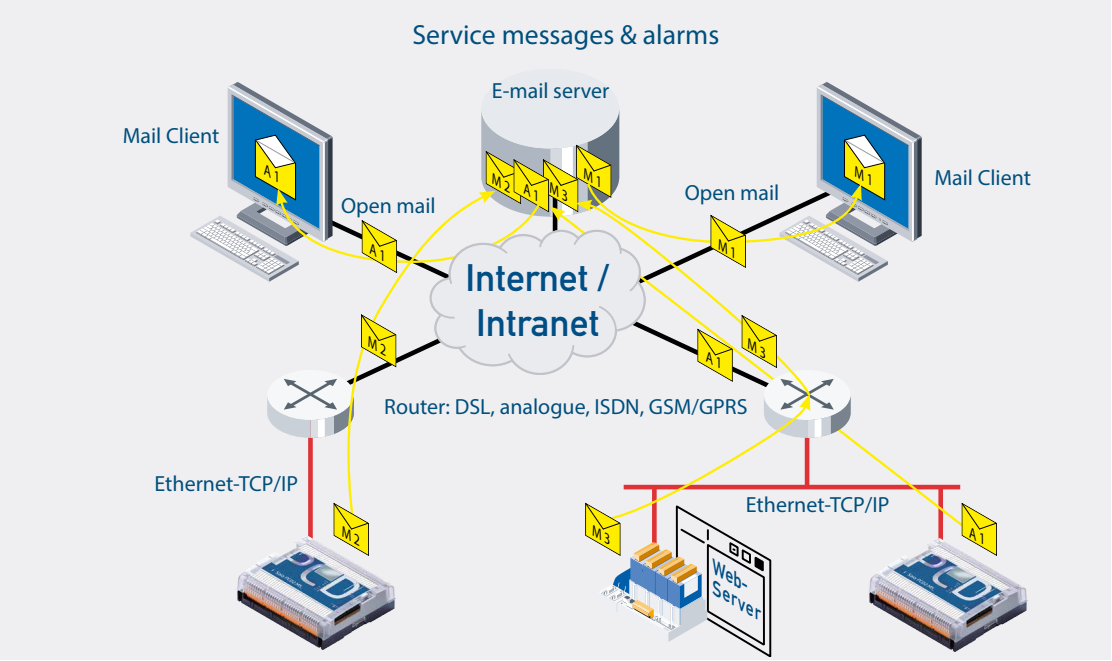
Le protocole SNTP ne fonctionne que via l'interface Ethernet. Les requêtes via l'interface PPP ne sont pas prises en charge.

Si un nom d'hôte URL est défini, le protocole du client DNS doit être activé.

# 6 E-mail

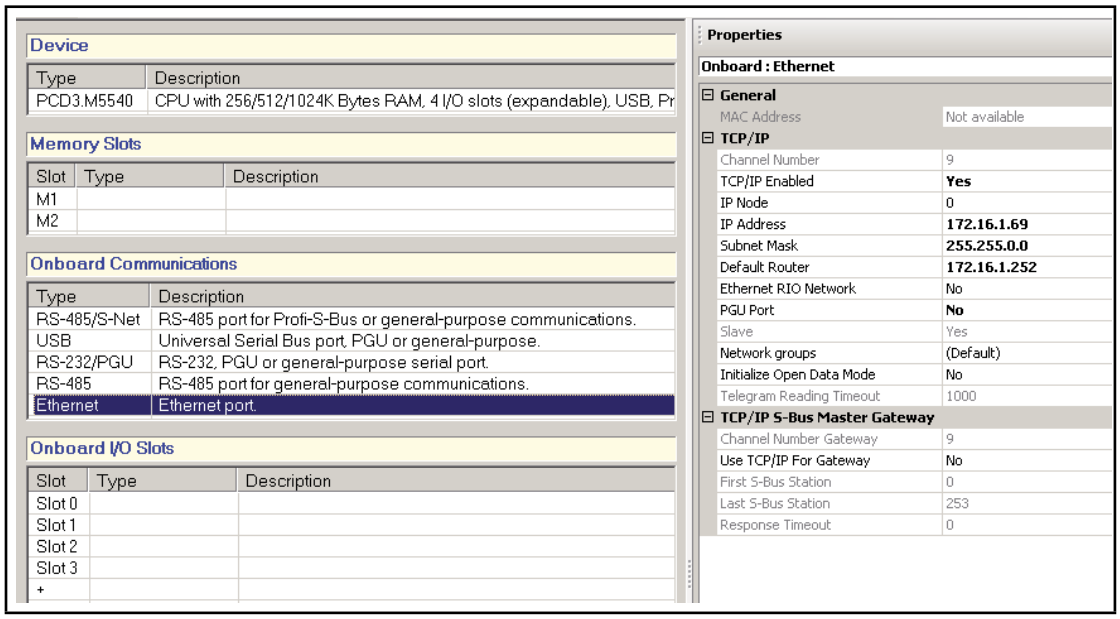
## 6.1 SMTP – Simple Mail Transfer Protocol

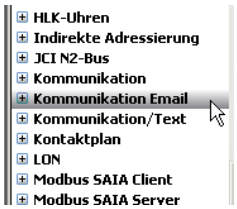
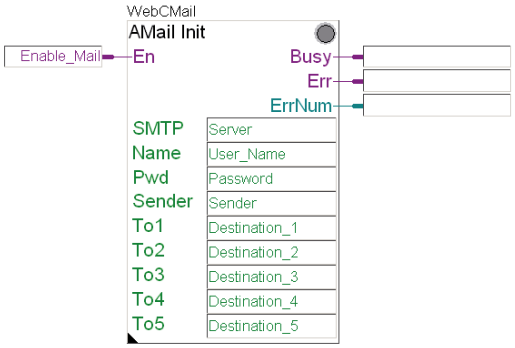
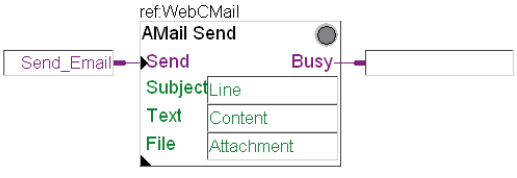
Grâce à la fonction de messagerie et au client SMTP (Simple Mail Transfer Protocol) intégral, les contrôleurs PCD peuvent transmettre à un serveur de messagerie les informations relatives aux processus et au système via l'interface Ethernet. Ainsi, les alarmes, messages de service, messages d'erreur ou toute information relative à un processus choisie peuvent être envoyés par e-mail au centre de contrôle et/ou au personnel de service. Des bibliothèques de boîtes de fonctions et de listes d'instructions sont disponibles afin d'intégrer simplement des fonctions de messagerie dans les programmes du PCD.



## 6.2 Utilisation de la fonctionnalité de messagerie avec des boîtes de fonctions

TCP/IP doit être configuré dans le configurateur matériel. Un routeur par défaut est nécessaire pour envoyer des e-mails. Votre support informatique sera en mesure de vous indiquer l'adresse du routeur par défaut si vous ne la connaissez pas (Ou par une configuration DHCP).




| | |
|---|---|
| Pour utiliser la fonctionnalité de messagerie sur votre PCD, utilisez la bibliothèque de boîtes de fonctions « Communication E-mail ». |  |
| Placez d'abord la boîte de fonctions Init pour activer la fonctionnalité de messagerie :<br>Le serveur SMTP est défini par son adresse IP. Pour utiliser la résolution des noms, veuillez vous reporter au chapitre DNS.<br><br>Si vous utilisez un adressage IP fixe, veuillez vérifier qu'il s'agit d'une adresse statique. |  |
| Envoyez l'e-mail avec ses fichiers joints aux adresses de destination sur un front positif. |  |

L'utilisation des caractères spéciaux $ et @ permet de créer des structures de texte dynamiques.

Pour plus de détails, veuillez vous reporter au manuel des listes d'instructions.

## 6.3 Systèmes Saia PCD® pris en charge

Systèmes PCD avec client SMTP : tous les PCD avec microprogramme NT.OS et PCD1.M135F655, PCD2.M150F655, PCD2.M170 avec PCD7.F655, PCD2.M480 avec PCD7.F655

Veuillez noter que toutes les améliorations TCP/IP, telles que DNS pour la résolution des noms, ne sont prises en charge que par les PCD dotés d'un microprogramme NT.OS.

## 6.4 List de Contrôle pour compte de messagerie

La liste de contrôle suivante vous aidera à vérifier si votre compte de messagerie est compatible avec la fonctionnalité de messagerie du PCD. D'après notre expérience, l'envoi d'e-mails ne dépend pas seulement de cette fonction, mais également des règles du FSI (fournisseur de services Internet). Les points suivants doivent être vérifiés afin de déterminer s'il sera possible d'envoyer des e-mails avant l'installation du PCD.

| | | |
|---|---|---|
| **MSA** (Mail Submission Agent) | | |
| Un MSA () est-il disponible ? | Il s'agit du serveur SMTP ou du serveur de messagerie qui recevra le message envoyé par le PCD (qui opère comme un MUA « Mail User Agent »). | ☐ yes<br>☐ no |
| **SMTP – Simple Mail Transfer Protocol** | | |
| Ce MSA prend-il en charge le protocole SMTP ? | Tous les MSA ne prennent pas en charge SMTP (il existe d'autres protocoles pour la livraison d'e-mails). | ☐ yes<br>☐ no |
| La méthode d'authentification « AUTH LOGIN » ou « AUTH PLAIN » est-elle acceptée ? | | ☐ yes<br>☐ no |
| **Compte** | | |
| Ai-je un compte sur le MSA correspondant ? | En général, il n'est possible d'envoyer des e-mails que si un compte correspondant est disponible. | ☐ yes<br>☐ no |
| **Joignable depuis le Saia PCD®** | | |
| Puis-je joindre ce serveur depuis mon PCD ? | Etant donné que SMTP est basé sur TCP/IP, une connexion au serveur est nécessaire. Si des pare-feux sont placés entre le PCD et le MSA, une règle permettant la connexion entre le PCD et le MSA doit exister.<br>Selon les règles du serveur SMTP, il est possible que ce serveur n'accepte que les e-mails provenant d'un réseau local. Certains FSI n'acceptent que les e-mails qui sont livrés à partir de leurs propres modems/connexions Internet (par ex. le fournisseur suisse Bluewin). | ☐ yes<br>☐ no |
| **Adresse du serveur de courrier électronique** | | |
| Quel est le nom d'hôte ou l'adresse IP du serveur ? | Nom d'hôte du serveur :<br>Adresse IP : | ☐ inconnu |
| L'adresse IP est nécessaire pour que le PCD sache où il doit se connecter pour envoyer des e-mails. Cette adresse IP doit être inscrite dans le champ « SMTP » de la boîte de fonctions « AMail Init ».<br>Si vous utilisez la résolution des noms, veuillez vous reporter au chapitre Protocole DNS. | | |
| **Port TCP connu** | | |
| Sur quel port TCP le MSA accepte-t-il les messages SMTP ? | Port : | ☐ inconnu |

| | | |
|---|---|---|
| En général, le port 25 est utilisé pour envoyer des e-mails mais certains serveurs utilisent parfois le port 587 (utilisé en général pour les utilisateurs authentifiés).<br>Veuillez configurer le port à l'aide du paramètre d'ajustement de la boîte de fonctions « SMTP server port ». | | |
| **Nom d'utilisateur, mot de passe** | | |
| Quel est le nom d'utilisateur et le mot de passe correspondant à l'envoi d'e-mails ? | utilisateur :<br>mot de passe : | ☐ inconnu |
| Saisissez votre nom d'utilisateur dans le champ « Name » de la boîte de fonctions. Le mot de passe doit être saisi dans la zone de texte fournie pour le champ « Pwd ». | | |
| **Adresse d'expéditeur valide** | | |
| Assurez-vous également que le texte entré pour le champ « Sender » de la boîte de fonctions est une adresse e-mail avec un nom de domaine correct (qui existe).<br>expéditeur : | | ☐ inconnu |
| Les entrées « To1 » à « To5 » de la boîte de fonctions correspondent aux destinations des e-mails. Ajoutez ici un texte qui comprend les adresses électroniques des destinataires des e-mails devant être envoyés. | | ☐ inconnu |

**Si vous répondez par l'affirmative à tous ces points, il est possible d'envoyer des e-mails.**

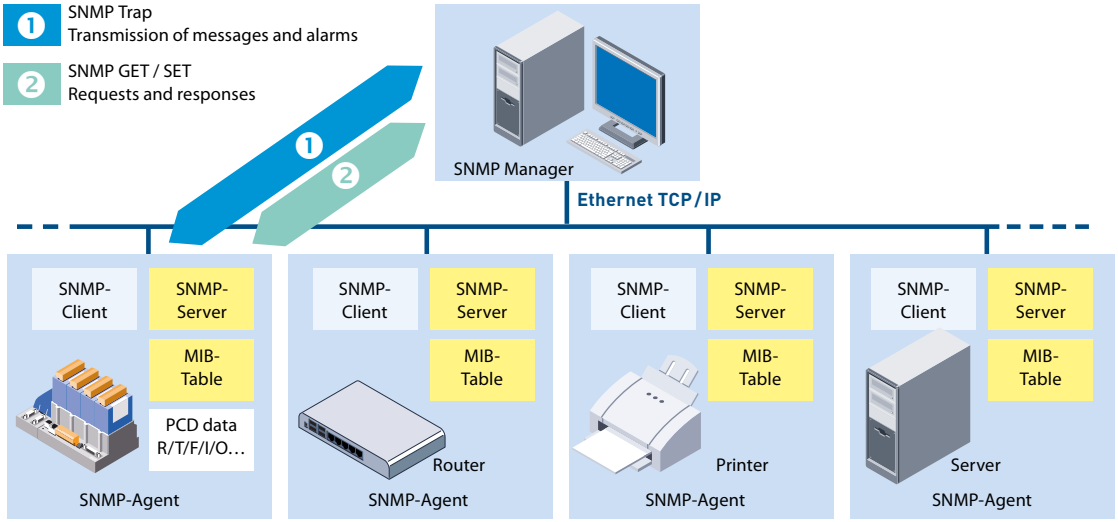
# 7 SNMP – Simple Network Management Protocol

## 7.1 Introduction

Le logiciel du superviseur SNMP est en général exécuté sur un serveur. Il contrôle et pilote les agents SNMP. Le superviseur SNMP lit et envoie les données de l'agent à l'aide de commandes permettant de récupérer les données d'état d'un élément du réseau (Get) et d'en modifier le paramétrage (Set). L'agent SNMP peut également envoyer des messages d'alarme (trap) au superviseur SNMP. Ceci permet, par exemple, de rapatrier directement les défauts.

Une Saia PCD® MIB a été définie pour les Saia PCD® sous SNMP. Elle renferme toutes les ressources qui font l'objet d'une requête SNMP et sont modifiables. Toutes les ressources du PCD sont accessibles (E/S, registres, indicateurs, blocs de données, etc.). Par contre, dans ce fichier MIB, le programmateur peut restreindre les droits d'accès à certaines zones.






Le protocole SNMP (Simple Network Management Protocol) a pour mission de surveiller et d'administrer des éléments du réseau (routeurs, serveurs et commutateurs) à partir d'un poste central. Son superviseur est en général un logiciel tournant sur un serveur, qui contrôle et pilote les agents SNMP. Ces derniers peuvent être n'importe quel dispositif accessible sur le réseau et prenant en charge SNMP. Avec le nouveau microprogramme, les Saia PCD® prennent en charge la fonctionnalité d'agent SNMP.

Les versions SNMP suivantes sont disponibles : v1, v2c, v3 (mécanisme de sécurité avec authentification MD5, chiffrement avec DES 56 bits). La norme v3 n'est pas encore très largement répandue. La version v2c reste, en principe, la norme actuelle. Les Saia PCD® prennent en charge la version v2c.

# 8 Diagnostic Web avancé

## 8.1 Introduction

La plupart des articles ou balises configurés pour les améliorations TCP/IP sont accessibles via l'interface Web CGI.

Veuillez vous reporter à la syntaxe d'accès de chaque protocole pour lire les valeurs de diagnostic.

L’accès par l’interface CGI est principalement fait pour lire des paramètres de configuration. Lors d’un accès d’écriture il doit être pris en considération que, si on débranche l’appareil, les valeurs de configuration peuvent être effacées et pour cette raison cet accès est recommandé uniquement pour des tests. La configuration correcte pour un fonctionnement permanent est garantie uniquement au moment d’une configuration à travers le Device Configurator de Saia PG5®.

Nous nous réservons également le droit d’apporter des modifications à la définition des Tags CGI.

## 8.2 Configuration PPP à l'aide de Web CGI

### 8.2.1 Syntaxe d'accès générique

Tous les éléments ou balises de configuration PPP sont accessibles via Web CGI avec la syntaxe suivante :

Valeurs de lecture :
http://hostname/cgi-bin/readVal.exe?<RegistreConfig>,<NomBalise>

| | |
|---|---|
| RegistreConfig | CFG-PPP, SYS-PPP |
| NomBalise | Correspond à la balise de configuration figurant dans le tableau des balises. |

### 8.2.2 Balises spéciales

Les balises suivantes ont un traitement spécifique :

- UpdateConfig : (CFG-PPP,UpdateConfig+1) : Mettre cette variable sur un (une seule fois) permet de valider la configuration actuelle, si et seulement si, le protocole PPP est en état INACTIF. Si elle est marquée comme valide, la configuration sera exécutée si elle est chargée à partir d'un fichier de configuration. Si un démarrage immédiat est requis, le protocole PPP sera lancé tel qu'il est configuré, après la temporisation définie. Le protocole PPP commence par exécuter les lignes de script PPP selon la procédure définie au paragraphe 2.2 ci-dessus.
- Save : (CFG-PPP,Save+1) : Mettre cette variable sur un (une seule fois) permet d'écrire la configuration actuelle dans un fichier. La configuration est également mise à jour (comme pour l'écriture de la balise UpdateConfig). Par défaut, le fichier « PPPConfig.txt » sera écrit et une entrée supplémentaire sera ajoutée dans le fichier « Config.txt ». Si la configuration enregistrée doit être sauvegardée dans une structure plate, la configuration actuelle sera sauvegardée directement dans le fichier « Config.txt ».
- Start : (CFG-PPP,Start+1) : Mettre cette variable sur un (une seule fois) permet de lancer immédiatement PPP en fonction de la configuration chargée. Le retard de démarrage n'est pas pris en compte. L'état de la connexion PPP peut être obtenu à l'aide des différentes balises d'état PPP.
- Stop : (CFG-PPP,Stop+1) : Mettre cette variable sur un (une seule fois) permet d'arrêter immédiatement PPP. Si l'indicateur de redémarrage est positionné, le protocole PPP sera automatiquement redémarré une fois le retard de temporisation spécifié écoulé. L'état de la connexion PPP peut être obtenu à l'aide des différentes balises d'état PPP.

### 8.2.3 Liste des balises PPP

Ce paragraphe présente la liste des balises utilisées par le module PPP. Le tableau comporte les informations suivantes :

- Nom ;
- Identifiant associé (utilisé dans l'appel de fonction CSF) (l'absence d'identifiant implique que la balise n'est pas accessible par le biais de l'instruction CSF) ;
- Balise de configuration ou pas (une balise de configuration est enregistrée dans le fichier de configuration associé) ;
- Type d'accès de la balise (lecture/écriture, lecture seule ou écriture seule) ;
- Sa valeur par défaut ;
- Eventuellement, sa valeur minimum et/ou maximum ;
- Définition et utilisation de la balise.



| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Enable | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) les fonctionnalités PPP. |
| DefaultRoute | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) l'interface PPP afin qu'elle soit l'itinéraire IP par défaut lorsqu'une adresse IP non accessible est fournie. |
| PeerAuth | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) l'authentification de l'homologue. Si elle est activée, le nom d'utilisateur / mot de passe doivent être fournis par l'homologue lors de l'établissement de la connexion. Cf. également le § 2.3 pour connaître le processus d'authentification. |
| Restart | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) la fonctionnalité PPP lorsque la connexion est fermée localement ou par l'hôte. Si elle est désactivée, la fonctionnalité d'établissement de la liaison PPP n'est pas redémarrée lorsque la connexion est fermée. |
| ImmStart | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) le lancement automatique de PPP en fonction des paramètres spécifiés. Le lancement automatique est effectué après l'écoulement du temps PPPStartDelay. Ce paramètre ne peut être configuré que dans le fichier de configuration et non pas par l'appel de fonction CSF. |
| PortID | RW | CFG | 1 | s.o. | Ce paramètre permet de définir sur quelle ligne série la connexion PPP sera établie. Les valeurs possibles sont les suivantes :<br><br>0, 1, 2, 3, 100, 101, 110, 111, 120, 121, 130, 131 |
| SerialPort | RO | SYS | s.o. | s.o. | Ce paramètre contient l'identifiant interne du port série une fois que la conversion de l'utilisateur a fourni le paramètre PortID. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Baudrate | RW | CFG | 115200 | s.o. | Ce paramètre permet de définir le débit en bauds devant être utilisé pour la communication PPP. Les valeurs possibles sont les suivantes :<br><br>2 400, 4 800, 9 600, 19 200, 38 400, 57 600, 115 200 |
| Mode | RW | CFG | 1 | 1 (SVR)<br>2 (CLI) | Ce paramètre définit le type de connexion qui sera établie entre les deux homologues.<br><br>Spécifier une connexion serveur signifie que le protocole PPP attendra que le partenaire établisse une connexion.<br><br>Spécifier une connexion client signifie que le protocole PPP initiera la connexion avec l'homologue. |
| StartDelay | RW | CFG | 5 | 0 / 60 | Ce paramètre définit le nombre de secondes devant s'écouler avant que le protocole PPP démarre. Ce paramètre ne peut être configuré que dans le fichier de configuration et non pas par l'appel de fonction CSF. |
| LocalAddress | RW | CFG | 0 | s.o. | Ce paramètre définit l'adresse IP devant être proposée pour l'adresse locale au cours de la négociation IPCP entre les deux homologues. Si 0 est spécifié, l'adresse locale sera fournie par l'homologue.<br><br>Normalement, une adresse IP doit être spécifiée en mode serveur alors qu'il n'est pas nécessaire de spécifier une adresse locale en mode client. Ce n'est toutefois pas toujours le cas.<br><br>L'adresse spécifiée peut ne pas être celle utilisée après une négociation IPCP réussie. |
| RemoteAddress | RW | CFG | 0 | s.o. | Ce paramètre définit l'adresse IP devant être proposée pour l'adresse du partenaire au cours de la négociation IPCP entre les deux homologues. Si 0 est spécifié, l'adresse du partenaire sera fournie par l'homologue.<br><br>Normalement, une adresse IP doit être spécifiée en mode serveur alors qu'il n'est pas nécessaire de spécifier une adresse de partenaire en mode client. Ce n'est toutefois pas toujours le cas.<br><br>L'adresse spécifiée peut ne pas être celle utilisée après une négociation IPCP réussie. |
| RemoteAuthUsername | RW | CFG | “” | s.o. | Ce paramètre contient le nom d'utilisateur qui sera utilisé pour authentifier le Saia PCD® auprès de l'hôte à distance. Reportez-vous au § 2.3 pour obtenir une description de l'authentification. La longueur maximale du nom d'utilisateur est 31 caractères. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| RemoteAuth-Passwd | RW | CFG | “” | s.o. | Ce paramètre contient le mot de passe qui sera utilisé pour authentifier le Saia PCD® auprès de l'hôte à distance. Reportez-vous au § 2.3 pour obtenir une description de l'authentification. La longueur maximale du mot de passe est 31 caractères. |
| PPPState | RO | SYS | | s.o. | Cette valeur indique l'état actuel du PPP :<br><br>1: Aucun périphérique PPP n'a été configuré sur ce système.<br>2: Le protocole PPP est en mode inactif.<br>3: Le protocole PPP est en train de lire le script de démarrage.<br>4: Le script a été exécuté. La connexion est en attente d'établissement.<br>5: Le protocole PPP est opérationnel.<br>Remarque : Lorsqu'elle est utilisée comme balise Web CGI, la valeur est directement convertie en une chaîne pertinente.<br><br>Remarque : La balise PPPState actuelle est accessible par le biais de l'appel de fonction CSF S.PPP.State (4ème paramètre).<br><br>Remarque : Les valeurs actuelles sont également décrites dans le fichier INC relatif au PG5, par ex. S.PPP.PPPState.STATE_SCRIPTING. |
| PPPLink | RO | SYS | - | s.o. | Indique l'état actuel de la liaison PPP. Les valeurs suivantes sont fournies :<br><br>1: Couche de liaison physique non prête.<br>2: Phase d'établissement de la liaison.<br>3: Phase de protocole de couche réseau.<br>4: Phase d'authentification.<br>5: Quelque chose impliquant une déconnexion survient.<br>6: La négociation est réussie.<br>Remarque : Lorsqu'elle est utilisée comme balise Web CGI, la valeur est directement convertie en une chaîne pertinente complète.<br><br>Remarque : La balise PPPLink actuelle est accessible par le biais de l'appel de fonction CSF S.PPP.State (1er paramètre).<br><br>Remarque : Les valeurs actuelles sont également décrites dans le fichier INC relatif au PG5, par ex. S.PPP.LNKValue.LINK_DOWN. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| PPPEvt | RO | SYS | - | s.o. | Indique les événements qui surviennent sur la liaison PPP. Les valeurs suivantes sont fournies :<br><br>1: La négociation LCP débute.<br>2: La négociation LCP est réussie.<br>3: L'authentification est réussie.<br>4: La négociation LCP ou l'authentification a échoué.<br>5: La couche LCP ferme la connexion.<br>6: La liaison est interrompue.<br>7: La négociation IPCP débute.<br>8: La couche IPCP est configurée et l'interface est opérationnelle.<br>9: La configuration de la couche IPCP a échoué.<br>10: Rapport d'état de l'authentification PAP.<br>11: Etat de l'authentification CHAP (MD5 et MS).<br>12: Etat de l'authentification MSCHAP.<br>Remarque : Lorsqu'elle est utilisée comme balise Web CGI, la valeur est directement convertie en une chaîne pertinente complète.<br><br>Remarque : La balise PPPEvt actuelle est accessible par le biais de l'appel de fonction CSF S.PPP.State (2ème paramètre).<br><br>Remarque : Les valeurs actuelles sont également décrites dans le fichier INC relatif au PG5, par ex. S.PPP.PPPEvt.EVT_LCP_SUCCESS. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| PPPSubE-vent | RO | SYS | - | s.o. | Ce paramètre apporte des informations supplémentaires sur la cause de l'échec pour les valeurs PPPEvt 4, 5 et 6 :<br><br>1: L'authentification a échoué.<br>2: Une requête d'arrêt a été reçue de l'homologue.<br>3: Le nombre maximum de requêtes d'écho a été envoyé sans réponse de la part de l'homologue.<br>4: La liaison physique est déconnectée.<br>5: L'application a appelé xxx.<br>6: Un rejet du protocole a été reçu.<br>7: Le nombre maximum de requêtes de configuration a été envoyé. Soit la négociation ne converge pas, soit l'homologue ne répond pas.<br>8: La configuration de la couche IPCP a échoué.<br>9: L'option nombre magique est activée et une ligne fonctionnant en boucle a été détectée.<br>Ce paramètre apporte des informations supplémentaires pour les valeurs PPPEvt 10 ou 11 :<br><br>10: L'authentification de l'hôte local a échoué.<br>11: L'authentification de l'hôte local a réussi.<br>12: L'authentification de l'homologue a échoué.<br>13: L'authentification de l'homologue a réussi.<br>14: Aucune réponse de la part de l'homologue.<br>Remarque : La balise LinkSubEvent actuelle est accessible par le biais de l'appel de fonction CSF S.PPP.State (3ème paramètre). |
| UseDefaultS-cript | RW | CFG | 1 | s.o. | Deux scripts de démarrage sont disponibles pour la connexion client ou serveur lorsqu'une connexion directe est établie entre un Saia PCD® et un PC (fonctionnant sous Win XP). En activant cette balise, le script par défaut correspondant au type de connexion est sélectionné et lu sur l'interface.<br><br>Si elle est désactivée, aucun script n'est fourni. Des lignes de scripts (le cas échéant) doivent être entrées (cf. § 2.2.4 ci-dessous). |
| UseModem | RW | CFG | 0 | s.o. | Mettre cette variable sur 1 permet de vérifier les signaux du modem sur la ligne série, en particulier les signaux DCD et DSR utilisés pour contrôler la déconnexion du modem. Il est nécessaire d'activer ces contrôles si un modem est utilisé.<br>Mettre cette variable sur 0 désactive le contrôle des lignes de modem, par ex. lorsqu'une connexion directe est utilisée. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| MSLa | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLb | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLc | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLd | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLe | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLf | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLg | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLh | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLi | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLj | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| MSLj | RW | CFG | - | s.o. | Cf. § 2.2 ci-dessous. |
| EnaIPFW | RW | CFG | 0 | - | Mettre cette variable sur 1 permet la transmission interne d'un message IP d'une interface (par ex. PPP) à une autre (par ex. eth0). Cette configuration requiert une bonne connaissance du routage entre des équipements différents.<br><br>Par défaut, le mécanisme de transmission IP est désactivé. |
| EnaEReq | RW | CFG | 0 | - | Mettre cette variable sur 1 permet d'envoyer un message de requête d'écho sur PPP. Elle peut être utilisée si une interface ne prend pas en charge les signaux DSR / DCD mais il faut quand même vérifier la ligne pour savoir si le partenaire est présent ou non. Les requêtes d'écho sont envoyées toutes les 10 secondes et, si aucune réponse n'est reçue après 5 tentatives, l'interface PPP est fermée (50 secondes environ).<br>Par défaut, l'envoi d'une requête d'écho est désactivé. |
| CheckDCD | RW | CFG | 0 | - | Mettre cette variable sur 1 permet de contrôler les signaux DCD avant de lancer le protocole PPP mais après que les scripts du modem aient été lus. Le temps écoulé avant la réception du signal DCD peut être configuré à l'aide du paramètre DCDTimeout (cf. ci-dessous).<br><br>Par défaut, le paramètre CheckDCD est désactivé.<br>Remarque : Les signaux DCD/DSR sont contrôlés en même temps que le paramètre UseModem. Si l'un des signaux est interrompu, la connexion PPP est arrêtée. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| DTRPulse | RW | CFG | 0 | - | Mettre cette variable sur 1 permet de libérer le signal DTR pendant une seconde avant que le script PPP soit lu. Le signal DSR est vérifié une fois que le signal DTR est à nouveau à l'état haut. Si le signal DSR est toujours à l'état bas après 5 secondes, la connexion PPP est abandonnée. Cette option n'est prise en compte que si le paramètre UseModem est TRUE.<br>S'il est configuré et que DTRPulse ne l'est pas, le signal DTR est à l'état haut, une petite boucle d'attente est exécutée et le signal DSR est contrôlé. S'il est à l'état bas, la connexion PPP est abandonnée.<br><br>Si le paramètre UseModem est à l'état bas, le signal DTR est à l'état haut mais le signal DSR n'est pas contrôlé. |
| LastError | RO | SYS | - | s.o. | La dernière erreur survenue lors du traitement de PPP est stockée dans cette variable. |
| ERTInterval | RW | CFG | 5 | 1..3600 | Ceci permet de définir l'intervalle entre 2 requêtes d'écho (lorsque la variable EnaEReq a été définie sur 1). La valeur par défaut est 5 secondes, la valeur maximale est 1 heure. |
| ERNumber | RW | CFG | 6 | 1..100 | Ceci permet de définir le nombre de requêtes d'écho qui sont envoyées sans réponse avant de fermer la connexion (lorsque la variable EnaEReq a été définie sur 1). La valeur par défaut est 6 requêtes, la valeur maximale est 100.<br><br>L'intervalle multiplié par le nombre donne le temps total avant que la déconnexion prenne effet. |
| DCDTimeout | RW | CFG | 1000 | 0 .. 1h | Lorsque le paramètre CheckDCD est mis à 1, le signal DCD est contrôlé avant de lancer le protocole PPP. Ce paramètre définit le temps pendant lequel le signal est contrôlé avant qu'une erreur soit retournée.<br><br>Lorsque la valeur du paramètre est 0, le contrôle est réalisé indéfiniment.<br><br>Le temps maximal est 1 heure exprimée en millisecondes. |
| ALAddress | RO | SYS | - | s.o. | Ce paramètre correspond à l'adresse IP réelle attribuée à la connexion PPP. Elle peut différer de celle spécifiée ou si aucune adresse n'a été spécifiée (paramètre LocalAddress). |
| ARAddress | RO | SYS | - | s.o. | Ce paramètre correspond à l'adresse IP réelle du partenaire de la connexion PPP. |

## 8.3 Diagnostic DHCP via l'interface Web CGI

### 8.3.1 Syntaxe d'accès

Toutes les balises de configuration DHCP et DNS sont accessibles via l'interface Web CGI.
L'accès a la syntaxe suivante :

Valeurs de lecture :
http://hostname/cgi-bin/readVal.exe?<RegistreConfig>,<NomBalise>

| | |
|---|---|
| RegistreConfig | CFG-DHCP, SYS-DHCP<br><br>CFG-DNS, SYS-DNS |
| NomBalise | Correspond à la balise de configuration figurant dans le tableau des balises. |

### 8.3.2 Balises spéciales



Les balises suivantes ont un traitement spécifique :

- UpdateConfig : [CFG-DHCP,UpdateConfig+1] [CFG-DNS,UpdateConfig+1] : Mettre cette variable sur un (une seule fois) permet de valider la configuration actuelle. Si elle est marquée comme valide, la configuration sera exécutée si elle est chargée à partir d'un fichier de configuration.
- Save : [CFG-DHCP,Save,1], [CFG-DNS,Save,1] : Mettre cette variable sur un (une seule fois) permet d'écrire la configuration actuelle dans un fichier. La configuration est également mise à jour (comme pour l'écriture de la balise UpdateConfig).
- Start : [CFG-DHCP,Start+1] : Mettre cette variable sur un (une seule fois) permet de lancer immédiatement DHCP en fonction de la configuration chargée. L'état du protocole DHCP peut être obtenu à l'aide des différentes balises d'état DHCP.
- Stop : (CFG-DHCP,Stop+1) : Mettre cette variable sur un (une seule fois) permet d'arrêter immédiatement DHCP. L'état du protocole DHCP peut être obtenu à l'aide des différentes balises d'état DHCP.

Veuillez noter qu'arrêter DHCP déconfigure l'interface IP et ne permet PAS d'y accéder via la réseau Ethernet.

### 8.3.3 Liste des balises DHCP et DNS

Ce paragraphe présente la liste des balises utilisées par les modules DHCP et DNS. Le tableau comporte les informations suivantes :

- Nom ;
- Balise de configuration ou pas (une balise de configuration est enregistrée dans le fichier de configuration associé) ;
- Type d'accès de la balise (lecture/écriture, lecture seule ou écriture seule) ;
- Sa valeur par défaut ;
- Eventuellement, sa valeur minimum et/ou maximum ;
- Définition et utilisation de la balise.

Le premier tableau contient les informations correspondant à DHCP et le second tableau les informations correspondant à DNS.

### 8.3.4 Tableau des balises DHCP

| Fichier Web CGI | | Type | Par déf. | Min./ max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Enable | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) les fonctionnalités DHCP. |
| Enabled | RO | SYS | - | - | Indique si le protocole DHCP est activé (1) ou désactivé (0). |
| ImmStart | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) le lancement immédiat de DHCP lorsque le Saia PCD® est sous tension. |
| SetGateway | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) la configuration automatique de l'adresse IP de la passerelle si ces informations sont reçues du serveur DHCP. |
| SetDNSInfo | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) la configuration automatique des informations concernant le DNS si ces informations sont reçues du serveur DHCP. L'utilisation de cette option permet d'éviter la configuration manuelle du DNS présentée dans le tableau des balises suivant. |
| Mode | RW | CFG | 0 | 0 | Réservé pour une extension future. Doit être mis sur 0. |

| Fichier Web CGI | | Type | Par déf. | Min./ max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| CurState | RO | SYS | - | - | Ce paramètre renvoie l'état actuel de la liaison DHCP.<br><br>0: (INIT) : DHCP n'est pas encore lancé.<br>1: (SELECTING) : DHCP sélectionne le serveur DHCP.<br>2: (REQUESTING) : DHCP demande les informations relatives au serveur DHCP.<br>3: (BOUND) : DHCP a reçu toutes les informations.<br>4: (RENEWING) : DHCP remplace les informations relatives au serveur DHCP.<br>5: (REBINDING) : DHCP établit une nouvelle liaison avec un serveur DHCP.<br>6: (INIT_REBOOT) : DHCP recommence sa séquence d'initialisation.<br>7: (REBOOTING) : DHCP redémarre pour obtenir les informations concernant le nouveau serveur DHCP.<br>Grâce à l'interface Web, le texte est écrit directement dans la page. |
| RejSVRa<br>RejSVRb<br>RejSVRc<br>RejSVRd | RW | CFG | 0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0 | s.o. | Une liste des serveurs DHCP devant être rejetés peut être spécifiée à l'aide de ces 4 paramètres. Si aucun serveur n'est indiqué, le premier serveur DHCP qui répondra sera utilisé pour la configuration IP. |
| AssignedIPAddr | RO | SYS | - | - | Ce paramètre indique l'adresse IP attribuée reçue du serveur DHCP. |
| AssignedSVRAddr | RO | SYS | - | - | Ce paramètre indique l'adresse IP du serveur DHCP sélectionné. |
| AssignedDNSSVRa | RO | SYS | - | - | Ce paramètre indique l'adresse IP du serveur DNS primaire reçue par le serveur DHCP. Si la balise SetDNSInfo est définie, ces informations seront utilisées pour les requêtes DNS. |
| AssignedDNSSVRb | RO | SYS | - | - | Ce paramètre indique l'adresse IP du serveur DNS secondaire reçue par le serveur DHCP. Si la balise SetDNSInfo est définie, ces informations seront utilisées pour les requêtes DNS. |
| AssignedGTWAddr | RO | SYS | - | - | Ce paramètre indique l'adresse IP de la passerelle reçue par le serveur DHCP. Cette adresse sera utilisée comme passerelle par défaut si la balise SetGateway est définie. |
| AssignedSNTPAddr | RO | SYS | - | - | Ce paramètre indique l'adresse IP du SNTP reçue par le serveur DHCP. Il peut être utilisé pour configurer le serveur SNTP mais ce n'est pas automatique (SNTP sera configuré séparément). |
| AssignedIPMask | RO | SYS | - | - | Ce paramètre indique le masque de réseau IP reçu par le serveur DHCP. Il est défini et utilisé immédiatement. |
| Hostname | RW | CFG | “” | s.o. | Ce paramètre indique le nom de l'hôte devant être configuré. Les informations sont transmises au serveur DHCP et, éventuellement, au serveur DNS associé. Elles peuvent ensuite être utilisées pour établir une connexion directe entre des Saia PCD® ou entre un PC et un PCD. |
| AssignedDomainName | RO | SYS | “” | s.o. | Ce paramètre indique le nom de domaine reçu par le serveur DHCP. |

| Fichier Web CGI | | Type | Par déf. | Min./ max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| FQDN | RW | CFG | “” | s.o. | Ce paramètre peut être configuré afin de spécifier le nom de domaine complet qui sera associé au nom d'hôte. Normalement, cette balise peut rester vide. |
| UpdateConfig | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet de valider la configuration actuelle. Si cette valeur est définie, le protocole DHCP peut être lancé immédiatement en fonction des balises de configuration définies. |
| Start | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet d'initier une connexion au serveur DHCP à l'aide du jeu de paramètres actuel. |
| Stop | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet d'arrêter le traitement DHCP actuel. Cet arrêt déconfigure l'adresse IP du Saia PCD®. Il ne pourra pas être joint sur le réseau Ethernet par la suite. |
| Save | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet d'écrire les paramètres de configuration actuels dans le fichier spécifique à DHCP. Reportez-vous au chapitre 4 pour obtenir des détails sur le(s) fichier(s) de configuration. |



### 8.3.5 Tableau des balises DNS

| Fichier Web CGI | | Type | Par déf. | Min./ max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Enable | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) les fonctionnalités de résolveur DNS. |
| UseDHC-PInfo | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) l'utilisation des informations reçues par DHCP pour les fonctionnalités DNS. |
| State | RO | SYS | 0 | s.o. | Mettre sur 1 si les fonctionnalités DNS ont été activées. SINON, mettre sur 0. |
| SVRa | RW | CFG | 0.0.0.0 | s.o. | Ce paramètre définit l'adresse IP du serveur DNS primaire devant être utilisé pour tenter de résoudre une adresse IP. |
| SVRb | RW | CFG | 0.0.0.0 | s.o. | Ce paramètre définit l'adresse IP du serveur DNS secondaire devant être utilisé pour tenter de résoudre une adresse IP. |
| Update-Config | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet de valider la configuration actuelle. |
| Save | WO | SYS | s.o. | s.o. | Attribuer un 1 à cette balise via l'interface Web CGI permet d'écrire les paramètres de configuration actuels dans le fichier spécifique à DNS. Reportez-vous au chapitre 4 pour obtenir des détails sur le(s) fichier(s) de configuration. |

## 8.4 Diagnostic SNTP via l'interface Web CGI

### 8.4.1 Syntaxe d'accès

Toutes les balises de configuration SNTP sont accessibles via l'interface Web CGI. L'accès a la syntaxe suivante :

Valeurs de lecture :
http://hostname/cgi-bin/readVal.exe?<RegistreConfig>,<NomBalise>

| | |
|---|---|
| RegistreConfig | CFG-SNTP, SYS-SNTP |
| NomBalise | Correspond à la balise de configuration figurant dans le tableau des balises. |

### 8.4.2 Balises spéciales

Les balises suivantes ont un traitement spécifique :

- UpdateConfig (CFG-SNTP,UpdateConfig+1) : Mettre cette variable sur un (une seule fois) permet de valider la configuration actuelle, si et seulement si, le protocole SNTP est en état INACTIF. Si elle est marquée comme valide, la configuration sera exécutée si elle est chargée à partir d'un fichier de configuration. Si un démarrage immédiat est requis, le protocole SNTP sera lancé tel qu'il est configuré après la temporisation définie.
- Save (CFG-SNTP,Save+1) : Mettre cette variable sur un (une seule fois) permet d'écrire la configuration actuelle dans un fichier. La configuration est également mise à jour (comme pour l'écriture de la balise UpdateConfig). Par défaut, le fichier « SNTPConfig.txt » sera écrit et une entrée supplémentaire sera ajoutée dans le fichier « Config.txt ». Si la configuration enregistrée doit être sauvegardée dans une structure plate, la configuration actuelle sera sauvegardée directement dans le fichier « Config.txt ».
- Start : (CFG-SNTP,Start+1) : Mettre cette variable sur un (une seule fois) permet de lancer immédiatement SNTP en fonction de la configuration chargée. Le retard de démarrage n'est pas pris en compte. L'état du traitement SNTP peut être obtenu à l'aide de la balise d'état SNTP.
- Stop : (CFG-SNTP,Stop+1) : Mettre cette variable sur un (une seule fois) permet d'arrêter immédiatement SNTP. L'état du traitement SNTP peut être obtenu à l'aide de la balise d'état SNTP.

### 8.4.3 Liste des balises SNTP

Ce paragraphe présente la liste des balises utilisées par le module SNTP. Le tableau comporte les informations suivantes :

- Nom ;
- Balise de configuration ou pas (une balise de configuration est enregistrée dans le fichier de configuration associé) ;
- Type d'accès de la balise (lecture/écriture, lecture seule ou écriture seule) ;
- Sa valeur par défaut ;
- Eventuellement sa valeur minimum et/ou maximum ;
- Définition et utilisation de la balise.

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Enable | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) les fonctionnalités SNTP. |
| Enabled | RO | SYS | - | - | Affiche l'état actuel de SNTP. |
| ImmStart | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) la fonctionnalité SNTP devant être lancée immédiatement (après un temps défini) après l'analyse syntaxique de la configuration. |
| Mode | RW | CFG | 0 | 0 / 1 | Spécifier un 0 signifie que le module SNTP utilisera la liste de serveurs NTP spécifiés et enverra une requête NTP afin de recevoir l'heure. Le premier serveur qui répondra à cette requête sera utilisé pour la synchronisation.<br><br>Spécifier un 1 signifie que le module SNTP écoutera les messages à diffusion générale depuis n'importe quel serveur NTP. Le premier serveur NTP qui enverra une requête de diffusion générale sera utilisé pour la synchronisation. |
| StartDelay | RW | CFG | 0 | s.o. | Ce paramètre définit le nombre de secondes devant s'écouler avant que SNTP démarre. |
| ClockDelta | RW | CFG | 2000<br><br>ms) | 100 (ms) 3 600(sec) | Ce paramètre définit le delta maximum entre l'horloge interne et l'heure reçue. L'horloge interne est mise à jour dès que le delta est dépassé. |
| SVRa<br>SVRb<br>SVRc<br>SVRd | RW | CFG | 0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0 | s.o. | Fournit les adresses IP des serveurs de nom (voir ci-dessous). |
| SVRNamea<br>SVRNameb<br>SVRNamec<br>SVRNamed | RW | CFG | 0.0.0.0<br>0.0.0.0<br>0.0.0.0<br>0.0.0.0 | s.o. | Fournit la liste des serveur de nom utilisé avec le mode 0. Jusqu'à 4 serveurs peuvent être spécifiés.<br>Si un SVRName est spécifié, la valeur correspondante SVR sera mis à jour.<br>Le SVRNamex pouvez spécifier une adresse IP (exprimé sous forme de chaîne, par exemple 182.75.22.198) ou un nom d'hôte.<br>Si un nom d'hôte est spécifié (par exemple hostname:www.ntp.srv.ch), une configuration DNS est également spécifiée. |
| UsedServer | RO | SYS | - | s.o. | Indique le serveur NTP réellement utilisé lorsque la synchronisation a été initialisée. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| TimeZone | OUI | | RW | s.o. | Un fuseau horaire peut être spécifié dans la définition du SNTP. L'heure SNTP reçue est toujours fournie en UTC. Il est possible d'indiquer le fuseau horaire local afin que l'heure soit correctement affichée.<br><br>Le format du fuseau horaire est défini comme suit :<br>`<NomFH>[+-]HH[:MM]` par ex. CET-01:00 ou CET-1<br><br>L'heure d'hiver peut être spécifiée en indiquant le second fuseau horaire et les dates auxquelles l'heure doit être changée.<br>`<NomFH2>[+-]HH[:MM]` par ex. CCET-2:00 ou CCET-2<br><br>`M<mois>.<semainedumois>.<jourdelasemaine>/HH[:MM]` par ex. M3.5.0/02:00<br><br>Les 4 définitions de champ doivent être spécifiées dans une chaîne, chaque champ étant séparé par une « , ».<br>Exemple<br><br>`CET-01,CEST-02,M3.5.0/2,M10.5.0/2`<br><br>Définir 5 comme semaine du mois indique qu'il s'agit de la dernière semaine du mois.<br>Définir 0 comme jour de la semaine indique qu'il s'agit d'un dimanche.<br>Les minutes peuvent être omises.<br>Pour spécifier un second fuseau horaire, les deux dates de changement d'heure doit être définies.<br>Il n'est pas nécessaire de spécifier un second fuseau horaire.<br>La valeur par défaut est le 1 présenté en exemple : heure d'été de l'Europe centrale (dimanche, dernière semaine de mars à 2h00 (avancée à 3h00) et dimanche, dernière semaine d'octobre à 3h00 (retardée à 2h00)). |
| UpdateConfig | WO | SYS | - | s.o. | Attribuer une fois un 1 à cette balise permet de noter la configuration spécifiée comme valide (si SNTP est en mode INACTIF) et de tester la configuration actuelle. |
| Start | WO | SYS | - | s.o. | Attribuer un 1 à cette balise permet de lancer manuellement la synchronisation SNTP. |
| Stop | WO | SYS | - | s.o. | Attribuer un 1 à cette balise permet d'arrêter la synchronisation SNTP. |
| Save | WO | SYS | - | s.o. | Attribuer une fois un 1 à cette balise permet d'enregistrer la configuration dans un fichier dans la mémoire FLASH. |
| Status | RO | SYS | - | - | Cette variable indique l'état du traitement SNTP (commencé, arrêté). |

## 8.5 Diagnostic SNMP via l'interface Web CGI

### 8.5.1 Syntaxe d'accès

Toutes les balises de configuration SNMP sont accessibles via l'interface Web CGI. L'accès a la syntaxe suivante :

Valeurs de lecture :
http://hostname/cgi-bin/readVal.exe?<RegistreConfig>,<NomBalise>

| | |
|---|---|
| RegistreConfig | CFG-SNMP, SYS-SNMP |
| NomBalise | Correspond à la balise de configuration figurant dans le tableau des balises. |

### 8.5.2 Liste des balises SNMP

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Enable | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) les fonctionnalités SNMP. |
| UseV3 | RW | CFG | 0 | s.o. | Active (1) ou désactive (0) la fonctionnalité V3 SNMP.<br>Actuellement, seule la V2 est prise en charge.<br>Le positionnement de cet indicateur n'a pas d'incidence. |
| StartDelay | RW | CFG | 5 | 0/60 | Définit le moment où l'agent SNMP est lancé après la mise sous tension. Ce temps est nécessaire pour permettre au Saia PCD® de définir la configuration IP avant que l'agent SNMP soit lancé.<br>Si le retard de démarrage est trop court, il est possible que l'événement d'alarme de redémarrage à froid ne puisse pas être envoyé.<br>Attribuer un 0 à cette balise permet de lancer SNMP immédiatement lorsque la syntaxe de la configuration IP a été analysée. |
| IOReadFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'entrée/sortie accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| IOReadLast | RW | CFG | 1024 | $2^{31} - 1$ | Définit la première adresse d'entrée/sortie NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `IOReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| IOWriteFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'entrée/sortie accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| IOWriteLast | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'entrée/sortie NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `IOWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| FlagReadFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'indicateur accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| FlagReadLast | RW | CFG | 8192 | $2^{31} - 1$ | Définit la première adresse d'indicateur NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `FlagReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| FlagWriteFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'indicateur accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| FlagWriteLast | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse d'indicateur NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `FlagWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| RegReadFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse de registre accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| RegReadLast | RW | CFG | 16364 | $2^{31} - 1$ | Définit la première adresse de registre NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `RegReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| RegWriteFirst | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse de registre accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| RegWriteLast | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse de registre NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `RegWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| TimerRead-First | RW | CFG | 0 | $2^{31} - 1$ | Définit la première adresse de registre d'horloge accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| Timer-ReadLast | RW | CFG | 32 | $2^{31}$ - 1 | Définit la première adresse de registre d'horloge NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `TimerReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| TimerWrite-First | RW | CFG | 0 | $2^{31}$ - 1 | Définit la première adresse de registre d'horloge accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| TimerWrite-Last | RW | CFG | 0 | $2^{31}$ - 1 | Définit la première adresse de registre d'horloge NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `TimerWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| CounterRead-First | RW | CFG | 32 | $2^{31}$ - 1 | Définit la première adresse de compteur accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| Counter-ReadLast | RW | CFG | 1600 | $2^{31}$ - 1 | Définit la première adresse de compteur NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `CounterReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| CounterWrite-First | RW | CFG | 0 | $2^{31}$ - 1 | Définit la première adresse de compteur accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si l'adresse est inférieure à la valeur spécifiée. |
| CounterWrite-Last | RW | CFG | 0 | $2^{31}$ - 1 | Définit la première adresse de compteur NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si l'adresse est inférieure à la valeur spécifiée mais supérieure ou égale à `CounterWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. |
| DBReadFirst | RW | CFG | 0 | $2^{31}$ - 1 | Définit le premier numéro de bloc de données accessible avec une requête GET/GETNEXT SNMP. La requête renvoie une erreur si le numéro est inférieur à la valeur spécifiée. Si un bloc de données est accessible, tous les éléments à l'intérieur du BD sont également accessibles. |
| DBReadLast | RW | CFG | 8192 | $2^{31}$ - 1 | Définit le premier numéro de bloc de données NON accessible avec une requête GET/GETNEXT SNMP. Les requêtes obtiendront une réponse sans erreur si le numéro est inférieur à la valeur spécifiée mais supérieur ou égal à `DBReadFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. Une fois qu'un accès en lecture a été défini pour un BD, l'ensemble du BD peut être lu. |

| Fichier Web CGI | | Type | Par déf. | Min./max. | Description |
|---|---|---|---|---|---|
| Nom de la balise | Accès | | | | |
| DBWriteFirst | RW | CFG | 0 | $2^{31}$ - 1 | Définit le premier numéro de bloc de données accessible avec une requête SET/CHECK SNMP. La requête renvoie une erreur si le numéro est inférieur à la valeur spécifiée. Si un bloc de données est accessible, tous les éléments à l'intérieur du BD sont également accessibles. |
| DBWriteLast | RW | CFG | 0 | $2^{31}$ - 1 | Définit le premier numéro de bloc de données NON accessible avec une requête SET/CHECK SNMP. Les requêtes obtiendront une réponse sans erreur si le numéro est inférieur à la valeur spécifiée mais supérieur ou égal à `DBWriteFirst`. Aucun accès n'est autorisé si les valeurs First et Last sont égales. Une fois qu'un accès en écriture a été défini pour un BD, l'ensemble du BD peut être écrit. |
| ReadCommunity | RW | CFG | « public » | 24 caract. max. | Définit la chaîne utilisée dans SNMP V2 pour accéder à des objets embarqués (commandes de lecture par ex. GET/GETNEXT). |
| WriteCommunity | RW | CFG | « private » | 24 caract. max. | Définit la chaîne utilisée dans SNMP V2 pour accéder à des objets embarqués (commandes d'écriture par ex. GET/GETNEXT). |
| TrapCommunity | RW | CFG | « public » | 24 caract. max. | Définit la chaîne utilisée lorsqu'une alarme est envoyée par l'agent au superviseur SNMP. |
| sysContact | RW | CFG | « Saia-Burgess Controls AG » | 100 caract. max. | Définit la chaîne affichée lors de l'accès à l'objet SNMP par défaut sysContact (défini dans SNMPv2-MIB) |
| sysLocation | RW | CFG | « CH-3280 Morat » | 100 caract. max. | Définit la chaîne affichée lors de l'accès à l'objet SNMP par défaut sysLocation (défini dans SNMPv1-MIB) |
| TrapxPort | RW | CFG | 0 | 65535 | Il est possible de définir jusqu'à trois récepteurs d'alarme SNMP. Le x doit être remplacé par a, b ou c. Le port correspond au port IP utilisé par le récepteur. Une valeur de 0 implique l'utilisation du port par défaut, normalement 162. |
| TrapxIPAddr | RW | CFG | 0.0.0.0 | s.o. | Il est possible de définir jusqu'à trois récepteurs d'alarme SNMP. Le x doit être remplacé par a, b ou c. L'adresse IP correspond à l'adresse IP utilisée par le récepteur. Une valeur de 0 implique qu'aucun récepteur n'est défini pour cette entrée d'alarme. |
| LifeTimeout | RW | CFG | 0 | 1 hr | Exprimée en millisecondes, elle définit le temps écoulé entre deux envois « Life Trap » aux superviseurs configurés. Mettre cette variable sur 0 désactive l'envoi de messages « life trap ». |

# A Annexe

## A.1 Icônes

| | |
|---|---|
|  | Ce symbole indique que des informations supplémentaires sur ce thème existent dans ce manuel ou dans un autre, ou encore dans des documents techniques. Il n'existe aucun renvoi direct à de tels documents. |
|  | Ce symbole avertit le lecteur que des composants peuvent être endommagés par une décharge électrostatique au contact.<br>Recommandation : touchez au minimum le pôle moins du système (boîtier de la fiche PGU) avant d'entrer en contact avec des pièces électroniques. Il est encore mieux de porter au poignet un bracelet mis à la terre, relié au pôle moins du système. |
|  | Ce symbole désigne des instructions qui doivent être strictement suivies. |
|   | Les explications à côté de ce symbole ne s'appliquent qu'à la série Saia PCD® Classic. |
|   | Les explications à côté de ce symbole ne s'appliquent qu'à la série Saia PCD® xx7. |

A

## A.2 Vue d'ensemble technique

| | | |
|---|---|---|
| Systèmes pris en charge | Nouveaux systèmes avec système d'exploitation NT.OS<br>Systèmes PCD1.M2xxx, PCD2.M5xx et PCD3 | |
| Configuration | Fichier de configuration avec balises créé avec le configurateur matériel (accessible avec une instruction CSF ou l'interface Web CGI). | |
| **PPP** | | |
| Norme | RFC-1661 | |
| Authentification | PAP, CHAP et MS-CHAP | |
| Connexions PPP simultanées | 1 seule connexion PPP (client ou serveur) par contrôleur Saia PCD® est possible. | |
| PPP sur Ethernet | Non | |
| Adresse IP | Client : adresse du serveur. | |
| Débit en bauds | Selon l'interface série. Jusqu'à 115 200 bauds | |
| Protocoles IP | HTTP, FTP, mode de données ouvert pour la programmation libre. Ether-S-Bus. Messagerie SMTP et autres. | |
| Passerelle S-Bus | Serial-S-Bus sur RS-485/422 | oui |
| | Ether-S-Bus | non |
| **DHCP** | | |
| Norme | RFC-2131 | |
| Port UDP | 67 pour le serveur, 68 pour le client | |
| Paramètres | Adresse IP<br>Masque de sous-réseau<br>Passerelle standard (en option)<br>Adresse DNS (en option) | |
| **DNS** | | |
| Norme | RFC 1035 | |
| Port | UDP 53 | |
| **SNTP** | | |
| Norme | RFC-2030 | |
| Port | UDP 123 | |
| Mode SNTP | Diffusion individuelle point à point (le client SNTP initie la requête)<br>Diffusion générale point à multipoint (un serveur NTP envoie l'heure à tous les clients) | |
| Serveur SNTP possible | Cf. notes d'application | |
| Format de l'heure | UTC (temps moyen de Greenwich)<br>Le fuseau horaire peut être modifié. | |
| Précision de l'heure | 500 ms pour la diffusion individuelle point à point<br>1 s pour la diffusion générale point à multipoint | |
| Requêtes | 10 s | |
| Interface | Ethernet<br>RS-232 série sur PPP | |
| **SMTP (envoi d'e-mails)** | | |
| Norme | RFC 821 | |
| Port | 25 | |
| Méthode d'authentification | AUTH LOGIN<br>AUTH PLAIN | |
| Chiffrement | Aucun | |
| **SNMP (agent)** | | |
| Norme | RFC 1157 | |
| Port | UDP 161 (commandes)<br>UDP 162 (traps) | |
| Format des messages trap | V1, V2C | |

A

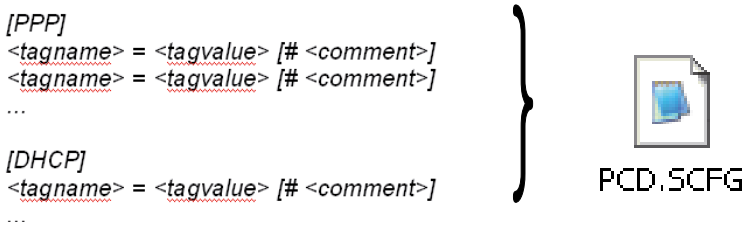
## A.3 Fichier de configuration

**Dans le projet :**

Tous les protocoles TCP/IP sont configurés à l'aide d'un fichier de configuration intitulé PCD.SCFG :

...\nom_projet\nom_périphérique\PCD.SCFG

Ce fichier de configuration comprend une section par protocole et chaque paramètre de configuration est défini par une balise de configuration :




Le commentaire est optionnel. Seules les balises de configuration seront utilisées comme paramètres de configuration.

**Sur le Saia PCD® :**

Sur le Saia PCD®, le fichier sera stocké dans le dossier système.

S'il existe plusieurs fichiers de configuration, la priorité est définie comme suit :

INTFLASH

M1 Flash

M2 Flash

SL0 Flash

Si le fichier de configuration n'est pas présent dans le système de fichiers du Saia PCD®, le microprogramme sera lancé avec les paramètres par défaut.

L'extension IP sera désactivée.

### A.3.1 Modification du fichier de configuration avec un éditeur de texte

Le fichier de configuration peut être modifié à l'aide de n'importe quel éditeur de texte. Ceci permet à l'utilisateur de modifier les paramètres sans installer le Saia PG5®.

Une fois modifié, le fichier est transmis au contrôleur par FTP.

Recommandation :

N'adaptez que des fichiers complets créés par le configurateur matériel du Saia PG5®.

## A.4 Adresses

**Saia-Burgess Controls AG**
Bahnhofstrasse 18
3280 Murten, Suisse

Téléphone standard..... +41 26 580 30 00
Téléphone support SBC ..... +41 26 580 31 00
Fax :..... +41 26 580 34 99

E-mail assistance : ..... support@saia-pcd.com
Page d'assistance : ..... www.sbc-support.com
Page d'accueil SBC :..... www.saia-pcd.com

Représentations internationales et
succursales SBC : www.saia-pcd.com/contact

**Adresse postale pour les retours effectués par les clients pour les ventes en Suisse**

**Saia-Burgess Controls AG**
Service Après-Vente
Bahnhofstrasse 18
3280 Murten, Suisse

A