

EcoStruxure Machine Expert

SnmpManager

Guide de la bibliothèque

EIO0000002798.02
12/2023

Mentions légales

Les informations fournies dans ce document contiennent des descriptions générales, des caractéristiques techniques et/ou des recommandations concernant des produits/solutions.

Ce document n'est pas destiné à remplacer une étude détaillée ou un plan de développement ou de représentation opérationnel et propre au site. Il ne doit pas être utilisé pour déterminer l'adéquation ou la fiabilité des produits/solutions pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur individuel d'effectuer, ou de faire effectuer par un professionnel de son choix (intégrateur, spécificateur ou équivalent), l'analyse de risques exhaustive appropriée ainsi que l'évaluation et les tests des produits/solutions par rapport à l'application ou l'utilisation particulière envisagée.

La marque Schneider Electric et toutes les marques de commerce de Schneider Electric SE et de ses filiales mentionnées dans ce document sont la propriété de Schneider Electric SE ou de ses filiales. Toutes les autres marques peuvent être des marques de commerce de leurs propriétaires respectifs.

Ce document et son contenu sont protégés par les lois sur la propriété intellectuelle applicables et sont fournis à titre d'information uniquement. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), à quelque fin que ce soit, sans l'autorisation écrite préalable de Schneider Electric.

Schneider Electric n'accorde aucun droit ni aucune licence d'utilisation commerciale de ce document ou de son contenu, sauf dans le cadre d'une licence non exclusive et personnelle, pour le consulter tel quel.

Schneider Electric se réserve le droit d'apporter à tout moment des modifications ou des mises à jour relatives au contenu de ce document ou à son format, sans préavis.

Dans la mesure permise par la loi applicable, Schneider Electric et ses filiales déclinent toute responsabilité en cas d'erreurs ou d'omissions dans le contenu informatif du présent document ou pour toute conséquence résultant de l'utilisation des informations qu'il contient.

Table des matières

Consignes de sécurité	5
QUALIFICATION DU PERSONNEL	5
INSTRUCTIONS D'UTILISATION	6
Avant de commencer	6
Démarrage et test	7
Fonctionnement et réglages	8
A propos de ce manuel	9
Informations générales	15
Présentation de la bibliothèque.....	16
Informations générales.....	17
Entrées et sorties communes	21
Fonctionnement des blocs fonction avec entrées <i>i_xEnable</i> et <i>i_xExecute</i>	21
Concept de diagnostic	22
Concept de diagnostic.....	22
Utilisation de SnmpManager pour gérer les appareils/clients dans un réseau	24
Principe.....	24
Énumérations et Structures.....	26
Énumérations.....	27
<i>ET_AuthenticationProtocol</i>	27
<i>ET_PrivacyProtocol</i>	27
<i>ET_Result</i>	28
<i>ET_SecurityLevel</i>	33
<i>ET_SnmpProtocolVersion</i>	33
<i>ET_SnmpRequest</i>	34
<i>ET_SnmpTag</i>	35
Structures	37
<i>ST_RequestInformation</i>	37
<i>ST_Request</i>	37
<i>ST_Response</i>	38
Variables globales.....	40
Liste des constantes globales.....	41
Liste des constantes globales (GCL)	41
Liste des paramètres globaux.....	42
Liste des paramètres globaux (GPL)	42
Interfaces	43
<i>IF_UserManagement</i>	44
<i>IF_UserManagement</i> - Informations générales.....	44
Unités d'organisation de programme (POU).....	45
Blocs fonction.....	46
<i>FB_SnmpManager</i>	46
<i>FB_UserManagement</i> - Informations générales	47
<i>FB_UserManagement</i> - <i>AddUser</i> (méthode)	48
<i>FB_UserManagement</i> - <i>DeleteUser</i> (méthode).....	49
Fonctions	51
<i>FC_EtResultToString</i>	51

Glossaire53

Index54

Consignes de sécurité

Informations importantes

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.



La présence de ce symbole sur une étiquette "Danger" ou "Avertissement" signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.



Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

Remarque Importante

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

QUALIFICATION DU PERSONNEL

Une personne qualifiée est une personne qui a les qualifications suivantes :

- Compétences et connaissances liées à la construction et à l'exploitation d'équipements électriques et à l'installation.
- Connaissances et expérience en programmation de contrôle industriel.

- A reçu une formation en sécurité permettant de reconnaître et d'éviter les dangers potentiels.

La personne qualifiée doit être capable de détecter d'éventuels dangers qui pourraient découler du paramétrage, de modifications des valeurs de paramétrage et plus généralement des équipements mécaniques, électriques ou électroniques. La personne qualifiée doit connaître les normes, dispositions et réglementations liées à la prévention des accidents de travail, et doit les observer lors de la conception et de l'implémentation du système.

INSTRUCTIONS D'UTILISATION

Ce produit est une bibliothèque à utiliser avec un système de commande et des servo-amplificateurs. La bibliothèque n'est conçue qu'en vue d'une utilisation telle que décrite dans la présente documentation, appliquée au secteur industriel.

Observez en permanence les instructions applicables liées à la sécurité, les conditions spécifiques et les données techniques.

Réalisez une analyse des risques en rapport avec l'utilisation spécifique avant d'utiliser ce produit. Prenez les mesures de sécurité qui découlent des résultats.

Étant donné que ce produit est utilisé au sein d'un système qui l'englobe, vous devez assurer la sécurité du personnel par la conception même du système global (la conception de la machine, par exemple).

Aucune autre utilisation n'est prévue. Toute autre utilisation pourrait être dangereuse.

Avant de commencer

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

AVERTISSEMENT

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automatisme et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE: La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

Démarrage et test

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠ AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

Fonctionnement et réglages

Les précautions suivantes sont extraites du document NEMA Standards
Publication ICS 7.1-1995 :

(En cas de divergence ou de contradiction entre une traduction et l'original
anglais, le texte original en anglais prévaudra.)

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit dérégulé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- L'opérateur ne doit avoir accès qu'aux réglages fonctionnels dont il a besoin. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Objectif du document

Ce document décrit la bibliothèque SnmpManager.

La bibliothèque SnmpManager implémente un gestionnaire pour le protocole Internet standard SNMP (Simple Network Management Protocol). Le gestionnaire SNMP permet à votre contrôleur de collecter et d'organiser les informations concernant les équipements pris en charge sur les réseaux IP (Internet Protocol) et de modifier ces informations afin d'ajuster la configuration de l'équipement.

La bibliothèque SnmpManager utilise des fonctions et des ressources système qui sont prises en charge sur certaines plates-formes de contrôleur avec ports Ethernet disponibles dans EcoStruxure Machine Expert.

Champ d'application

Ce document a été actualisé pour le lancement de EcoStruxure™ Machine Expert V2.2.

Document(s) à consulter

Titre du document	Référence
Recommandations de cybersécurité pour les solutions d'automatisme	EIO0000004242
Meilleures pratiques en matière de cybersécurité	https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/
EcoStruxure Machine Expert - Fonctions et bibliothèques - Guide de l'utilisateur	EIO0000002829 (ENG); EIO0000002830 (FRE); EIO0000002831 (GER); EIO0000002832 (ITA); EIO0000002833 (SPA); EIO0000002834 (CHS);
EcoStruxure Machine Expert - Guide de programmation	EIO0000002854 (ENG); EIO0000002855 (FRE); EIO0000002856 (GER); EIO0000002857 (ITA); EIO0000002858 (SPA); EIO0000002859 (CHS);

Les documents sont accessibles à partir du centre de téléchargement Schneider Electric (www.se.com/fr/fr/download/).

Informations produit

⚠ AVERTISSEMENT

PERTE DE CONTROLE

- Réalisez une analyse des modes de défaillance et de leurs effets (FMEA) ou une analyse de risques équivalente sur l'application et appliquez les contrôles de prévention et de détection appropriés avant la mise en œuvre.
- Prévoyez un état de repli pour les événements ou séquences de commande indésirables.
- Le cas échéant, prévoyez des chemins de commande séparés et redondants.
- Définissez les paramètres appropriés, notamment pour les limites.
- Examinez les conséquences des retards de transmission et prenez les mesures correctives nécessaires.
- Examinez les conséquences des interruptions de la liaison de communication et prenez des mesures correctives nécessaires.
- Prévoyez des chemins indépendants pour les fonctions de commande critiques (arrêt d'urgence, dépassement de limites, conditions d'erreur, etc.) en fonction de votre évaluation des risques ainsi que des réglementations et consignes applicables.
- Appliquez les réglementations et les consignes locales de sécurité et de prévention des accidents.¹
- Testez chaque mise en œuvre d'un système pour vérifier son bon fonctionnement avant de le mettre en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

¹ Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), *Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems* (Normes de sécurité relatives à la construction et manuel de sélection, d'installation et d'exploitation de variateurs de vitesse) ou leur équivalent en vigueur dans votre pays.

Avant de tenter de fournir une solution (machine ou processus) pour une application spécifique en utilisant les POU trouvés dans la bibliothèque, vous devez tenir compte de la réalisation et de l'exécution des bonnes pratiques. La liste non exhaustive de ces pratiques liées à cette bibliothèque inclut l'analyse des risques, la sécurité fonctionnelle, la compatibilité des composants, les tests et la validation du système.

⚠ AVERTISSEMENT

UTILISATION INCORRECTE DES UNITES ORGANISATIONNELLES DU PROGRAMME

- Effectuez une analyse de la sécurité de l'application et des équipements installés.
- Vérifiez que les POU sont compatibles avec les équipements du système et n'ont pas d'effets inattendus sur le bon fonctionnement du système.
- Assurez-vous que l'axe est en position d'origine et que le référencement est valide avant d'utiliser des mouvements absolus ou des POU utilisant des mouvements absolus.
- Utilisez les paramètres appropriés, notamment les valeurs limites, et observez l'usure de la machine et son fonctionnement à l'arrêt.
- Vérifiez que les capteurs et déclencheurs sont compatibles avec les POU sélectionnés.
- Testez de manière approfondie toutes les fonctions durant la vérification et la mise en service dans tous les modes de fonctionnement.
- Indiquez des méthodes indépendantes pour les fonctions de contrôle critiques (arrêt d'urgence, conditions des valeurs limites dépassées, etc.) conformément à une analyse de sécurité, aux règles en vigueur et aux réglementations applicables.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

Actualisez votre programme d'application, si nécessaire, en portant une attention particulière aux réglages de l'adresse d'E/S, dès que vous modifiez la configuration matérielle.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Les transferts incomplets, qu'il s'agisse de fichiers de données, d'application et/ou de micrologiciel, peuvent avoir des conséquences graves sur votre machine ou votre contrôleur. En cas de coupure de courant (volontaire ou non) ou d'interruption de la communication pendant un transfert de fichier, votre machine peut devenir inopérante ou votre application peut tenter d'utiliser un fichier de données endommagé. En cas d'interruption, relancez le transfert. Veillez à inclure l'impact des fichiers de données endommagés dans votre analyse des risques.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT, PERTE DE DONNEES OU FICHIER ENDOMMAGE

- N'interrompez pas un transfert de données en cours.
- Si le transfert est interrompu pour une raison quelconque, relancez-le.
- Ne mettez pas votre machine en service tant que le transfert de fichier n'est pas terminé, sauf si vous avez pris en compte les fichiers endommagés dans votre analyse des risques et si vous avez mis en place des mesures appropriées pour prévenir les conséquences potentiellement graves dues à des échecs de transfert.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Informations concernant la terminologie inclusive/sensible

Schneider Electric s'efforce de mettre constamment à jour ses communications et ses produits pour respecter ses engagements en matière de terminologie inclusive/sensible. Il se peut malgré tout que nos contenus présentent encore des termes jugés inappropriés par certains clients.

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant sur les produits eux-mêmes proviennent généralement des normes internationales.

Dans le domaine des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, il s'agit par exemple de termes tels que *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation de défaut*, *dysfonctionnement*, *panne*, *erreur*, *message d'erreur*, *dangereux*, etc.

Ces normes incluent notamment :

Norme	Description
IEC 61131-2:2007	Automates programmables, partie 2 : Spécifications et essais des équipements.
ISO 13849-1:2023	Sécurité des machines : Composants liés à la sécurité dans les systèmes de commande. Principes généraux de conception
EN 61496-1:2013	Sécurité des machines : Equipement de protection électrosensible. Partie 1 : Exigences générales et tests.
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Equipement électrique des machines - Partie 1 : exigences générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception

Norme	Description
IEC 62061:2021	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmables relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Exigences concernant la sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables liés à la sécurité : Configuration logicielle requise.
IEC 61784-3:2021	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain liés à la sécurité fonctionnelle - Règles générales et définitions de profil.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes utilisés dans le présent document peuvent provenir d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* peut être utilisé dans le contexte de la description de dangers spécifiques et a la même signification que *zone à risque* ou *zone dangereuse* dans la directive *Machines (2006/42/EC)* et *ISO 12100:2010*.

NOTE: Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Informations générales

Contenu de cette partie

Présentation de la bibliothèque	16
Entrées et sorties communes	21
Concept de diagnostic	22
Utilisation de SnmpManager pour gérer les appareils/clients dans un réseau	24

Présentation de la bibliothèque

Contenu de ce chapitre

Informations générales	17
------------------------------	----

Informations générales

Présentation de la bibliothèque

La bibliothèque SnmpManager implémente un gestionnaire pour le protocole Internet standard SNMP (Simple Network Management Protocol). Le gestionnaire SNMP permet à votre contrôleur de collecter et d'organiser les informations concernant les équipements pris en charge sur les réseaux IP (Internet Protocol) et de modifier ces informations afin d'ajuster la configuration de l'équipement.

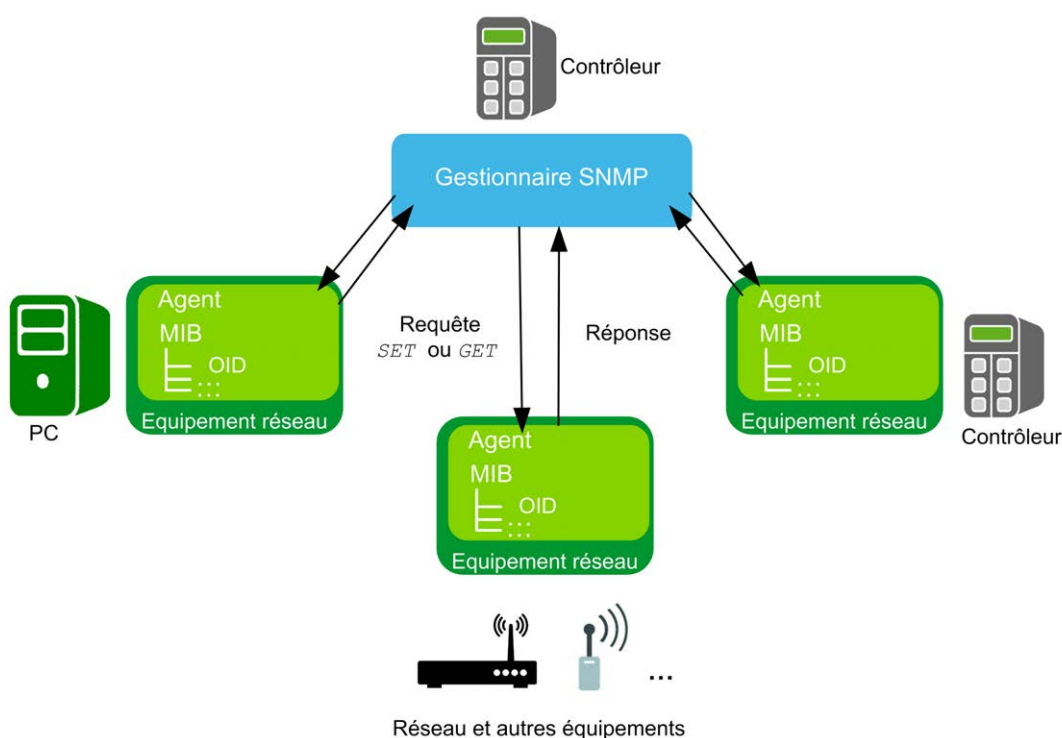
Le gestionnaire SNMP peut communiquer avec les équipements gérés via :

- Protocole SNMPv1 tel que défini dans IETF RFC 1157
- Protocole SNMPv2c (basé sur la communauté) tel que défini dans la norme IETF RFC 1901...1907
- Protocole SNMPv3 tel que défini dans IETF RFC 3412, 3414 et 3826

Il fournit les fonctions suivantes :

- Génération et transmission d'une requête *GET* pour un identifiant d'objet (OID).
- Génération et transmission d'une requête *SET* pour un OID.
- Réception et structuration de la réponse de l'agent.
- Mise à disposition de la valeur décodée d'une réponse dans un type de système approprié.
- Codage d'une valeur donnée pour une requête *SET* correspondante.
- Gestion des erreurs détectées.
- Gestion des demandes d'authentification.
- Cryptage de l'unité de données de protocole (PDU) d'une requête.

Un agent peut être un équipement réseau exécutant des fonctionnalités SNMP, comme un commutateur, un routeur, une imprimante ou d'autres contrôleurs. Vous devez fournir des informations sur la structure MIB (Management Information Base) spécifique et les OID correspondants pour chaque agent.



Caractéristiques de la bibliothèque

Le tableau suivant indique les caractéristiques de la bibliothèque :

Caractéristique	Valeur
Titre de la bibliothèque	SnmprManager
Société	Schneider Electric
Catégorie	Communication
Composant	Suite de protocoles Internet
Espace de noms par défaut	SE_SNMP
Attribut de modèle de langage	Accès qualifié uniquement (voir EcoStruxure Machine Expert, Fonctions et bibliothèques, Guide de l'utilisateur)
Bibliothèque post-compatible	Oui (FCL (voir EcoStruxure Machine Expert, Fonctions et bibliothèques, Guide de l'utilisateur)

NOTE: Cette bibliothèque est paramétrée pour l'accès qualifié uniquement. Cela signifie qu'il n'est possible d'accéder aux POU, structures de données, énumérations et constantes qu'en utilisant l'espace de noms de la bibliothèque. L'espace de noms par défaut de la bibliothèque est **SE_SNMP**.

Remarques générales

Prenez en compte les limites suivantes de la communication SNMP :

- Seul le protocole Internet version 4 (IPv4) est pris en charge.
- Une seule requête vers un agent SNMP est autorisée à la fois.
- Un seul identifiant OID peut être traité par requête.
- La bibliothèque SnmprManager intègre des pointeurs sur les adresses.

L'exécution de la commande **Changement en ligne** peut modifier le contenu des adresses.

⚠ ATTENTION
POINTEUR NON VALIDE Vérifiez la validité des pointeurs lors de leur utilisation sur les adresses et de l'exécution de la commande Changement en ligne. Le non-respect de ces instructions peut provoquer des blessures ou des dommages matériels.

La bibliothèque de gestionnaire SNMP repose sur les communications UDP.

NOTE: Le protocole UDP n'établit pas de connexion de bout en bout dédiée. La communication entre homologues s'effectue en transmettant les informations de la source vers la destination. Elle ne permet pas de vérifier si un message a atteint l'homologue destinataire ou si des informations ont été perdues pendant le transfert. Le protocole UDP ne prévoit pas d'options d'acquiescement, de retransmission ou de timeout.

La bibliothèque décrite dans ce document utilise la bibliothèque TcpUdpCommunication en interne.

Les bibliothèques TcpUdpCommunication (Schneider Electric) et CAA Net Base Services (CAA Technical Workgroup) utilisent les mêmes ressources système sur le contrôleur. Leur utilisation simultanée dans la même application peut perturber le fonctionnement du contrôleur.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPRÉVU DE L'ÉQUIPEMENT

N'utilisez pas en même temps la bibliothèque TcpUdpCommunication (Schneider Electric) et la bibliothèque CAA Net Base Services (groupe de travail technique CAA).

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Considérations relatives à la cybersécurité

Les fonctions de la bibliothèque SnmpManager ne prennent pas en charge les connexions sécurisées telles que TLS (Transport Layer Security) ou SSL (Secure Socket Layer). La communication ne peut s'effectuer qu'au sein de votre réseau industriel, isolé des autres réseaux de votre entreprise et protégé d'Internet.

NOTE: Schneider Electric respecte les bonnes pratiques de l'industrie, en vigueur dans le développement et la mise en œuvre des systèmes de contrôle. Cette approche, dite de « défense en profondeur », permet de sécuriser les systèmes de contrôle industriels. Elle place les contrôleurs derrière des pare-feu pour restreindre leur accès aux seuls personnels et protocoles autorisés.

⚠ AVERTISSEMENT

ACCES NON AUTHENTIFIE ET EXPLOITATION PAR CONSEQUENT NON AUTORISEE DES MACHINES

- Estimez si votre environnement ou vos machines sont connecté(e)s à votre infrastructure vitale et, le cas échéant, prenez les mesures nécessaires de prévention, basées sur le principe de défense en profondeur, avant de connecter le système d'automatisme à un réseau quelconque.
- Limitez au strict nécessaire le nombre d'équipements connectés à un réseau.
- Isolez votre réseau industriel des autres réseaux au sein de votre société.
- Protégez chaque réseau contre les accès non autorisés à l'aide d'un pare-feu, d'un VPN ou d'autres mesures de sécurité éprouvées.
- Surveillez les activités au sein de votre système.
- Empêchez tout accès direct ou liaison directe aux équipements sensibles par des utilisateurs non autorisés ou des actions non authentifiées.
- Préparez un plan de récupération intégrant la sauvegarde des informations de votre système et de votre processus.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Pour plus d'informations sur les mesures organisationnelles et les règles d'accès aux infrastructures, reportez-vous aux normes suivantes : famille de normes ISO/IEC 27000, Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, Cybersecurity Framework (Cadre de cybersécurité) du NIST, Standard of Good Practice for Information Security (Bonne pratique de sécurité de l'information) de l'Information Security Forum. Consultez également le document Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment.

Entrées et sorties communes

Contenu de ce chapitre

Fonctionnement des blocs fonction avec entrées <i>i_xEnable</i> et <i>i_xExecute</i>	21
--	----

Fonctionnement des blocs fonction avec entrées *i_xEnable* et *i_xExecute*

Informations générales

Avec l'entrée *i_xEnable* définie sur TRUE, le bloc fonction lance le processus d'activation. Le bloc fonction poursuit l'initialisation et la sortie *q_xActive* est définie sur TRUE. Une fois l'initialisation terminée et le bloc fonction prêt, la sortie *q_xReady* est définie sur TRUE.

Un front montant de l'entrée *i_xExecute* lance l'exécution du bloc fonction. Le bloc fonction poursuit son exécution et la sortie *q_xBusy* est définie sur TRUE. Un front montant sur l'entrée *i_xExecute* est ignoré pendant l'exécution du bloc fonction.

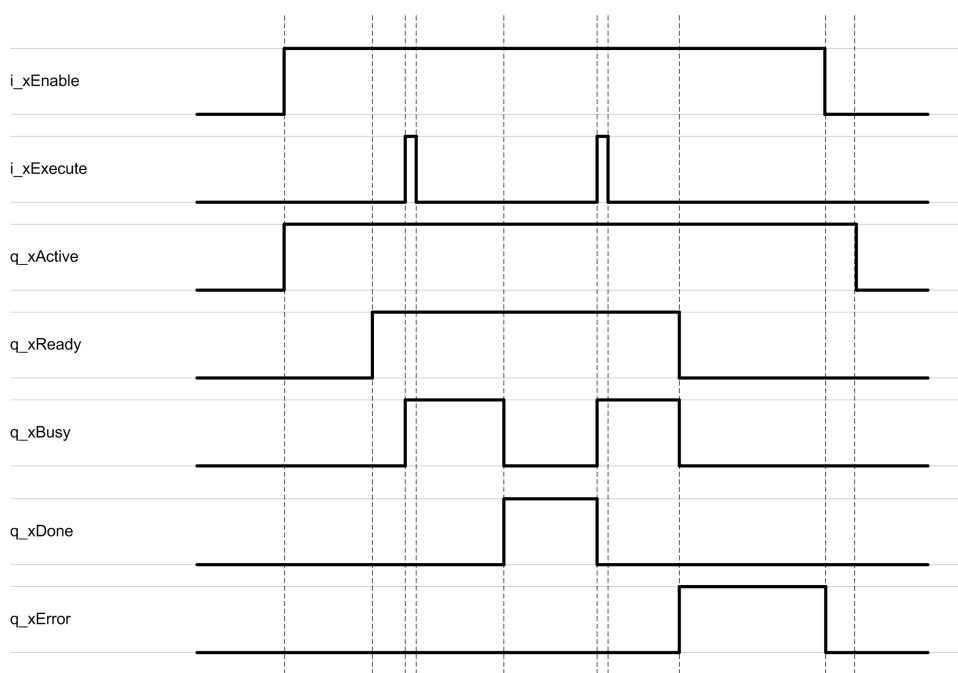
Une fois l'exécution terminée, les sorties *q_xDone* ou *q_xError* sont définies en fonction du résultat.

La sortie *q_xDone* indique une exécution réussie et elle garde la valeur TRUE jusqu'au front montant suivant de l'entrée *i_xExecute*.

Si *q_xError* indique TRUE, une erreur a été détectée pendant l'exécution. Une nouvelle exécution du bloc fonction est impossible tant que l'état d'erreur est présent. Le bloc fonction doit être désactivé afin de réinitialiser l'état d'erreur.

Avec l'entrée *i_xEnable* définie sur FALSE, la fonction lance le processus de désactivation. L'appel du bloc fonction se poursuit tant que la sortie *q_xActive* a la valeur TRUE.

Exemple



Concept de diagnostic

Contenu de ce chapitre

Concept de diagnostic	22
-----------------------------	----

Concept de diagnostic

Présentation

EcoStruxure Machine Expert fournit un concept de diagnostic à trois niveaux pour les bibliothèques. Ce concept est valable pour les bibliothèques Technologie/Module (par exemple, la bibliothèque CommonToolbox) et utilise des énumérations pour le codage de diagnostic.

En principe, les informations de diagnostic sont organisées selon les niveaux suivants :

1. Informations générales sur l'exception. Aucune connaissance particulière concernant le fonctionnement du POU n'est requise.
2. Messages d'état et de diagnostic propres aux POU (partie 1) : Informations détaillées sur la source qui déclenche les messages de diagnostic ou d'état.
3. Messages d'état et de diagnostic propres aux POU (partie 2) : Informations détaillées et dynamiques sur la source qui déclenche les messages de diagnostic ou d'état.

Ces informations changent lors de l'exécution (par exemple, informations sur la condition des paramètres d'entrée). Cette sortie de diagnostic est facultative pour les POU.

Le concept de diagnostic présente les avantages suivants :

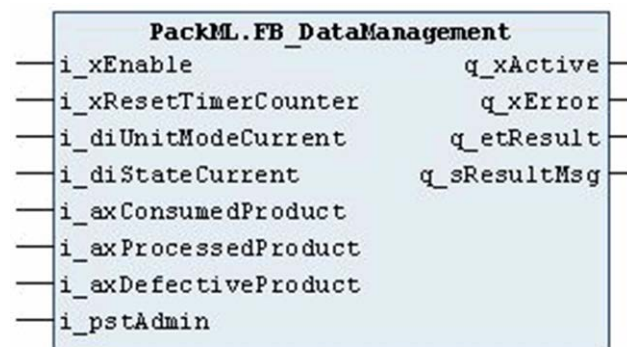
- Affichage en ligne des messages de diagnostic
- Informations détaillées sur les événements de diagnostic via les codes de diagnostic
- Présentation de l'état ou de la condition exceptionnelle d'un POU
- Suggestions pertinentes pour corriger les causes de conditions exceptionnelles
- Messages de diagnostic au format énumération permettant la prise en charge multilingue des afficheurs IHM

Sorties de diagnostic

Les blocs fonction et les fonctions ou méthodes peuvent avoir les trois sorties de diagnostic *q_xError*, *q_etResult* et *q_sResultMsg*. Ces sorties sont définies l'une après l'autre dans le POU.

Sortie	Type de données	Signification
<i>q_xError</i>	BOOL	La sortie <i>q_xError</i> est définie sur TRUE lorsqu'une erreur a été détectée pendant l'exécution du bloc fonction. Les sorties <i>q_etResult</i> et <i>q_sResultMsg</i> fournissent le code d'erreur correspondant et des informations en texte simple.
<i>q_etResult</i>	ET_Result ⁽¹⁾	Fournit des informations de diagnostic et d'état sous la forme d'une valeur numérique. If <i>q_xError</i> = FALSE, <i>q_etResult</i> fournit des informations d'état. If <i>q_xError</i> = TRUE, <i>q_etResult</i> fournit des informations de diagnostic / d'erreur. L'énumération <i>ET_Result</i> contient les valeurs possibles des résultats du fonctionnement du POU.
<i>q_sResultMsg</i>	STRING	Fournit des informations supplémentaires sur l'état actuel du POU. Si le POU est en état d'erreur (<i>q_xError</i> = TRUE), le message fournit des informations supplémentaires sur la cause de l'erreur et suggère éventuellement une solution possible. Si le POU est occupé, le processus ou l'état actuel est indiqué au niveau de cette sortie.
(1) Chaque bibliothèque fournit sa propre énumération <i>ET_Result</i> qui contient la somme des sorties <i>q_etResult</i> possibles dans l'ensemble de la bibliothèque.		

Exemple d'informations de diagnostic :



Utilisation de SnmpManager pour gérer les appareils/clients dans un réseau

Contenu de ce chapitre

Principe	24
----------------	----

Principe

Configuration système requise

Agent SNMP exécuté sur un équipement/client prenant en charge la version v1 ou v2c du protocole

Informations requises

- Structure de la MIB avec son OID (Object Identifier).
- Port et adresse IP de l'équipement / du client sur lequel l'agent SNMP s'exécute.
- Noms de communauté configurés dans l'agent SNMP pour la lecture et l'écriture.

Comment définir une nouvelle valeur dans un OID (exemple)

Déclaration :

```
PROGRAM SetRequest
VAR
    sNewSysName          : STRING[60];
    fbSnmpManager        : SE_SNMP.FB_SnmpManager;
    stRequestInfo        : SE_SNMP.ST_RequestInformation;
    etRequest            : SE_SNMP.ET_SnmpRequest;
    etProtocolVersion    : SE_SNMP.ET_SnmpProtocolVersion;
    xError               : BOOL;
    xDone               : BOOL;
    xBusy               : BOOL;
    xActive              : BOOL;
    xReady              : BOOL;

    etResult             : SE_SNMP.ET_Result;
    sResultMsg           : STRING(255);
END_VAR
```

Mise en œuvre :

```
sNewSysName := 'SchneiderSystem';
stRequestInfo.i_stRequest.pbyValueBuffer := ADR
(sNewSysName);
stRequestInfo.i_stRequest.dwNumBytesValue := 60;
stRequestInfo.i_stRequest.sAgentIp := '10.128.154.41';
stRequestInfo.i_stRequest.sOid := '1.3.6.1.2.1.1.5.0';
//SysName
stRequestInfo.i_stRequest.uiAgentSnmpPort := 161;
stRequestInfo.i_stRequest.etValueType := SE_SNMP.ET_SnmpTag.
OctetString;
etRequest := SE_SNMP.ET_SnmpRequest.SetRequest;
etProtocolVersion := SE_SNMP.ET_SnmpProtocolVersion.
Version2c
```

```
fbSnmpManager( i_xEnable := TRUE,
               i_xExecute := TRUE,
               i_etRequest := etRequest,
               i_etVersion := etProtocolVersion,
               iq_stRequestInfo := stRequestInfo,
               q_xActive => xActive,
               q_xReady => xReady,
               q_xBusy => xBusy,
               q_xDone => xDone,
               q_xError => xError,
               q_etResult => etResult,
               q_sResultMsg => sResultMsg
             )
```

Désignation des paramètres utilisés :

Etape	Action
1	Dans <i>stRequestInfo.i_stRequest</i> , spécifiez l'adresse IP (<i>sAgentIp</i>) de l'équipement sur lequel l'agent SNMP s'exécute. Par exemple, 10.128.154.47.
2	Dans <i>stRequestInfo.i_stRequest</i> , indiquez le port (<i>uiAgentSnmpPort</i>) de l'agent SNMP. Port standard de SNMP et port par défaut de la bibliothèque : 161.
3	Dans <i>stRequestInfo.i_stRequest</i> , spécifiez l'identifiant OID (<i>sOid</i>) de la valeur à modifier. Par exemple, 1.3.6.1.2.1.1.5.0 (<i>SysName</i>).
4	Dans <i>stRequestInfo.i_stRequest</i> , spécifiez le pointeur (<i>pbValueBuffer</i>) vers la valeur à modifier dans l'OID. Pour une <i>GetRequest</i> , définissez le pointeur vers le tampon où la valeur reçue est stockée.
5	Dans <i>stRequestInfo.i_stRequest</i> , spécifiez le type de valeur (<i>etValueType</i>). Par exemple, <i>OctetString</i> . Ce paramètre n'est pas utilisé pour une <i>GetRequest</i> .
6	Dans <i>stRequestInfo.i_stRequest</i> , spécifiez la taille de votre valeur (<i>dwNumBytesValue</i>). Par exemple, 60. Pour une <i>GetRequest</i> , spécifiez la taille de votre tampon de valeurs. NOTE: Dans le cas des chaînes, ajoutez un octet supplémentaire pour le caractère de fin de chaîne.
7	Dans <i>ET_SnmpProtocolVersion</i> , spécifiez le type de version du protocole SNMP. La version par défaut de la bibliothèque est définie sur <i>Version2c</i> .
8	Dans <i>ET_SnmpRequest</i> , spécifiez le type de requête. Par exemple, <i>SetRequest</i> .
9	Appelez <i>FB_SnmpManager</i> avec les valeurs/paramètres/variables ci-dessus.

Énumérations et Structures

Contenu de cette partie

Énumérations27

Structures.....37

Énumérations

Contenu de ce chapitre

<i>ET_AuthenticationProtocol</i>	27
<i>ET_PrivacyProtocol</i>	27
<i>ET_Result</i>	28
<i>ET_SecurityLevel</i>	33
<i>ET_SnmpProtocolVersion</i>	33
<i>ET_SnmpRequest</i>	34
<i>ET_SnmpTag</i>	35

ET_AuthenticationProtocol

Présentation

Type :	Enumération
Disponible à partir de :	V1.3.4.0

Description

L'énumération *ET_AuthenticationProtocol* contient les méthodes prises en charge pour l'authentification d'utilisateur à l'intérieur de requêtes SNMPv3.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>None</i>	BYTE	0	Aucune authentification.
<i>SHA1</i>	BYTE	1	Authentification avec le protocole SHA1.
<i>MD5</i>	BYTE	2	Authentification avec le protocole MD5.

Utilisé par

- *FB_UserManagement*

ET_PrivacyProtocol

Présentation

Type :	Enumération
Disponible à partir de :	V1.3.4.0

Description

L'énumération *ET_PrivacyProtocol* contient les méthodes prises en charge pour le cryptage des unités de données de protocole (PDU) dans les requêtes SNMPv3.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>None</i>	BYTE	0	Pas de cryptage.
<i>DES</i>	BYTE	1	Chiffrement avec le protocole DES.
<i>AES128</i>	BYTE	2	Chiffrement avec le protocole AES128.

Utilisé par

- *FB_UserManagement*

ET_Result

Présentation

Type :	Enumération
Disponible à partir de :	V1.0.0.0

Description

L'énumération *ET_Result* contient les valeurs possibles qui indiquent le résultat et les codes d'erreur étendus des opérations exécutées par le bloc fonction.

Si des erreurs détectées sont reçues dans le télégramme de réponse de l'agent, les sorties *iq_stRequestInfo.q_stResponse.sOID* et *iq_stRequestInfo.q_stResponse.sAgentIp* sont toujours définies avec les données de la requête qui a causé l'erreur.

Eléments d'énumération

Nom	Type de données	Valeur	Description
Si le paramètre <i>q_xError</i> du bloc fonction est FALSE, les messages d'état suivants s'affichent :			
<i>Ok</i>	UDINT	0	L'opération a abouti et le bloc fonction est inactif.
<i>NotReady</i>	UDINT	2	L'opération demandée ne peut pas être exécutée dans l'état actuel.
<i>Disabled</i>	UDINT	3	Le bloc fonction est désactivé.
<i>Sending</i>	UDINT	4	Le bloc fonction envoie un télégramme de requête avec les informations spécifiées dans l'entrée <i>iq_stRequestInfo.i_stRequest</i> .
<i>Listening</i>	UDINT	5	Le bloc fonction attend une réponse de l'agent.
<i>Evaluating</i>	UDINT	6	Le bloc fonction traite le télégramme reçu.
Si le paramètre <i>q_xError</i> du bloc fonction est TRUE, les messages d'état suivants s'affichent :			
<i>UnknownState</i>	UDINT	1	L'opération n'a pas abouti en raison d'une erreur indéterminée.
<i>InitAsyncManagerUnsuccessful</i>	UDINT	8	Une erreur interne a été détectée durant l'initialisation du gestionnaire asynchrone.
<i>AsyncTaskStartUnsuccessful</i>	UDINT	9	Une erreur interne a été détectée durant le démarrage de la tâche asynchrone.
<i>MaxNumberUserTooSmall</i>	UDINT	13	Le nombre maximal de comptes utilisateur est insuffisant. Le nombre maximum de comptes utilisateur est limité à 100.
<i>MaxTelegramSize</i>	UDINT	14	La longueur maximale d'un télégramme est dépassée. La longueur maximale d'un télégramme est de 2000 octets.
<i>GplMaxUserDataTooBig</i>	UDINT	15	<i>GPL.Gc_dwMaxSizeUserData</i> est hors plage. Vérifiez les réglages de la liste des paramètres globaux, page 42.
<i>GplMaxUserDataTooSmall</i>	UDINT	16	<i>GPL.Gc_dwMaxSizeUserData</i> est hors plage. Vérifiez les réglages de la liste des paramètres globaux, page 42.
<i>GplMaxOidTooBig</i>	UDINT	17	<i>GPL.Gc_dwMaxSizeOid</i> est hors plage. Vérifiez les réglages de la liste des paramètres globaux, page 42.
<i>GplMaxOidTooSmall</i>	UDINT	18	<i>GPL.Gc_dwMaxSizeOid</i> est hors plage. Vérifiez les réglages de la liste des paramètres globaux, page 42.
<i>GplTimeoutZero</i>	UDINT	19	<i>GPL.Gc_udiTimeout</i> est hors plage. Vérifiez les réglages de la liste des paramètres globaux, page 42.
<i>InputMissingOid</i>	UDINT	20	L'entrée obligatoire <i>iq_stRequestInfo.i_stRequest.sOid</i> n'est pas valide. Vérifiez que l'entrée est affectée.
<i>InputInvalidBufferSize</i>	UDINT	21	La taille du tampon doit être supérieure à zéro. La taille de la mémoire tampon est fournie par la valeur de <i>iq_stRequestInfo.i_stRequest.dwNumBytesValue</i> .
<i>InputInvalidRequest</i>	UDINT	22	Seuls <i>ET_SnmpRequest.GetRequest</i> et <i>ET_SnmpRequest.SetRequest</i> sont pris en charge.
<i>InputInvalidOid</i>	UDINT	23	L'OID doit être fourni en tant que STRING contenant une suite de nombres séparés par des points. Le premier chiffre doit être 0, 1 ou 2.

Nom	Type de données	Valeur	Description
<i>InputInvalidIp</i>	UDINT	24	L'adresse IP n'est pas valide. Vérifiez que l'adresse IP est fournie en tant que STRING contenant une suite de 4 ensembles de nombres séparés par des points. Les valeurs représentées par les ensembles de nombres doivent être comprises entre 0 et 255.
<i>InputInvalidPointer</i>	UDINT	25	Le tampon référencé par le pointeur <i>iq_stRequestInfo.i_stRequest.pbyValueBuffer</i> n'est pas valide. Vérifiez l'adresse du pointeur référençant le tampon, la taille du tampon et son accès en écriture.
<i>InputSize32BitValue</i>	UDINT	26	Le type de données référencé par <i>iq_stRequestInfo.i_stRequest.etValueType</i> autorise des valeurs d'une taille maximale de 4 octets.
<i>InputSize64BitValue</i>	UDINT	27	Le type de données référencé par <i>iq_stRequestInfo.i_stRequest.etValueType</i> autorise des valeurs d'une taille maximale de 8 octets.
<i>InputInvalidValueIp</i>	UDINT	28	Type de données référencé par <i>iq_stRequestInfo.i_stRequest.etValueType</i> nécessite un format spécifique : un type STRING contenant une suite de 4 ensembles de nombres séparés par des points. Les valeurs représentées par les ensembles de nombres doivent être comprises entre 0 et 255.
<i>InputInvalidValueOid</i>	UDINT	29	Le type de données référencé par <i>iq_stRequestInfo.i_stRequest.etValueType</i> nécessite un format spécifique : un type STRING contenant une suite de nombres séparés par des points. Le premier chiffre doit être 0, 1 ou 2.
<i>InputInvalidValueVersion</i>	UDINT	30	Le type de données d'entrée <i>i_etVersion</i> du bloc fonction. <i>FB_SnmppManager</i> autorise uniquement les valeurs <i>Version1</i> , <i>Version2c</i> et <i>Version3</i> .
<i>UserNotFound</i>	UDINT	31	Aucun compte utilisateur portant le nom spécifié n'a été trouvé.
<i>InputInvalidUserManagement</i>	UDINT	32	Si un compte utilisateur est spécifié, <i>i_ifUserManagement</i> ne peut pas avoir la valeur 0.
<i>InvalidUserConfiguration</i>	UDINT	33	Le compte d'utilisateur spécifié ne répond pas aux exigences associées au niveau de sécurité sélectionné.
<i>InputInvalidSecurityLevel</i>	UDINT	34	Le niveau de sécurité spécifié n'est pas valide.
<i>InputInvalidUser</i>	UDINT	35	Le compte utilisateur spécifié pour le niveau de sécurité configuré n'est pas valide.
<i>UdpIssue</i>	UDINT	40	Problème TCP générique. Consultez le Guide de la bibliothèque TcpUdpCommunication.
<i>UdpNotSupported</i>	UDINT	41	Ce contrôleur ne prend pas en charge l'opération UDP demandée.
<i>UdpSocketMngListTooSmall</i>	UDINT	42	Impossible d'ouvrir le socket UDP car la liste de gestion des sockets internes est saturée. <i>GPL_Gc_uiSocketManagementListSize</i> doit être augmenté dans la bibliothèque TcpUdp.
<i>UdpNumBytesSendOutOfRange</i>	UDINT	43	Le nombre d'octets à envoyer dépasse la plage valide. Contactez votre service d'assistance Schneider Electric local.
<i>UdpInvalidBufferAddress</i>	UDINT	44	L'adresse du tampon de télégramme n'est pas valide. Contactez votre service d'assistance Schneider Electric local.
<i>UdpInvalidIp</i>	UDINT	45	L'adresse IP fournie n'est pas valide. Vérifiez l'entrée <i>iq_stRequestInfo.i_stRequest.sAgentIp</i> donnée.
<i>UdpReceiveBufferSizeOutOfRange</i>	UDINT	46	La taille du tampon de réception dépasse la plage valide. Contactez votre service d'assistance Schneider Electric local.
<i>UdpNotReady</i>	UDINT	47	La requête UDP ne peut pas être exécutée pour le moment.
<i>UdpTimeout</i>	UDINT	48	Aucune réponse reçue de la part de l'agent dans le temps imparti, avec le nombre de tentatives indiqué. Essayez d'augmenter <i>GPL_Gc_udiTimeout</i> et / ou <i>GPL_Gc_uiMaxNumberRetries</i> .

Nom	Type de données	Valeur	Description
<i>ValidateRequestIdNoMatch</i>	UDINT	60	L'ID de requête reçu dans la réponse de l'agent ne correspond pas à l'ID de requête envoyé à l'agent. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>ValidateOidNoMatch</i>	UDINT	61	L'OID reçu dans la réponse de l'agent ne correspond pas à l'OID demandé. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>ValidateBufferTooSmall</i>	UDINT	62	Le tampon fourni dans <i>iq_stRequestInfo.i_stRequest.pbyValueBuffer</i> est insuffisant pour la valeur reçue de l'agent. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message ainsi que le nombre d'octets reçus pour la valeur. NOTE: Si la valeur reçue est de type <i>ObjectId</i> , la valeur décodée fait généralement plus de deux fois le nombre d'octets reçus. Planifiez la taille du tampon en conséquence.
<i>ValidateVersionNotSupported</i>	UDINT	63	La version de protocole ne correspond pas dans la requête/réponse.
<i>ValidateAuthenticationUnsuccessful</i>	UDINT	64	La réponse n'a pas été authentifiée.
<i>CorruptedResponse</i>	UDINT	65	La réponse n'est pas conforme au protocole SNMP sélectionné.
<i>ValidateMessageIdNoMatch</i>	UDINT	66	L'ID de message de la réponse n'est pas conforme à la requête.
<i>ValidateNoValue</i>	UDINT	69	Le télégramme reçu de l'agent ne contenait aucune valeur et aucun message d'erreur. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseGenErr</i>	UDINT	70	Message d'erreur générique reçu d'un agent SNMP. Aucune autre erreur n'a été détectée. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseTooBig</i>	UDINT	71	Réponse d'un agent à une requête <i>GET</i> ou <i>SET</i> . Le message de réponse est trop volumineux pour que l'agent puisse l'envoyer. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseSetNoAccess</i>	UDINT	72	Réponse d'un agent à une requête <i>SET</i> . Accès refusé à l'OID demandé. Vérifiez le nom de communauté dans <i>iq_stRequestInfo.i_stRequest.sCommunityName</i> . Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseSetWrongType</i>	UDINT	73	Réponse d'un agent à une requête <i>SET</i> . Le type de valeur ne correspond pas au type de valeur spécifié par l'OID. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseSetWrongLength</i>	UDINT	74	Réponse d'un agent à une requête <i>SET</i> . La longueur de la valeur n'est pas cohérente avec la longueur définie de la valeur OID. Vérifiez la longueur de la valeur OID. Si le message d'erreur persiste, contactez votre service d'assistance Schneider Electric local. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmResponseSetWrongEncoding</i>	UDINT	75	Réponse d'un agent à une requête <i>SET</i> . Un codage incorrect a été utilisé pour la valeur. Contactez votre service d'assistance Schneider Electric local. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.

Nom	Type de données	Valeur	Description
<i>SnmpResponseSetWrongValue</i>	UDINT	76	Réponse d'un agent à une requête <i>SET</i> . La valeur indiquée pour cet OID n'est pas valide ou n'est pas prise en charge. Vérifiez les données d'entrée dans <i>iq_stRequestInfo.i_stRequest</i> . Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseSetNotWritable</i>	UDINT	77	Réponse d'un agent à une requête <i>SET</i> . La valeur indiquée pour cet OID n'est pas valide ou n'est pas prise en charge. Vérifiez les données d'entrée dans <i>iq_stRequestInfo.i_stRequest</i> . Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseSetNoSuchName</i>	UDINT	78	Réponse d'un agent à une requête <i>SET</i> . Le nom est incohérent ou n'existe pas et n'a pas pu être créé. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseSetInconsistentValue</i>	UDINT	79	Réponse d'un agent à une requête <i>SET</i> . La valeur n'a pas pu être définie ou la ressource nécessaire pour définir cette valeur n'est pas disponible. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseSetNoCreation</i>	UDINT	80	Réponse d'un agent à une requête <i>SET</i> . La valeur n'existe pas et ne peut pas être créée. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseGetNoSuchObject</i>	UDINT	81	Réponse d'un agent à une requête <i>GET</i> . Le préfixe d'OID ne correspond à aucun préfixe d'OID de variables accessibles. Vérifiez l'OID dans <i>iq_stRequestInfo.i_stRequest.sOid</i> . Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseGetNoSuchInstance</i>	UDINT	82	Réponse d'un agent à une requête <i>GET</i> . Aucune correspondance exacte pour l'OID. Vérifiez l'OID dans <i>iq_stRequestInfo.i_stRequest.sOid</i> . Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseEndofMibView</i>	UDINT	83	Réponse d'un agent à une requête <i>GET</i> . Aucune autre variable dans l'ordre lexicographique. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>SnmpResponseV1WrongErrorState</i>	UDINT	84	La valeur renvoyée de <i>ErrorState</i> ne peut pas être traitée par le protocole version 1.
<i>SnmpVersion1SetCounter64</i>	UDINT	88	Counter64 n'est pas disponible pour SNMPv1.
<i>ValueNotSupported</i>	UDINT	90	La réponse de l'agent contient une valeur impossible à déterminer. Seuls les types de valeur fournis par <i>ET_SnmpTag</i> sont pris en charge. Consultez <i>iq_stRequestInfo.q_stResponse</i> pour savoir quel agent (adresse IP) et quel OID ont provoqué ce message.
<i>UnknownResult</i>	UDINT	99	Retour de <i>FC_EtResultToString</i> en cas de valeur <i>EtResult</i> impossible à déterminer.
<i>EncryptionUnsuccessful</i>	UDINT	110	Une erreur interne a été détectée lors du cryptage/décryptage des données.
<i>InputInvalidKey</i>	UDINT	111	La longueur de la clé dépasse la plage autorisée de 1 à 64 octets.

En cas de timeouts ou autres erreurs de communication récurrents, vérifiez :

- les connexions physiques du contrôleur, de l'agent SNMP, etc.
- la configuration de la connexion du contrôleur et de l'agent SNMP.
- l'itinéraire de communication entre le contrôleur et l'agent SNMP. Par exemple, les paramètres de commutateur, de routeur et de pare-feu (la communication UDP et les ports SNMP doivent être autorisés).

- l'adresse IP et le port SNMP fournis dans *iq_stRequestInfo.i_stRequest*.
- le nom de communauté fourni dans *iq_stRequestInfo.i_stRequest*.

Utilisé par

- *FB_SnmManager*
- *FB_UserManagement*

ET_SecurityLevel

Présentation

Type :	Enumération
Disponible à partir de :	V1.3.4.0

Description

L'énumération *ET_SecurityLevel* indique le niveau de sécurité associé à la requête SNMPv3 envoyée par le gestionnaire SNMP.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>NotDefined</i>	BYTE	0	Aucun niveau de sécurité n'est défini.
<i>NoAuthNoPriv</i>	BYTE	1	Sans authentification ni confidentialité.
<i>AuthNoPriv</i>	BYTE	2	Avec authentification mais sans confidentialité.
<i>AuthPriv</i>	BYTE	3	Avec authentification et confidentialité.

Utilisé par

- *FB_UserManagement*

ET_SnmpProtocolVersion

Présentation

Type :	Enumération
Disponible à partir de :	V1.0.0.0

Description

L'énumération *ET_SnmProtocolVersion* définit les types de protocole SNMP qu'un agent *SNMP* peut gérer. L'énumération peut être exécutée par le bloc fonction, page 46 *FB_SnmManager* via l'entrée *i_etVersion*.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>Version1</i>	BYTE	0	Type de protocole SNMP SNMPv1 utilisé pour la communication entre le gestionnaire SNMP et l'agent SNMP
<i>Version2c</i>	BYTE	1	Type de protocole SNMP SNMPv2c utilisé pour la communication entre le gestionnaire SNMP et l'agent SNMP
<i>Version3</i>	BYTE	3	Type de protocole SNMP SNMPv3 utilisé pour la communication entre le gestionnaire SNMP et l'agent SNMP

Utilisé par

- *FB_SnmManager*

ET_SnmRequest

Présentation

Type :	Énumération
Disponible à partir de :	V1.0.0.0

Description

L'énumération *ET_SnmRequest* définit les types de requêtes (PDU) pouvant être exécutées par le bloc fonction, page 46 *FB_SnmManager* en utilisant *i_etRequest*.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>NoCommand</i>	BYTE	0	Aucun type de requête n'est défini. Etat initial et valeur par défaut.
<i>GetRequest</i>	BYTE	1	Les requêtes <i>GET</i> demandent à un agent de fournir la valeur référencée par l'OID.
<i>SetRequest</i>	BYTE	4	Les requêtes <i>SET</i> définissent une valeur référencée par l'OID sur un agent.

Utilisé par

- *FB_SnmManager*

ET_SnmTag

Présentation

Type :	Enumération
Disponible à partir de :	V1.0.0.0

Description

L'énumération *ET_SnmTag* décrit les types de valeurs qu'il est possible d'envoyer avec une requête *SET*.

NOTE: Le type de valeur *Counter64* n'est pas pris en charge dans SNMPv1.

Le type de tampon suggéré (voir le tableau ci-dessous) indique le type de variable qui doit être référencé par le pointeur *iq_stRequestInfo.i_stRequest.pbyValueBuffer*.

- Pour une requête *SET*, ces types de variables sont obligatoires.
- Pour les types de valeur reçus par une requête *GET*, le type de tampon suggéré renvoie au type de valeur utilisé par le bloc fonction pour représenter les données reçues.

Éléments d'énumération

Nom	Type de données	Valeur	Description
<i>Integer</i>	BYTE	2	Valeur de type entier signé (32 bits). Type de tampon suggéré : DINT
<i>OctetString</i>	BYTE	4	Valeur de type chaîne avec des caractères de 8 bits. Type de tampon suggéré : STRING
<i>ObjectID</i>	BYTE	6	Valeur de type ObjectID. Type de tampon suggéré : STRING (suite de nombres séparés par des points)
<i>IpAddress</i>	BYTE	64	Valeur de type OctetString(4). Type de tampon suggéré : STRING[15]
<i>Counter32</i>	BYTE	65	Valeur de type entier non signé (32 bits). Type de tampon suggéré : UDINT
<i>Gauge32</i>	BYTE	66	Valeur de type entier non signé (32 bits). Type de tampon suggéré : UDINT
<i>TimeTicks</i>	BYTE	67	Valeur de type entier non signé (32 bits). Type de tampon suggéré : UDINT
<i>Counter64</i>	BYTE	70	Valeur de type entier non signé (64 bits). Type de tampon suggéré : ULINT Non pris en charge dans SNMPv1.

Utilisé par

- *FB_SnmManager*

Structures

Contenu de ce chapitre

<i>ST_RequestInformation</i>	37
<i>ST_Request</i>	37
<i>ST_Response</i>	38

ST_RequestInformation

Présentation

Type :	Structure
Disponible à partir de :	V1.0.0.0
Hérite de :	—

Description

La structure *ST_RequestInformation* contient deux structures : une pour les données d'entrée nécessaires à l'envoi d'une requête et une autre pour les données de sortie qui présentent la réponse à l'utilisateur.

Éléments de la structure

Nom	Type de données	Description
<i>i_stRequest</i>	<i>ST_Request</i> , page 37	Structure contenant les données d'entrée utilisateur requises
<i>q_stResponse</i>	<i>ST_Response</i> , page 38	Structure contenant la réponse à la requête de l'utilisateur

Utilisé par

- *FB_SnmpManager*

ST_Request

Présentation

Type :	Structure
Disponible à partir de :	V1.0.0.0
Hérite de :	—

Description

La structure *ST_Request* contient les informations spécifiques à l'utilisateur pour l'envoi d'une requête SNMP à un agent.

Éléments de la structure

Nom	Type de données	Description
<i>sOid</i>	STRING[GPL.Gc_dwMaxSizeOid]	OID demandé Format : suite de nombres séparés par des points, par exemple, 1.3.6.1.2.1.1.5.0.
<i>sAgentIp</i>	STRING[15]	Adresse IP de l'agent SNMP
<i>pbyValueBuffer</i>	POINTER TO BYTE	Pointeur désignant le premier octet du tampon. Pour les requêtes <i>SET</i> , il s'agit du tampon contenant les données utilisateur à définir sur l'agent. Pour les requêtes <i>GET</i> , il s'agit du tampon où le bloc fonction stocke la réponse de l'agent.
<i>dwNumBytesValue</i>	DWORD	Taille du tampon ou de la valeur stockée dans le tampon Le tampon est référencé par le pointeur <i>pbyValueBuffer</i> . Pour les requêtes <i>GET</i> , définit la taille du tampon qui stocke les valeurs reçues. Pour les requêtes <i>SET</i> , définit la taille de la valeur dans le tampon à envoyer. NOTE: Dans le cas des chaînes, ajoutez un octet supplémentaire pour le caractère de fin de chaîne.
<i>etValueType</i>	ET_SnmpTag, page 35	Type de la valeur à définir par les requêtes <i>SET</i> (les requêtes <i>GET</i> ne l'utilisent pas).
<i>uiAgentSnmpPort</i>	UINT	Port SNMP de l'agent Valeur par défaut : 161
<i>sCommunityName</i>	STRING[255]	Nom de communauté de la requête Valeurs par défaut : - Requête SET : privée - Requête GET : publique
<i>sContextName</i>	STRING[255]	Nom de contexte utilisé dans la requête SNMPv3 lancée par une entité SNMP pour identifier une instance d'un contexte.

Utilisé par

- *FB_SnmpManager*

ST_Response

Présentation

Type :	Structure
Disponible à partir de :	V1.0.0.0
Hérite de :	—

Description

La structure *ST_Response* fournit les informations reçues d'un agent SNMP à la suite d'une requête.

Éléments de la structure

Nom	Type de données	Description
<i>sOid</i>	STRING[<i>GPL.Gc_dwMaxSizeOid</i>]	OID auquel l'agent a répondu. Cette information supplémentaire permet de faire le lien entre votre requête et la réponse.
<i>sAgentIp</i>	STRING[15]	Adresse IP de l'agent qui envoie la réponse. Cette information supplémentaire permet de faire le lien entre votre requête et la réponse.
<i>pbyValueBuffer</i>	POINTER TO BYTE	Pointeur vers le tampon contenant la valeur référencée par l'OID reçu sur une requête <i>GET</i> (tampon fourni par <i>iq_stRequestInfo.i_stRequest.pbyValueBuffer</i>). Dans le cas d'une requête <i>SET</i> , rien n'est écrit dans le tampon.
<i>dwNumBytesValue</i>	DWORD	Taille de la valeur référencée par l'OID qui a été défini/obtenu par la requête précédente.
<i>etProtocolVersion</i>	<i>ET_SnmpProtocolVersion</i>	Version du protocole SNMP envoyée par l'agent.

Utilisé par

- *FB_SnmpManager*

Variables globales

Contenu de cette partie

Liste des constantes globales.....41

Liste des paramètres globaux.....42

Liste des constantes globales

Contenu de ce chapitre

Liste des constantes globales (GCL).....41

Liste des constantes globales (GCL)

Présentation

Type :	Constantes globales
Disponible à partir de :	V1.0.0.0

Description

La liste des constantes globales contient les constantes globales de la bibliothèque SnmpManager.

Constantes globales

Variable	Type de données	Valeur	Description
<i>Gc_dwMaxLimitUserData</i>	DWORD	1500	Taille maximale de la combinaison de l'OID et de la valeur dans le télégramme SNMP, en octets. Cette valeur limite le paramètre <i>Gc_MaxSizeUserData</i> .
<i>Gc_uiDefaultPortSnmp</i>	UINT	161	Numéro de port de l'agent qui envoie/reçoit les requêtes SNMP. La valeur par défaut est le port standard 161.
<i>Gc_sLibraryVersion</i>	STRING[80]	Vx.x.x.0 ¹	Version de bibliothèque
<i>Gc_uiMaxLengthKey</i>	UINT	80	Longueur maximale du mot de passe d'authentification et de confidentialité.
<i>Gc_uiMaxNumOfUser</i>	UINT	100	Nombre maximal de comptes utilisateur pouvant être créés.
¹ Cette valeur varie selon la version de la bibliothèque.			

Liste des paramètres globaux

Contenu de ce chapitre

Liste des paramètres globaux (GPL)	42
--	----

Liste des paramètres globaux (GPL)

Présentation

Type :	Paramètres globaux
Disponible à partir de :	V1.0.0.0

Description

Cette liste contient les paramètres globaux de la bibliothèque SnmpManager. Vous pouvez les modifier en fonction de votre projet dans le **Gestionnaire de bibliothèques**.

Paramètres globaux

Variable	Type de données	Plage de valeurs	Description
<i>Gc_udiTimeout</i>	UDINT	> 0	Délai maximum d'attente d'une réponse de l'agent (millisecondes). Valeur par défaut : 10000
<i>Gc_uiMaxNumberRetries</i>	UINT	0 à 65355	Nombre maximum de tentatives d'envoi d'une requête après un timeout. Valeur par défaut : 2
<i>Gc_dwMaxSizeOid</i>	DWORD	1... <i>GPL.Gc_dwMaxSizeUserData</i>	Taille maximale pour STRING <i>i_q_stRequestInfo.i_stRequest.sOid</i> . Valeur par défaut : 255
<i>Gc_dwMaxSizeUserData</i>	DWORD	1... <i>GCL.GC_MaxLimitUserData</i> .	Taille maximale de la combinaison de l'OID et de la valeur en octets dans le télégramme SNMP. Cette valeur est limitée par <i>Gc_dwMaxLimitUserData</i> . Valeur par défaut : 1400

Interfaces

Contenu de cette partie

<i>IF_UserManagement</i>	44
--------------------------------	----

IF_UserManagement

Contenu de ce chapitre

IF_UserManagement - Informations générales	44
--	----

IF_UserManagement - Informations générales

Présentation

Type :	Interface
Disponible à partir de :	V1.3.4.0
Hérite de :	—

Tâche

Interface fournissant une référence à la gestion des utilisateurs.

Description

Cette interface fournit une référence à la gestion des utilisateurs.

L'interface est implémentée par le bloc fonction *FB_SnmManager*, page 46.

Unités d'organisation de programme (POU)

Contenu de cette partie

Blocs fonction	46
Fonctions.....	51

Blocs fonction

Contenu de ce chapitre

<i>FB_SnmprManager</i>	46
<i>FB_UserManagement</i> - Informations générales	47
<i>FB_UserManagement</i> - <i>AddUser</i> (méthode)	48
<i>FB_UserManagement</i> - <i>DeleteUser</i> (méthode)	49

FB_SnmprManager

Présentation

Type :	Bloc fonction
Disponible à partir de :	V1.0.0.0



Tâche

Le bloc fonction *FB_SnmprManager* permet d'envoyer des requêtes SNMP aux équipements gérés sur des réseaux IP (Internet Protocol).

Description fonctionnelle

Le bloc fonction *FB_SnmprManager* est l'interface utilisateur des communications SNMP.

Une seule requête à un agent peut être prise en charge à la fois.

Le bloc fonction doit être activé et prêt à traiter une requête. Au début de l'exécution d'une requête, les entrées *i_etRequest* et *iq_stRequestInfo* doivent être définies. Les informations des entrées servent à créer un télégramme SNMP contenant la requête puis à l'envoyer à l'agent via UDP. L'entrée *i_ifUserManagement* est utilisée pour référencer l'instance de *FB_SnmprManager* qui contient l'utilisateur spécifié dans l'entrée *i_sUser*. Les données utilisateur sont utilisées pour authentifier et crypter la requête SNMPv3. Le bloc fonction attend une réponse de l'agent, la traite et présente les informations reçues dans *iq_stRequestInfo.stResponse*. Tant que le bloc fonction exécute une requête, la sortie *q_xBusy* est à TRUE et *q_etResult* indique l'état de l'opération. La sortie *q_xDone* signale une exécution réussie et *q_xError* indique si le bloc fonction détecte une erreur lors de l'exécution, avec *q_etResult* et *q_sResultMsg* présentant des informations complémentaires sur la nature ou la cause de l'erreur détectée. Si une erreur est détectée, le bloc fonction doit être réinitialisé en le désactivant et en le réactivant.

Interface

Entrée	Type de données	Description
<i>i_xEnable</i>	BOOL	Activation et initialisation du bloc fonction.
<i>i_xExecute</i>	BOOL	La commande spécifiée dans <i>i_etRequest</i> est exécutée sur le front montant de cette entrée.
<i>i_etRequest</i>	<i>ET_SnmppRequest</i> , page 34	Requête SNMP exécutée si <i>i_xExecute</i> est TRUE. Assurez-vous que <i>iq_stRequestInfo</i> est disponible avant l'exécution de la requête SNMP.
<i>i_etVersion</i>	<i>ET_SnmppProtocolVersion</i> , page 33	Spécifie la version du protocole pour la communication avec l'agent. La valeur par défaut est <i>ET_SnmppProtocolVersion.Version2c</i> .
<i>i_etSecurityLevel</i>	<i>ET_SecurityLevel</i> , page 33	Niveau de sécurité associé à l'envoi des messages SNMPv3. NOTE: Le compte utilisateur spécifié dans <i>i_sUser</i> doit être configuré en fonction du niveau de sécurité sélectionné.
<i>i_sUser</i>	STRING	Nom du compte utilisateur pour l'authentification et le cryptage de la requête SNMPv3.
<i>i_ifUserManagement</i>	<i>IF_UserManagement</i> , page 44	Référence à l'instance <i>FB_UserManagement</i> dans laquelle le compte utilisateur a été créé. NOTE: Cette entrée peut être ignorée si aucun compte utilisateur n'est spécifié par <i>i_sUser</i> .

Entrée/sortie	Type de données	Description
<i>iq_stRequestInfo</i>	<i>ST_RequestInformation</i>	Permet de transmettre la structure contenant les informations pour l'envoi d'une requête à un agent et la structure pour la présentation de la réponse reçue de l'agent.

Sortie	Type de données	Description
<i>q_xActive</i>	BOOL	Si le bloc fonction est actif, cette sortie est TRUE.
<i>q_xReady</i>	BOOL	Si l'initialisation réussit, cette sortie est TRUE tant que le bloc fonction accepte des entrées.
<i>q_xBusy</i>	BOOL	Si cette sortie est TRUE, le bloc fonction est en train d'exécuter la commande spécifiée dans <i>i_etRequest</i> .
<i>q_xDone</i>	BOOL	Si cette sortie est TRUE, le bloc fonction a exécuté avec succès la commande spécifiée dans <i>i_etRequest</i> . Des données supplémentaires sont fournies dans <i>iq_stRequestInfo.q_stResponse</i> .
<i>q_xError</i>	BOOL	Si cette sortie est TRUE, une erreur a été détectée. Pour plus d'informations, consultez <i>q_etResult</i> et <i>q_etResultMsg</i> .
<i>q_etResult</i>	<i>ET_Result</i>	Fournit des informations de diagnostic et d'état.
<i>q_sResultMsg</i>	STRING[255]	Fournit des informations supplémentaires de diagnostic et d'état.

FB_UserManagement - Informations générales

Présentation

Type :	Bloc fonction
Disponible à partir de :	V1.3.4.0

Tâche

FB_UserManagement est utilisé pour gérer les comptes d'utilisateurs pour les communications SNMPv3.

Description fonctionnelle

Le bloc fonction *FB_UserManagement* permet de gérer les comptes utilisateur pour le modèle de sécurité basé sur l'utilisateur dans la version 3 du protocole SNMP (SNMPv3). Il doit être instancié à l'intérieur de l'application utilisateur. Pour conserver les données utilisateur enregistrées dans un tableau de l'instance de bloc fonction après une réinitialisation du contrôleur, il est également possible d'utiliser une mémoire de conservation.

Le bloc fonction implémente l'interface *IF_UserManagement*, page 44. Par conséquent, il peut être référencé par le bloc fonction *FB_SnmprManager*, page 46 via l'entrée *i_ifUserManagement*.

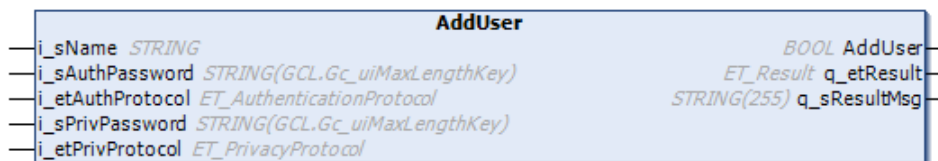
Propriétés

Propriété	Type de données	Accès	Description
<i>NumberOfAddedUser</i>	UDINT	Get	Indique le nombre de comptes utilisateur ajoutés.

FB_UserManagement - *AddUser* (méthode)

Présentation

Type :	Bloc fonction
Disponible à partir de :	V1.3.4.0



Tâche

Créez un compte utilisateur en fournissant les informations liées à l'authentification et au cryptage.

Description fonctionnelle

La méthode *AddUser* est utilisée pour créer un compte utilisateur en fournissant les informations liées à l'authentification et au cryptage.

Interface

Entrée	Type de données	Description
<i>i_sName</i>	STRING	Nom du compte utilisateur.
<i>i_sAuthPassword</i>	STRING(<i>GCL_internal.Gc_uiMaxLengthKey</i>)	Mot de passe d'authentification à utiliser avec le protocole d'authentification.
<i>i_etAuthProtocol</i>	<i>ET_AuthenticationProtocol</i> , page 27	Type de protocole d'authentification utilisé pour authentifier les messages envoyés de la part de ce compte utilisateur.
<i>i_sPrivPassword</i>	STRING(<i>GCL_internal.Gc_uiMaxLengthKey</i>)	Mot de passe de confidentialité à utiliser avec le protocole de confidentialité.
<i>i_etPrivProtocol</i>	<i>ET_PrivacyProtocol</i> , page 27	Type de protocole de confidentialité utilisé pour protéger les messages envoyés de la part de ce compte utilisateur contre la divulgation.

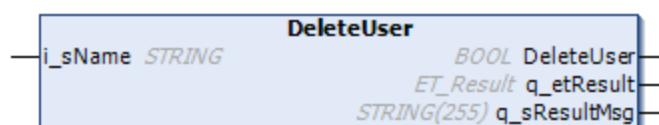
Valeur renvoyée

Sortie	Type de données	Description
<i>AddUser</i>	BOOL	Indique TRUE si le compte utilisateur a été créé.
<i>q_etResult</i>	<i>ET_Result</i>	Fournit des informations de diagnostic et d'état.
<i>q_sResultMsg</i>	STRING[255]	Fournit des informations supplémentaires de diagnostic et d'état.

FB_UserManagement - DeleteUser (méthode)

Présentation

Type :	Bloc fonction
Disponible à partir de :	V1.3.4.0



Tâche

Supprimer un compte utilisateur.

Description fonctionnelle

La méthode *DeleteUser* est utilisée pour supprimer un compte utilisateur.

Interface

Entrée	Type de données	Description
<i>i_sName</i>	STRING	Nom du compte utilisateur à supprimer.

Valeur renvoyée

Sortie	Type de données	Description
<i>DeleteUser</i>	BOOL	Indique TRUE si le compte utilisateur a bien été supprimé.
<i>q_etResult</i>	<i>ET_Result</i>	Fournit des informations de diagnostic et d'état.
<i>q_sResultMsg</i>	STRING[255]	Fournit des informations supplémentaires de diagnostic et d'état.

Fonctions

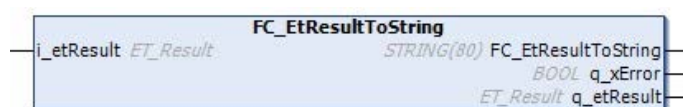
Contenu de ce chapitre

FC_EtResultToString51

FC_EtResultToString

Présentation

Type :	Fonction
Disponible à partir de la version :	V1.0.0.0
Hérite de :	–
Met en œuvre :	–



Tâche

Convertir un élément d'énumération *ET_Result* en variable STRING.

Description fonctionnelle

FC_EtResultToString est utilisé pour convertir une variable d'élément *ET_Result* en variable STRING.

Interface

Entrée	Type de données	Description
<i>i_etResult</i>	<i>ET_Result</i>	Énumération avec le résultat.

Sortie	Type de données	Description
<i>q_xError</i>	BOOL	Si cette sortie est TRUE, une erreur a été détectée.
<i>q_etResult</i>	<i>ET_Result</i>	Énumération avec le résultat.

Valeur retournée

Type de données	Description
STRING[80]	Variable <i>ET_Result</i> convertie en texte.

Glossaire

I

IP:

Acronyme de *Internet Protocol*, protocole Internet. Le protocole IP fait partie de la famille de protocoles TCP/IP, qui assure le suivi des adresses Internet des équipements, achemine les messages sortants et reconnaît les messages entrants.

M

MIB:

Acronyme de *Management Information Base*, base d'informations de gestion. Base de données orientée objets contrôlée par un système de gestion de réseaux tel que SNMP. SNMP surveille des équipements qui sont définis par leurs MIBs. Schneider Electric a obtenu une base MIB privée, appelée groupeschneider (3833).

S

SNMP:

Acronyme de *simple network management protocol*, protocole de gestion de réseau simple. Protocole qui peut contrôler un réseau à distance en interrogeant les équipements pour obtenir leur état et en affichant les informations liées à la transmission de données. Il peut aussi être utilisé pour gérer des logiciels et des bases de données à distance, et il permet d'effectuer des tâches de gestion actives, comme la modification et l'application d'une nouvelle configuration.

U

UDP:

Acronyme de *User Datagram Protocol*, protocole de datagramme utilisateur. Protocole de mode sans fil (défini par la norme IETF RFC 768) dans lequel les messages sont livrés dans un datagramme vers un ordinateur cible sur un réseau IP. Le protocole UDP est généralement fourni en même temps que le protocole Internet. Les messages UDP/IP n'attendent pas de réponse et, de ce fait, ils sont particulièrement adaptés aux applications dans lesquelles aucune retransmission des paquets envoyés n'est nécessaire (comme dans la vidéo en continu ou les réseaux exigeant des performances en temps réel).

Index

A

AddUser, méthode 48

B

bibliothèques
SnmManager 17

C

Concept de diagnostic 22

D

DeleteUser, méthode 49

E

entrées et sorties communes
comportement des blocs fonction avec entrées *i_*
 xEnable et *i_xExecute* 21
ET_AuthenticationProtocol 27
ET_PrivacyProtocol 27
ET_Result 28
 AsyncTaskStartUnsuccessful 29
 CorruptedResponse 31
 Disabled 29
 EncryptionUnsuccessful 32
 Evaluating 29
 GplMaxOidTooBig 29
 GplMaxOidTooSmall 29
 GplMaxUserDataTooBig 29
 GplMaxUserDataTooSmall 29
 GplTimeoutZero 29
 InitAsyncManagerUnsuccessful 29
 InputInvalidBufferSize 29
 InputInvalidIp 30
 InputInvalidKey 32
 InputInvalidOid 29
 InputInvalidPointer 30
 InputInvalidRequest 29
 InputInvalidSecurityLevel 30
 InputInvalidUser 30
 InputInvalidUserManagement 30
 InputInvalidValueIp 30
 InputInvalidValueOid 30
 InputInvalidVersion 30
 InputMissingOid 29
 InputSize32BitValue 30
 InputSize64BitValue 30
 InvalidUserConfiguration 30
 Listening 29
 MaxNumberUserTooSmall 29
 MaxTelegramSize 29
 NotReady 29
 Ok 29
 Sending 29
 SnmResponseEndofMibView 32
 SnmResponseGenErr 31
 SnmResponseGetNoSuchInstance 32
 SnmResponseGetNoSuchObject 32
 SnmResponseSetInconsistentValue 32
 SnmResponseSetNoAccess 31

SnmResponseSetNoCreation 32
SnmResponseSetNoSuchName 32
SnmResponseSetNotWritable 32
SnmResponseSetWrongEncoding 31
SnmResponseSetWrongLength 31
SnmResponseSetWrongType 31
SnmResponseSetWrongValue 32
SnmResponseTooBig 31
SnmResponseV1WrongErrorState 32
SnmVersion1SetCounter64 32
UdpInvalidBufferAddress 30
UdpInvalidIp 30
UdpIssue 30
UdpNotReady 30
UdpNotSupported 30
UdpNumBytesSendOutOfRange 30
UdpReceiveBufferSizeOutOfRange 30
UdpSocketMngListTooSmall 30
UdpTimeout 30
UnknownResult 32
UnknownState 29
UserNotFound 30
ValidateAuthenticationUnsuccessful 31
ValidateBufferTooSmall 31
ValidateMessageIdNoMatch 31
ValidateNoValue 31
ValidateOidNoMatch 31
ValidateRequestIdNoMatch 31
ValidateVersionNotSupported 31
ValueNotSupported 32
ET_SecurityLevel 33
ET_SnmRequest 34
 GetRequest 34
 NoCommand 34
 SetRequest 34
ET_SnmTag 35
 Counter32 35
 Counter64 35
 Gauge32 35
 Integer 35
 IpAddress 35
 ObjectId 35
 OctetString 35
 TimeTicks 35

F

FB_SnmManager 46
FB_UserManagement 47
FC_EtResultToString 51

G

GCL (liste des constantes globales)
 SnmManager 41
GPL (liste des paramètres globaux)
 SnmManager 42

I

IF_UserManagement 44

L

Limitations du transfert SNMP 18

Q

q_etResult	22
q_sResultMsg	22
q_xError	22

S

SnmpManager	17
GCL (liste des constantes globales)	41
GPL (liste des paramètres globaux)	42
<i>ST_Request</i>	37
<i>ST_RequestInformation</i>	37
<i>ST_Response</i>	38

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Les normes, spécifications et conceptions pouvant changer de temps à autre, veuillez demander la confirmation des informations figurant dans cette publication.

© 2023 Schneider Electric. Tous droits réservés.

EIO0000002798.02