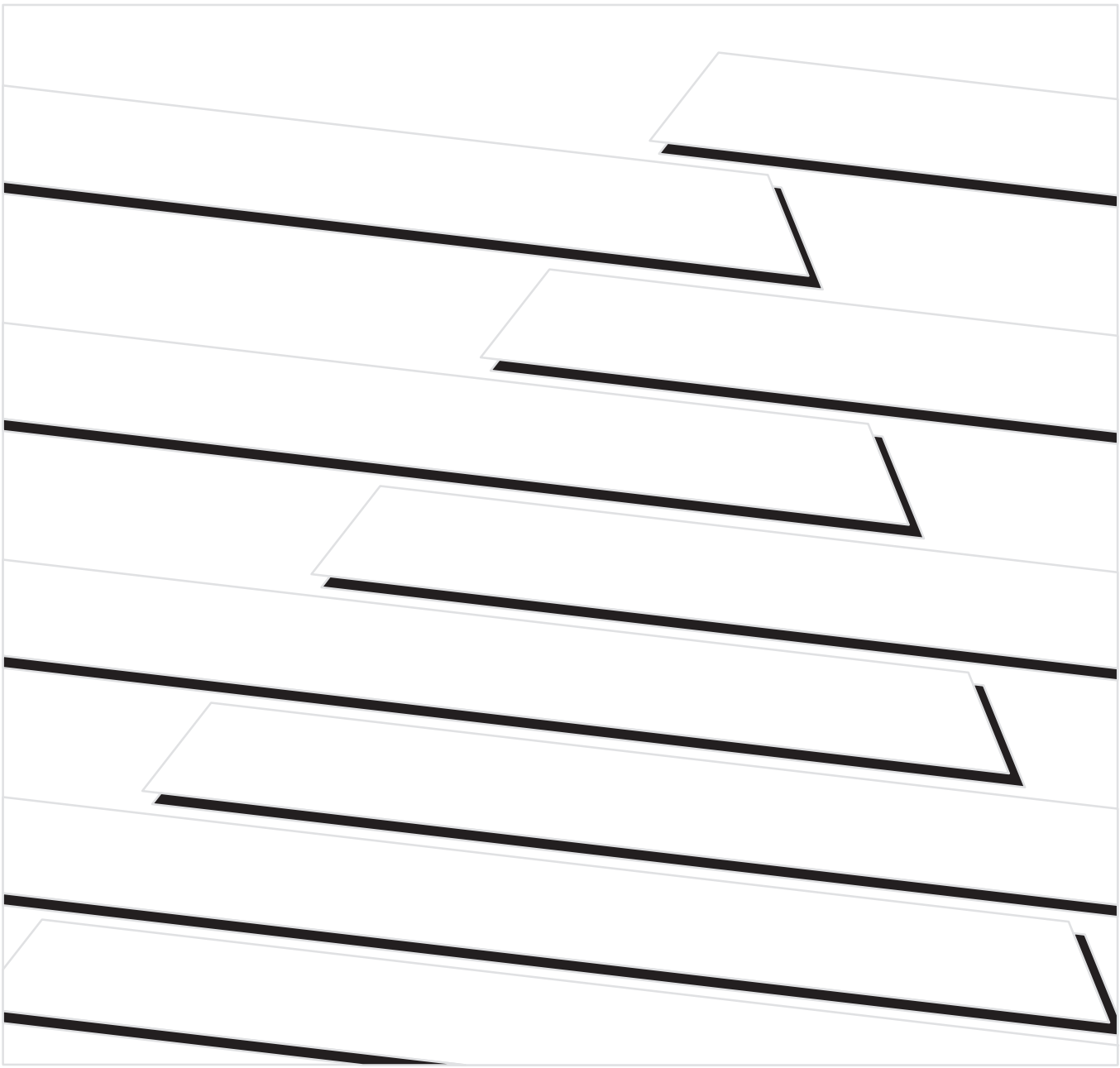
ALLEN-BRADLEY

Processeurs protégés PLC-5

(Réf. 1785-L26B, -L46B et -L86B)

Supplément



Informations utilisateurs

En raison de la diversité des utilisations des produits décrits dans le présent manuel, les personnes qui en sont responsables doivent s'assurer que toutes les mesures ont été prises pour que l'application et l'utilisation des produits soient conformes aux exigences de performance et de sécurité, ainsi qu'aux lois, règlements, codes et normes en vigueur.

Les illustrations, schémas et exemples de programmes contenus dans ce manuel sont présentés à titre indicatif seulement. En raison des nombreuses variables et impératifs associés à chaque installation, la société Allen-Bradley ne saurait être tenue pour responsable ou redevable (y compris en matière de propriété intellectuelle) des suites d'utilisation réelle basée sur les exemples et schémas présentés dans ce manuel.

La publication SGI-1.1 « Safety Guidelines for the Application, Installation, and Maintenance of Solid-State Control » (disponible auprès de votre agence commerciale Allen-Bradley) décrit certaines différences importantes entre les équipements électroniques et les équipements électromécaniques qui devront être prises en compte lors de l'application de ces produits comme indiqué dans la présente publication.

Des remarques sont utilisées tout au long de ce manuel pour attirer votre attention sur les mesures de sécurité à prendre en compte :

ATTENTION : Indique les informations sur les pratiques ou circonstances pouvant entraîner des dommages corporels, des dégâts matériels ou des pertes financières.

Les encarts « Attention » vous aident à :

- identifier un danger
- éviter ce danger
- en discerner les conséquences

Important : Indique les informations déterminantes pour la bonne compréhension et application du produit.

Contenu du supplément

Introduction

Ce supplément décrit l'utilisation des fonctions de sécurité spécifiques au processeur protégé PLC-5/26™, PLC-5/46™ ou PLC-5/86™.

A qui s'adresse ce document

Les informations contenues dans ce supplément sont principalement destinées à l'**administrateur système**— utilisateur à privilèges uniques pouvant commander l'acccès aux zones critiques du programme d'un processeur protégé. **Les utilisateurs finals**—opérateurs disposant d'un accès restreint au programme du processeur—peuvent également tirer profit de la lecture de ce supplément.

En tant qu'ingénieur ou technicien, vous devez connaître les applications des systèmes de commande et être familiarisé avec :

- les systèmes de commande en temps réel programmables
- le système de commande du PLC-5®
- les principales exigences de sécurité de votre application

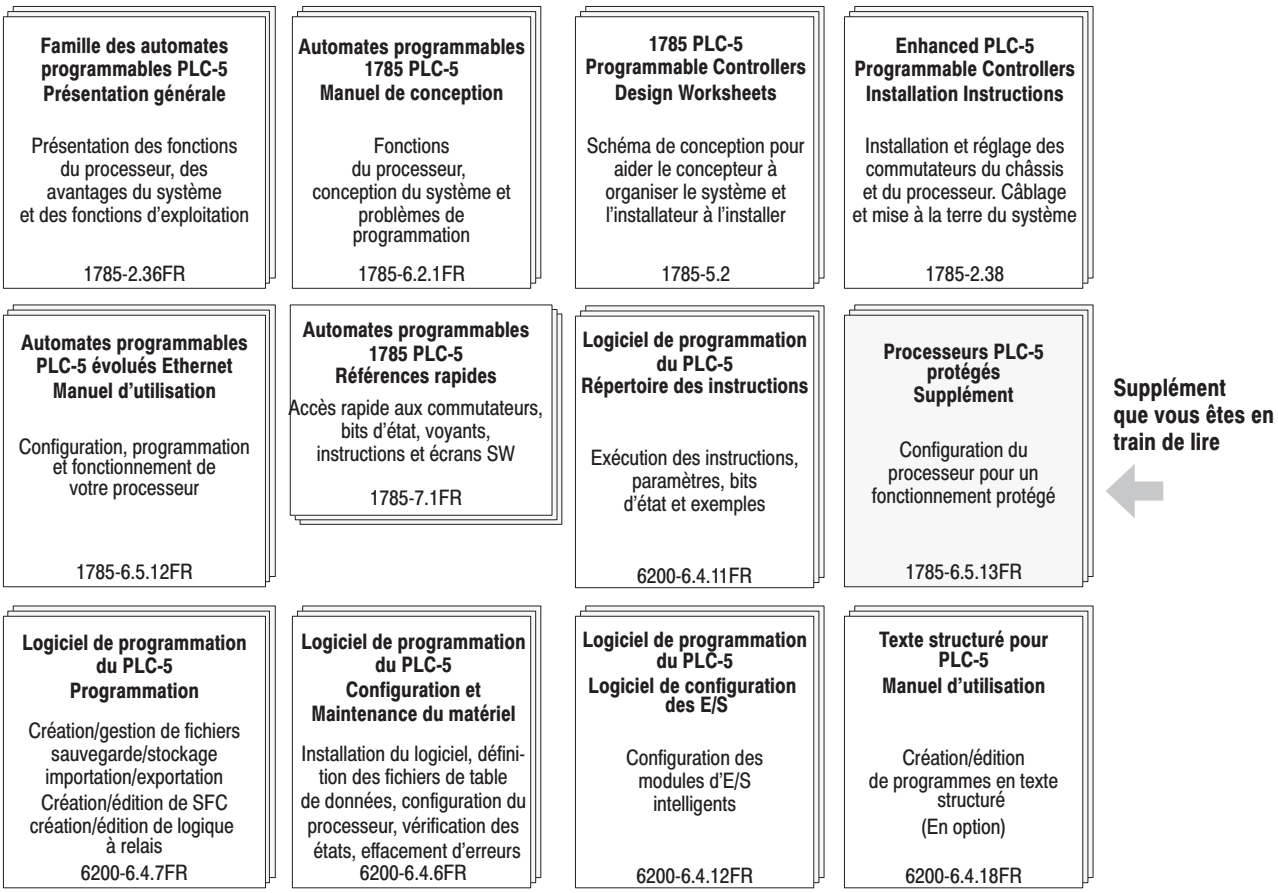
Contenu

Terminologie

Terme	Définition
DTEP	Protection d'éléments de la table de données
Utilisateur final	Utilisateur d'un processeur protégé, qui, généralement **ne peut pas** modifier les privilèges ou les mots de passe et par conséquent **n'a pas** l'autorisation de passer outre la DTEP du processeur
Classe	Un des quatre groupes de privilèges, définis par l'administrateur, autorisant l'utilisateur à effectuer certaines opérations spécifiques de commande du processeur. Chaque utilisateur peut accéder à une classe par un mot de passe attribué par l'administrateur
Commande filtrée	Commande de communications utilisée dans l'interface entre le processeur et le logiciel de programmation, filtrée pour dépister les violations des mécanismes de protection du processeur protégé PLC-5
Administrateur système	Utilisateur d'un processeur protégé, qui, **peut** généralement modifier les privilèges et les mots de passe et, par conséquent, **a** l'autorisation de passer outre la DTEP du processeur
Privilège	Capacité à effectuer une opération de commande acceptée par le processeur protégé PLC-5, y compris : • modification des privilèges • création/suppression des fichiers dans la table de données • création/suppression des fichiers programme • écriture logique • écriture physique • lecture logique • lecture physique • changement de mode • forçage d'E/S • forçage de SFC • effacement de la mémoire • restauration • édition en ligne

Documents associés

La documentation de l'automate programmable PLC-5 1785 est organisée en manuels en fonction des tâches à effectuer.



Pour plus d'informations sur les automates programmables PLC-5 1785 ou les publications ci-dessus, adressez-vous à votre agence, distributeur ou intégrateur système Allen-Bradley.

Table des matières

Organisation d'un système protégé

Chapitre 1

Configuration des mots de passe et des privilèges

Chapitre 2

Configuration et utilisation de la protection d'éléments de la table de données

Chapitre 3

Chapitre 1

Organisation d'un système protégé

Introduction

Les caractéristiques de sécurité du processeur PLC-5 protégé sont conçues pour restreindre l'accès aux zones critiques de votre programme :

- en assurant un fonctionnement plus homogène de votre machine/application
- en vous aidant à réduire les risques dus à une modification non autorisée du programme

Le processeur protégé est conçu pour améliorer la sécurité en vous permettant d'éviter :

- le forçage des E/S de groupes de module spécifiques
- la manipulation non autorisée de certains segments de mots de la table de données par
  - commandes d'écriture
  - instructions de sortie

ATTENTION : Les processeurs protégés ne peuvent pas à eux **seuls** assurer la protection d'un système PLC. La sécurité d'un système repose à la fois sur le processeur protégé, le logiciel et la connaissance de l'application.

Caractéristiques d'un système protégé

Tous les processeurs PLC-5(PLC-5/11, -5/20, –5/20E, -5/26, -5/30, -5/V30, -5/40, -5/40E, -5/40L, -5/V40, -5/V40L, -5/46, -5/60, -5/60L, -5/80, -5/80E et -5/86) permettent à l'administrateur système de configurer de 1 à 4 classes de privilèges, protégées par mot de passe, et de définir chaque classe en leur donnant accès à une seule combinaison d'opérations logicielles. En tant qu'administrateur système, vous pouvez également définir les privilèges d'écriture et de lecture limitant l'accès aux :

- voies de communication
- fichiers programme
- fichiers de données
- stations connectées à la liaison Data Highway Plus™ (DH+™)

Important : Vous devez activer la fonction privilèges et mots de passe lors de l'installation initiale de votre logiciel de programmation Série 6200 si vous souhaitez utiliser les caractéristiques de protection de votre processeur.

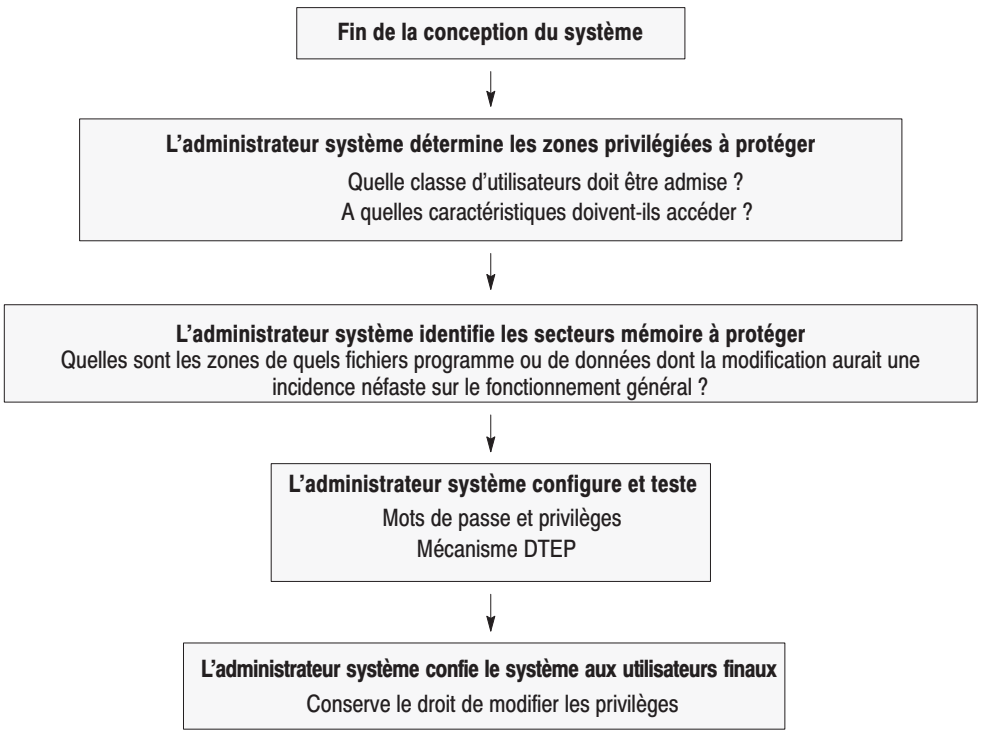
Pour commander	Le processeur PLC-5 évolué vous permet :	De plus, le processeur protégé vous permet d'utiliser la DTEP pour
Forçage d'E/S	d'attribuer ou de refuser **le privilège de forçage des E/S** à une classe d'utilisateurs de donner uniquement un contrôle total ou aucun contrôle	empêcher les modifications de groupes de modules spécifiques par forçage d'E/S initié par un utilisateur final
Ecriture dans la table des données	• d'attribuer ou de refuser le **privilège d'écriture logique** à une classe d'utilisateurs de donner uniquement un contrôle total ou aucun contrôle • de définir **une protection en lecture seule** pour certains fichiers Aucun des mécanismes n'empêche l'utilisateur d'écrire une logique contournant les protections pour modifier un emplacement dans la table de données	empêcher les écritures sur des segments spécifiques de mots de la table de données en : • envoyant les commandes d'écriture directement à la table de données • ajoutant ou modifiant les instructions à relais pouvant écrire dans la zone protégée

Exigences d'un système protégé

Matériel requis	Logiciel requis
Automate programmable PLC-5/26, -5/46 ou -5/86 (1785-L26B, -L46B ou -L86B ; Série C, Révision G ou ultérieure)	Logiciel de programmation du PLC-5 Série 6200, Version 5.0 ou ultérieure

Directives de mise en application

Après avoir terminé la conception de votre système de processeur PLC-5 protégé, votre premier rôle en tant qu'administrateur système consiste à empêcher les utilisateurs finals de déjouer les mécanismes de sécurité que vous avez définis pour le système.



Mots de passe et privilèges

Conseil Garder le contrôle du **droit de modifier les privilèges** est l'élément majeur de la réussite du mécanisme DTEP.

Les classes de privilège d'un processeur PLC-5 ne sont pas nécessairement hiérarchiques. Les privilèges de la Classe 1 sont considérés comme « supérieurs » aux autres uniquement parce que personne ne peut supprimer le droit de modifier les privilèges de la classe 1. Il semblerait logique que l'administrateur système traite la classe 1 comme la classe supérieure et définisse les privilèges en conséquence, c'est-à-dire en ordre décroissant jusqu'à la classe 4. En général, il doit garantir le droit de modifier les privilèges uniquement au niveau le plus élevé et ne jamais révéler le mot de passe aux autres utilisateurs. De ce fait, il doit anticiper les besoins des utilisateurs finals et définir les mots de passe et privilèges en conséquence.

En tant qu'administrateur système, vous devez protéger les fichiers de données et les fichiers programme critiques en fonction de vos besoins—c'est-à-dire en classant ces fichiers en « lecture seule » ou « aucune lecture, aucune écriture » pour toutes les classes sauf la classe 1. Ceci constitue une protection contre toute modification de votre logique et détermine également les fichiers programme à filtrer lors du chargement. Vous devez également configurer toutes les voies de communication—y compris les voies inutilisées actuellement—en fonction des classes de privilège appropriées.

Protection d'éléments de la table de données (DTEP)

Les fonctions de sécurité spécifiques au processeur PLC-5 protégé vous permettent de définir les secteurs mémoire qui ne peuvent pas être modifiés par des utilisateurs autres que ceux de la classe 1. Au cours de la programmation en ligne par des utilisateurs finals, le processeur PLC-5 protégé agit comme filtre pour trier et empêcher les requêtes comme :

- l'ajout d'un code à relais qui permettrait d'écrire ou de manipuler les adresses protégées de la table de données
- la modification
  - de mots protégés de la table de données par des opérations d'écriture
  - d'éléments protégés d'image des E/S par le forçage d'E/S

Lorsque	et que	Résultat
l'utilisateur final n'est pas autorisé à modifier les privilèges	le fichier d'état du processeur contient la valeur d'un fichier DTEP (voir page 3-2)	La DTEP est activée
la DTEP est activée	le processeur reçoit une requête de commande filtrée (voir page 3-5)	L'option de filtrage s'effectue lors de l'édition en ligne d'un programme

Conseil

L'emplacement dans le fichier d'état de la valeur du fichier DTEP (S:63) est automatiquement protégé : vous n'avez donc pas à le protéger individuellement.

Parmi les secteurs mémoire qu'il est utile de protéger à l'aide du mécanisme DTEP, citons :

- les mots de sortie critiques en matière de sécurité
- certains compteurs, temporisateurs ou structures de commande BT/MG/PD
- les registres de stockage de nombres entiers
- les mots de la table de données utilisés pour spécifier les adresses indirectes dans les tables de données critiques
- les mots du fichier d'état du processeur qui configurent le système, tels que :

Mot(s)	Utilisation
S:9	Temps de scrutation maximum①
S:26	Bits de commande utilisateur
S:29	Numéro du sous-programme de gestion des défauts
S:30-31	Configuration de l'interruption temporisée programmable (STI)
S:46-50	Configuration de l'interruption d'entrée du processeur (PII)
S:54	Temps de scrutation STI maximum①
S:56	Temps de scrutation PII maximum①
S:77	Tranche de temps de communication
S:78-123	Configuration du programme de commande principal (MCP) et temps maximum de chaque scrutation MCP①

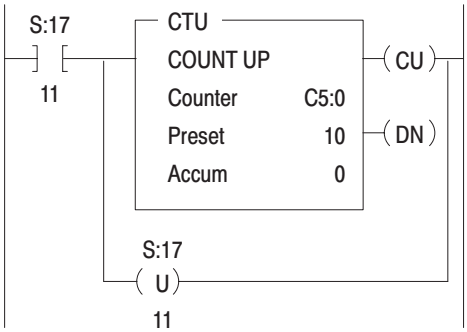
① Pour vérifier que les paramètres de performance ne sont pas violés, par exemple.

En tant qu'administrateur système, vous pouvez donner aux utilisateurs finals une certaine souplesse d'intégration au système mais vous devez conserver le contrôle des logiques critiques STI, PII ou des sous-programmes de gestion des défauts. Après avoir protégé les registres ci-dessus au moyen de la DTEP, vous pouvez définir certains fichiers à relais vides non protégés et inclure des sauts vers des sous-programmes (JSR) faisant référence à ces fichiers à la fin de programmes critiques. L'utilisateur final peut ensuite ajouter une logique à une STI par exemple, sans ouvrir le véritable fichier STI pour le modifier.

Le mécanisme de DTEP assure également une certaine protection contre les changements non autorisés effectués par un utilisateur final à l'aide du logiciel de programmation hors ligne :

- Au cours du chargement d'un fichier image de processeur protégé, le processeur protégé filtre tous les fichiers programme de type à relais de l'utilisateur final—y compris les fichiers en texte structuré et SFC—pour dépister les opérandes en dehors des plages de DTEP.
- Les opérations de forçage des E/S ne peuvent pas être chargées et doivent donc être effectuées en ligne.
- Les changements hors ligne des valeurs stockées dans les emplacements protégés de la table de données peuvent être annulés si l'administrateur système adopte de bonnes méthodes de programmation et initialise tous les emplacements de la table de

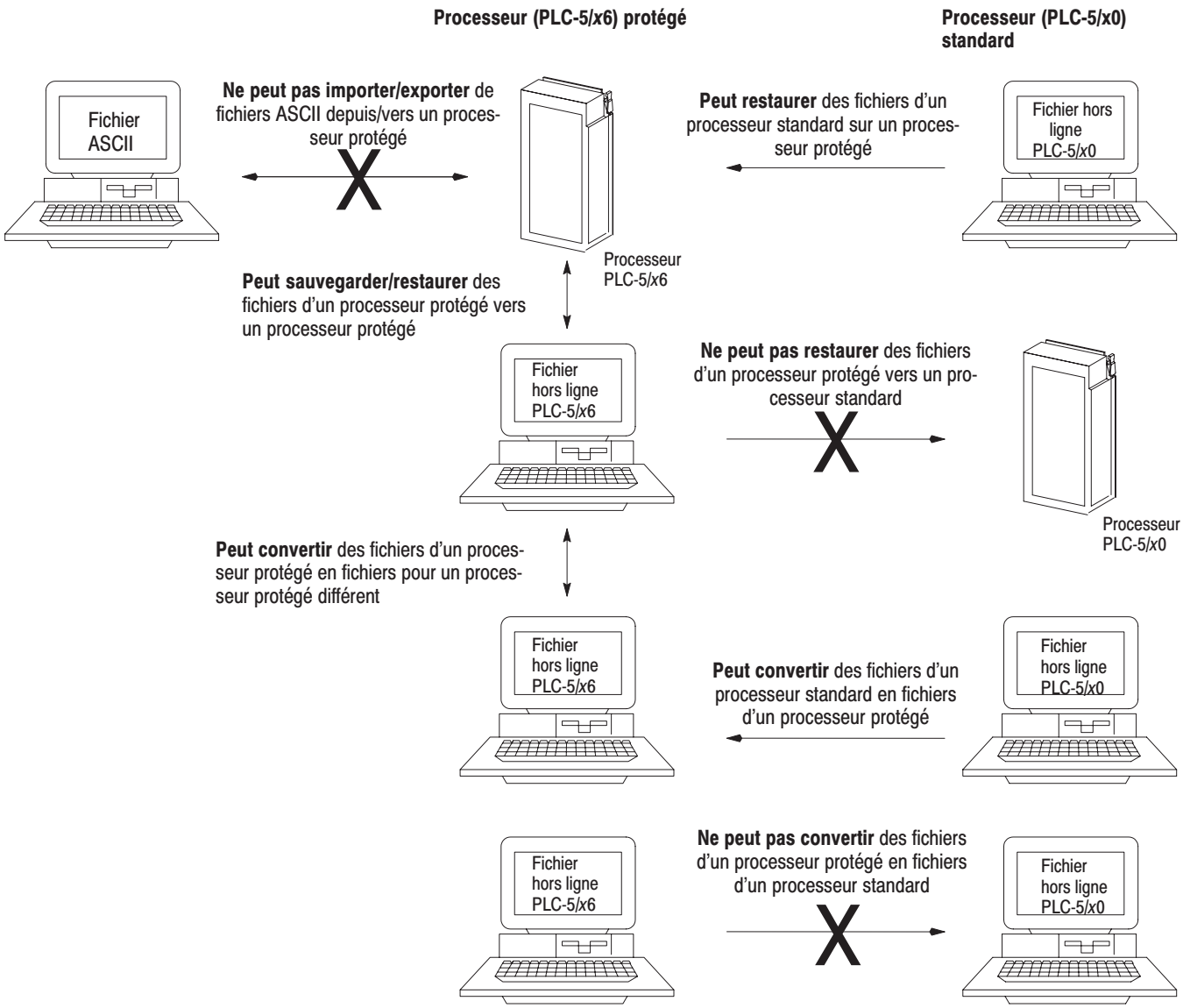
données aux valeurs souhaitées en dehors de l'indicateur de première scrutation du processeur (S:1/15).



Vous pouvez utiliser le bit de défaut mineur du fichier d'état (S:17/11) comme moyen de surveillance des tentatives de contournement des mécanismes de protection par les utilisateurs finals. Ce bit signale une tentative de violation des protections. Il peut être utilisé pour compter les tentatives d'intrusion, si vous ajoutez à la logique à relais une ligne qui incrémente un compteur et efface le bit de défaut mineur à chaque tentative.

Règles de conversion des fichiers programme

Suivez les règles ci-dessous lors du partage de fichiers programme entre des processeurs standard PLC-5 évolués et des processeurs PLC-5 protégés.

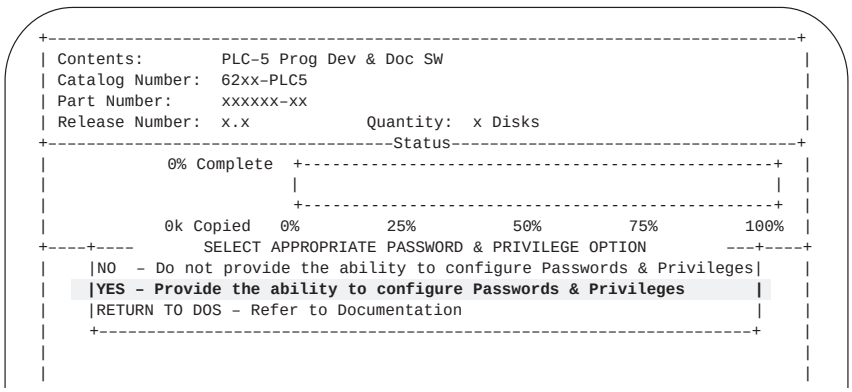


Chapitre 2

Configuration des mots de passe et des privilèges

Contenu du chapitre

Important : Lorsque vous installez le logiciel de programmation du PLC-5 série 6200 pour la première fois, l'écran suivant apparaît :



Vous devez choisir l'option suivante :

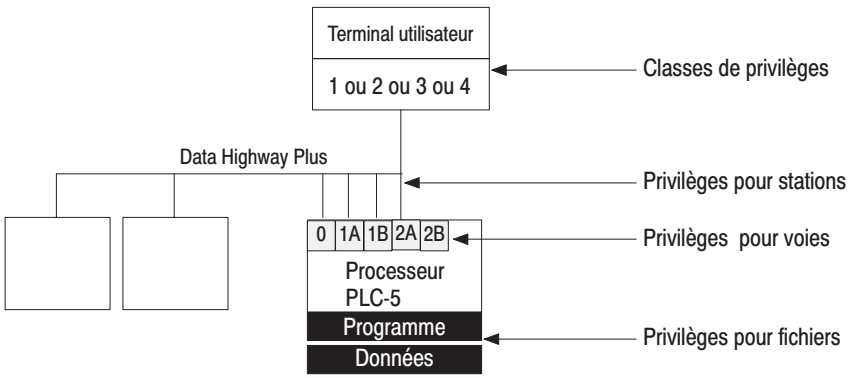
```
YES - Provide the ability to configure Passwords &
Privileges
```

Pour plus d'informations sur l'installation du logiciel et la configuration des mots de passe et des privilèges, consultez la publication 6200-6.4.6FR « Logiciel de programmation du PLC-5 – Configuration et maintenance du matériel ».

Directives pour l'attribution des mots de passe et des privilèges

Les classes de privilèges forment le niveau supérieur de la structure des mots de passe.

Hiérarchie des privilèges



L'administrateur système doit :

Définir les mots de passe et les privilèges de chaque processeur du système

↓

Attribuer les privilèges de classe par défaut aux voies de communication et fichiers hors ligne

↓

Définir l'accès lecture et écriture aux écrans de configuration des voies

↓

Attribuer les privilèges pour toute station nécessitant des privilèges autres que les privilèges par défaut des voies

↓

Définir l'accès lecture et écriture aux fichiers programme

↓

Définir l'accès lecture et écriture aux fichiers de données

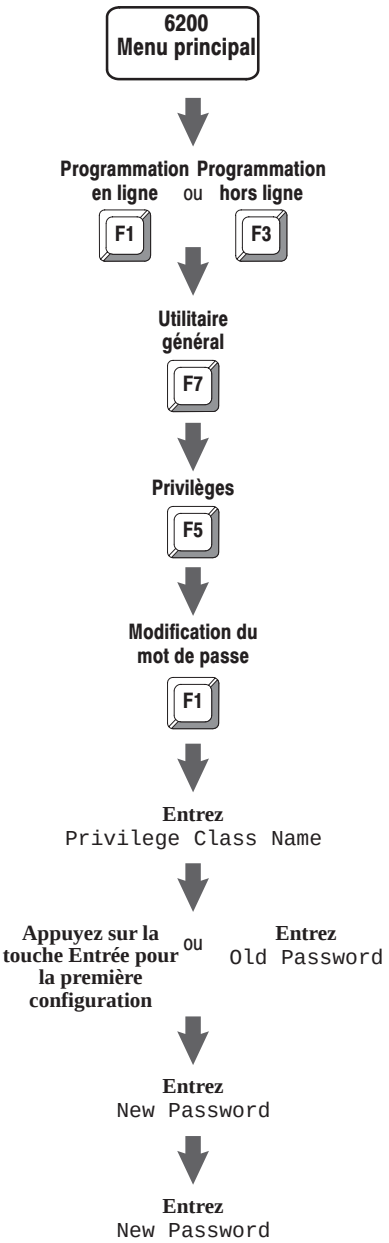
↓

Indiquer aux utilisateurs les classes de privilèges qu'ils peuvent utilliser et les mots de passe correspondants

L'utilisateur final doit entrer dans une autre classe avec un autre mot de passe pour acquérir les privilèges d'une classe autre que la classe par défaut

Attribution des mots de passe et des privilèges aux classes

L'administrateur système peut attribuer un mot de passe unique à chacune des quatre classes de privilèges (classes de 1 à 4). Pour chacune des classes, il peut ensuite attribuer l'accès à certaines opérations logicielles (telles que la modification de fichiers programme, fichiers de table de données ou de configurations de voies).



Attribution des mots de passe aux classes

Pour attribuer un mot de passe à une classe, suivez les étapes indiquées à gauche.

```
   Current: Class1        Privilege Class Information        Default: Class1
+=============================================================================+
|   Privileges \ Privilege Class Names       Class1   Class2   Class3   Class4 |
|-----------------------------------------------------------------------------|
|    Modify Privileges                      |   X    |   X    |   X    |   X    |
|    Data Table File Create/Delete          |   X    |   X    |   X    |   X    |
|    Program File Create/Delete             |   X    |   X    |   X    |   X    |
|    Logical Write                          |   X    |   X    |   X    |   X    |
|    Physical Write                         |   X    |   X    |   X    |   X    |
|    Logical Read                           |   X    |   X    |   X    |   X    |
|    Physical Read                          |   X    |   X    |   X    |   X    |
|    Mode Change                            |   X    |   X    |   X    |   X    |
|    I/O Force                              |   X    |   X    |   X    |   X    |
|    SFC Force                              |   X    |   X    |   X    |   X    |
|    Clear Memory                           |   X    |   X    |   X    |   X    |
|    Restore                                |   X    |   X    |   X    |   X    |
|    On-line Editing                        |   X    |   X    |   X    |   X    |
+=============================================================================+

Press a function key.
>
Rem Prog                                              5/46 File PROTECT
Modify                                                          Toggle
Passwrd                                                          Priv
  F1                                                              F10
```

Important : En tant qu'administrateur système, **vous devez retenir votre mot de passe**. Sans ce mot de passe, il n'existe aucune solution pour vous ou Allen-Bradley pour revenir en ligne et effectuer une fonction d'administration du système, telle que la redéfinition des mots de passe et des privilèges. Si vous risquez d'oublier votre mot de passe ou de ne pas en disposer en temps opportun, écrivez-le et conservez-le en lieu sûr.

Attribution des privilèges à une classe

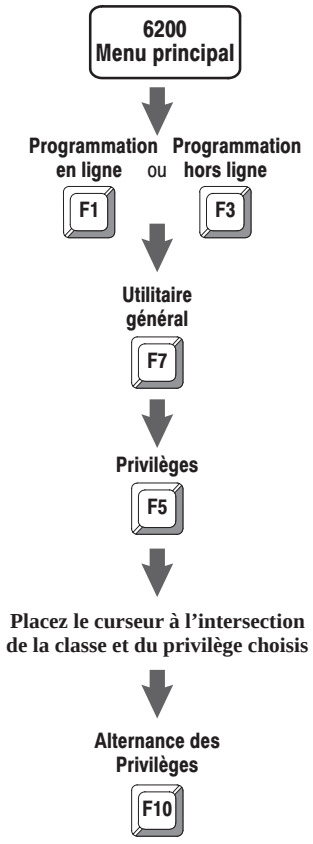
Vous pouvez définir la classe 1 comme classe ayant tous les privilèges, c'est-à-dire ceux de l'administrateur système. Vous devez ensuite définir les trois classes restantes en leur attribuant moins de privilèges et en vous assurant que seul l'administrateur système conserve le droit de modifier les privilèges.

Vous pouvez, par exemple, décider que la classe 1 est réservée à l'administrateur système, la classe 2 aux ingénieurs d'usine, la classe 3

aux ingénieurs de maintenance et la classe 4 aux opérateurs. Vous pouvez alors établir les classes de privilèges comme suit :

Privilège	Classe 1	Classe 2	Classe 3	Classe 4
Modifier les privilèges	X①			
Créer/supprimer des fichiers de données	X	X		
Créer/supprimer des fichiers programme	X	X	X	
Charger des blocs de mémoire processeur (Ecriture logique)	X	X	X	X
Charger toute la mémoire processeur (Ecriture physique)	X	X	X	X
Transférer des blocs de mémoire processeur② (Lecture logique)	X	X	X	X
Transférer toute la mémoire processeur (Lecture physique)	X	X	X	X
Changer le mode processeur	X	X	X	X
Forcer les E/S	X	X	X	
Forcer des transitions dans les SFC	X	X	X	
Effacer la mémoire	X			
Restaurer la mémoire à partir de l'archive	X	X	X	
Editer en ligne	X	X		

① X indique que le privilège est activé pour cette classe.
② Sans ce transfert, un utilisateur ne peut même pas voir le répertoire programme. Requis pour tout sauf la lecture physique.



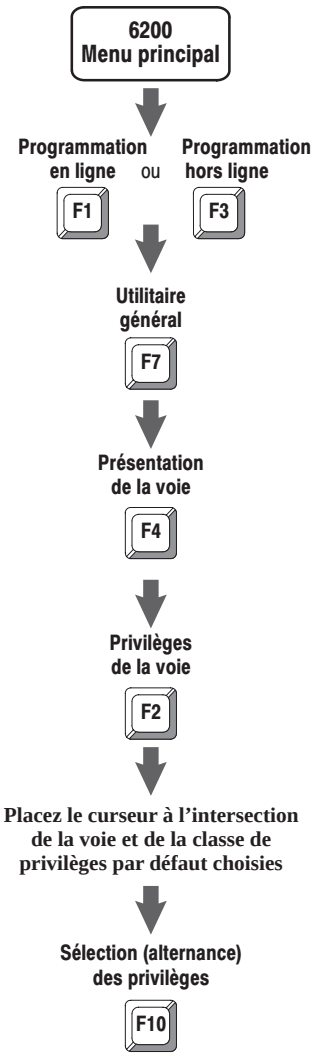
Active ou désactive un privilège d'une classe en suivant les étapes indiquées à gauche.

```
   Current: Class1        Privilege Class Information        Default: Class1
+=============================================================================+
|   Privileges \ Privilege Class Names       Class1   Class2   Class3   Class4 |
|-----------------------------------------------------------------------------|
|    Modify Privileges                     |   X   |   X    |   X    |   X    |
|    Data Table File Create/Delete         |   X   |   X    |   X    |   X    |
|    Program File Create/Delete            |   X   |   X    |   X    |   X    |
|    Logical Write                         |   X   |   X    |   X    |   X    |
|    Physical Write                        |   X   |   X    |   X    |   X    |
|    Logical Read                          |   X   |   X    |   X    |   X    |
|    Physical Read                         |   X   |   X    |   X    |   X    |
|    Mode Change                           |   X   |   X    |   X    |   X    |
|    I/O Force                             |   X   |   X    |   X    |   X    |
|    SFC Force                             |   X   |   X    |   X    |   X    |
|    Clear Memory                          |   X   |   X    |   X    |   X    |
|    Restore                               |   X   |   X    |   X    |   X    |
|    On-line Editing                       |   X   |   X    |   X    |   X    |
+=============================================================================+

Press a function key.
>
Rem Prog                                              5/46 File PROTECT
Modify                                                          Toggle
Passwrd                                                          Priv
  F1                                                              F10
```

Si vous souhaitez qu'une classe puisse	Activez ce privilège/opération
Activer/désactiver les privilèges pour chaque classe **Important** : Si vous utilisez la DTEP, désactivez ce privilège pour toutes les classes **sauf** la classe 1 (administrateur système).	`Modify Privileges`[①]
Créer ou supprimer des fichiers de table de données	`Data Table File Create/Delete`
Créer ou supprimer des fichiers programme	`Program File Create/Delete`
Restaurer un fichier de mémoire processeur en utilisant une adresse logique En général, ceci doit être couplé avec une Ecriture physique	`Logical Write`[①]
Restaurer un fichier de mémoire processeur en utilisant une adresse physique En général, ceci doit être couplé avec une Ecriture logique	`Physical Write`
Lire le processeur en utilisant une adresse logique En général, ceci doit être couplé avec une Lecture physique **Important** : Sans ceci, l'utilisateur ne peut pas même voir un répertoire programme. Requis pour tout sauf pour la Lecture physique.	`Logical Read`[①]
Lire la mémoire processeur en utilisant une adresse physique En général, ceci doit être couplé avec une Lecture logique	`Physical Read`
Changer le mode processeur lorsque le commutateur à clé du processeur est sur REMOTE	`Mode Change`
Activer ou désactiver les forçages dans le système ; effacer tous les forçages d'E/S	`I/O Force`
Activer ou désactiver des forçages SFC ; forcer les transitions individuelles sur on ou off, ou effacer tous les forçages SFC	`SFC Force`
Effacer la mémoire processeur	`Clear Memory`
Restaurer ou fusionner d'un fichier de mémoire processeur	`Restore`
Editer un fichier programme dans n'importe quel mode processeur	`Online Editing`

① **Important** : Vous ne pouvez pas supprimer ce privilège de la classe 1 (administrateur système).

Attribution des classes de privilèges par défaut pour les voies de communication et les fichiers hors ligne



Une classe de privilèges par défaut détermine la classe d'une voie spécifique et de toutes les stations/postes reliés à cette voie. Si un poste spécifique nécessite des privilèges différents de ceux attribués par la classe de la voie, vous pouvez spécifier séparément la classe de privilèges pour ce poste (voir page 2-8).

Les voies de communication et les fichiers hors ligne commencent par les privilèges de la classe 1. Attribuez une nouvelle classe de privilèges par défaut pour une voie de communication ou un fichier hors ligne en suivant les étapes indiquées à gauche.

```
                              Channel Privileges

                                 Default                  Privilege Class
                                Priv. Class    Class 1    Class 2    Class 3    Class 4
Channel 0:  SYSTEM (P-2-P)      CLASS 1         RW         RW         RW         RW

Channel 1A: DH+                 CLASS 1         RW         RW         RW         RW
Channel 1B: SCANNER MODE        CLASS 1         RW         RW         RW         RW
Channel 2A: UNUSED              CLASS 1         RW         RW         RW         RW
Channel 2B: UNUSED              CLASS 1         RW         RW         RW         RW

Channel 3A: N/A                 CLASS 1

Offline:                        CLASS 3




Press a function key or enter a value.
>
Rem Prog   Forces:None                                        5/46 File   PROTECT
                  Node                                                      Select
                  Priv                                                       Priv
                   F3                                                        F10
```

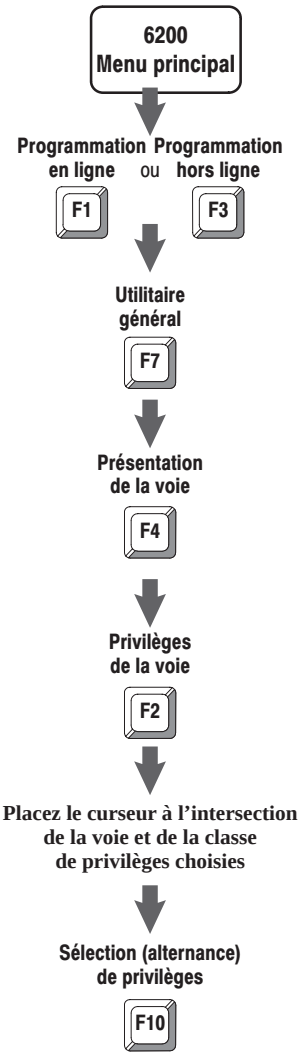
Important : Si vous utilisez la DTEP, attribuez les classes par défaut à toutes les voies— y compris les voies actuellement non utilisées.

Attribution des privilèges de lecture et d'écriture pour les voies de communication

Les privilèges de lecture et d'écriture qui s'affichent à l'écran « Channel Privileges » s'appliquent à l'accès lecture et écriture d'une classe de privilèges de l'écran « Channel Configuration » (Configuration de voie) de chaque voie.

Important : La suppression des accès lecture et écriture de la classe 1 pour une voie empêche l'administrateur système de configurer cette voie. Assurez-vous que la classe 1 conserve l'accès nécessaire à chaque voie.

L'administrateur système spécifie les privilèges de lecture et d'écriture de chaque voie en suivant les étapes indiquées à gauche.

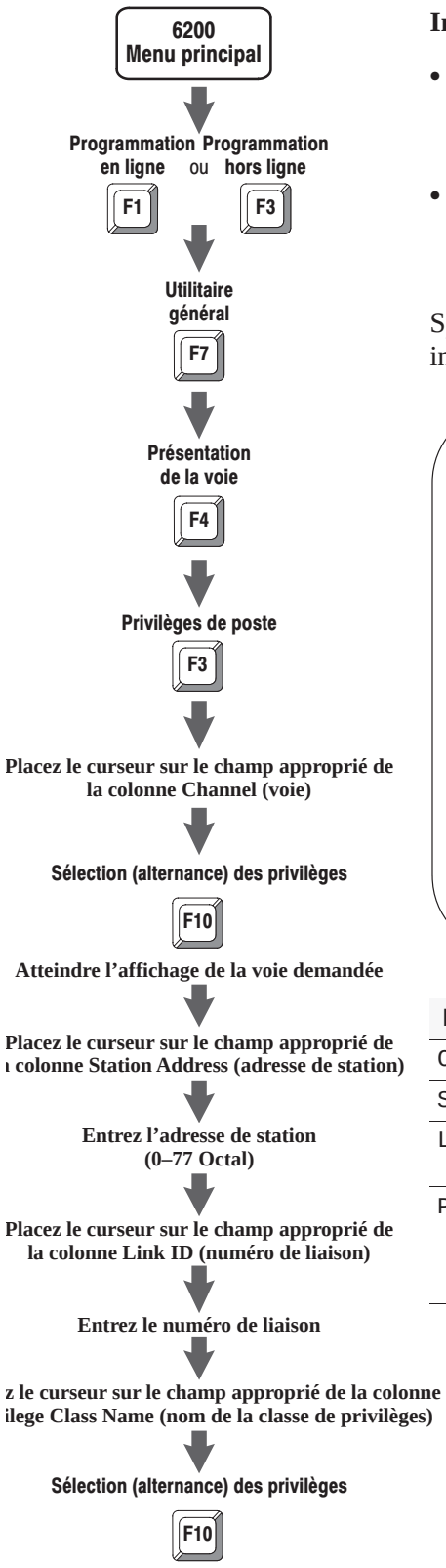



```
                          Channel Privileges

                                Default                 Privilege Class
                              Priv. Class    Class 1   Class 2   Class 3   Class 4
Channel 0:  SYSTEM (P-2-P)    CLASS 1         RW        RW        RW        RW

Channel 1A: DH+               CLASS 1         RW        RW        RW        RW
Channel 1B: SCANNER MODE      CLASS 1         RW        RW        RW        RW
Channel 2A: UNUSED            CLASS 1         RW        RW        RW        RW
Channel 2B: UNUSED            CLASS 1         RW        RW        RW        RW

Channel 3A: N/A               CLASS 1

Offline:                      CLASS 3




Press a function key or enter a value.
>
Rem Prog   Forces:None                                    5/46 File   PROTECT
                  Node                                                  Select
                  Priv                                                   Priv
                   F3                                                    F10
```

Si vous voulez que la classe puisse	Sélectionnez l'option
Lire les informations de configuration uniquement	R
Lire et modifier les informations de configuration	RW
Ni lire ni modifier les informations de configuration de voie	(Blank)

Définissez les privilèges de lecture et d'écriture pour le fichier diagnostic de chaque voie (écran « Channel Status » – Etat de la voie), via l'écran « Data Table Privileges » (Privilèges de la table des données) (voir page 2-10).

Attribution des privilèges pour les stations/postes spécifiques



Chaque station/poste relié à la voie DH+® du processeur prend par défaut la classe de privilèges correspondant à sa voie. Cependant, l'administrateur système peut attribuer une classe de privilèges unique à un poste spécifique.

Important :

- Les classes de privilèges des postes ont priorité sur la classe de privilèges par défaut de la voie, attribuée sur l'écran « Channel Privilege ».
- Si vous attribuez la classe 1 de privilèges à un poste, un utilisateur final peut configurer un terminal et le relier à ce poste, générant ainsi un risque en matière de sécurité.

Spécifiez une classe de privilèges pour un poste suivant les étapes indiquées à gauche.

```
                          Node Privilege Class

  Channel       Station Address      Link ID       Privilege Class Name

     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0
     0              0                   0

Press a function key or enter a value.
>
Rem Prog   Forces:None                                  5/46 File PROTECT
                                                                    Select
                                                                     Priv
                                                                      F10
```

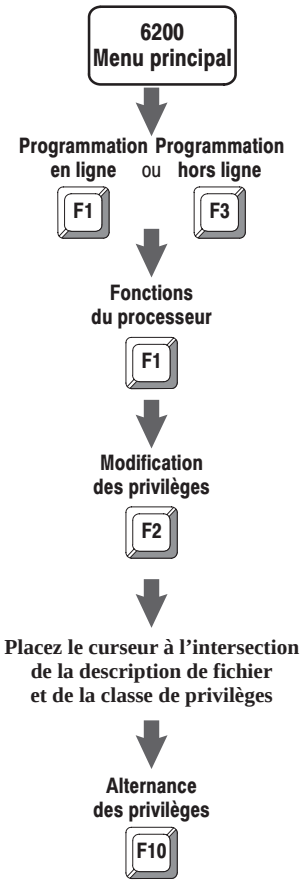
Le champ	Indique
Channel	la voie à laquelle le poste est relié
Station Address	l'adresse de station du poste sur la voie
Link ID	le numéro de liaison utilisé pour identifier la liaison DH+ à laquelle le poste spécifié est relié
Privilege Class Name	la classe de privilèges du poste Par défaut, la classe de privilèges du poste correspond à la classe de privilèges de la voie

Attribution des privilèges de lecture et d'écriture pour un fichier programme

L'administrateur système peut attribuer des privilèges de lecture et d'écriture pour chaque fichier programme de manière à limiter les possibilités d'affichage ou de modification par les utilisateurs.

Important :

- Vous ne pouvez pas modifier les privilèges de lecture et d'écriture pour le fichier système (fichier 0) ou des fichiers non définis.
- La suppression de l'accès lecture et écriture de la classe 1 pour un fichier programme empêche même l'administrateur système d'accéder à ce fichier. Assurez-vous que la classe 1 conserve l'accès nécessaire à chaque fichier.
- Le filtrage de chargement pour les violations DTEP concerne des fichiers programme dont les classes 2 à 4 possèdent des privilèges d'écriture. Si vous générez des fichiers hors ligne commandant la logique critique, vous devez supprimer tous les privilèges d'écriture des classes 2 à 4 avant que la DTEP ne vous permette de charger ces fichiers.



Pour spécifier les privilèges de lecture et d'écriture d'un fichier programme, suivez les étapes indiquées à gauche.

```
+= PROGRAM FILE PRIVILEGES ======================================[ OFFLINE ]===+
|  File   Name           Type              Class1   Class2   Class3   Class4   |
|-------------------------------------------------------------------------------|
|    0                   system              RW       RW       RW       RW     |
|    1                   undefined           RW       RW       RW       RW     |
|    2                   ladder              RW       RW       RW       RW     |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
+===============================================================================+

Press a function key to toggle the privilege.
>
Rem Prog               PLC-5/46 Series C  Revision G     5/46 File PROTECT
                                                                        Toggle
                                                                         Priv
                                                                          F10
```

Si vous voulez que la classe puisse	Sélectionnez l'option
Lire le fichier programme uniquement	R
Lire et modifier le fichier programme	RW
Ni lire ni modifier le fichier programme	(Vide)①

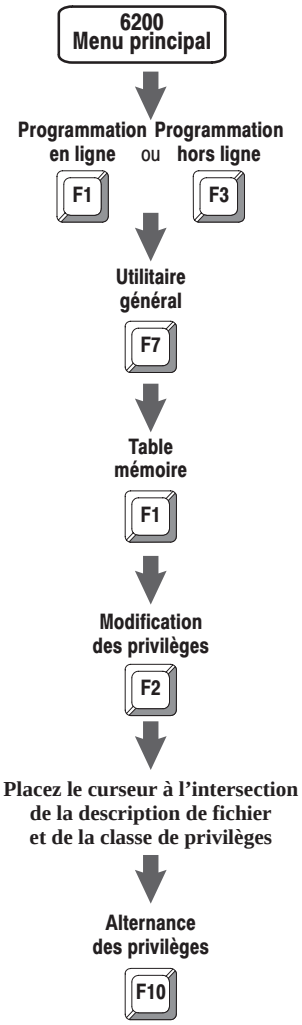
① Vous pouvez utiliser cette méthode pour empêcher l'affichage des algorithmes exclusifs.

Attribution des privilèges pour un fichier de table de données

En tant qu'administrateur système, vous pouvez attribuer les privilèges de lecture et d'écriture pour chaque fichier de la table de données afin de limiter les possibilités d'affichage ou de modification des valeurs par les utilisateurs finals.

Important :

- Vous ne pouvez pas modifier les privilèges de lecture et d'écriture pour des fichiers non définis.
- La suppression de l'accès lecture et écriture de la classe 1 pour un fichier de table de données empêche même l'administrateur système, d'accéder à ce fichier. Assurez-vous que la classe 1 conserve l'accès nécessaire à chaque fichier.

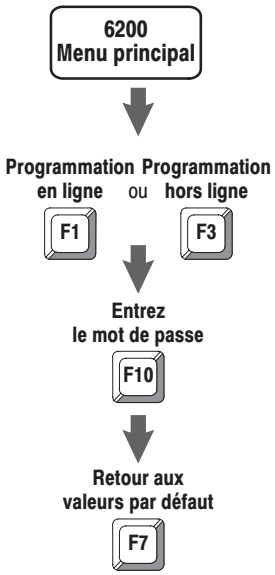


Pour spécifier les privilèges de lecture et d'écriture d'un fichier de la table de données, suivez les étapes indiquées à gauche.

```
                              DATA TABLE PRIVILEGES
FILE          TYPE            Class 1   Class 2   Class 3   Class 4
   0      O  output             RW        RW        RW        RW
   1      I  input              RW        RW        RW        RW
   2      S  status             RW        RW        RW        RW
   3      B  binary or bit      RW        RW        RW        RW
   4      T  timer              RW        RW        RW        RW
   5      C  counter            RW        RW        RW        RW
   6      R  control            RW        RW        RW        RW
   7      N  integer            RW        RW        RW        RW
   8      F  floating point     RW        RW        RW        RW
   9         unused             RW        RW        RW        RW
  10         unused             RW        RW        RW        RW

                           PROCESSOR MEMORY LAYOUT
                 821 words of memory used in  64 data table files
                   23 words of memory used in   3 program files
                 48678 words of unused memory available

Press a function key to toggle the privilege.
>
Rem Prog               PLC-5/46 Series C  Revision G     5/46 File PROTECT
                                                                    Toggle
                                                                     Priv
                                                                      F10
```

Si vous voulez que la classe puisse	Sélectionnez l'option
Lire le fichier de table de données uniquement	R
Lire et modifier le fichier de table de données	RW
Ni lire ni modifier le fichier de table de données	(Vide)

Restauration des classes de privilèges par défaut

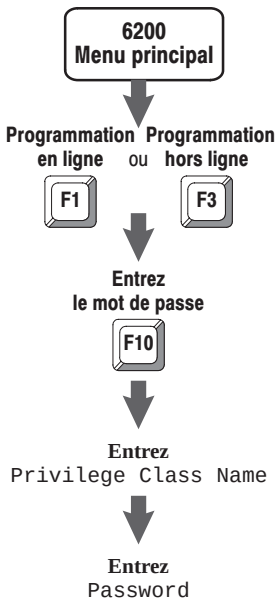


En tant qu'administrateur système, vous pouvez restaurer les privilèges par défaut d'une classe si les modifications en cours n'ont pas encore été sauvegardées.

Pour restaurer les privilèges par défaut, suivez les étapes indiquées à gauche.

```
+= PROGRAM DIRECTORY FOR PROCESSOR: PROTECT=======================[ OFFLINE ]===+
|  File   Name           Type              Size(words)                          |
|-------------------------------------------------------------------------------|
|    0                   system            4                                    |
|    1                   undefined         0                                    |
|    2                   ladder            1                                    |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
| += Select New Privilege Class =========+                                      |
| |                                      |                                      |
| | Privilege Class Name                 |                                      |
| | Password:                            |                                      |
| |                                      |                                      |
| += ESC exits ==========================+                                      |
|                                                                               |
+===============================================================================+

Enter the class name and password or press a function key.

Rem Prog                                                      5/46 File PROTECT
                                                    Return
                                                    Default
                                                      F7
```

Sélection d'une autre classe



Si vous souhaitez acquérir les privilèges d'une autre classe (différente de celle pour laquelle le terminal de programmation est configuré), vous devez entrer le nouveau nom de classe et le nouveau mot de passe.

Pour aquérir les privilèges d'une autre classe, suivez les étapes indiquées à gauche.

```
+= PROGRAM DIRECTORY FOR PROCESSOR: PROTECT=======================[ OFFLINE ]===+
|  File   Name           Type              Size(words)                          |
|-------------------------------------------------------------------------------|
|    0                   system            4                                    |
|    1                   undefined         0                                    |
|    2                   ladder            1                                    |
|                                                                               |
|                                                                               |
|                                                                               |
|                                                                               |
| += Select New Privilege Class =========+                                      |
| |                                      |                                      |
| | Privilege Class Name                 |                                      |
| | Password:                            |                                      |
| |                                      |                                      |
| += ESC exits ==========================+                                      |
|                                                                               |
+===============================================================================+

Enter the class name and password or press a function key.

Rem Prog                                                      5/46 File PROTECT
                                                    Return
                                                    Default
                                                      F7
```

Conseil

Vous pouvez également appuyer sur `ALT-P` pour sélectionner une nouvelle classe de privilèges.

Chapitre 3

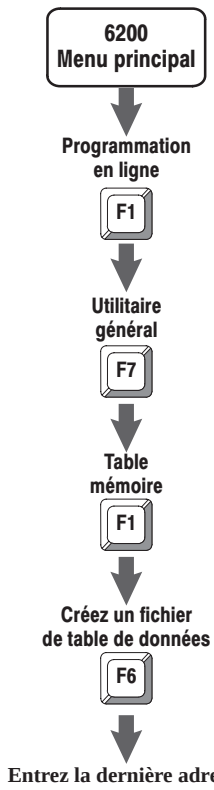
Configuration et utilisation de la protection d'éléments de la table de données

Contenu du chapitre

En tant qu'administrateur système, exploitez la DTEP en :

- obtenant les privilèges de l'administrateur système (classe 1)
- créant un fichier de table de données de nombres entiers comme fichier DTEP
- entrant le numéro du fichier d'entiers choisi dans le fichier d'état du processeur (fichier de table de données 2)
- entrant dans le fichier DTEP les plages de la table des données à protéger

Création d'un fichier de protection

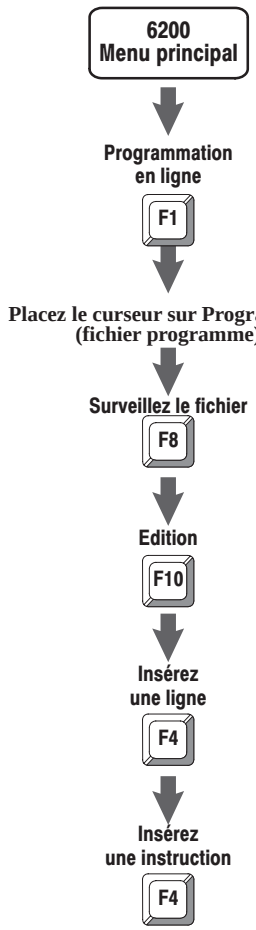


En tant qu'administrateur système, suivez les étapes indiquées à gauche pour créer un fichier de table de données de nombres entiers à utiliser comme fichier DTEP.

Assurez-vous que ce fichier est juste assez grand pour contenir un nombre d'éléments représentant 3 fois le nombre de plages à protéger. Vous trouverez les directives de définition de la taille de votre fichier de protection à la page 3-3.

```
                                DATA TABLE MAP
 FILE          TYPE          LAST ADDRESS      SIZE (elements)    SIZE (words)
    0      O  output            O:177             128                134
    1      I  input             I:177             128                134
    2      S  status            S:127             128                134
    3      B  binary or bit     B3/15               1                  7
    4      T  timer             T4:0                1                  9
    5      C  counter           C5:0                1                  9
    6      R  control           R6:0                1                  9
    7      N  integer           N7:30              31                 37
    8      F  floating point    F8:0                1                  8
    9      F  floating point    F9:0                1                  8
   10         unused                                0                  6

                        PROCESSOR MEMORY LAYOUT
                  853 words of memory used in 64 data table files
                    108 words of memory used in 16 program files
                       48191 words of unused memory available

Enter address to create
> N10:10
Rem Prog               PLC-5/46 Series C Revision G      5/46 File PROTECT
```

Mise en service du mécanisme de protection



L'entrée du numéro de fichier DTEP dans l'élément 63 du fichier d'état (S:63) amorce automatiquement le mécanisme de DTEP destiné à l'utilisateur final.

En tant qu'administrateur système, suivez les étapes indiquées à gauche et entrez une instruction à relais déplaçant le numéro de fichier DTEP souhaité dans S:63 du fichier d'état.

Cette instruction à relais peut être temporaire si toutefois elle s'exécute une fois pour définir la valeur dans le fichier d'état. Ensuite, vous pouvez supprimer l'instruction à relais et le programme peut être archivé (sauvegardé) avec la protection en place.

Important : La validité d'un numéro de fichier placé dans l'adresse S:63 est vérifiée uniquement après qu'un utilisateur final ait reçu une commande filtrée au cours d'une programmation en ligne. Si cette valeur est incorrecte :

- un code d'erreur est renvoyé
- une défaut mineur (S:17/12) est défini

Pour forcer la validation de ce numéro de fichier avant de confier l'exploitation aux utilisateurs individuels, l'administrateur système doit procéder selon les étapes indiquées à la page 3-8.

Le mécansime de protection reste effectif au niveau de l'utilisateur final tant que :

- vous ne donnez pas le droit de modifier les privilèges à l'utilisateur final
- vous n'effacez pas l'entrée du fichier DTEP dans le fichier d'état

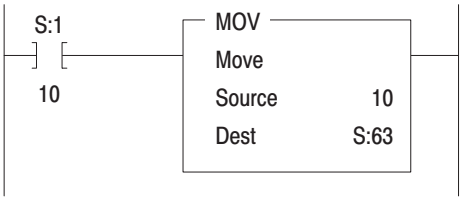
Lorsque la DTEP prend effet, les éléments suivants sont automatiquement protégés contre des modifications apportées par les commandes d'un utilisateur final :

- l'élément 63 du fichier d'état
- l'intégralité du fichier DTEP

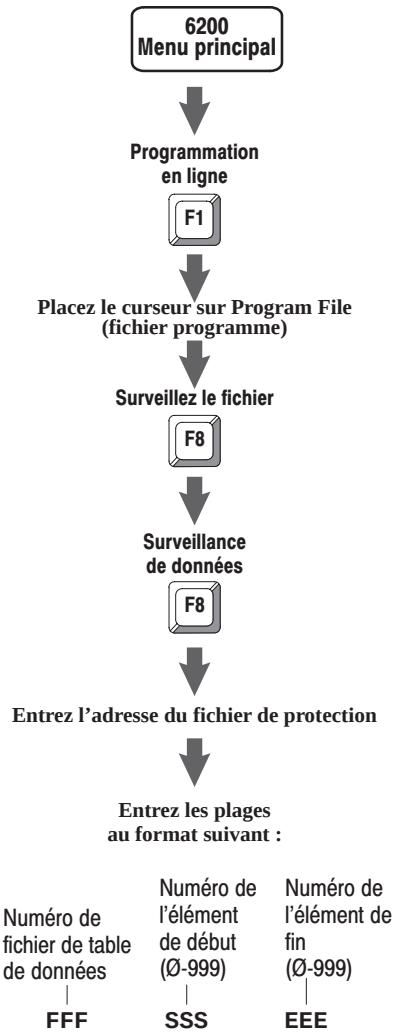
Important : Pour l'administrateur système, la propriété du droit de modifier les privilèges a priorité sur le mécanisme de protection.

Ligne conditionnée par le premier bit de scrutation.

Déplace la valeur 10 dans S:63, ce qui configure le fichier de protection comme fichier 10.



Entrée des plages de la table de données dans le fichier de protection



En tant qu'administrateur système, spécifiez les plages de protection dans le fichier DTEP à l'aide de trois mots consécutifs pour chaque entrée de plage.

Entrez les plages de fichier que vous souhaitez protéger en suivant les étapes indiquées à gauche.

```
  Address     0      1      2      3      4      5      6      7      8      9
N10:0           0      0      0      0      0      0      0      0      0      0
N10:10          0      0      0      0      0      0      0      0


Press a function key or enter a value.
N10:0 =
Rem Prog   Forces:None      Data:Decimal   Addr:Decimal  5/46 File PROTECT
Change                         Specify          Next    Prev
 Radix                         Address          File    File
  F1                             F5              F7      F8
```

Conformez vous aux directives ci-dessous :

- Saisissez l'entrée de trois mots de la plage de protection en commençant à l'élément zéro (`0`) et en continuant avec des entrées contiguës pour toutes les plages à spécifier.
- L'élément de début et l'élément de fin de chaque entrée de plage doivent être en ordre croissant—sauf pour la protection d'un seul élément où ils sont alors égaux.
- Spécifiez un élément de début de zéro (0) et un élément de fin de 999 pour protéger la totalité du fichier quel que soit le nombre d'éléments dans le fichier.
- Indiquez intentionnellement les entrées de plage de protection inutilisées dans le fichier DTEP en plaçant un '`-1`' dans le champ Numéro de fichier de table de données.
- Entrez autant de plages que souhaité jusqu'à 333.
- Agrandissez le fichier DTEP, mais pas plus que nécessaire, pour spécifier le nombre de plages de protection requis.

  Bien que le mécanisme de protection n'affecte pas de façon notable les performances d'exécution du programme en mode Run, il peut affecter la réaction du processeur aux commandes reçues de l'utilisateur final. Suivez les directives ci-dessous pour minimiser ces effets :

  - Réduisez le nombre de plages de protection spécifié.

    Au lieu de spécifier plusieurs plages de protection dans un fichier de table de données, prévoyez la possibilité de protéger la totalité du fichier dans une seule plage.

  - La taille du fichier DTEP ne doit pas être plus grande que nécessaire pour le nombre de plages de protection requis.

Conseil

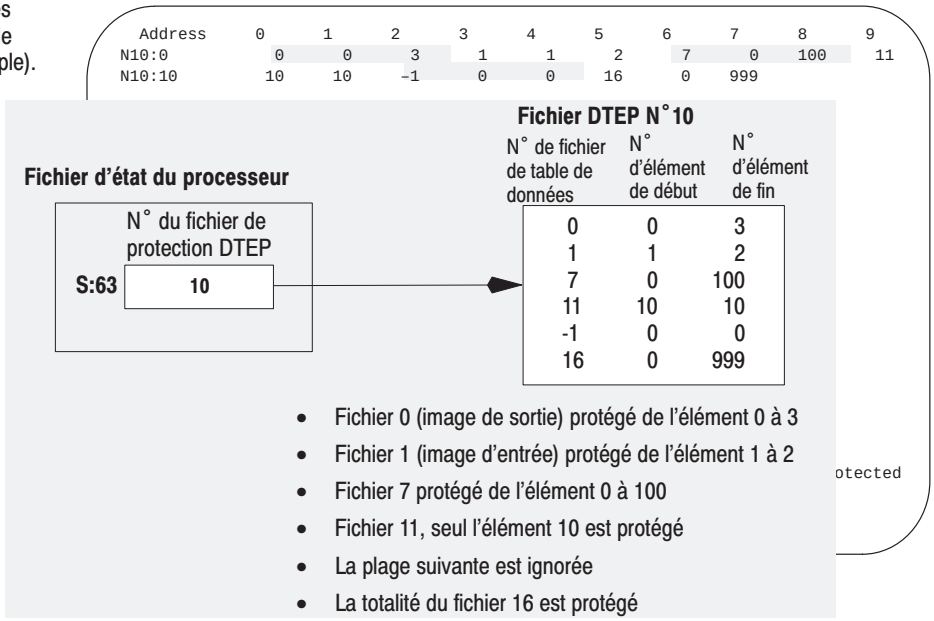
Par défaut, l'espace excédentaire du fichier DTEP est comblé par des zéros ; tout groupe de « 0 0 0 » devra donc être interprété comme le fichier de protection 0, élément 0— c.à.d. O:Ø. Evitez ceci en plaçant un '–1' dans tout espace intentionnellement inutilisé.

Conseil

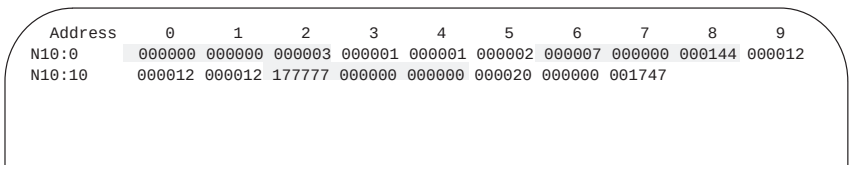
Même si l'administrateur système a déjà supprimé le privilège écriture dans un fichier de table de données, il peut encore le protéger avec la DTEP et bénéficier des fonctions de protection plus évoluées de la DTEP (contre les écritures non autorisées par instructions de sortie de l'utilisateur final, par exemple).

Ce dernier point est important car le processeur protégé scrute le fichier entièrement, du premier au dernier élément, lorsqu'il vérifie le fichier et lorsqu'il filtre des commandes filtrées pour DTEP.

Figure 3.1
Entrée de plages dans un fichier DTEP



Ces plages sont entrées en décimales, par défaut. Si vous entrez la plage d'un des fichiers-image des E/S, vous pouvez appuyer sur `F1 – Change Radix`, puis sur `F2 – Octal Data` et entrer la plage en Octal. Lorsque vous repassez en décimales, la conversion est faite automatiquement.



Important : La validité des entrées de plage de protection n'est pas vérifiée lorsque vous les saisissez via la surveillance des données, mais elles sont validées lorsqu'une commande filtrée est reçue d'un utilisateur final au cours de la programmation en ligne. Si les entrées sont incorrectes :

- un code d'erreur est renvoyé
- un défaut mineur (S:17/12) est défini

En tant qu'administrateur système, vous devez suivre les étapes indiquées à la page 3-8 pour forcer la validation de ces entrées avant de confier l'exploitation du système aux utilisateurs finals.

Filtrage des commandes

Lorsqu'un utilisateur final édite un programme en ligne, le processeur protégé filtre toutes les commandes de communication pouvant être utilisées pour modifier les éléments de la table de données, manipuler les adresses ou forcer les E/S. Si le mécanisme de DTEP est activé — c'est-à-dire si l'utilisateur ne peut pas modifier les privilèges et que le numéro de fichier DTEP indiqué dans S:63 est correct — le processeur protégé filtre chaque commande d'accès aux zones protégées de la table de données. Ce procédé vérifie toutes les plages du fichier DTEP. Si une violation est trouvée, la requête est rejetée, un code d'erreur est renvoyé — `Data Table Element Protection Violation` — et le bit de défaut mineur S:17/11 est défini.

Protection contre les modifications hors ligne

Le filtrage des commandes s'effectue lorsqu'un utilisateur final programme en ligne — c'est-à-dire lorsque le logiciel de programmation est connecté directement au processeur. Lorsqu'un utilisateur final modifie l'image du processeur hors ligne — c'est-à-dire lorsque le logiciel de programmation est connecté à une image fichier du processeur — la plupart des commandes ne peuvent pas être directement filtrées par le processeur pour dépister les violations de protection. Pour les modifications hors ligne, il existe donc d'autres méthodes de prévention des violations de protection.

Fichiers de table de données

En tant qu'administrateur système, vous devez adopter de bonnes méthodes de programmation et initialiser tous les emplacements de la table de données aux valeurs souhaitées en dehors de l'indicateur de première scrutation du processeur (S:1/15). Comme le fichier DTEP spécifie uniquement les plages et non les valeurs de chaque emplacement, le processeur protégé ne peut pas éviter ou détecter la modification apportée à ces valeurs stockées dans les fichiers de table de données lors de la programmation hors ligne. Lorsque vous initialisez tous les emplacements de table de données à leurs valeurs souhaitées en dehors de l'indicateur de première scrutation, tout problème causé par une violation de protection pendant l'écriture hors ligne dans les emplacements de la table de données est annulé.

Tables de forçage des E/S

Pour protéger le fonctionnement du processeur contre les éventuelles opérations de forçage des E/S intégrées dans l'image du processeur lors de la programmation hors ligne, le processeur protégé n'accepte pas les modifications apportées à la table de forçage des E/S en mode Chargement. Les données des tables de forçage des E/S restent inchangées. A la fin d'un chargement vers un processeur protégé, les tables de forçage des E/S sont vidées de tout forçage et un message s'affiche sur votre terminal pour indiquer qu'aucun forçage du fichier d'archive n'a été chargé.

Eléments insérés

Lors du chargement, le processeur protégé filtre les instructions à relais et les instructions d'éléments insérés en texte structuré de manière à vérifier

que les adresses protégées par le mécanisme DTPE n'ont pas été re-programmées.

En tant qu'administrateur système, vous devez avoir défini la protection de base de l'application du processeur au moyen des mots de passe et des privilèges, présentés au chapitre 2. Vous devez également avoir supprimé les privilèges d'écriture de toutes les classes (sauf la classe 1) pour tous vos fichiers programme et de données considérés comme critiques pour la sécurité du programme d'application. Les fichiers programme créés ultérieurement par les utilisateurs finals ne sont pas protégés de cette manière et ils attribuent par défaut aux 4 classes des privilèges d'écriture et de lecture. Cette distinction permet au processeur d'adapter son filtrage à n'importe quelle requête de chargement ayant pour destinataire un fichier programme à relais ou en texte structuré ainsi que des privilèges d'écriture pour classe 2.

Toute violation de la protection entraîne l'abandon du chargement, l'écran de chargement affiche le message `Data Table Element Protection Violation`, et continue à afficher le numéro du fichier programme qui a provoqué la violation de protection. Utilisez cette information pour rechercher la combinaison instruction/opérande qui a provoqué cette violation.

Lors de la détection d'une erreur de violation de protection en mode Chargement, le processeur réagit comme si un timeout de chargement s'était produit, définit de nouveau le mode processeur sur Programme (ou Programme à distance) et définit un défaut majeur « Bad User Program Memory » avec le code d'erreur « Download Aborted » (19).

Restrictions du système

Pour réduire les risques relatifs à la sécurité, l'utilisation d'un système protégé est assujetti aux restrictions suivantes :

Adressage indirect

Comme l'adressage indirect laisse à l'utilisateur final le soin de déterminer l'adresse effective de la table de données au moment de l'exécution en manipulant l'emplacement indirect dans le programme à relais, un risque existe en matière de sécurité. Lorsque la DTEP est activée et que l'utilisateur final n'a pas la possibilité de modifier les privilèges, le processeur protégé recherche l'adressage indirect dans les instructions à relais et en texte structuré. Le système de sécurité :

- rejette l'adressage indirect au niveau du fichier—ex., N[N7:0]:20
- autorise les adresses indirectes au niveau de l'élément—ex., N12:[N7:0]—uniquement si le fichier spécifié ne contient pas d'élément protégé
- rejette l'adressage indirect au niveau de l'élément si le fichier spécifié contient un élément protégé

Si une violation de protection se produit, la requête est rejetée, un code d'erreur est renvoyé (`Data Table Element Protection Violation`) et le bit de défaut mineur S:17/11 est défini.

Adressage indexé

Comme l'adressage indexé laisse à l'utilisateur final le soin de déterminer l'adresse effective de la table de données au moment de l'exécution en manipulant l'emplacement du mot d'index du fichier d'état (S:24) dans le programme à relais, ceci constitue un nouveau risque. Lorsque la DTEP est activée et que l'utilisateur final n'a pas la possibilité de modifier les privilèges, le processeur protégé recherche l'adresse indexée et empêche son insertion si le numéro de fichier adressé croise une plage protégée du fichier DTEP. Si une violation de protection se produit, la requête est rejetée, un code d'erreur est renvoyé (`Data Table Element Protection Violation`) et le bit de défaut mineur S:17/11 est défini.

Comme le processeur n'empêche pas le dépassement des limites du fichier de la table de données à travers l'utilisation de l'adressage indexé, un petit risque subsiste avec ce filtrage. Bien que le mécanisme de filtrage s'assure qu'il n'y a aucun élément protégé dans le fichier adressé, il ne peut pas vérifier l'éventualité d'écrasement d'un élément protégé dans les fichiers suivants et ne peut pas savoir :

- le nombre de fichiers de table de données affectés par l'instruction indexée au cours de l'exécution
- la valeur du champ .POS de la structure de commande au moment de l'exécution

Important : Assurez-vous que les instructions d'adresse indexée ne dépassent pas la limite du fichier.

Ecriture de données dans la mémoire via le port du coprocesseur

Les produits utilisant le port du coprocesseur mettent en oeuvre deux mécanismes de transfert de données brutes qui n'entrent pas dans les capacités actuelles des fonctions de mot de passe et des privilèges. Aucun coprocesseur ne peut donc écrire de données brutes dans la mémoire processeur lorsque le mécanisme DTEP est activé. Le privilège supérieur, « Modifier les privilèges », n'a aucun effet dans ce cas, car aucun privilège n'est associé aux mécanismes de transfert de données brutes du port du coprocesseur.

Lors de la détection d'une requête de transfert de données brutes entraînant une violation de protection, le processeur répond en définissant un indicateur d'erreur sur le coprocesseur et le bit de défaut majeur « Channel 3 Device Fault » (bit 6), avec le code d'erreur `COPRO Transfer Not Valid with Data Table Element Protection Invoked` (106).

Les commandes filtrées provenant du port du coprocesseur sont filtrées selon les règles du mécanisme DTEP standard.

Importation et exportation de fichiers ASCII

En raison des aspects de protection des données que le processeur est censé traiter, vous ne pouvez pas utiliser les fonctions d'importation ou d'exportation ASCII de mémoire processeur du logiciel de programmation 6200 sur un fichier mémoire de processeur protégé.

Test du fichier de protection

Lors de l'exécution de chaque commande filtrée, lorsque la protection est activée, le procédé de validation vérifie que :

- le fichier DTEP
  - existe
  - est un fichier de nombres entiers
- le numéro de fichier de table de données est valide
- la plage des valeurs du fichier DTEP est valide
- les numéros de fichier existent
- les valeurs jumelées de début et de fin sont égales ou en ordre croissant
- les plages représentent des mots qui sont effectivement placés dans le fichier de table de données spécifié

Si tel n'est pas le cas,

- un code d'erreur (`DTE Protection File Invalid`) est renvoyé
- un défaut mineur (S:17/12) est défini

La valeur '-1' est acceptée pour annuler une entrée inutilisée et n'est pas détectée comme erreur. Le champ d'éléments de fin peut être défini à '999' indépendamment du nombre effectif d'éléments dans un fichier et n'est pas détecté comme une erreur lors de la validation du fichier de protection.

Important : Toute condition invalide empêche l'utilisateur final d'effectuer une commande filtrée pour DTEP tant que le problème n'est pas résolu.

En tant qu'administrateur système, testez rigoureusement le fichier DTEP avant de confier son exploitation aux utilisateurs finals, en suivant les étapes ci-dessous :

1. Remplacez votre classe de privilèges par des classes préalablement définies comme classes d'utilisateurs finals.
2. Essayez d'effectuer une opération d'écriture (surveillance de la table de données) sur une adresse protégée de la table de données.

   Ceci force la validation du fichier DTEP. Si le fichier n'est pas valide, le bit de défaut mineur S:17/12 est défini et les opérations d'écriture suivantes sont bloquées jusqu'à correction de l'erreur. Si la DTEP fonctionne correctement, un code d'erreur (`Data Table Element Protection Violation`) est renvoyé et le bit de défaut mineur S:17/11 est défini.
3. Essayez d'effectuer une opération d'écriture sur une adresse non protégée de la table de données.

   Cette opération doit réussir.
4. Revenez à la classe de privilèges 1 et corrigez les erreurs.

Si vous devez revebir en arrière et ajouter d'autres éléments de la table de données aux mécanismes DTEP existants suite à l'intégration d'un système, vérifiez tout d'abord que les utilisateurs finals n'ont pas déjà accédé à un des éléments qui devait en être protégés lors de leur adressage d'instructions. L'ajout d'un mécanisme de protection à des éléments déjà utilisés verrouille la logique des utilisateurs finals.

L

M

N

O

P

Rockwell Automation

Rockwell Automation contribue à l'amélioration du retour sur investissements chez ses clients par le regroupement de marques leaders en automatismes industriels, créant ainsi une des plus larges gammes de produits faciles à intégrer. Leur support technique est assuré par des ressources locales démultipliées à travers le monde, par un réseau international de partenaires offrant des solutions globales, sans oublier les compétences en technologies avancées de Rockwell.

Présent dans le monde entier.

Allemagne • Arabie Saoudite • Argentine • Australie • Autriche • Bahreïn • Belgique • Bolivie • Brésil • Bulgarie • Canada • Chili • Chypre • Colombie • Corée • Costa Rica
Croatie • Danemark • Egypte • Emirats Arabes Unis • Equateur • Espagne • Etats-Unis • Finlande • France • Ghana • Grèce • Guatemala • Honduras • Hong Kong • Hongrie
Inde • Indonésie • Iran • Irlande • Islande • Israël • Italie • Jamaïque • Japon • Jordanie • Koweït • Liban • Macao • Malaisie • Malte • Maroc • Mexique • Nigeria • Norvège
Nouvelle-Zélande • Oman • Pakistan • Panama • Pays-Bas • Pérou • Philippines • Pologne • Porto Rico • Portugal • Qatar • République d'Afrique du Sud • République
Dominicaine • République Populaire de Chine • République Tchèque • Roumanie • Royaume-Uni • Russie • Salvador • Singapour • Slovaquie • Slovénie • Suède • Suisse
Taiwan • Thaïlande • Trinidad • Tunisie • Turquie • Uruguay • Venezuela

Siège mondial de Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tél. (1) 414 382–2000, Fax. (1) 414 382–4444
Siège européen de Rockwell Automation, 46, avenue Herrmann Debrouxlaan, 1160 Bruxelles, Belgique, Tél. 32–(0) 2 663 06 00, Fax. 32–(0) 2 663 06 40
Siège Asie Pacifique de Rockwell Automation, 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tél. (852) 2887 4788, Fax. (852) 2508 1846

Publication 1785–6.5.13FR – Janvier 1995
Remplace la publication 1785–2.25FR – Mars 1994
PN 956543–77