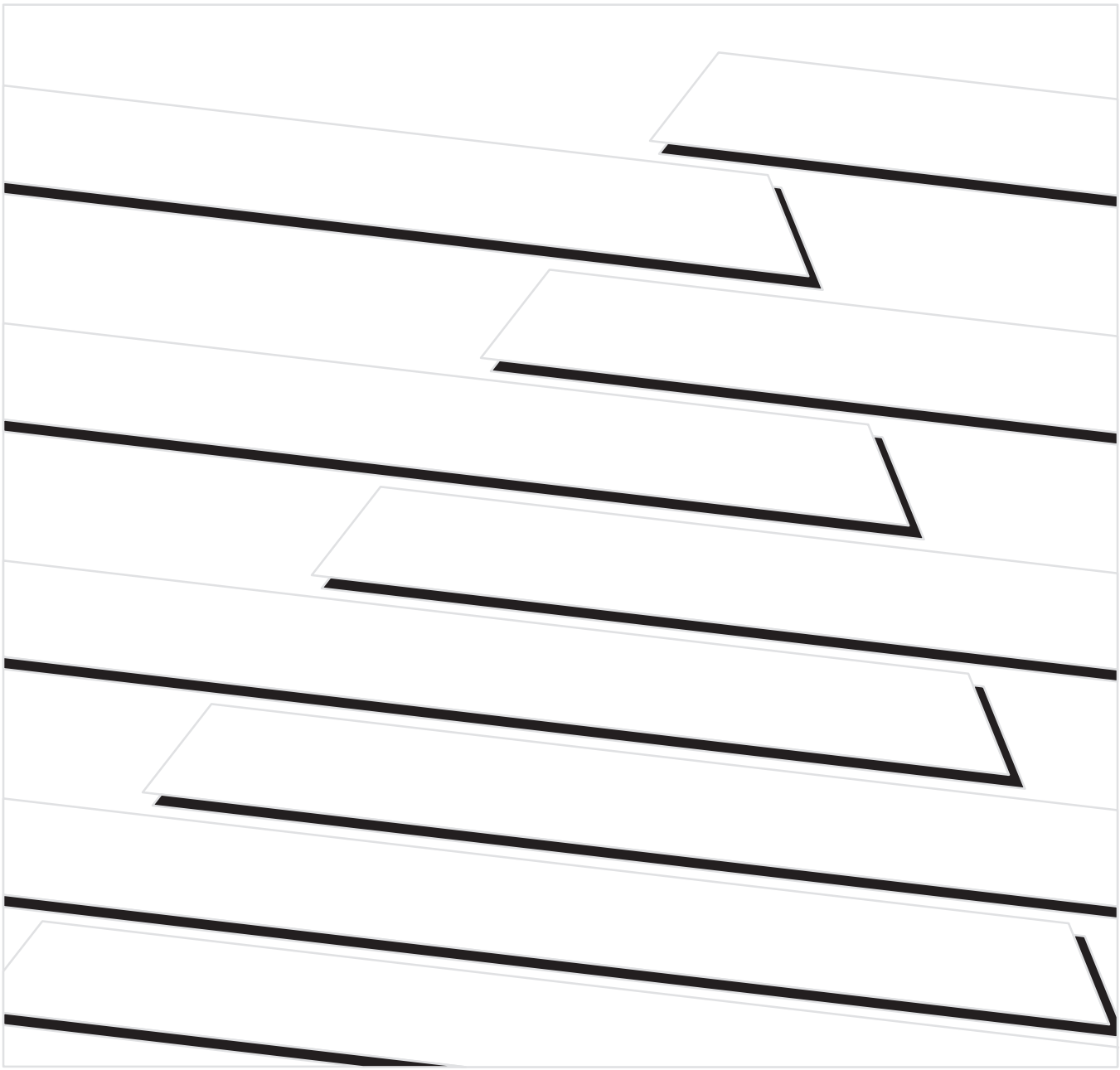
ALLEN-BRADLEY

Procesadores protegidos PLC-5

(No. de cat. 1785-L26B, -L46B y -L86B)

Suplemento



Información importante para el usuario

Debido a la variedad de usos de los productos descritos en esta publicación, las personas responsables de la aplicación y uso de este equipo de control deben asegurarse de que se han seguido todos los pasos necesarios para que cada aplicación y uso cumplan con todos los requisitos de rendimiento y seguridad, incluyendo leyes, regulaciones, códigos y normas aplicables.

Los ejemplos de ilustraciones, gráficos, programas y esquemas mostrados, en esta guía tienen la única intención de ilustrar el texto. Debido a las muchas variables y requisitos asociados con cualquier instalación particular, Allen-Bradley no puede asumir responsabilidad u obligación (incluyendo responsabilidad de propiedad intelectual) por el uso real basado en los ejemplos mostrados en esta publicación.

La publicación de Allen-Bradley SGI-1.1, *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* (disponible en la oficina de Allen-Bradley local), describe algunas diferencias importantes entre equipos transistorizados y dispositivos electromecánicos, las cuales deben tomarse en consideración al usar productos tales como los descritos en esta publicación.

En este manual hacemos anotaciones para advertirle sobre consideraciones de seguridad:

ATENCION: Identifica información o prácticas o circunstancias que pueden conducir a lesiones personales o la muerte, daños materiales o pérdidas económicas

Las notas de “Atención” le ayudan a:

- identificar un peligro
- evitar un peligro
- reconocer las consecuencias

Importante: Identifica información crítica para una correcta aplicación y entendimiento del producto.

Cómo usar este suplemento

Presentación

Este suplemento describe cómo usar las características de seguridad proporcionadas por un procesador protegido PLC-5/26™, PLC-5/46™ o PLC-5/86™ protected processor.

Usuarios

La información en este suplemento es principalmente para el **administrador del sistema**—usuario con privilegios únicos que puede controlar el acceso a áreas críticas del programa del procesador protegido.
Los usuarios finales—operadores con acceso restringido al programa del procesador—también pueden aprovechar este manual.

Usted debe ser ingeniero o técnico con experiencia en la aplicación de sistemas de control, además de estar familiarizado con:

- los sistemas de control programables de tiempo real
- el sistema de control PLC-5®
- los requisitos de seguridad básicos de su operación

Contenido

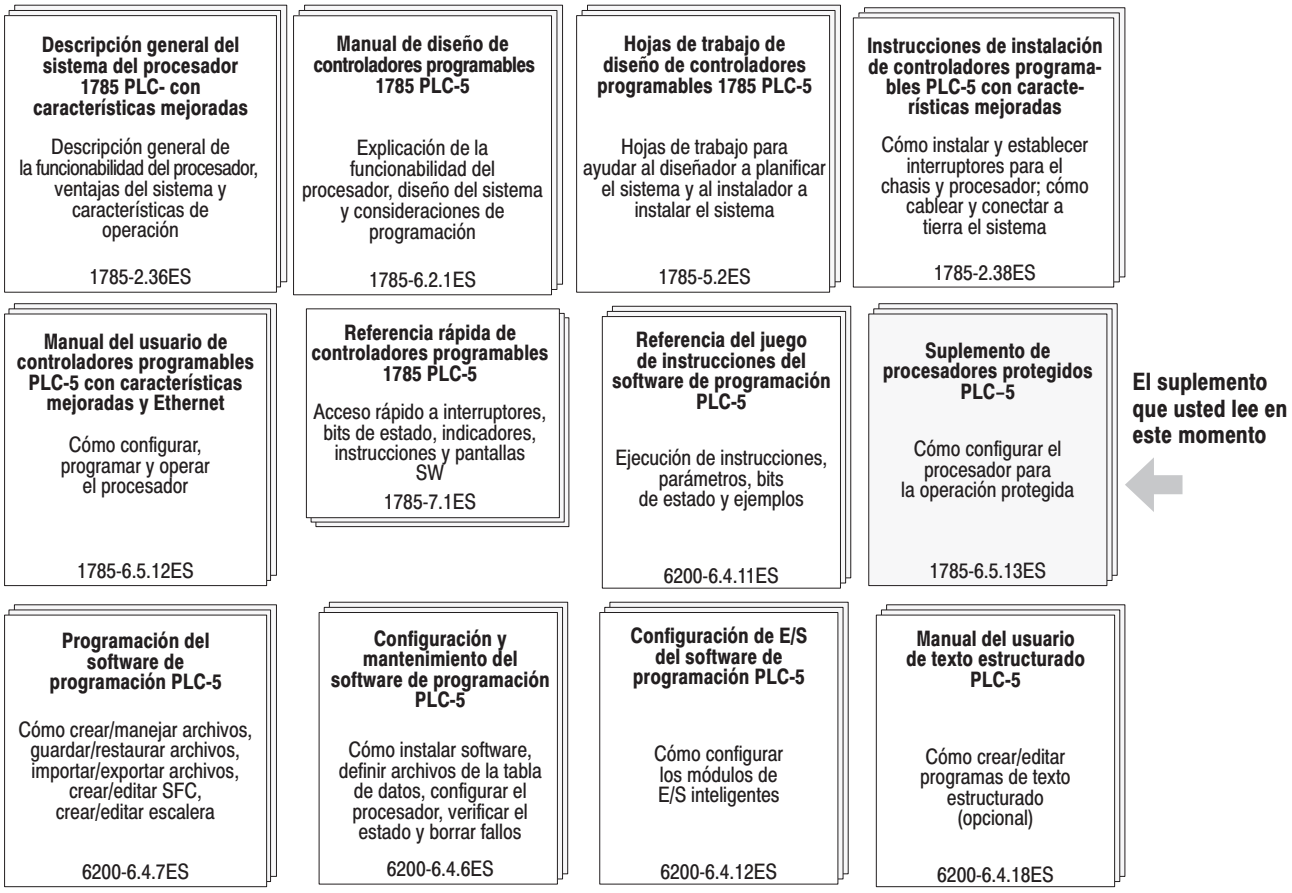
Si usted desea leer acerca de:	Vea el capítulo:
Cómo planificar un sistema protegido	1
Cómo configurar contraseñas y privilegios	2
Cómo configurar y usar protección de elemento de la tabla de datos	3

Terminología

Término	Definición
DTEP	Protección de elemento de la tabla de datos
Usuario final	El usuario de un procesador protegido que típicamente **no** puede modificar los privilegios ni contraseñas y, por lo tanto, **no** tiene autoridad de anular el DTEP proporcionado por el procesador
Clase	Uno de cuatro grupos de privilegios definidos por el administrador que permiten al usuario realizar operaciones específicas de comando del procesador; se puede obtener acceso a cada clase con una contraseña asignada por el administrador
Comando examinado	El comando de comunicaciones usado en el interface entre el procesador y el software de programación que es examinado en busca de violaciones de los mecanismos de protección proporcionados por el procesador protegido PLC-5
Administrador del sistema	El usuario de un procesador protegido que típicamente **puede** modificar los privilegios y contraseñas y, por lo tanto, **tiene** autoridad de anular el DTEP proporcionado por el procesador
Privilegio	La capacidad de realizar una operación de comando apoyada por el procesador protegido PLC-5, incluyendo cualquiera de las siguientes: • modificar privilegios • crear/eliminar archivo de la tabla de datos • crear/eliminar archivo de programa • escritura lógica • escritura física • lectura lógica • lectura física • cambiar modo • forzado de E/S • forzado de la tabla de función secuencial (SFC) • borrar memoria • restaurar • editar en línea

Publicaciones asociadas

La documentación del controlador programable 1785 PLC-5 se organiza en manuales según las tareas que se efectúan.



Para obtener más información acerca de los controladores programables 1785 PLC-5 ó las publicaciones anteriores, comuníquese con su oficina de ventas, distribuidor o integrador de sistema local de Allen-Bradley.

Tabla de contenido

Cómo planificar un sistema protegido

Capítulo 1

Cómo configurar contraseñas y privilegios

Capítulo 2

Cómo configurar y usar la protección de elemento de la tabla de datos

Capítulo 3

Capítulo 1

Cómo planificar un sistema protegido

Presentación

Las características de seguridad del procesador protegido PLC-5 han sido diseñadas para restringir el acceso a las áreas críticas del programa a fin de:

- proporcionar la operación más consistente de la máquina/proceso
- ayudarle a reducir los riesgos asociados con la modificación de programa no autorizada

El procesador protegido ha sido diseñado para mejorar la seguridad ayudándole a evitar:

- los forzados de E/S para grupos de módulo específicos
- el manejo no autorizado de segmentos específicos de palabras de la tabla de datos usando
  - comandos de escritura
  - instrucciones de salida

ATENCION: Los procesadores protegidos **solos** no pueden asegurar el sistema de seguridad PLC. La seguridad del sistema es el resultado de una combinación del procesador protegido, el software y el conocimiento de la aplicación.

Características

Todos los procesadores con características mejoradas (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 y -5/86) permiten al administrador del sistema establecer de una a cuatro clases de privilegio protegidas por contraseña y definir cada clase proporcionándole a ésta el acceso a una combinación única de operaciones de software. Como administrador del sistema, usted también puede establecer privilegios de lectura y escritura para restringir el acceso a:

- los canales de comunicaciones
- los archivos de programa
- los archivos de datos
- los nodos conectados a la red Data Highway Plus™ (DH+™)

Importante: Usted debe habilitar la función de contraseñas y privilegios cuando instala el software de programación de serie 6200 por primera vez si desea usar las características de protección del procesador.

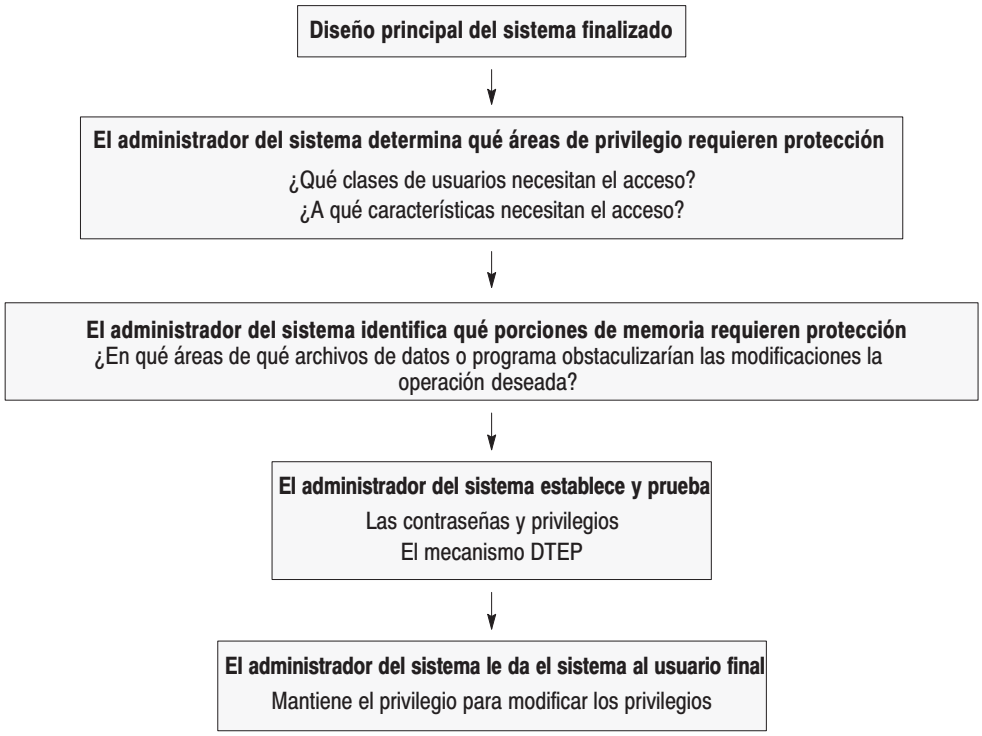
Para controlar:	Los procesadores PLC-5 con características mejoradas le permiten:	Además, los procesadores protegidos le permiten usar DTEP para:
Los forzados de E/S	Permitir o negar el **privilegio de forzados de E/S** para una clase de usuarios Da sólo control total o ningún control	Evitar modificaciones de grupos de módulo específicos con los forzados de E/S iniciados por un usuario final
La escritura de la tabla de datos	• Permitir o negar el p**rivilegio de escritura lógica** para una clase de usuarios Da sólo control total o ningún control • Establecer la **protección de lectura solamente** en determinados archivos Estos mecanismos no evitan que un usuario escriba lógica que evada la protección para modificar una ubicación específica de la tabla de datos.	Evitar escrituras a segmentos específicos de palabras de la tabla de datos al: • enviar comandos de escritura directamente a la tabla de datos • añadir o modificar instrucciones de escalera que pueden escribir al área protegida

Requisitos

Hardware requerido	Software requerido
Controlador programable PLC-5/26, -5/46 ó -5/86 (1785-L26B, -L46B ó -L86B; serie C, revisión G o posteriores)	Software de programación PLC-5, serie 6200, versión 5.0 ó posteriores

Pautas de utilización

Después de finalizar el diseño de un sistema de procesador protegido PLC-5, su papel principal como administrador del sistema es evitar que los usuarios finales anulen los mecanismos de seguridad que usted ha diseñado en el sistema.



Contraseñas y privilegios

Ojo

El mantener control del **privilegio de modificar los privilegios** es esencial para el uso exitoso del mecanismo DTEP.

Las clases de privilegio en un procesador PLC-5 no son necesariamente jerárquicas. Los privilegios de clase 1 se consideran “superiores” que los otros solamente porque nadie puede eliminar el privilegio para modificar los privilegios de la clase 1. Como administrador del sistema, le sería lógico tratar la clase 1 como la clase más alta y definir los privilegios en conformidad hacia la clase 4. Típicamente, usted debe otorgar el privilegio de modificar los privilegios solamente al nivel más alto y nunca divulgar la contraseña a otros usuarios. Por eso, debe prever las necesidades de los usuarios finales y establecer contraseñas y privilegios en la debida forma.

Como administrador del sistema, usted debe proteger los archivos de datos y programa críticos según sus necesidades—es decir, estableciendo estos archivos como “sólo lectura” o “no lectura, no escritura” para todas las clases distintas de la clase 1. Esto protege contra modificaciones de la lógica además de determinar qué archivos de programa son examinados durante el modo de descarga. También debe configurar todos los canales de comunicaciones—incluyendo los canales actualmente no usados—a las clases de privilegio apropiadas.

Protección de elemento de la tabla de datos

Las características de seguridad únicas del procesador protegido PLC-5 le permiten definir áreas de memoria que no se pueden modificar por nadie a no ser un usuario de la clase 1. Durante la programación en línea por los usuarios finales, el procesador protegido PLC-5 sirve como filtro para examinar y evitar peticiones de:

- añadir un código de escalera que podría escribir a o manipular de cualquier modo las direcciones protegidas de la tabla de datos
- modificar
  - las palabras protegidas de la tabla de datos vía operaciones de escritura
  - los elementos protegidos de imagen de E/S vía forzados de E/S

Cuando:	Y:	Esto ocurre:
El usuario final no tiene autoridad de modificar los privilegios	El archivo de estado del procesador contiene el valor para un archivo DTEP (vea la página 3–2)	DTEP se habilita
DTEP se habilita	Una petición de comando examinado es recibida por el procesador (vea la página 3–5)	La opción de examen ocurre durante la edición del programa en línea

Ojo

La ubicación del archivo de estado del valor para el archivo DTEP (S:63) se protege automáticamente; por lo tanto, usted no tiene que protegerlo individualmente.

Las áreas de memoria que usted debe proteger usando el mecanismo DTEP podrían incluir, por ejemplo:

- palabras de salida críticas para la seguridad
- determinadas estructuras de control del contador, temporizador o BT/MG/PD
- registros de almacenamiento de enteros
- palabras de la tabla de datos usadas para especificar direcciones indirectas en tablas de datos críticas
- palabras del archivo de estado de procesador que configuran el sistema, tal como:

Palabra(s)	Uso
S:9	Tiempo de escán máximo①
S:26	Bits de control de usuario
S:29	Número de rutina de fallo
S:30-31	Configuración de interrupción temporizada seleccionable (STI)
S:46-50	Configuración de interrupción de entrada del procesador (PII)
S:54	Tiempo de escán máximo STI①
S:56	Tiempo de escán máximo PII①
S:77	Segmento de tiempo de comunicación
S:78-123	Configuración de programa de control principal (MCP) y tiempos de escán máximos individuales MCP①

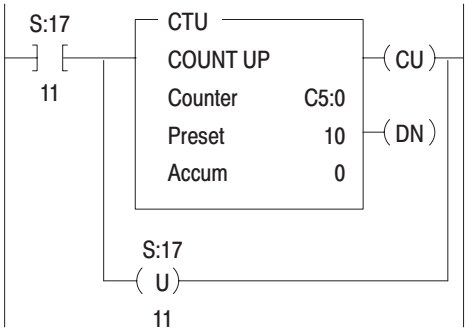
① Por ejemplo, si verifica que los parámetros de rendimiento no sean violados.

Como administrador del sistema, usted puede ofrecerles un poco de flexibilidad a los usuarios finales en cuanto a integrar un sistema y mantener control de la lógica STI, PII o rutina de fallo. Después de asegurar los registros anteriores con DTEP, puede definir un número de archivos de escalera vacíos y no protegidos e incluir saltos a subrutinas (JSR) especificando estos archivos al final de rutinas críticas. Luego, el usuario final puede añadir lógica a un STI, por ejemplo, sin abrir el archivo STI mismo para modificarlo.

El mecanismo DTEP también proporciona ciertas protecciones contra cambios no autorizados efectuados por un usuario final que usa software de programación fuera de línea:

- Durante la descarga de un archivo de imagen del procesador protegido, el procesador protegido examina todos los archivos de programa de tipo escalera de usuario final—incluso los archivos de texto estructurado y SFC—en busca de operandos que violan los rangos DTEP.
- Las operaciones de forzados de E/S no se pueden descargar; por lo tanto, es necesario realizarlas en línea.
- Los cambios fuera de línea hechos a los valores almacenados en las ubicaciones de la tabla de datos protegida se pueden anular si usted, el administrador del sistema, observa las buenas prácticas de programación e inicializa todas las ubicaciones de la tabla de datos a

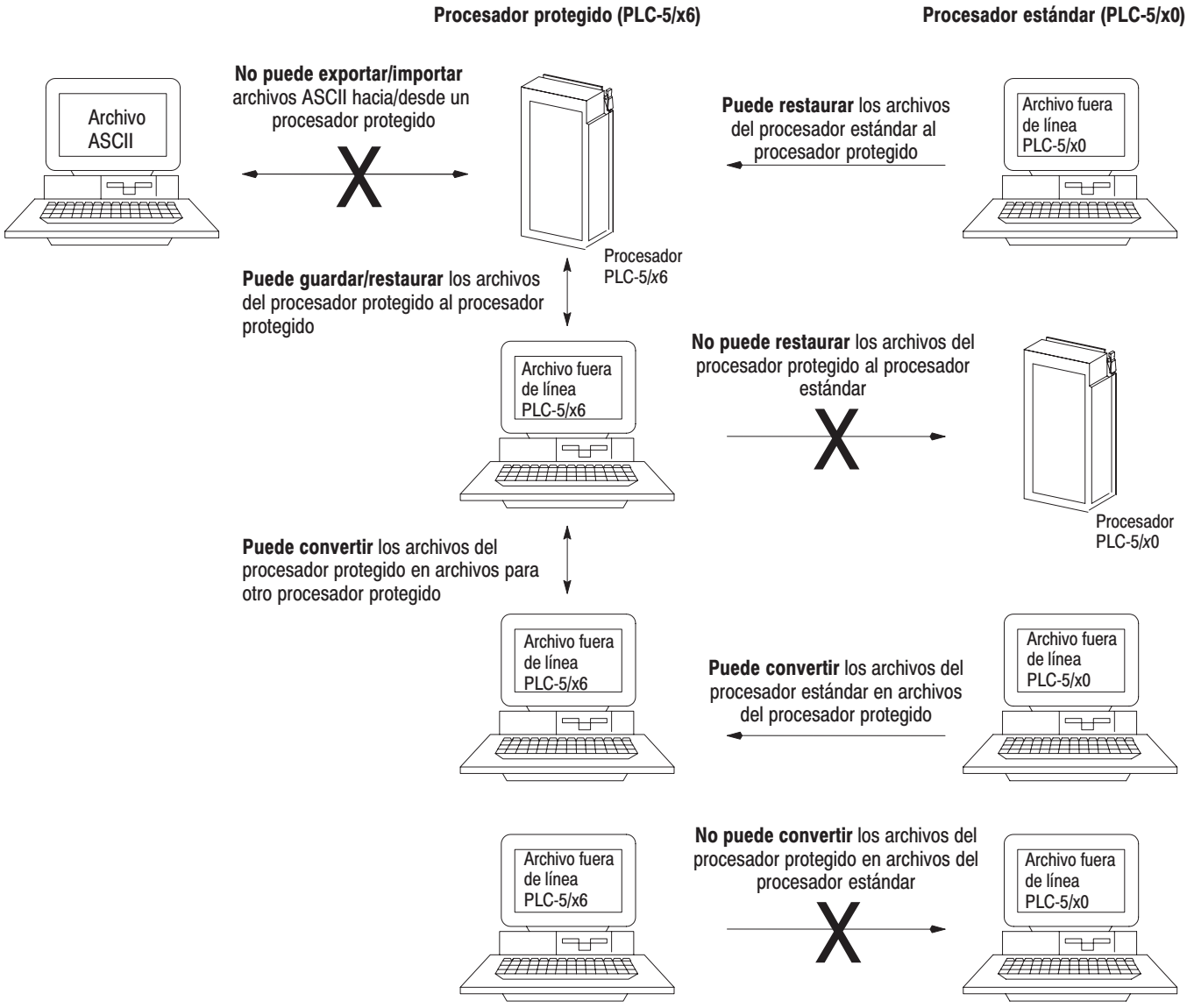
los valores deseados según el primer indicador de escán del procesador (S:1/15).



Como método de monitorizar los intentos por usuarios finales de evadir los mecanismos de seguridad, usted puede monitorizar el bit de fallo menor del archivo de estado (S:17/11). Este bit indica un intento de violar la protección. Se puede usar para contar los intentos de violación si añade un renglón de lógica de escalera que incrementa un contador y pone a cero el bit de fallo menor durante cada intento.

Reglas de conversión del archivo de programa

Siga las reglas descritas a continuación cuando comparta archivos de programa con los procesadores PLC-5 estándar con características mejoradas y procesadores protegidos PLC-5.

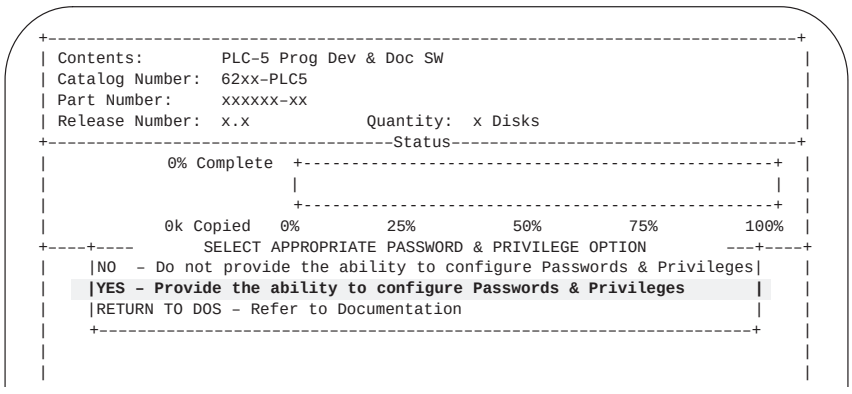


Capítulo 2

Cómo configurar contraseñas y privilegios

Cómo usar este capítulo

Importante: Cuando usted instala el software de programación PLC-5 de la serie 6200 por primera vez, esta pantalla aparece:



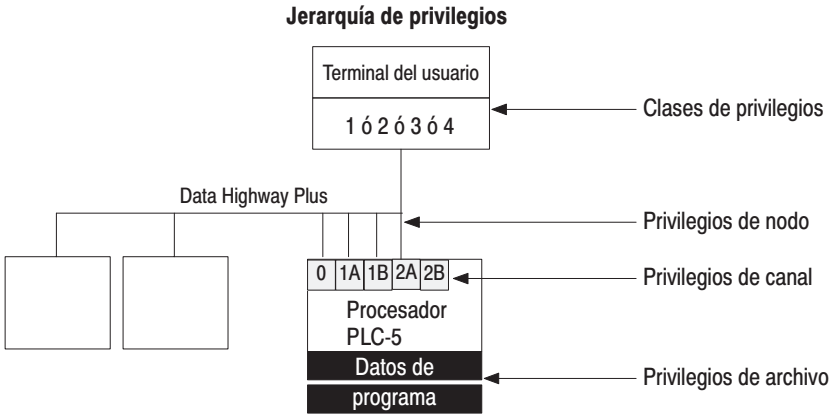
Debe seleccionar la opción siguiente:

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

Para obtener más información acerca de cómo instalar así como configurar contraseñas y privilegios, vea el manual de Configuración y mantenimiento de software de programación PLC-5, publicación 6200-6.4.6ES.

Pautas para la asignación de contraseñas y privilegios

Las clases de privilegios son la organización del nivel superior para la estructura de contraseñas.



Como administrador del sistema, usted debe:

Definir las contraseñas y privilegios para cada procesador en el sistema

↓

Asignar privilegios de clase predeterminados a los canales de comunicación y los archivos fuera de línea

↓

Establecer el acceso de lectura y escritura a las pantallas de configuración de canal

↓

Asignar privilegios para los nodos que necesitan privilegios distintos de los predeterminados del canal

↓

Establecer el acceso de lectura y escritura a los archivos de programa

↓

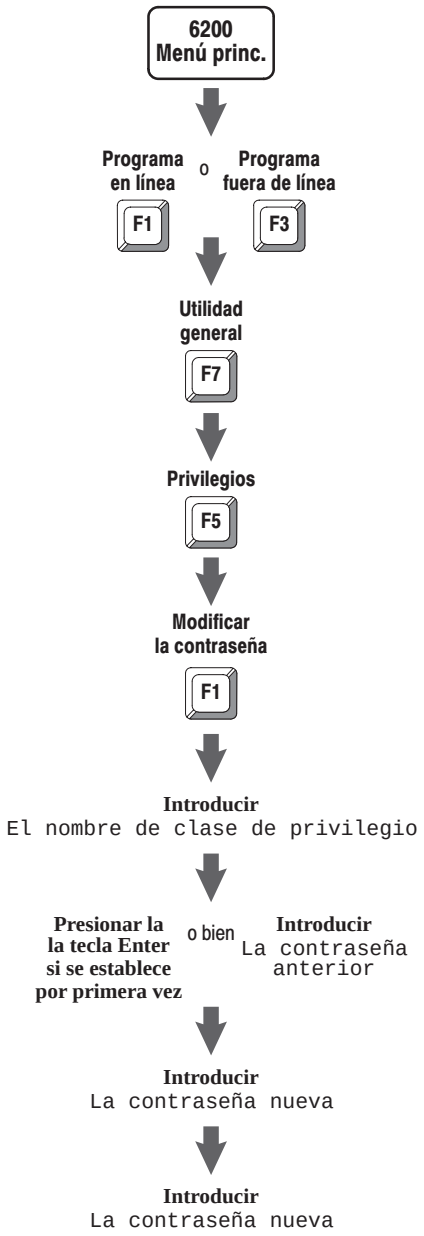
Establecer el acceso de lectura y escritura a los archivos de datos

↓

Indicarles a los usuarios qué clases de privilegios pueden usar y las contraseñas correctas
El usuario final debe introducir la clase y contraseña nuevas para obtener acceso a una clase distinta de la predeterminada

Cómo asignar contraseñas y privilegios a clases

Como administrador del sistema, usted puede asignar una contraseña única a cada una de cuatro clases de privilegios (clases 1–4). Para cada clase, puede asignar el acceso a determinadas operaciones de software (tal como la modificación de archivos de programa, archivos de la tabla de datos o configuraciones de canal).



Cómo asignar contraseñas a clases

Para asignar una contraseña a una clase, siga los pasos a la izquierda.

```
  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
```

Importante: Como administrador del sistema, **usted debe recordar su contraseña.** No existe ningún modo para usted o Allen-Bradley de volver en línea y realizar funciones administrativas del sistema, tal como el restablecimiento de contraseñas y privilegios, sin dicha contraseña. Si es posible que usted la olvide o no esté disponible cuando se necesite la contraseña, escriba la contraseña y póngala en un lugar seguro.

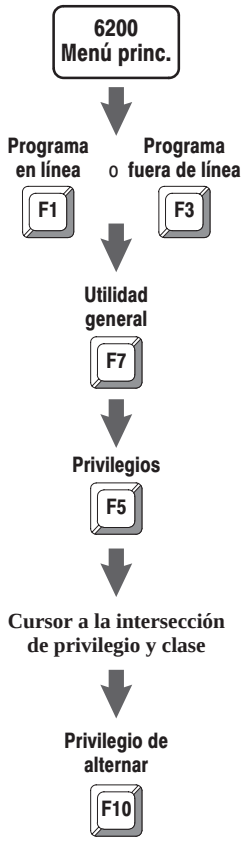
Cómo asignar privilegios a una clase

Puede definir la clase 1 como la clase que tiene todos los privilegios equivalentes o los del administrador del sistema. En este caso, debe definir las tres clases remanentes como clases con menos privilegios y asegurarse que solamente usted, el administrador del sistema, retenga el privilegio de modificar los privilegios..

Por ejemplo, puede decidir que la clase 1 es para el administrador del sistema, la clase 2 para los ingenieros de la planta, la clase 3 para los ingenieros de mantenimiento y la clase 4 para los operadores. Puede establecer las clases de privilegios de la manera siguiente:

Privilegio	Clase1	Clase2	Clase3	Clase4
Modificar los privilegios	X①			
Crear/eliminar archivos de datos	X	X		
Crear/eliminar archivos de programa	X	X	X	
Descargar bloques de mem. procesador (Escritura lógica)	X	X	X	X
Descargar toda la memoria procesador (Escritura física)	X	X	X	X
Cargar bloques de mem. procesador② (Lectura lógica)	X	X	X	X
Cargar toda la memoria procesador (Lectura física)	X	X	X	X
Cambiar el modo del procesador	X	X	X	X
Forzados de E/S	X	X	X	
Forzados de transiciones en las tablas de función secuencial	X	X	X	
Borrar memoria	X			
Restaurar memoria desde el archivo	X	X	X	
Editar en línea	X	X		

① X indica que el privilegio está habilitado para esta clase.
② Sin este privilegio, un usuario ni siquiera puede ver el directorio de programa; requerido para todas las lecturas menos las físicas.



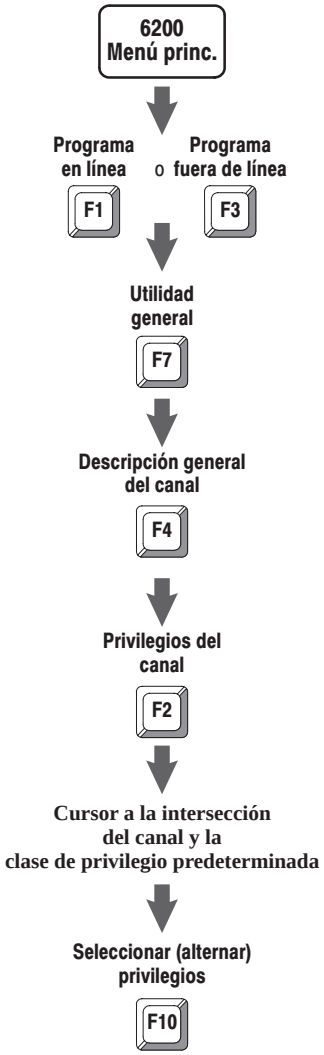
Habilite o inhabilite un privilegio para una clase siguiendo los pasos a la izquierda.

```
   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 usted desea que una clase tenga capacidad para:	Habilite este privilegio/operación:
Habilitar/inhabilitar privilegios para cada clase **Importante**: Si usa DTEP, inhabilite este privilegio para cada clase **menos** la clase 1 (administrador del sistema).	`Modify Privileges`[①]
Crear o eliminar archivos de la tabla de datos	`Data Table File Create/Delete`
Crear o eliminar archivos de programa	`Program File Create/Delete`
Restaurar un archivo de memoria de procesador usando una dirección lógica Por lo general, esto se debe combinar con una escritura física	`Logical Write`[①]
Restaurar un archivo de memoria de procesador usando una dirección física Por lo general, esto se debe combinar con una escritura lógica	`Physical Write`
Leer desde el procesador usando una dirección lógica Por lo general, esto se debe combinar con una lectura física **Importante**: Sin esto, un usuario ni siquiera puede ver el directorio de programa; requerido para todas las lecturas menos las físicas.	`Logical Read`[①]
Leer la memoria del procesador con una dirección física Por lo general, esto se debe combinar con una lectura lógica.	`Physical Read`
Cambiar el modo de procesador cuando el interruptor de llave en el procesador está en la posición REMOTA	`Mode Change`
Habilitar o inhabilitar forzados en el sistema; borrar todos los forzados de E/S	`I/O Force`
Habilitar o inhabilitar forzados SFC; forzar transiciones individuales a la posición activada o desactivada; o borrar todos los forzados SFC	`SFC Force`
Borrar la memoria del procesador ó	`Clear Memory`
Restaurar o mezclar un archivo de memoria de procesador	`Restore`
Editar un archivo de programa en cualquier modo de procesador	`Online Editing`

[①] **Importante**: Usted no puede eliminar este privilegio de la clase 1 (administrador del sistema).

Cómo asignar clases de privilegio predeterminadas a canales de comunicación y archivos fuera de línea



Una clase de privilegio predeterminada determina la clase de un determinado canal y de todas las estaciones/nodos conectadas por medio de ese canal. Si usted tiene un nodo específico que requiere privilegios distintos de los que la asignación de clase del canal permite, puede especificar la clase de privilegio para dicho nodo separadamente (vea la página 2–8).

Los canales de comunicación y archivos fuera de línea comienzan con privilegios de la clase 1. Asigne una clase de privilegio predeterminada nueva para un canal de comunicación o archivo fuera de línea siguiendo los pasos a la izquierda.

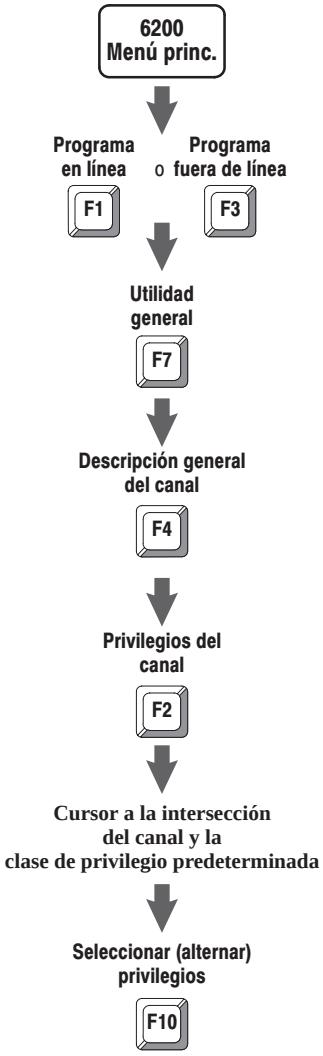
```
                          Channel Privileges

                             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
```

Importante: Si usa DTEP, asigne clases predeterminadas a todos los canales—incluyendo cualesquier canales actualmente no usados.

Cómo asignar privilegios de lectura y escritura para canales de comunicación

Los privilegios de lectura y escritura que usted ve en la pantalla de privilegios de canal se aplican al acceso de lectura y escritura de la clase de privilegios a la pantalla de configuración de canal de cada canal.

Importante: El eliminar el acceso de lectura y escritura de la clase 1 para un canal prohibe que aun usted mismo, el administrador del sistema, configure dicho canal. Asegúrese que la clase 1 retenga el acceso necesario a cada canal.



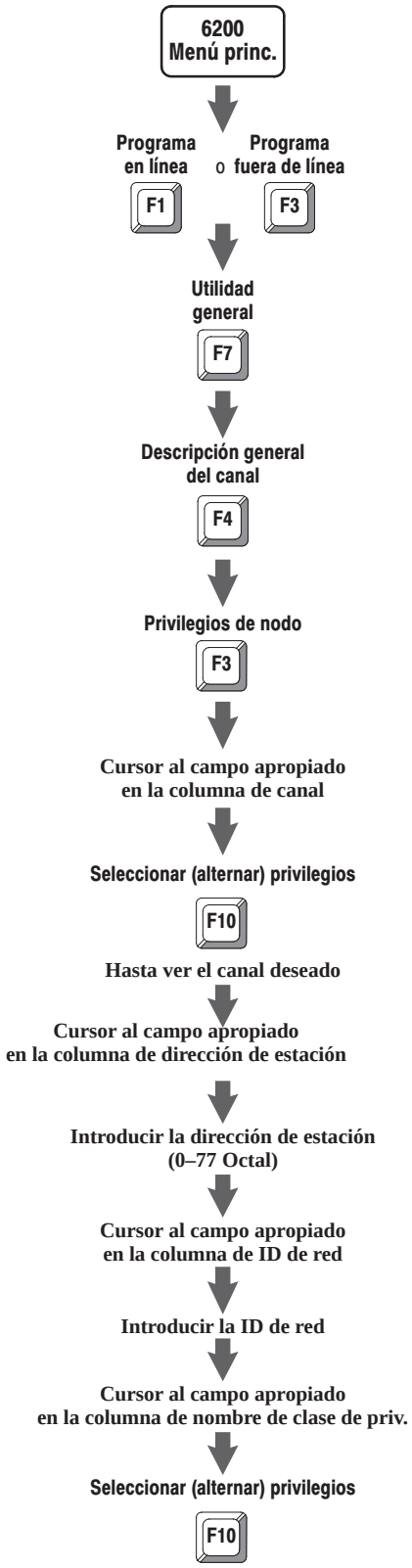
Como administrador del sistema, usted especifica los privilegios de lectura y escritura para un canal siguiendo los pasos a la izquierda.

```
                          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 usted desea que la clase pueda:	Seleccione esta opción:
Leer la información de configuración solamente	R
Leer y cambiar la información de configuración	RW
No leer ni modificar la información de configuración del canal	(En blanco)

Establezca los privilegios de lectura y escritura para el archivo de diagnóstico de cada canal (pantalla de estado de canal) por medio de la pantalla de privilegios de la tabla de datos (vea la página 2–10).

Cómo asignar privilegios para estaciones/nodos específicos



Cada estación/nodo que se conecta al canal DH+® de este procesador retorna a la clase de privilegio predeterminada asignada a su canal; sin embargo, como administrador del sistema, usted puede dar a un nodo determinado una clase de privilegio única.

Importante:

- Las clases de privilegio anulan la clase de privilegio predeterminada del canal asignado en la pantalla de privilegio de canal.
- Si otorga privilegios de clase 1 al nodo, un usuario final puede configurar una terminal para que se conecte como ese nodo, creando así un posible riesgo de seguridad.

Especifique una clase de privilegio para un nodo siguiendo los pasos a la izquierda.

```
                          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
     0               0                  0

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

El campo en esta columna:	Especifica:
Canal	el canal al cual el nodo está conectado
Dirección de estación	la dirección de estación del nodo en el canal
ID de red	el número de red usado para identificar la red DH+ a la cual está conectado el nodo que usted especifica
Nombre de clase de privilegio	clase de privilegio del nodo La clase de privilegio predeterminada del nodo es la clase de privilegio del canal

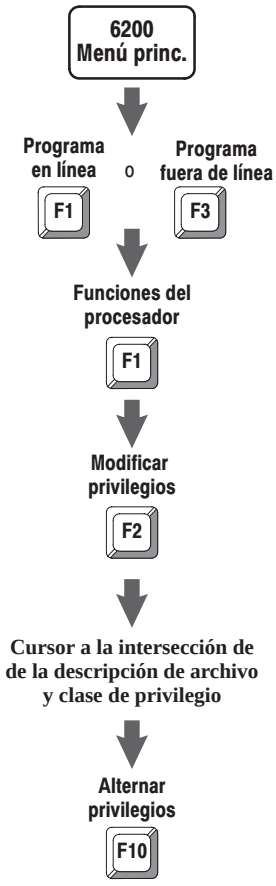
Cómo asignar privilegios de lectura y escritura para un archivo de programa

Como administrador del sistema, usted puede asignar privilegios de lectura y escritura para cada archivo de programa en un procesador a fin de restringir la posibilidad de verlo o cambiarlo por parte de los usuarios.

Importante:

- No puede modificar los privilegios de lectura y escritura al sistema (archivo 0) o archivos no definidos.
- El eliminar el acceso de lectura y escritura de la clase 1 para un canal prohibe que aun usted mismo, el administrador del sistema, configure dicho canal. Asegúrese que la clase 1 retenga el acceso necesario a cada canal.
- El examen de descarga para las violaciones DTEP es dirigido a archivos de programa para los cuales las clases 2–4 tienen privilegios de escritura. Si genera archivos fuera de línea que controlan la lógica crítica, debe eliminar todos los privilegios para poder escribir esos archivos de las clases 2–4 antes de que DTEP le permita descargar dichos archivos.

Para especificar los privilegios de lectura y escritura para un archivo de programa, siga los pasos a la izquierda.




```
+= 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 usted desea que la clase pueda:	Seleccione esta opción:
Leer el archivo de programa solamente	R
Leer y cambiar el archivo de programa	RW
Ni leer ni modificar el archivo de programa	(en blanco)①

① Puede usar esto para proteger contra la visualización de los algoritmos de propiedad.

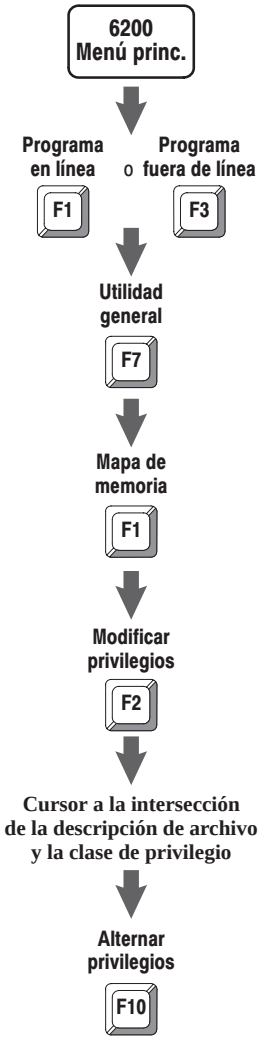
Cómo asignar privilegios para una archivo de la tabla de datos

Como administrador del sistema, usted puede asignar privilegios de lectura y escritura para cada archivo de la tabla de datos para restringir el acceso de ver o cambiar valores de archivo de la tabla de datos por parte de los usuarios.

Importante:

- No puede modificar los privilegios de lectura y escritura a los archivos no definidos.
- El eliminar el acceso de lectura y escritura de la clase 1 para un canal prohibe que aun usted mismo, el administrador del sistema, configure dicho canal. Asegúrese que la clase 1 retenga el acceso necesario a cada canal.

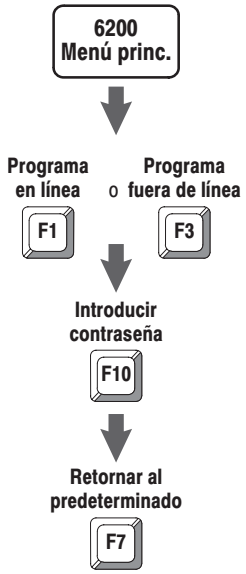
Para especificar los privilegios de lectura y escritura para un archivo de la tabla de datos, siga los pasos a la izquierda.




```
                              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 usted desea que la clase pueda:	Seleccione esta opción:
Leer el archivo de la tabla de datos solamente	R
Leer y cambiar el archivo de la tabla de datos	RW
Ni leer ni modificar el archivo de la tabla de datos	(En blanco)

Cómo restaurar las clases de privilegios predeterminadas

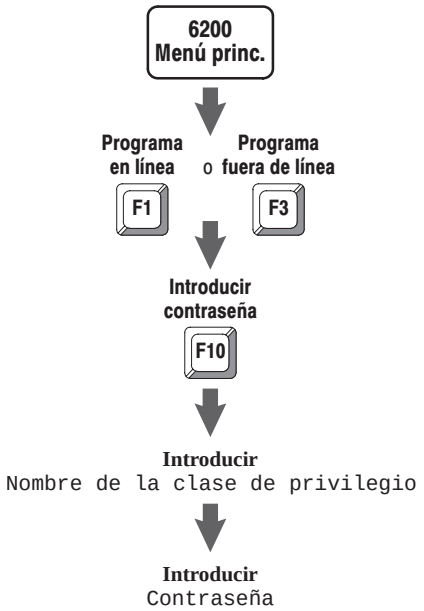


Como administrador del sistema, usted puede restaurar los privilegios predeterminados para una clase si las ediciones actuales todavía no se han guardado.

Para restaurar los privilegios predeterminados, siga los pasos a la izquierda.

```
+= 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
```

Cómo cambiar a otra clase



Si usted desea obtener los privilegios de otra clase (distinta de la clase para la cual la terminal de programación está configurada actualmente), debe introducir la clase y contraseña nuevas.

Para obtener los privilegios de otra clase, siga los pasos a la izquierda.

```
+= 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
```

Ojo También puede presionar `ALT-P` para seleccionar una clase de privilegio nueva.

Capítulo **3**

Cómo configurar y usar la protección de elemento de la tabla de datos

Cómo usar este capítulo

Si usted desea leer acerca de:	Pase a la página:
Cómo crear un archivo de protección	3–1
Establecer un archivo de protección	3–2
Introducir rangos de la tabla de datos en un archivo de protección	3–3
Cómo examinar comandos	3–5
Cómo proporcionar protección contra los cambios fuera de línea	3–5
Comprensión de las restricciones instaladas en el sistema	3–6
Cómo probar el archivo de protección	3–8

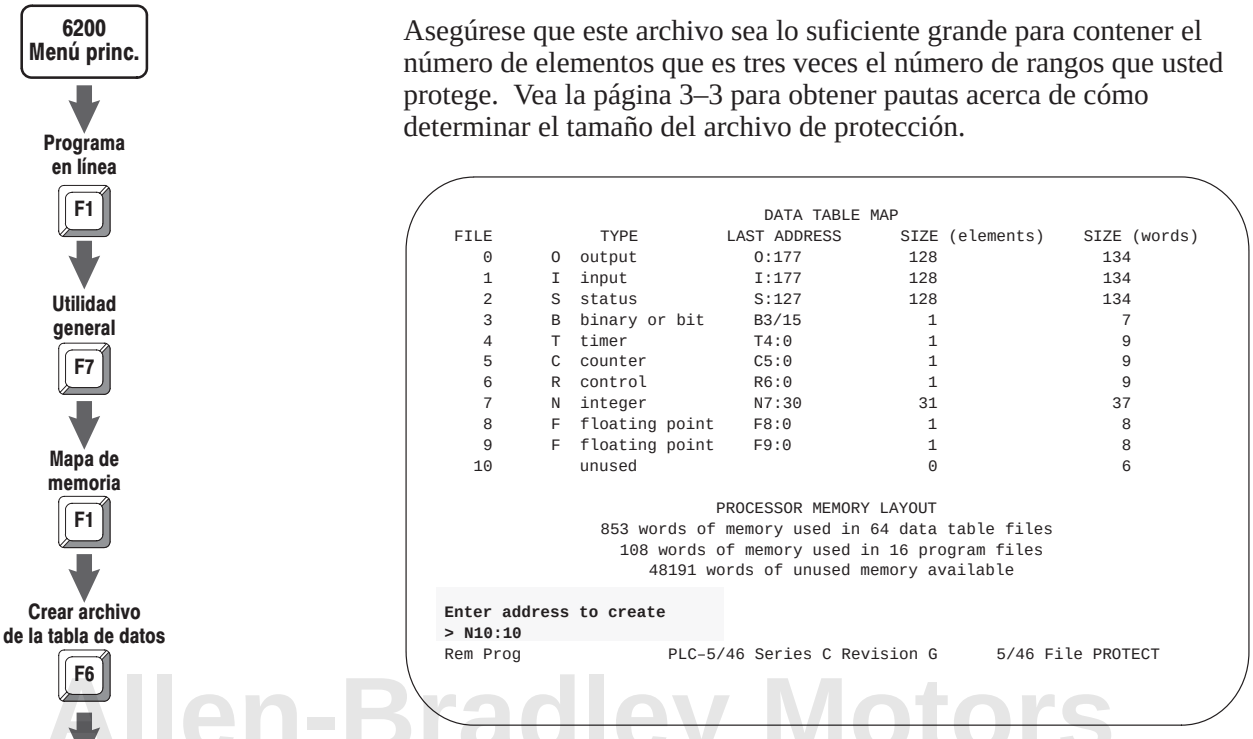
Como administrador del sistema, implemente DTEP por medio de:

- obtención de privilegios de administrador del sistema (clase 1)
- creación de un archivo entero de la tabla de datos para servir como el archivo DTEP
- introducción del número del archivo entero en el archivo de estado del procesador (archivo 2 de la tabla de datos)
- introducción de los rangos de la tabla de datos que se deben proteger en el archivo DTEP

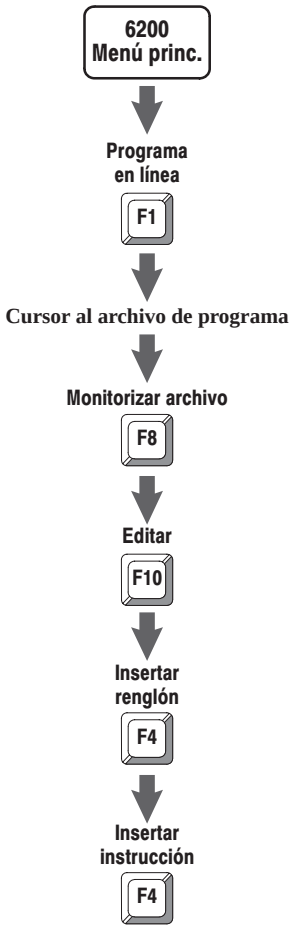
Cómo crear un archivo de protección

Como administrador del sistema, usted debe seguir los pasos a la izquierda para crear un archivo entero de la tabla de datos que va a usarse como el archivo DTEP.

Asegúrese que este archivo sea lo suficiente grande para contener el número de elementos que es tres veces el número de rangos que usted protege. Vea la página 3–3 para obtener pautas acerca de cómo determinar el tamaño del archivo de protección.



Cómo iniciar el mecanismo de protección



El introducir el número de archivo del archivo DTEP en el elemento 63 del archivo de estado (S:63) inicia automáticamente el mecanismo DTEP para los usuarios finales.

Cómo administrador del sistema, usted debe usar los pasos a la izquierda e introducir una instrucción de escalera a fin de mover el número de archivo DTEP deseado al S:63 del archivo de estado.

Esta instrucción de escalera puede ser temporal siempre que se ejecute una vez para establecer el valor en el archivo de estado. Luego, puede eliminar la instrucción de escalera y el programa se puede archivar (guardar) con la protección incorporada.

Importante: La validez del número de archivo movido a la dirección S:63 no se verifica hasta que un comando de examen se reciba de un usuario final durante la programación en línea. Si no es válido:

- un código de error retorna
- un fallo menor (S:17/12) se establece

Usted, como administrador del sistema, debe seguir los pasos en la página 3–8 para forzar la validación de este número de archivo antes de presentar el sistema a los usuarios finales.

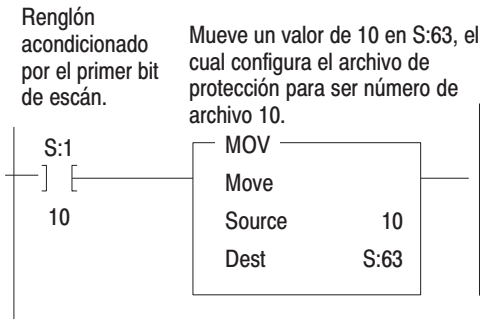
El mecanismo de protección continúa vigente para el usuario final hasta que usted:

- transfiere el privilegio de modificar los privilegios al usuario final, o
- borra la introducción del archivo DTEP del archivo de estado

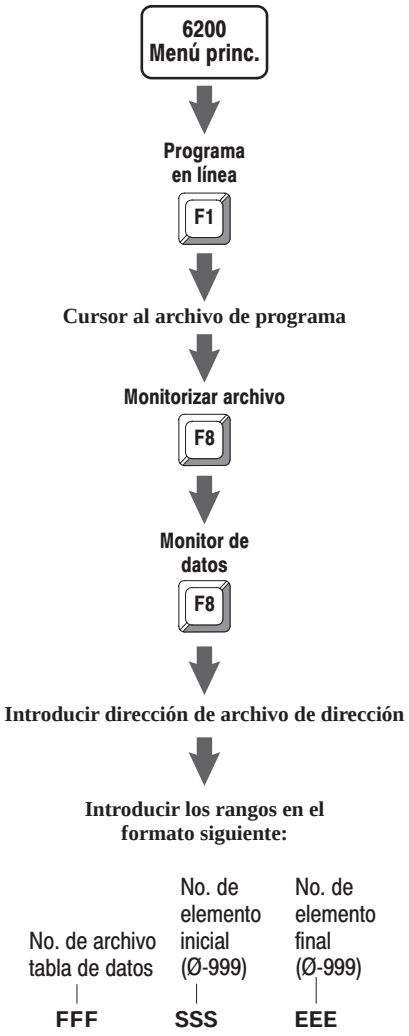
Cuando DTEP está vigente, lo siguiente es protegido automáticamente contra modificación por comandos emitidos por un usuario final:

- el elemento 63 del archivo de estado
- todo el archivo DTEP

Importante: Para el administrador del sistema, la posesión del privilegio de modificar los privilegios anula el mecanismo de protección.



Cómo introducir rangos de la tabla de datos en el archivo de protección



Como administrador del sistema, usted especifica los rangos de protección en el archivo DTEP usando tres palabras consecutivas para cada introducción de rango.

Introduzca los rangos de archivo que desea protegidos siguiendo los pasos a la izquierda.

```
  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
```

Siga estas pautas:

- Introduzca las introducciones de tres palabras del rango de protección a partir del elemento cero (0) y continúe con las introducciones contiguas para todos los rangos que se deben especificar.
- Los elementos iniciales y finales dentro de cada introducción de rango deben aparecer en orden ascendente—excepto cuando protege un elemento solamente; en tal caso, los elementosson iguales.
- Especifique un elemento inicial de cero (0) y un elemento final de 999 para proteger un archivo entero, pese a la cantidad de elementos que se encuentren en el archivo.
- Indique las introducciones de rango de protección intencionalmente no usadas en el archivo DTEP colocando `'-1'` en el campo del número de archivo de la tabla de datos.
- Introduzca cualquier número de rangos de protección hasta 333.
- Haga el archivo DTEP solamente tan grande como sea necesario para especificar todos los rangos de protección requeridos.

  Aunque el uso del mecanismo de protección no afecta el rendimiento de la ejecución del programa de modo de marcha de manera importante, sí puede afectar la sensibilidad del procesador a comandos que se reciben desde el usuario final. Siga estas pautas para minimizar esta posibilidad:

  - Minimice el número de rangos de protección especificados.

    En lugar de especificar varios rangos de protección en un archivo de la tabla de datos, considere proteger todo el archivo con un solo rango.

  - Mantenga el tamaño del archivo DTEP al mínimo requerido para el número de rangos de protección requeridos.

Ojo

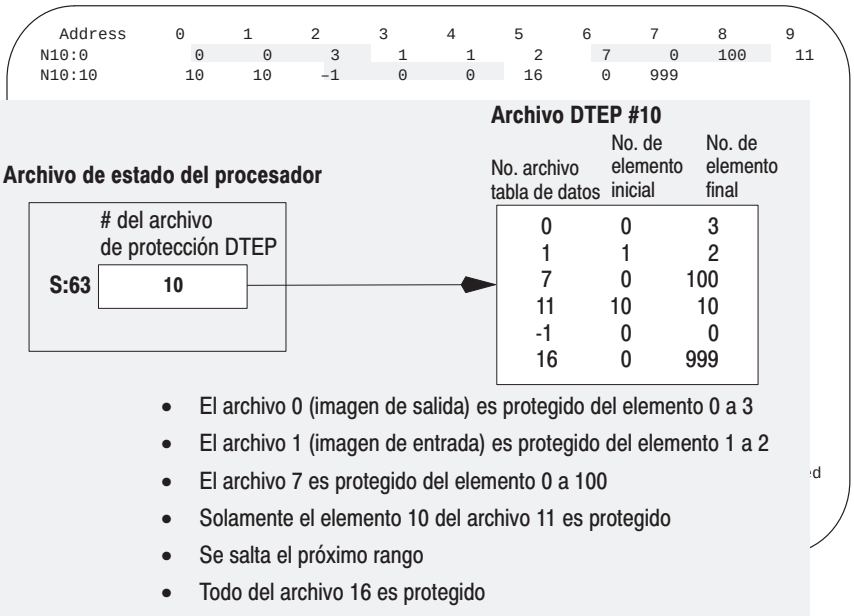
El exceso de espacio en el archivo DTEP se llena de ceros predeterminadamente; cualquier agrupación “0 0 0” resultante se interpretaría como archivo de protección 0, elemento 0 — es decir, O:Ø. Evite esto colocando un ‘–1’ en cualquier espacio que intencionalmente no ha sido usado.

Ojo

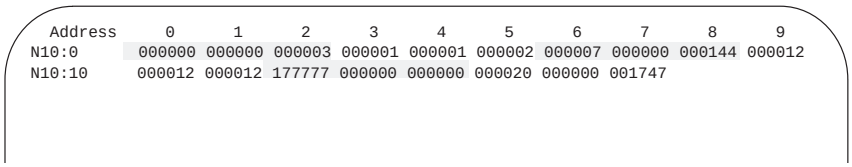
Aun si usted, el administrador del sistema, ya ha eliminado el privilegio de escribir a un archivo de la tabla de datos, todavía puede protegerlo con DTEP y aprovechar las características de protección más amplias de DTEP (por ejemplo, protección contra las escrituras no autorizadas por instrucciones de salida de usuarios finales).

Esto es importante porque el procesador protegido escanea el archivo completamente, desde el primero hasta el último elemento, cuando verifica el archivo así como cuando examina los comandos de la pantalla DTEP.

Figura 3.1
Cómo introducir los rangos en un archivo DTEP



Estos rangos se introducen en decimal predeterminadamente. Si introduce un rango desde uno de los archivos de imagen de E/S, puede presionar `F1 – Change Radix` y `F2 – Octal Data` e introducir el rango en octal. Cuando retorna al decimal, la conversión se realiza por usted.



Importante: La validez de las introducciones del rango de protección no se verifica cuando las introduce vía el monitor de datos, pero son validadas cuando un comando examinado se recibe de un usuario final durante la programación en línea. Si no son válidas:

- un código de error retorna
- un fallo menor (S:17/12) se establece

Usted, como administrador del sistema, debe seguir los pasos en la página 3–8 para forzar la validación de estas introducciones antes de presentar el sistema a los usuarios finales.

Comandos de examen

Durante la edición de programa en línea por el usuario final, el procesador protegido examina todos los comandos de comunicaciones que se pueden usar para modificar los elementos de la tabla de datos, manipular direcciones o forzar E/S. Si el mecanismo DTEP se habilita—es decir, el usuario no puede modificar los privilegios y hay un archivo DTEP válido indicado en S:63—el procesador protegido examina cada comando en busca de acceso a las áreas de la tabla de datos protegidas. Este procesador verifica todos los rangos en el archivo DTEP. Si se encuentra una violación, la petición es rechazada, un código de error—`Data Table Element Protection Violation`—retorna y un bit de fallo menor S:17/11 se establece.

Protección contra cambios fuera de lína

El examen de los comandos ocurre durante la programación en línea por un usuario final—es decir, cuando el software de programación está conectado directamente al procesador. Cuando un usuario final cambia una imagen de procesador fuera de línea—es decir, cuando el software de programación está conectado a una imagen de archivo del procesador—la mayor parte de los comandos no se puede examinar directamente por el procesador en busca de violaciones de protección. Para los cambios fuera de línea, por lo tanto, hay otros métodos que ayudan a evitar violaciones de protección.

Archivos de la tabla de datos

Como administrador del sistema, usted debe seguir las buenas prácticas de programación e inicializar todas las ubicaciones de tabla de datos a los valores deseados según el primer indicador de escán (S:1/15) del procesador. Ya que el archivo DTEP especifica solamente los rangos y no los valores que se deben encontrar en cada ubicación, el procesador protegido no puede evitar ni detectar cambios efectuados a los valores que son almacenados en los archivos de la tabla de datos durante la programación fuera de línea. Cuando inicializa todas las ubicaciones de la tabla de datos a los valores deseados según el primer indicador de escán del procesador, todos los problemas que pueden haber ocurrido debido a violaciones de protección realizadas durante la escritura a ubicaciones de la tabla de datos fuera de línea son anulados.

Tablas de forzados de E/S

Para proteger la operación del procesador contra las posibles operaciones de forzados de E/S incluidas en la imagen del procesador por medio de programación fuera de línea, los procesadores protegidos no aceptan cambios de la tabla de forzados de E/S en el modo de descarga. Los datos en las tablas de forzados de E/S permanecen sin cambio. Al final de cualquier descarga a un procesador protegido, las tablas de forzados de E/S se borran de forzados y una advertencia aparece en la terminal que indica que los forzados en el archivo de disco no se descargaron.

Cómo insertar elementos

El procesador protegido examina instrucciones de escalera y de inserción de elemento de texto estructurado durante la descarga para asegurar que las direcciones protegidas por el mecanismo DTEP no se vuelvan a programar.

Como administrador del sistema, usted debe haber establecido la protección básica para la aplicación de procesador usando las contraseñas y capacidades de privilegios mencionadas en el capítulo 2. Cuando lo hizo, debe haber eliminado los privilegios de escritura de todas las clases (menos la clase 1) para todos los archivos de programa y datos que considera como críticos para la seguridad del programa de aplicación. Los archivos de programa que los usuarios finales crean más adelante no son protegidos de esta manera y retornan al estado predeterminado para permitir que todas las cuatro clases tengan privilegios de lectura y escritura. Esta diferencia permite que el procesador ligue el examen de descarga a cualquier petición de descarga efectuada que tiene un archivo de programa de escalera o de texto estructurado como el destino final y que, además, tiene privilegios de escritura permitidos para la clase 2.

Una violación de protección causa que la descarga se cancele, la pantalla de descarga muestra el mensaje `Data Table Element Protection Violation` y la pantalla continúa mostrando el número de archivo de programa que causó la violación de protección. Use esta información para localizar la combinación de instrucción/operando que causó la violación de protección.

Al detectar un error de violación de protección durante el modo de descarga, el procesador responde como si ocurriera un límite de tiempo sobrepasado de descarga, establece el modo de procesador a programa (o programa remoto) y establece el fallo mayor de “mala memoria de programa del usuario” con un código de fallo de “descarga anulada” (19).

Comprensión de las restricciones instaladas en el sistema

Para reducir los riesgos de seguridad, las restricciones siguientes han sido aplicadas al uso de un sistema protegido.

Direccionamiento indirecto

Ya que el direccionamiento indirecto le permite al usuario final determinar la dirección de tabla de datos efectiva al momento de marcha manipulando la ubicación indirecta en el programa de escalera, un riesgo de seguridad podría existir. Cuando DTEP se habilita y el usuario final no tiene la capacidad para modificar los privilegios, el procesador protegido examina en busca del direccionamiento indirecto en las instrucciones de escalera y de texto estructurado que se insertan. El sistema de seguridad:

- rechaza todo el direccionamiento indirecto al nivel de archivo—por ejemplo, N[N7:0]:20
- permite las direcciones indirectas al nivel de elemento—por ejemplo, N12:[N7:0]—solamente si el archivo especificado no contiene elementos protegidos
- rechaza el direccionamiento indirecto al nivel de elemento si el archivo especificado contiene elementos protegidos

Si una violación de protección ocurre, la petición es rechazada, un código de error (`Data Table Element Protection Violation`) retorna y un bit de fallo menor S:17/11 se establece.

Direccionamiento indexado

Ya que el direccionamiento indexado le permite al usuario final determinar la dirección de tabla de datos efectiva al momento de marcha manipulando la ubicación de la palabra de índice del archivo de estado (S:24) en el programa de escalera, podría existir otro riesgo. Cuando DTEP se habilita y el usuario final no tiene la capacidad para modificar los privilegios, el procesador protegido examina en busca del direccionamiento indexado y previene la inserción si el número de archivo direccionado intersecta con cualquiera de los rangos protegidos en el archivo DTEP. Si una violación de protección ocurre, la petición es rechazada, un código de error (`Data Table Element Protection Violation`) retorna y el bit de error menor S:17/11 se establece.

Ya que el procesador no prohibe el cruce de los límites del archivo de tabla de datos por medio del direccionamiento indexado, todavía existe un riesgo de seguridad menor con este examen. Mientras que este mecanismo de examen verifique que no existan elementos protegidos en el archivo direccionado, el mecanismo no puede buscar la posibilidad de sobrescribir un elemento protegido en los archivos subsiguientes ya que no sabe:

- cuántos archivos de la tabla de datos que la instrucción indexada podría afectar posiblemente durante la ejecución
- qué será el valor del campo .POS de la estructura de control al momento de ejecución

Importante: Asegúrese que las instrucciones indexadas no excedan el límite del archivo.

Cómo escribir datos a memoria mediante el puerto del coprocesador

Los productos que usan el puerto del coprocesador utilizan dos mecanismos de transferencia de datos sin procesar que no se categorizan en la funcionalidad de contraseñas y privilegios actuales. Por lo tanto, al coprocesador se le prohibe escribir datos sin procesar a la memoria del procesador cuando el mecanismo DTEP está habilitado. El privilegio de anulación, modificar los privilegios, no tiene efecto en este caso porque no hay privilegios asociados con los mecanismos de transferencia de datos sin procesar del puerto del coprocesador.

Cuando detecta una petición de transferencia de datos sin procesar que provoca una violación de protección, la respuesta del procesador es retornar un indicador de fallo al coprocesador y establecer un fallo mayor de “fallo de dispositivo de canal 3” (bit 5) en el procesador con un código de fallo de `COPRO Transfer Not Valid with Data Table Element Protection Invoked` (106).

Los comandos examinados que pasan por el puerto del coprocesador son examinados según las reglas del mecanismo DTEP estándar.

Cómo importar y exportar archivos ASCII

Debido a las cuestiones de protección de datos que el procesador protegido ha sido diseñado para direccionar, usted no puede usar las funciones ASCII de importación o exportación de memoria de procesador del software de programación de serie 6200 en un archivo de memoria del procesador protegido.

Cómo probar el archivo de protección

Cuando procesa cada comando examinado de protección mientras que la protección está habilitada, el proceso de validación verifica que:

- el archivo DTEP
  - existe
  - es un archivo entero
- el número de archivo de la tabla de datos es válido
- el rango de valores en el archivo DTEP es válido
- el número de archivo existe
- los pares de valor de elemento inicial/final son iguales o aparecen en orden ascendente
- los rangos representan palabras que se encuentran en el archivo de la tabla de datos indicado

Si uno de los anteriores no es el caso,

- un código de error (`DTE Protection File Invalid`) retorna
- un fallo menor (S:17/12) se establece

El valor '–1' se acepta para anular una introducción no usada y no se detecta como error. El campo del elemento final se puede establecer a '999' pese al número de elementos que realmente se encuentra en un archivo, y eso no se detecta como error cuando se valida el archivo de protección.

Importante: Las condiciones inválidas prohiben los intentos por parte del usuario final de efectuar comandos examinados DTEP hasta que el problema se resuelva.

Como administrador del sistema, pruebe bien a fondo el archivo DTEP antes de utilizarlo para el usuario final siguiendo estos pasos:

1. Cambie la clase de privilegio a una de las clases de usuario final previamente definidas.
2. Intente una operación de escritura (monitor de la tabla de datos) a una dirección de tabla de datos protegida.

   Esto fuerza la validación del archivo DTEP. Si el archivo no es válido, el bit de fallo menor S:17/12 se establece y las operaciones de escritura subsiguientes se prohiben hasta que el error de archivo se corrija. Si DTEP funciona correctamente, un código de error (`Data Table Element Protection Violation`) retorna y el bit de fallo menor S:17/11 se establece.
3. Intente una operación de escritura a una dirección de tabla de datos no protegida.

   Esta operación debe resultar exitosa.
4. Retorne la clase de privilegio a la clase 1 y corrija los errores.

Si tiene que volver a añadir más elementos de la tabla de datos a los DTEP existentes después de la integración de un sistema, primero verifique que los usuarios finales todavía no hayan obtenido acceso a los elementos que se van a proteger en el direccionamento de instrucción. Si añade protección a los elementos que ya han sido usados, en efecto usted bloquea a los usuarios finales de su propia lógica.

A

B

C

R

S

T

U

V

Publication 1747-2.30FR – Février 1996

Rockwell *Automation*

Rockwell Automation ayuda a sus clientes a lograr mejores ganancias de sus inversiones integrando marcas líder de la automatización industrial y creando así una amplia gama de productos de integración fácil. Estos productos disponen del soporte de proveedores de soluciones de sistema además de los recursos de tecnología avanzada de Rockwell.

Con oficinas en las principales ciudades del mundo.

Alemania • Arabia Saudita • Argentina • Australia • Bahrein • Bélgica • Bolivia • Brasil • Bulgaria • Canadá • Chile • Chipre • Colombia • Corea • Costa Rica • Croacia Dinamarca • Ecuador • Egipto • El Salvador • Emiratos Arabes Unidos • Eslovaquia • Eslovenia • España • Estados Unidos • Finlandia • Francia • Ghana • Grecia • Guatemala Holanda • Honduras • Hong Kong • Hungría • India • Indonesia • Irán • Irlanda • Islandia • Israel • Italia • Jamaica • Japón • Jordania • Katar • Kuwait • Las Filipinas • Líbano Macao • Malasia • Malta • México • Morruecos • Nigeria • Noruega • Nueva Zelanda • Omán • Pakistán • Panamá • Perú • Polonia • Portugal • Puerto Rico • Reino Unido República Checa • República de Sudáfrica • República Dominicana • República Popular China • Rumania • Rusia • Singapur • Suecia • Suiza • Taiwan • Tailandia • Trinidad Tunicia • Turquía • Uruguay • Venezuela

Sede central de Rockwell Automation: 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414–382–2000, Fax: (10) 414–382–4444
Sede central europea de Rockwell Automation: Avenue Herrmann Debrouxlaan, 46, 1160 Bruselas, Bélgica, Tel: (32) 2 663 06 00, Fax: (32) 2 663 06 40
Sede central de Asia–Pacífico de Rockwell Automation: 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publicación 1785-6.5.13ES – Enero de 1995

PN 956543–80