Wprowadzenie do środowiska projektowego TIA Portal dla sterowników S7-1500

Przegląd funkcji zabezpieczeń CPU

Środowisko projektowe Totally Integrated Automation Portal firmy Siemens jest pierwszym współdzielonym środowiskiem pracy integrującym rozwiązania techniczne różnych systemów SIMATIC udostępnianych w jednolitej strukturze. Dlatego też TIA Portal po raz pierwszy umożliwia niezawodną i wygodną współpracę różnych systemów. Wszystkie wymagane pakiety oprogramowania, od konfiguracji sprzętowej, przez programowanie, aż do wizualizacji procesów są dostępne w jednym, zintegrowanym środowisku projektowym. W artykule skupiamy się na zilustrowaniu dodawania urządzeń z bibliotek i ich konfiguracji HMI w pakiecie TIA Portal.

W tym odcinku naszego cyklu wprowadzającego do tajników sterowników z rodziny S7-1500 przedstawiamy funkcje zabezpieczeń systemu automatyki przed nieautoryzowanym dostępem:

- ochrona dostępu,
- ochrona „know-how”,
- zabezpieczenie przed kopiowaniem,
- ochrona przez zablokowanie CPU.

Ochronę przed nieautoryzowanym dostępem do funkcji i danych CPU S7-1500 ze źródeł zewnętrznych oraz przez sieć można zwiększyć stosując następujące dodatkowe środki ochrony:

- deaktywację serwera sieci Web,
- deaktywację synchronizacji czasu przez serwer czasu NTP (Network Time Protocol),
- deaktywację komunikacji z użyciem instrukcji PUT/GET.

Gdy jest używany serwer sieci Web, to system automatyki S7-1500 można chronić przed nieautoryzowanym dostępem poprzez ustawienie uprawnień dostępu chronionego hasłem dla poszczególnych użytkowników w systemie zarządzania użytkownikami.

Na wyświetlaczu LCD systemu S7-1500 można zablokować dostęp do chronionego hasłem CPU (blokada lokalna). Blokada dostępu jest aktywna tylko wtedy, gdy przełącznik trybu pracy jest w pozycji RUN.

Blokada dostępu działa niezależnie od zabezpieczenia hasłem, czyli jeśli ktoś stara się uzyskać dostęp do CPU za pomocą podłą-

Tabela 1. Poziomy dostępu do CPU

Poziomy dostępu	Ograniczenia dostępu
Dostęp całkowity (bez ochrony)	Konfiguracja sprzętu oraz bloki mogą być odczytywane i zmieniane przez wszystkich użytkowników.
Dostęp do odczytu	Na tym poziomie dostępu, bez wprowadzania hasła jest możliwy tylko dostęp do odczytu konfiguracji sprzętowej i bloków, co oznacza, że można załadować konfigurację sprzętową i bloki kodu do urządzenia programującego. Dostęp do HMI oraz do danych diagnostycznych jest również możliwy. Bez wprowadzania hasła, nie można załadować bloków i konfiguracji sprzętowej do CPU. Oprócz tego, bez podania hasła nie są możliwe następujące operacje: testowanie z zapisywaniem, zmiana trybu pracy (RUN/STOP) oraz aktualizacja oprogramowania firmware (online).
Dostęp do HMI	Na tym poziomie dostępu, bez wprowadzania hasła jest możliwy tylko dostęp do HMI oraz do danych diagnostycznych. Bez wprowadzania hasła, nie można załadować bloków i konfiguracji sprzętowej do CPU, ani bloków i konfiguracji sprzętowej z CPU do urządzenia programującego. Oprócz tego, bez podania hasła nie są możliwe następujące operacje: testowanie z zapisywaniem, zmiana trybu pracy (RUN/STOP) oraz aktualizacja oprogramowania firmware (online).
Brak dostępu (pełna ochrona)	Kiedy CPU jest całkowicie chroniony, wtedy nie jest możliwy dostęp do odczytu i zapisu konfiguracji sprzętowej i bloków. Również, dostęp do HMI nie jest możliwy. Na tym poziomie dostępu, funkcja serwera komunikacji za pomocą instrukcji PUT/GET jest wyłączona (nie można tego zmienić). Autoryzacja za pomocą hasła ponownie zapewni pełny dostęp do CPU.

czonego urządzenia programującego i wprowadzi poprawne hasło, to dostęp do CPU będzie nadal zablokowany.

Blokada dostępu może być ustawiona oddzielnie dla każdego poziomu dostępu na wyświetlaczu LCD, tak że, na przykład, dostęp do odczytu jest lokalnie dozwolony, ale dostęp do zapisu nie jest lokalnie dozwolony.

Jeśli poziom dostępu za pomocą hasła jest konfigurowany w STEP 7, to dostęp można blokować na wyświetlaczu LCD.

Aby na wyświetlaczu LCD ustawić ochronę lokalnego dostępu dla CPU S7-1500, należy postępować w następujący sposób:

1. Na ekranie wybrać menu „Settings” (Ustawienia) > „Protection” (Ochrona).
2. Potwierdzić wybór za pomocą przycisku „OK”, i dla każdego poziomu dostępu skonfigurować, czy dostęp przy ustawieniu przełącznika trybu pracy w pozycji RUN jest dozwolony, czy nie:
   - Ustawienie „Allow” (Zezwalaj): Dostęp do CPU jest możliwy, pod warunkiem, że w programie STEP 7 zostanie wprowadzone odpowiednie hasło.
   - Ustawienie „Deactivated in RUN” (Deaktywowane w trybie RUN): Gdy przełącznik trybu pracy jest w pozycji RUN, nikt z użytkowników z uprawnieniami tego poziomu dostępu nie może się zalogować do CPU, nawet jeśli zna hasło. W trybie pracy STOP, dostęp jest możliwy po wprowadzeniu hasła.

Ochrona „know-how” pozwala chronić przed nieautoryzowanym dostępem do jednego lub kilku bloków OB, FB, lub FC oraz globalnych bloków danych w programie. W celu ograniczenia dostępu do bloku kodu, można wprowadzić hasło. Ochrona hasłem zabezpiecza przed nieautoryzowanym odczytem lub modyfikowaniem bloku kodu.

Bez wprowadzenia hasła można odczytać tylko następujące dane dotyczące bloku kodu:

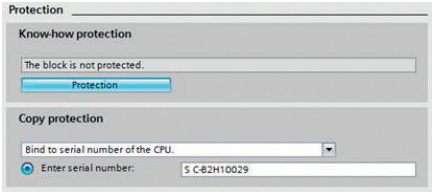
- nazwę bloku, komentarze i właściwości bloku,
- parametry bloku (INPUT, OUTPUT, IN, OUT, RETURN),
- strukturę wywołującą program,
- globalne zmienne bez informacji gdzie są używane.

Inne operacje, które mogą być przeprowadzone na chronionym bloku:

- kopiowanie i usuwanie,
- wywoływanie w programie,
- porównywanie online/offline,
- ładowanie.

Ustawienie ochrony „know-how” bloku kodu:

1. Należy otworzyć właściwości danego bloku kodu.
2. Wybieramy opcję „Protection” (Ochrona) pod pozycją „General” (Ogólne).



3. Klikamy przycisk „Protection” (Ochrona), aby wyświetlić okno dialogowe „Know-how protection” (Ochrona „know-how”).

4. Klikamy przycisk „Define” (Definiuj), aby otworzyć okno dialogowe „Define password” (Definiuj hasło).

5. W polu „New password” (Nowe hasło) wprowadzamy nowe hasło. To samo hasło wprowadzić w polu „Confirm password” (Potwierdź hasło).
6. Klikamy przycisk „OK”, aby potwierdzić wprowadzenie hasła.
7. Zamykamy okno dialogowe „Know-how protection” (Ochrona „know-how”) klikając przycisk „OK”. W rezultacie wybrane bloki kodu będą objęte ochroną „know-how”. Bloki kodu objęte ochroną „know-how” są oznaczone w drzewie projektu za pomocą symbolu kłódki. Wprowadzone hasło odnosi się do wszystkich wybranych bloków kodu.

Otwieranie bloków objętych ochroną „know-how”:

1. Dwukrotnie klikamy blok kodu, aby otworzyć okno dialogowe „Access protection” (Ochrona dostępu).
2. Wprowadzamy hasło dla bloku kodu objętego ochroną „know-how”.
3. Klikamy przycisk „OK”, aby potwierdzić wpis. W rezultacie blok kodu objęty ochroną „know-how” zostanie otwarty.

Po otwarciu bloku można edytować kod programu oraz blokowy interfejs bloku dopóty, dopóki blok lub TIA Portal nie zostaną zamknięte. Hasło należy wprowadzić ponownie przed następnym otwarciem bloku. Jeśli okno dialogowe „Access protection” (Ochrona dostępu) zostanie zamknięte po kliknięciu przycisku „Cancel” (Anuluj), to blok zostanie otwarty, ale kod bloku nie zostanie wyświetlany i nie będzie można edytować bloku. Ochrona „know-how” bloku nie zostanie usunięta, jeśli, na przykład, blok zostanie skopiowany lub dodany do biblioteki. Kopie będą również objęte ochroną „know-how”.

Usuwanie ochrony „know-how” bloku:

1. Wybieramy blok, dla którego ma być usunięta ochrona „know-how”. Chroniony blok nie może być otwarty w edytorze programu.
2. W menu „Edit” (Edycja), wybieramy polecenie „Know-how protection” (Ochrona „know-how”), aby otworzyć okno dialogowe „Know-how protection” (Ochrona „know-how”).
3. Odznaczamy pole wyboru „Hide code (Know-how protection)” (Ukryj kod (ochrony „know-how”).

4. Wprowadzamy hasło.

5. Kliknamy przycisk „OK”, aby potwierdzić. W rezultacie dla wybranego bloku została usunięta ochrona „know-how”.

Zabezpieczenie przed kopiowaniem umożliwia powiązanie programu lub bloków kodu z określoną kartą pamięci SIMATIC lub CPU. Przez powiązanie z numerem seryjnym karty pamięci SIMATIC lub CPU użycie danego programu lub bloku jest możliwe tylko w połączeniu z określoną kartą pamięci SIMATIC lub CPU. Dzięki tej funkcji program lub blok kodu można przesyłać drogą elektroniczną (np. przez e-mail) lub za pomocą modułu pamięci.

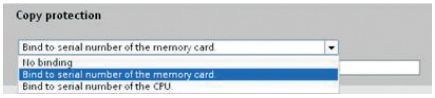
Ustawiając zabezpieczenie przed kopiowaniem dla danego bloku kodu, można również ten blok objąć ochroną „know-how”. Bez ochrony „know-how”, każdy może zresetować zabezpieczenie przed kopiowaniem. Jednak najpierw trzeba ustawić zabezpieczenie przed kopiowaniem, ponieważ ustawienia zabezpieczenia przed kopiowaniem są tylko do odczytu, jeśli blok jest już objęty ochroną „know-how”.

Konfiguracja poziomu dostępu nie zastępuje ochrony „know-how"
Konfiguracja poziomów dostępu zapobiega nieautoryzowanym zmianom w CPU, przez ograniczenie uprawnień do ładowania (wczytywania). Jakkolwiek, bloki kodu na kartach pamięci SIMATIC nie są zabezpieczone przez odczytem lub zapisem. Aby chronić kod bloków na kartach pamięci SIMATIC, należy stosować ochronę „know-how".

Konfigurowanie zabezpieczenia przed kopiowaniem:

1. Otwieramy właściwości danego bloku.
2. Wybieramy opcję „Protection" (Ochrona) pod pozycją „General" (Ogólne).

3. Z listy rozwijanej pola „Copy protection" (Zabezpieczenie przed kopiowaniem) należy wybrać opcję „Bind to serial number of the CPU" (Powiąż z numerem seryjnym CPU), lub „Bind to serial number of the memory card" (Powiąż z numerem seryjnym karty pamięci).



4. Wprowadzamy numer seryjny CPU lub karty pamięci SIMATIC.

5. Teraz można skonfigurować ochronę „know-how" bloku w obszarze „Know-how protection" (Ochrona „know-how").

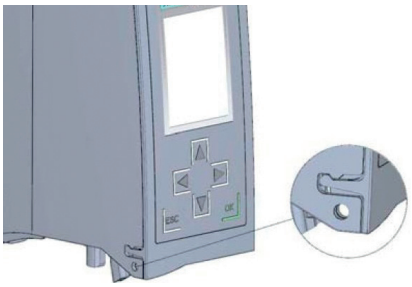
Jeśli blok zabezpieczony przed kopiowaniem będzie ładowany do urządzenia, którego numer seryjny jest nieodpowiedni, to cała operacja ładowania zostanie odrzucona. Oznacza to, że bloki bez zabezpieczenia przed kopiowaniem również nie będą ładowane.

Usuwanie zabezpieczenia przed kopiowaniem:

1. Usuwamy istniejącą ochronę „know-how".
2. Otwieramy właściwości danego bloku.
3. Wybieramy „Protection" (Ochrona) pod pozycją „General" (Ogólne).
4. Z listy rozwijanej pola „Copy protection" (Zabezpieczenie przed kopiowaniem) należy wybrać opcję „No binding" (Bez powiązania).

CPU należy chronić przed nieautoryzowanym dostępem za pomocą przedniej pokrywy odpowiednio zabezpieczonej. Zatrzask na pokrywie modułu CPU pozwala na zastosowanie następujących możliwości:

- założenie plomby,
- zabezpieczenie przedniej pokrywy za pomocą kłódki (średnica pałąka: 3 mm).



Poziomy dostępu do CPU przedstawiono w **tabeli 1**.

Każdy poziom dostępu umożliwia nieograniczony dostęp do niektórych funkcji, bez wprowadzania hasła, np. identyfikacji przy użyciu funkcji „Accessible devices" (Dostępne urządzenia). Domyślnymi ustawieniami CPU jest „No restriction" (Bez ograniczeń) oraz „No password protection" (Brak zabezpieczenia hasłem). W celu ochrony dostępu do procesora, należy edytować właściwości CPU i skonfigurować hasło. Komunikacja pomiędzy jednostkami CPU (za pomocą instrukcji komunikacyjnych w blokach kodu) nie jest ograniczona przez poziom ochrony CPU, chyba że komunikacja za pomocą instrukcji PUT/GET jest wyłączona. Wprowadzenie poprawnego hasła umożliwia dostęp do wszystkich funkcji, które są dozwolone na odpowiednim poziomie dostępu.

Procedura konfiguracji poziomów dostępu:

Aby skonfigurować poziomy dostępu do CPU S7-1500, należy wykonać następujące kroki:

1. W oknie Inspektor otworzyć właściwości CPU S7-1500.
2. W obszarze nawigacji wybrać pozycję „Protection" (Ochrona). W oknie Inspektor pojawi się tabela z możliwymi poziomami dostępu.

3. W pierwszej kolumnie tabeli uaktywnić pożądany poziom ochrony. Zielone znaki wyboru w kolumnach po prawej stronie odpowiedniego poziomu dostępu pokazują, które operacje są nadal dostępne bez wprowadzania hasła.
4. W kolumnie „Password" (Hasło) wprowadzić hasło dla wybranego poziomu dostępu. W kolumnie „Confirmation" (Potwierdzenie) ponownie wprowadzić hasło, aby zapobiec niepoprawnym wprowadzeniom.

Upewnić się, że hasło jest wystarczająco bezpieczne, to znaczy, że nie jest utworzone na wzór, który może być rozpoznany przez maszynę!

Hasło należy wprowadzić w pierwszym wierszu (dla poziomu dostępu „Full access" (Pełny dostęp)). To umożliwia uzyskać nieograniczony dostęp do CPU tym użytkownikom, którzy znają hasło, niezależnie od wybranego poziomu ochrony.

1. Zgodnie z wymaganiami przypisać dodatkowe hasła do innych poziomów dostępu, o ile dla wybranego poziomu można to zrobić.
2. Załadować konfigurację sprzętu do CPU, dzięki czemu poziom dostępu będzie obowiązywać.

Funkcjonowanie CPU chronionego hasłem

Ochrona CPU obowiązuje po załadowaniu ustawień konfiguracyjnych do CPU. Przed wykonaniem funkcji online, są sprawdzane wymagane uprawnienia i jeśli to konieczne, użytkownik zostanie poproszony o wprowadzenie hasła. W tym samym czasie funkcje chronione hasłem mogą być wykonywane tylko przez jedno urządzenie programujące lub jeden komputer PC. Inne urządzenia programujące lub komputery PC nie mogą się zalogować. Autoryzacja dostępu do chronionych danych obowiązuje na czas trwania połączenia online, lub do czasu, gdy zostanie ręcznie anulowana przez wybranie polecenia „Online" > „Delete access rights" (Usuń uprawnienia dostępu). Dostęp do chronionego hasłem CPU w trybie RUN może być ograniczony lokalnie na wyświetlaczu, tak że dostęp z użyciem hasła również nie będzie możliwy.

Jeśli poziom ochrony „Complete protection" (Pełna ochrona) został ustawiony dla CPU, to urządzenie HMI może uzyskać dostęp do CPU tylko za pomocą hasła tam przechowywanego.

Ta funkcja jest dostępna tylko w urządzeniach HMI firmy SIEMENS. W rezultacie:

1. W drzewie projektu należy otworzyć edytor „Connections" (Połączenia).
2. Wybieramy zintegrowane połączenie.
3. W polu „Password" (Hasło) wprowadzamy hasło dla CPU.

Od tego momentu urządzenie HMI może komunikować się i wymieniać dane z CPU.

Tomasz Starak, EP

Artykuł powstał na bazie dokumentacji firmy Siemens.