Problemy bezpieczeństwa cybernetycznego w zakresie stosowania systemów nadzoru stanu technicznego majątku produkcyjnego

Ryszard Nowicki

Streszczenie: Systemy nadzoru stanu technicznego wykorzystują techniki cyfrowe. Z tego powodu mogą z jednej strony być celem ataków hakerskich, natomiast z drugiej mogą być także wykorzystywane jako narzędzia do ataków na powiązane z nimi, bardziej odpowiedzialne systemy. We wstępie wyspecyfikowano główne elementy systemu nadzoru, do których w dalszych częściach odnoszono się, omawiając możliwe zagrożenia hakerskie. Przedstawiono przykłady kilku naruszeń bezpieczeństwa cybernetycznego z obszaru działalności technicznej, które dotyczyły systemów w mniejszym lub większym stopniu pozostających w powiązaniu z systemami nadzoru stanu technicznego. Omówiono kierunki zagrożeń dla wybranych komponentów składowych systemu nadzoru, a także sposoby ich zabezpieczenia oraz certyfikacji, posługując się przykładami systemów najbardziej rozpowszechnionych. Przytoczono wybrane standardy, które mogą być pomocne w realizacji programu podniesienia bezpieczeństwa cybernetycznego w przedsiębiorstwie oraz opisano jego najważniejsze elementy. Zwrócono również uwagę na ważność wprowadzenia wystarczająco precyzyjnych zapisów w tzw. SiWZ-ach, aby uniknąć dostawy przypadkowych rozwiązań systemów wspomagających nadzór stanu technicznego – także ze względu na bezpieczeństwo cybernetyczne.

1. Wprowadzenie

Aby ustosunkowywać się do zagrożeń dla bezpieczeństwa cybernetycznego systemów nadzoru stanu technicznego majątku produkcyjnego, trzeba być świadomym komponentów stosowanego na tę okoliczność systemu. Współcześnie system taki posiada elementy, jak pokazane na rys. 1 [1] gdzie występujący w opisie skrót „A/D" oznacza akwizycję danych przez system diagnostyki. Opis komponentów nie uwzględnia *explicite* wykorzystywanych coraz częściej systemów detekcji anomalii (czy to stanu technicznego, czy też dodatkowo także dla realizowanego procesu produkcyjnego), które również mogą przyczyniać się do zaistnienia takich zagrożeń. Można przyjąć, że w przypadku sprzętowych systemów detekcji anomalii zagrożenia bezpieczeństwa cybernetycznego są podobne jak w przypadku dwóch, a czasem trzech najniższych elementów pokazanej struktury, natomiast w przypadku programowych systemów detekcji anomalii możliwe zagrożenia mogą wystąpić dla poziomu trzeciego i czwartego (licząc od dołu).

Praktycznie na każdym z wyszczególnionych poziomów systemu nadzoru może dojść do naruszenia bezpieczeństwa cybernetycznego [2]. Następuje to wtedy, kiedy stosowane środki techniczne oraz oprogramowanie nie cechują się wystarczająco poprawną konstrukcją lub również wtedy, kiedy ich interfejsowanie z różnymi innymi systemami wykorzystywanymi przez przedsiębiorstwo (w tym: ICS, SCADA, PCS, DCS) nie jest przeprowadzone z zachowaniem wymaganych procedur.

W artykule po kolei omówione zostaną przykłady naruszenia bezpieczeństwa cybernetycznego systemów

CYBER-SECURITY PROBLEMS WITH APPLICATION OF CONDITION MANAGEMENT SYSTEMS OF PRODUCTION ASSETS

Abstract: *Technical condition management systems (=CMaS) use digital techniques. For this reason, they can be the target of hacker attacks but also be used as the interface to launch an attack on other systems connected to the same network.*

This paper introduces the main components of the CMaS, and discusses the possible risks and threats of hacking.

It presents examples of a number of breaches of cyber security in the area of technical activity for systems that can be interfaced with CMaS.

The paper also discusses threats to chosen components of the CMaS, as well as ways that they can be protected by use of certified cyber-security techniques – using as examples the most popular systems available in the market.

A selection of standards is reviewed that can be helpful in the implementation of a program of cyber security improvements, and the most important elements of such program are described.

The paper also highlights the importance of introducing some sufficiently precise provisions in tender documents to prevent accidentally delivered CMaS components, and systems which do not assure enough high cyber-security.

Rys. 1. Komponenty współczesnego systemu wspomagania zarządzania majątkiem

technicznych – w tym także systemów wspomagania nadzoru stanu technicznego majątku produkcyjnego; w odniesieniu do wybranych elementów struktury systemu nadzoru stanu technicznego pokazanych na rys. 1 przeprowadzona zostanie dyskusja możliwych dróg naruszania tego bezpieczeństwa oraz stosowanych na tę okoliczność rozwiązań i środków prewencyjnych; omówione zostaną wybrane standardy dotyczące poruszanej tematyki, które winny być stosowane tak przy wdrażaniu nowych systemów nadzoru stanu technicznego, jak i w procesie unowocześniania systemów wdrożonych w przeszłości. W obu przypadkach jednym z podstawowych warunków zapewniających poprawność techniczną zrealizowania inwestycji jest poprawna redakcja SIWZ-ów. W przypadku bardziej odpowiedzialnych rozwiązań systemowych systemy nadzoru stanu winny posiadać certyfikację na okoliczność zapewnianego przez nie poziomu bezpieczeństwa cybernetycznego. Omówione zostaną przykładowe systemy wykorzystywane dla nadzoru stanu technicznego, które posiadają lub też nie taką właśnie certyfikację.

2. Przykłady zakłócenia poprawności działania systemów technicznych

Incydenty naruszające bezpieczeństwo cybernetyczne dzielą się po połowie na przypadkowe oraz intencjonalne [3]. Naruszenie bezpieczeństwa cybernetycznego może być inspirowane tak przez organizacje, jak i przez pojedyncze osoby oraz może być ukierunkowane równie dobrze na organizacje rządowe, systemy bankowe, jak i na szeroko rozumiane cele przemysłowe. Ocenia się, że w przypadku ataków intencjonalnych 60% jest przeprowadzanych z pomocą malware, 22% przez ataki z zewnątrz (ukierunkowane na przedsiębiorstwa, organizacje, kraje etc.), a pozostałe 18% to ataki od wewnątrz przedsiębiorstwa (czyli sabotaż).

Wg danych z roku 2012 [4] ponad jedna trzecia ataków cybernetycznych jest ukierunkowana na systemy techniczne (24% ogólnej liczby ataków przypada na obiekty produkcyjne oraz 10% na szeroko rozumiany obszar energetyki, włączając w to elektrownie, elektrociepłownie i dystrybutorów energii). Więcej danych statystycznych dotyczących tematyki cyberbezpieczeństwa można znaleźć w [5], natomiast poniżej przedstawiono kilka wybranych przykładów ataków na systemy techniczne, które w mniejszym lub większym stopniu są powiązane z systemami nadzoru stanu technicznego albo z systemami komputerowymi, które z systemami nadzoru mogą być interfejsowane.

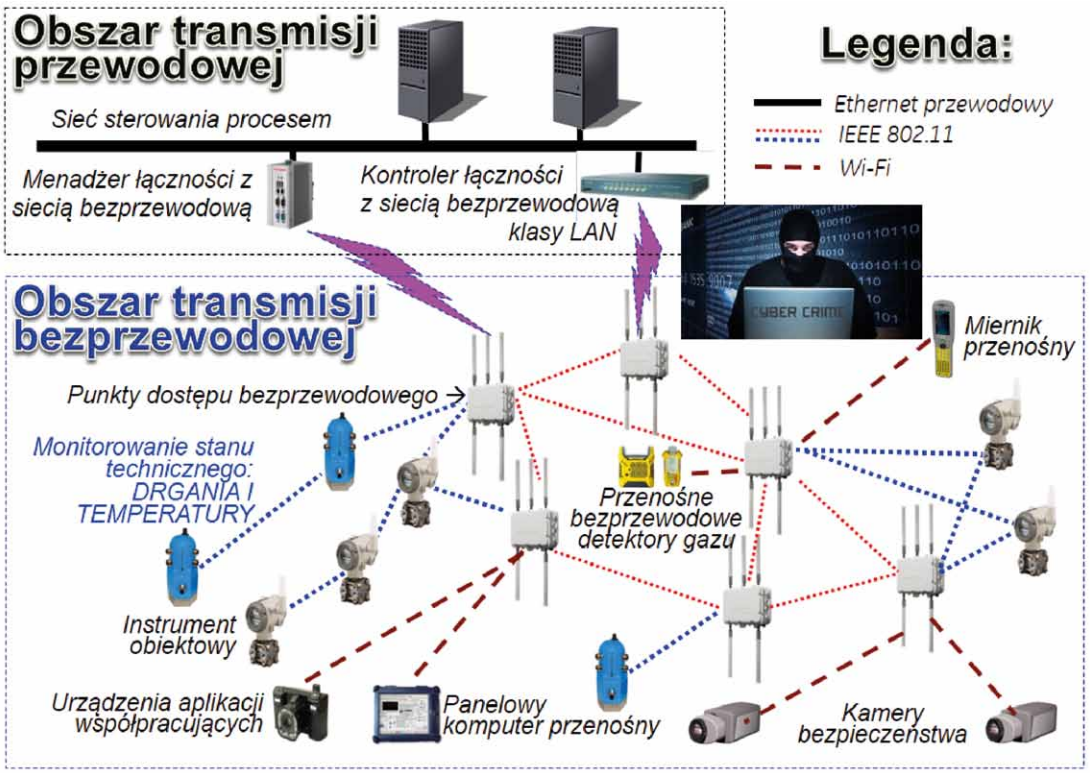
Przykład 1: W roku 2008 NASA potwierdziła, że zostały zawirusowane systemy komputerowe międzynarodowej stacji kosmicznej ISS. W ramach wydanego komunikatu ujawniono, że znaleziono wirusy Gammima.AG i Trojan-GameThief.Win32. Magania oraz stwierdzono, że nie był to pierwszy przypadek rozpoznania wirusa na ISS.

Zauważmy, że działalność podobna do chęci przejęcia kontroli lub zakłócenia misji stacji kosmicznej może również dotyczyć samolotu. W tym przypadku działania sabotażowe mogą być prowadzone także przez osoby znajdujące się bezpośrednio na pokładzie lecącej maszyny.

Przykład 2: W roku 2010 miała miejsce epidemia robaka STUXnet. Jest to klasyczny przykład zagrożenia dla integralności mechanicznej systemu produkcyjnego. STUXnet został napisany z przeznaczeniem do rozprzestrzeniania się na określonych sterownikach firmy SIEMENS, które były wykorzystywane w Natanz w ramach irańskiego programu nuklearnego do sterowania działaniem wirówek wykorzystywanych do wzbogacania uranu oraz dodatkowo także (!) do nadzoru stanu technicznego tych wirówek.

Każdy system wirnikowy winien pracować z obrotami wystarczająco dalekimi od jego częstotliwości rezonansowej. W przypadku wirówek w Natanz nominalna prędkość obrotowa pracy wynosiła ~1064 s^{-1}, natomiast najbliższa prędkość rezonansowa nieco powyżej obrotów ~1380 s^{-1}. Działanie robaka charakteryzowało się: (i) długotrwałym okresem uczenia się szczegółów działania systemu technicznego sterowania wirówkami; (ii) wprowadzaniem wirówek na okres krótkotrwałej pracy (około 15 minut) z obrotami wyższymi (docelowo 1410 s^{-1}, a więc nieznacznie powyżej częstotliwości drgań rezonansowych systemu wirnikowego) oraz niższymi (tu ok. 2 s^{-1}); sprowadzaniem układu wirnikowego do pracy z bardzo niskimi obrotami, a następnie powrót do obrotów nominalnych powodował konieczność przejścia przez częstotliwości rezonansowe układu wirnikowego położone poniżej prędkości nominalnej, czyli doprowadzono go do okresowej pracy z prędkością, przy której dochodziło do znacznego kiwania się wirnika; tak sterowane zmiany prędkości obrotowej (w górę i w dół) przyczyniały się przyspieszonej kumulacji naprężeń w różnych podzespołach wirówki, powodując znaczące skrócenie ich żywotności; (iii) w czasie, w którym wirówki pracowały z obrotami różnymi od nominalych, robak STUXnet przekazywał ze sterowników SIEMENSA do wyświetlaczy operatorskich zafałszowane dane o rzeczywistej prędkości obrotowej wirników wirówek: operatorzy widzieli na swoich monitorach dane o obrotach takich, jakie „powinny być", a nie takich, „jakie były faktycznie" (iv) w czasie sterowania obrotami wirówek, mającego na celu zwiększenie zagrożenia dla ich integralności mechanicznej w konsekwencji przyspieszonej kumulacji naprężeń, robak dodatkowo aktywował blokowanie możliwości ich awaryjnego odstawienia przez operatorów.

Wg różnych źródeł zniszczeniu uległo od 1000 do 5000 wirówek, a proces wzbogacania został opóźniony o kilka lat.



Rys. 2. Bezprzewodowy system transmisji danych pomiarowych dedykowanych procesowi i nadzorowi stanu technicznego

Specjaliści ocenili, że koszt wyprodukowania robaka STUXnet wynosił co najmniej ~10 milionów USD. Jego podstawowym obszarem działania był faktycznie Iran, natomiast (takie jest prawo niekontrolowanej epidemii) pojawił się on w szeregu innych krajów – o czym poniżej.

Przykład 3 z elektrowni jądrowych: Początek irańskiego programu nuklearnego cechowały cele pokojowe (rok 1957 – US ATOM). Program nabrał przyspieszenia w roku 1974, kiedy to zaplanowano wybudowanie 4 elektrowni jądrowych o łącznej mocy ~23 GWe i na tę okoliczność została podpisana umowa wstępna z Siemens KWU oraz Framatome. Jednym z celów było wybudowanie elektrowni w Bushehr. Budowa została zapoczątkowana w roku 1975 z pomocą firm niemieckich, natomiast ich zaangażowanie zostało zastopowane z początkiem rewolucji islamskiej (1979). Do postawionego zadania powrócono w początku lat 90. XX w., podpisując kontrakt z Rosją, mający na celu dokończenie i uruchomienie elektrowni. Po pokonaniu wielu problemów pierwszy blok został uruchomiony w początku bieżącej dekady i pracuje pod wspólnym nadzorem specjalistów miejscowych oraz rosyjskich.

Robak STUXnet dedykowany Iranowi i jego programowi nuklearnemu uwidocznił się w elektrowniach jądrowych innych krajów. W roku 2003 został zidentyfikowany w NPP OHIO. Dziesięć lat później ekspert wirusowy E. Kaspersky poinformował, że oprogramowanie antywirusowe produkowane przez jego firmę miało rozpoznać robaka STUXnet także w jednej z rosyjskich elektrowni jądrowych.

Przykład 4: Na początku ubiegłego roku w raporcie BSI[1] za rok poprzedzający poinformowano, że jedna z hut niemieckich przeżyła atak wirusowy, w wyniku którego została m.in. uszkodzona spora część majątku produkcyjnego – w tej liczbie m.in. został poważnie uszkodzony wielki piec. Agresor, aby przeprowadzić taki atak, musiał doskonale znać struktury powiązań między wewnętrznymi sieciami zakładu oraz sposób ich zabezpieczenia.

Przykład 5: 5 sierpnia 2008 roku nastąpiło poważne uszkodzenie rurociągu Baku/Azerbejdżan – Tbilisi/Gruzja – Ceyhan/Turcja. Bezpośrednią przyczyną było przeciążenie ciśnieniowe rurociągu. Doszło do niego w wyniku przejęcia kontroli nad sterowanymi bezprzewodowo zaworami stacji przesyłowej gazu w pobliżu miejscowości Erzincan (wschodnia Turcja) przez dwie osoby znajdujące się poza terytorium stacji, w którym to celu zostały wykorzystane narzędzia komputerowe. Na zdarzenie to można spojrzeć przez pryzmat koincydencji w czasie z początkiem wojny w Osetii Południowej (zaczęła się w kilkadziesiąt godzin po eksplozji rurociągu).

Przykład 6: 23 grudnia 2015 roku zostały zainfekowane (wirusy: BlackEnergy oraz KillDisk) komputery trzech regionalnych dystrybutorów energii elektrycznej OBLENERGOS we wschodniej Ukrainie. Wg różnych źródeł energii elektrycznej zostało pozbawionych między 225 tysiącami a 1 milionem odbiorców.

W kilka miesięcy później grupa specjalistów z Wydziału Utrzymania Ruchu jednej z polskich elektrowni, straciła

w krótkiej przestrzeni czasu zasoby zgromadzone na dyskach komputerów osobistych oraz możliwość posługiwania się tymi komputerami.

Przykład 7: Szacuje się, że w Stanach pracuje ~57 000 przemysłowych systemów sterowania, które są podłączone do Internetu. „The Wall Street Journal" informował o 295 atakach hakerskich na te systemy w roku 2015 (w latach 2013 i 2014 liczba tych ataków kształtowała się na poziomie ~250). 24 marca 2016 r. Departament Sprawiedliwości USA opublikował informację o 7-osobowej irańskiej grupie przestępczej, która w latach 2011–2013 dopuściła się cyberataków na 46 dużych instytucji – głównie zlokalizowanych w USA i przede wszystkim finansowych [6]. Natomiast jeden z członków tej grupy oskarżony jest również o nieuprawnioną ingerencję w system SCADA tamy Bowman Dam w pobliżu Nowego Jorku, co miało miejsce o okresie VIII–IX 2013 roku.

Rys. 3. Przenośny zbieracz i analizator sygnałów nowej generacji oraz przykłady wybranych ekranów

3. Drogi naruszania bezpieczeństwa cybernetycznego i stosowane środki prewencyjne

Droga nr 1: W niektórych przedsiębiorstwach stosuje się coraz częściej bezprzewodowe przetworniki do nadzoru procesu oraz bezprzewodowe przetworniki i/lub bezprzewodowe czujniki do kontroli stanu technicznego majątku produkcyjnego. Przykłady wybranych zadań realizowanych z pomocą sieci bezprzewodowej wraz z jej podłączeniem do sieci przewodowej pokazano na rys. 2. Na rysunku także pokazano graficznie możliwość potencjalnego zagrożenia bezpieczeństwa cybernetycznego dla obu sieci, tzn. przewodowej oraz bezprzewodowej.

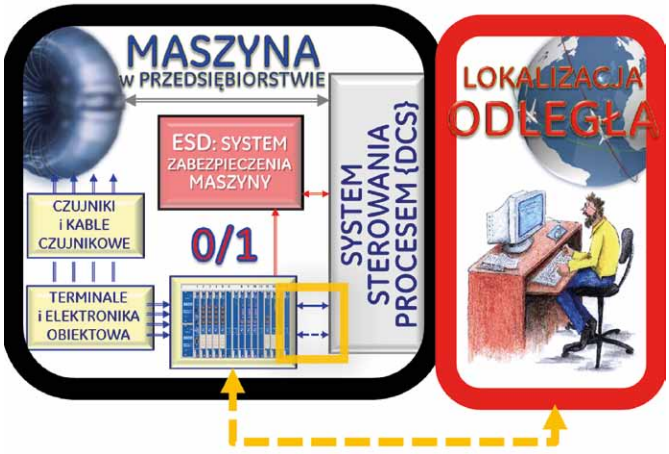
Podobnie jak w przypadku transmisji przewodowej, która może wykorzystywać zróżnicowane protokoły transmisji, również w przypadku transmisji bezprzewodowej możliwe jest wykorzystywanie zróżnicowanych protokołów. Poczynając od WTP i WAP, kończąc na ISA 100.11a oraz Wireless HART. Stosowane protokoły transmisji bezprzewodowej winny zapewniać nie tylko integralność transmitowanych danych, ale także cyberbezpieczeństwo transmisji.

Protokół ISA 100.11a jest pierwszym protokołem transmisji bezprzewodowej, który został stworzony z myślą o zapewnieniu cyberbezpieczeństwa na odpowiednio wysokim poziomie. Inne, stosowane wcześniej protokoły, nie posiadały pierwotnie takiej właściwości. I tak Wireless HART dopiero od wersji 4 uzyskał certyfikat Achillesa [7] dla strefy 1, który jednak wciąż wymaga stosowania punktu dostępu określonego typu dla zapewnienia deklarowanego poziomu bezpieczeństwa.

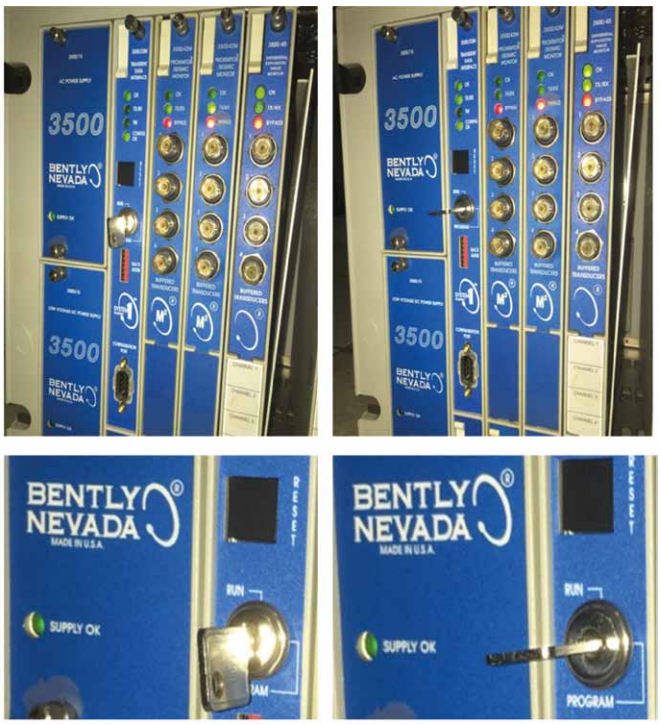
Droga nr 2: W legendzie rys. 2 opisano dwa standardy, które mogą być wykorzystywane w budowie połączeń bezprzewodowych. Takich standardów jest oczywiście wielokrotnie więcej. Przykładowo w najnowszych rozwiązaniach sprzętowych dedykowanych nadzorowi stanu technicznego wykorzystywane są przenośne zbieracze i analizatory sygnałów dynamicznych: drgania mechaniczne, pulsacje ciśnienia płynów oraz drgania elektryczne, dla których dostępne są prezentacje sygnałów czasowych, analiz widmowych, analizy orbity, pomiary w zdefiniowanych pasmach częstotliwościowych sygnału, analizy wektorowe wspomagające proces wyważania maszyn wirnikowych i inne. Te przyrządy nowej generacji nie posiadają własnych wyświetlaczy. Do komunikowania się człowieka z przyrządem są wykorzystywane bądź to tablety, bądź też telefony komórkowe, dla których zostały napisane dedykowane aplikacje. Komunikacja między środkami technicznymi jest realizowana z pomocą technologii bezprzewodowej komunikacji krótkiego zasięgu Bluetooth. Przykład takiego zestawu (SCOUT 220) oraz przykłady wybranych analiz wykonywanych z jego pomocą pokazano na rys. 3.

Oprócz wspomnianego już Bluetootha SCOUT 220 wykorzystuje również inne formy transmisji bezprzewodowej. Do połączenia z serwerem akwizycji danych może być wykorzystywana sieć telefonii komórkowej lub lokalna sieć Wi-Fi – jeśli jest dostępna. Fakt dostępności online serwera danych stwarza dodatkowe możliwości. Można wyeliminować niezależny krok w procedurze gromadzenia danych, który miał miejsce w przypadku przenośnych zbieraczy starszej generacji i polegał na przewodowej transmisji danych pomiarowych ze zbieracza do komputera. Bowiem, w przypadku posiadania dostępu do serwera, transmisja danych może być realizowana już w czasie wykonywania pomiarów i rejestracji sygnałów. Zauważmy, że dostęp online do serwera stwarza także dodatkową możliwość, jaką jest ściąganie danych historycznych zgromadzonych na komputerze i ich porównywanie z danymi bieżącymi, pozyskiwanymi w czasie wykonywania pomiarów.

Transmisja Wi-Fi to jednak z drugiej strony także zagrożenie. W związku z tym, że serwer akwizycji danych wykorzystuje dla opisanego systemu przenośnego to samo oprogramowanie, które pracuje w reżimie online dla akwizycji danych gromadzonych dla maszyn krytycznych (w tym przypadku jest to SYSTEM 1) oraz może być dodatkowo także włączony do sieci zakładowej, a ponadto mogą się z nim komunikować komputery odległe, niezbędne jest zapewnienie bezpieczeństwa pracy takiego systemu ze względu na dane przesyłane drogą bezprzewodową. W tym celu między wykorzystywanym w celach gromadzenia danych oprogramowaniem SYSTEM 1 a zestawem przenośnym uruchamiana jest jeszcze jedna dodatkowa aplikacja, której zadaniem jest zapewnienie bezpieczeństwa pracy serwera akwizycji danych przy komunikowaniu się z zestawem przenośnym.



Rys. 4. Połączenie odległe do systemu monitorowania i zabezpieczeń maszyny



Rys. 5. Przykład fizycznego zabezpieczenia możliwości konfiguracji i rekonfiguracji kasety: z lewej programowanie dozwolone; z prawej możliwość programowania zablokowana

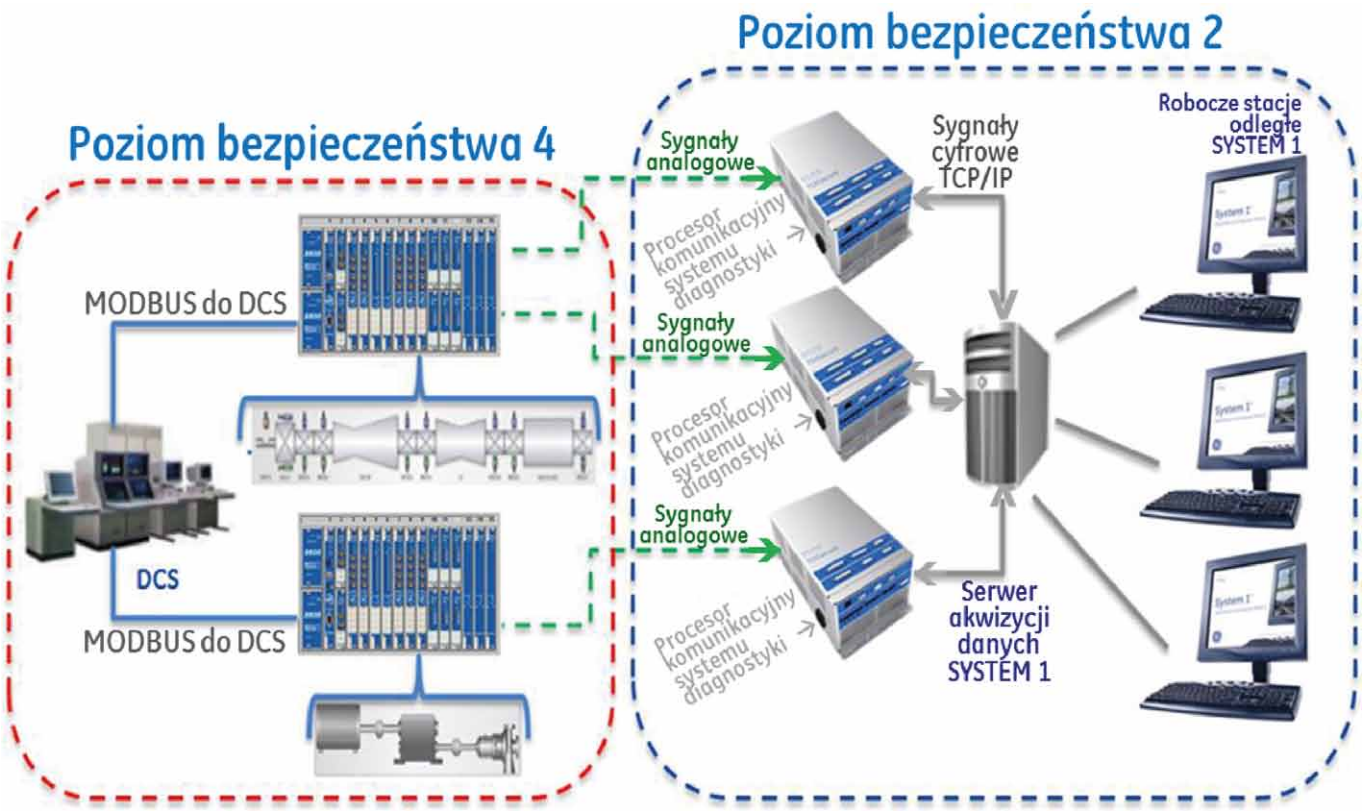
Droga nr 3: Systemy monitorowania stanu technicznego zaczęto stosować w drugiej połowie XX wieku. Początkowo były to systemy analogowe. W roku 1998 Bently Nevada wprowadziła do sprzedaży pierwszy na świecie cyfrowy system nadzoru (SYSTEM 3300, który do dziś jest jeszcze wykorzystywany do zabezpieczenia wielu maszyn – także w Polsce). Współcześnie w celu monitorowania i zabezpieczenia stanu technicznego stosuje się systemy o zróżnicowanym stopniu zaawansowania oraz o różnej liczbie kanałów służących do podłączenia sygnałów z czujników. Liczba kanałów zawiera się w przedziale od 1 do kilkudziesięciu. Obserwuje się następującą korelację: wraz ze wzrostem liczby kanałów ma miejsce większe zaawansowanie funkcjonalne systemu monitorowania. Przykładowe, bardziej zaawansowane funkcjonalności to: (a) możliwość cyfrowego interfejsowania systemu monitorowania z DCS, (b) możliwość dostępu na odległość do systemu monitorowania oraz (c) możliwość podłączenia do systemu diagnostyki. Druga z wymienionych funkcjonalności może być realizowana w celu przeprowadzenia działań niestandardowych, jak np.: (i) dostęp serwisowy w celu rozpoznania kodu błędu sygnalizowanego podczas pracy systemu; (ii) dostęp w celu rekonfiguracji nastaw alarmowych systemu monitorowania i zabezpieczeń; (iii) dostęp celem importu danych pomiarowych zgromadzonych przez procesor komunikacyjny systemu diagnostyki, stanowiący jeden z modułów systemu monitorowania, w przypadku takim, w którym ten procesor nie jest podłączony do systemu diagnostyki online.

Przeanalizujmy kwestię potencjalnego zagrożenia w przypadku realizowania takiego połączenia na przykładzie najbardziej rozpowszechnionego w Polsce oraz na świecie systemu monitorowania i zabezpieczeń maszyn, jakim jest SYSTEM 3500, z którego to pomocą monitorowanych jest ponad 75 000 maszyn.

Wprost na maszynie i w jej bezpośredniej bliskości zainstalowane są czujniki, kable czujnikowe oraz elektronika obiektowa – *vide* rys. 4. Sygnały z czujników są podłączone do wejść sygnałowych systemu monitorowania i zabezpieczeń. Po przekroczeniu progów zabezpieczeniowych (tak w systemie zabezpieczeń procesowych w DCS, jak i w systemie monitorowania stanu technicznego maszyny) wyjścia przekaźnikowe generują sygnały binarne do systemu awaryjnego odstawienia maszyny (tu: ESD), co symbolizują na rysunku strzałki czerwone. Ponadto system monitorowania i zabezpieczeń jest interfejsowany cyfrowo z DCS co pokazano na rysunku strzałkami niebieskimi.

Podłączenie się do kasety systemu monitorowania i zabezpieczeń jest także możliwe z lokalizacji odległej. Takie połączenie odległe może mieć intencje szeroko rozumianej optymalizacji działania systemu (jak opisane powyżej) lub działania sabotażowe. Natomiast nie dla każdego systemu przeprowadzenie takiego sabotażu jest możliwe. Dla wykorzystywanego w tym przykładzie SYSTEMU 3500 byłyby one jedynie możliwe w przypadku współpracy z kimś wewnątrz przedsiębiorstwa.

Aby przeprowadzić rekonfigurację SYSTEMU 3500, niezbędne jest wykorzystanie fizycznego klucza, który musi zostać wprowadzony do zamka kasety i ustawiony w pożądanej pozycji – co zostało pokazane na rys. 5. W górnej części rysunku pokazano przedni fragment kasety SYSTEM 3500, która wykorzystuje taką właśnie formę zabezpieczenia, natomiast moduł pokazany jako następny za zasilaczami jest odpowiedzialny m.in. za konfigurowanie kasety oraz zawiera fizyczny zamek umożliwiający wprowadzenie fizycznego klucza i w konsekwencji prowadzenia takiego działania – co pokazano w powiększeniu w dolnej części rysunku. Tak długo, jak klucz w zamku znajduje się w pozycji „RUN" (tak jak to pokazano z lewej strony na rysunku), tak długo przeprogramowanie kasety nie jest możliwe. Dopiero zmiana położenia klucza do pozycji „PROGRAM" (co pokazano z prawej strony rysunku) daje możliwość przeprogramowania kasety czy to z pomocą komputera podłączonego



Rys. 6. Przykład realizacji struktury systemu nadzoru stanu technicznego wybranych maszyn dla bloku elektrowni jądrowej

bezpośrednio do kasety czy też z lokalizacji odległej, jak to pokazano na rys. 4. Usunięcie klucza z zamka uniemożliwia tak programowanie, jak i reprogramowanie kasety.

Dodatkowo wszystkie zmiany skonfigurowania kasety SYSTEM 3500 są odnotowywane na jej wewnętrznej liście zdarzeń, co stwarza możliwość spostrzeżenia przeprowadzonych a nieuprawnionych działań przez specjalistów odpowiedzialnych za prawidłowe działanie przedmiotowego systemu zabezpieczeń.

Droga nr 4: Trzecim od dołu elementem systemu nadzoru stanu technicznego pokazanym na rys. 1 jest system diagnostyki. System ten zajmuje się gromadzeniem danych oraz ich przetwarzaniem. Na system diagnostyki składają się na ogół następujące elementy: (i) serwer akwizycji danych; (ii) oprogramowanie diagnostyczne; (iii) procesor komunikacyjny umożliwiający przejęcie sygnałów z systemu monitorowania i zabezpieczeń celem ich transmisji do serwera akwizycji danych oraz (iv) sieć systemu diagnostyki umożliwiająca transmisję danych gromadzonych z różnych systemach monitorowania i zabezpieczeń do serwera. Różne systemy diagnostyki umożliwiają podłączenie do pojedynczego serwera akwizycji danych różnej liczby maszyn, a także umożliwiają zróżnicowaną akwizycję danych (tylko w stanach ustalonych bądź dodatkowo także w stanach przejściowych; niektóre nowoczesne procesory komunikacyjne realizują także specjalną akwizycję danych w stanach alarmowych etc.). O dostępnych możliwościach w tym zakresie decydują przede wszystkim właściwości procesora komunikacyjnego.

Procesory komunikacyjne zostały wprowadzone do stosowania przez BENTLY NEVADA we wczesnych latach 80. XX w. Wykorzystywane w tamtych latach do konstrukcji elementy elektroniki nie pozwalały na zaawansowaną miniaturyzację procesorów. Tak więc ówczesne procesory posiadały gabaryty porównywalne z gabarytami kasety systemu monitorowania. W ciągu kolejnych prawie 20 lat procesory zostały zminiaturyzowane na tyle, że najpierw procesor dla gromadzenia danych w stanach ustalonych, a następnie także procesor umożliwiający akwizycję w stanach przejściowych przyjęły gabaryty dające podstawy ich lokalizacji wewnątrz kaset systemów monitorowania i zabezpieczeń.

Natomiast nowe standardy, mające na uwadze bezpieczeństwo działania majątku i systemów pracujących w strefach najwyższej krytyczności (na rys. 6 jest to strefa 4) dopuszczają jedynie transmisję między kasetą systemu monitorowania a DCS-em (np. z wykorzystaniem protokołu MODBUS) oraz transmisję jednokierunkową do procesora komunikacyjnego systemu diagnostyki. Tak jak to pokazano na rysunku, wszystkie komponenty systemu diagnostyki są już zlokalizowane w strefie 2 (która jest strefą z niższymi wymaganiami w zakresie bezpieczeństwa niż strefa 4). Tutaj, na połączeniu między procesorem komunikacyjnym a serwerem systemu diagnostyki, dopuszcza się dwukierunkowe przekazywanie danych i sterowań.

Pokazana na rys. 6 struktura systemu zmusiła ponownie producentów systemów monitorowania i zabezpieczeń do

zastosowania rozwiązania, w którym procesor komunikacyjny stanowi element zewnętrzny w stosunku do kasety. Jest to procesor typu TDISecure, który umożliwia akwizycję do 24 sygnałów dynamicznych. Procesory TDISecure mogą być wykorzystywane z różnymi systemami monitorowania i zabezpieczeń. W konsekwencji, w przypadku systemów monitorowania o dużej liczbie podłączonych czujników, może zachodzić potrzeba podłączenia 2 takich procesorów do pojedynczej kasety. Na rysunku pokazano przykładowo dwie maszyny, z których jedna (ta pokazana niżej) jest bardziej kompaktowa, w związku z czym nadzorowana jest z pomocą niewielkiej liczby czujników i w konsekwencji pojedynczy TDISecure zapewnia kompletną transmisję sygnałów do systemu diagnostyki. W przypadku drugiej z pokazanych maszyn, mimo faktu, że wykorzystywany jest system monitorowania tego samego typu, to jednak fakt, że liczba czujników przekracza 24, powoduje, że dla zapewnienia ich transmisji do systemu diagnostyki muszą być wykorzystywane 2 sztuki procesorów TDISecure.

Należy dodać, że nie tylko system monitorowania wymaga połączenia z DCS (tak jak to pokazano na rys. 4), ale także serwer akwizycji danych winien posiadać online'owe z nim połączenie. Są ku temu dwie przyczyny: (i) oprócz danych symptomatycznych dla zmiany stanu technicznego gromadzonych poprzez procesory komunikacyjne, w szeregu przypadków winien on również gromadzić wybrane dane procesowe i środowiskowe, które mogą być w jakimś stopniu skorelowane z gromadzonymi symptomami; (ii) oprócz ww. pomiarów niezbędna jest również okresowa synchronizacja czasu systemowego; wszystkie interfejsowane systemy posiadają swoje zegary, tak więc w przypadku generowania systemowych list zdarzeń i alarmów winny być one etykietowane z pomocą zsynchronizowanego czasu – właściwego dla instalacji, bloku energetycznego etc[2].

Droga nr 5: Serwer systemu diagnostyki może udostępniać zgromadzone dane odległym stacjom roboczym, co wymaga zainstalowania na nich oprogramowania systemowego oraz posiadania autoryzacji administratora systemu umożliwiającej realizację dostępu. Na rysunku pokazano takie odległe robocze stacje lokalizowane w tej samej strefie, w której jest zlokalizowany serwer systemu diagnostyki, natomiast mogą się one znajdować także poza tą strefą.

W przeszłości te krajowe przedsiębiorstwa, które zaczęły wdrażać systemy diagnostyki (proces ten rozpoczął się w początku lat 90. XX w.) posiadały zespół diagnostyki, w skład którego wchodzili specjaliści posiadający wystarczający poziom wiedzy, aby zgromadzone w systemie diagnostyki dane przekształcać w informacje użyteczne dla wydziału utrzymania ruchu. W przypadku koncernów zespoły diagnostyki nie są przyporządkowane do poszczególnych przedsiębiorstw wchodzących w skład grupy, a zorganizowany jest na ogół jeden wydział diagnostyki, który obsługuje wszystkie przedsiębiorstwa grupy. W związku z tym niezbędny jest dostęp odległy do serwerów akwizycji danych online, zlokalizowanych w poszczególnych przedsiębiorstwach. W przypadku Polski takie centralne zespoły diagnostyczne pracują w dwóch koncernach energetycznych.

W niektórych przypadkach wnioskowanie diagnostyczne prowadzone jest w oparciu o umowy outsourcingowe [8]. Aktualnie co najmniej jeden krajowy koncern energetyczny oraz jedno przedsiębiorstwo z branży chemicznej korzysta z takiego rozwiązania. W obu przypadkach dostęp z firmy outsourcingowej do online'owego serwera systemu diagnostyki jest prowadzony periodycznie.

W każdym z opisanych przypadków niezbędne jest zapewnienie odpowiednich procedur tak, aby ryzyko naruszenia bezpieczeństwa cybernetycznego było minimalne.

Droga nr 6: W minionej dekadzie równolegle do systemów wspomagania nadzoru stanu technicznego pojawiły się systemy detekcji anomalii. Detekcja anomalii może być wykorzystywana tak w celach rozpoznawania naruszenia integralności mechanicznej środków produkcji, jak również w celu rozpoznawania anomalii procesowych. Idea działania takich systemów wraz z przykładami zastosowania dla określonych klas maszyn została opisana w [9, 10]. W wielu przypadkach systemy te pracują na warunkach usługi outsourcingowej – tak jak to było opisane powyżej. W [10] podano, że z takiego odległego centrum detekcji anomalii A&PC nadzorowanych jest ~4500 maszyn. Aktualnie liczba ta wzrosła do ponad 5500.

Także w tym przypadku opisywana usługa wiąże się z koniecznością zapewnienia takich warunków odległego dostępu do serwerów akwizycji danych, aby nie było naruszone bezpieczeństwo cybernetyczne.

4. Standardy

Ważność tematyki bezpieczeństwa cybernetycznego spowodowała potrzebę opracowania standardów dedykowanych tej tematyce. Niektóre z nich winny być brane pod uwagę przy implementacji systemów nadzoru stanu technicznego w krajowych przedsiębiorstwach, jak np.:

- ANSI/ISA-99 – wprowadza definicję różnych stref, w tym także stref bezpieczeństwa [11] oraz definiuje sposób przekazywania danych i informacji między strefami;
- ISA/IEC-62443 – jest to grupa standardów i dokumentów dedykowanych bezpiecznej implementacji przemysłowych systemów automatyki oraz sterowania procesem; standard ten jest tworzony i promowany przez ETSI[3], a dokładniej przez wyłonioną wewnątrz tej organizacji grupę specjalistów zainteresowanych bezpieczeństwem cybernetycznym[4]; grupa ta postawiła sobie za cel wygenerowanie 14 dokumentów, z czego 5 już doczekało się publikacji lub jest jej bliskie ze względu na zaawansowany proces redakcji; w dokumencie IEC-62443-1-1 można znaleźć definicje poziomów/stref bezpieczeństwa (0; 1; 2; 2,5; 3 i 4 – gdzie 0 jest poziomem najbardziej krytycznym, bowiem dotyczy bezpośrednio miejsca lokalizacji środków produkcji, a 4 jest poziomem najniższego bezpieczeństwa, bowiem dotyczy sieciowej struktury na poziomie przedsiębiorstwa wraz z podłączonymi do niej komputerami).

W [12] zamieszczono przykład zdefiniowania różnych stref bezpieczeństwa dla dużej rafinerii wraz z opisem różnych środków technicznych (w tym także systemów nadzoru stanu technicznego) i opisem ich zlokalizowania wewnątrz właściwej dla nich strefy.

Wg ww. standardów systemy monitorowania i zabezpieczenia stanu technicznego majątku produkcyjnego (tzn. czujniki pracujące tak w reżimie przewodowym, jak i bezprzewodowym oraz systemy monitorowania i zabezpieczenia stanu technicznego, tak jak np. SYSTEM 3500; ADAPT; DSM systemu TREND-MASTER) są zlokalizowane w „STREFIE 1".

5. Poprawa bezpieczeństwa cybernetycznego w przedsiębiorstwie

Światowe straty będące konsekwencją naruszania bezpieczeństwa cybernetycznego w skali jednego roku są aktualnie szacowane na ~350 miliardów EUR, z czego ponad jedną trzecią stanowią straty ponoszone przez kraje Europy. W [4] zaprezentowano podejście, mające na celu zwiększenie bezpieczeństwa cybernetycznego przedsiębiorstwa. Przyjmuje się w nim, że:

- obszary odpowiedzialności są definiowane przez zarząd przedsiębiorstwa;
- system bezpieczeństwa przedsiębiorstwa jest budowany (lub modernizowany) dla użytkowanego majątku;
- bezpieczeństwo cybernetyczne winno stać się integralną częścią kultury działania przedsiębiorstwa.

Dla zapewnienia ciągłości bezpieczeństwa cybernetycznego zdefiniowano proces składający się z pięciu kroków, który winien powtarzać się okresowo, a mianowicie:

- Ustalenie zakresu działań i określenie priorytetów. W tym kroku należy dokonać m.in. wyboru majątku krytycznego, który winien podlegać zabezpieczeniu. Majątek krytyczny jest z reguły wyposażony w systemy nadzoru stanu technicznego na poziomie systemów monitorowania i zabezpieczeń (jeśli stosowane jest prewencyjne utrzymanie ruchu), a także dodatkowo systemów diagnostyki (jeśli stosowane jest predykcyjne lub bardziej od niego zaawansowane utrzymanie ruchu).
- Zrozumienie ekspozycji na zagrożenia. Tutaj należy dokonać oceny zagrożeń i ocenić wrażliwość dotychczas wykorzystywanego systemu na hipotetyczne zagrożenia. Systemy nadzoru stanu technicznego są interfejsowane z różnymi komponentami DCS zlokalizowanymi w przedsiębiorstwie, a także mogą uczestniczyć w chwilowej lub ciągłej łączności na okoliczność transmisji danych lub sterowań na odległość, np. w celu realizacji optymalizacji działania alarmów [14].
- Przeprowadzenie ocen ilościowych dla wyróżnionych zagrożeń. W ramach tego kroku winny zostać oszacowane ryzyka strat finansowych, które mogłyby zostać poniesione przez przedsiębiorstwo w przypadku, gdyby bezpieczeństwo cybernetyczne (także na kierunku systemów nadzoru stanu technicznego) zostało skutecznie naruszone.

- Ocena rozważanych opcji poprawy sytuacji. W tym kroku dokonuje się opracowania możliwych rozwiązań zapobiegawczych oraz przeprowadza się oszacowanie kosztów niezbędnych do poniesienia w przypadku podjęcia decyzji o implementacji. Rozwiązania te mogą charakteryzować się różnym poziomem doskonałości, w konsekwencji także nakłady związane z ich implementacją mogą się znacząco różnić. W procesie analizy niezbędne jest także przeprowadzenie oszacowania pozostałego (po implementacji) ryzyka oraz niezbędnych nakładów na usuwanie/minimalizowanie jego skutków w przypadku zaistnienia.
- Wybór ostatecznego rozwiązania i jego implementacja. W kroku tym oprócz działań prowadzonych bezpośrednio na rzecz implementacji rozwiązań sprzętowych i programowych równolegle przygotowuje się i przeprowadza kampanię informacyjno-szkoleniową dla pracowników.

Konieczność cyklicznego powtarzania powyższych pięciu kroków wynika z ciągłego rozwoju technik komputerowych, wdrażania nowych systemów wewnątrz przedsiębiorstwa, wprowadzania nowych sposobów interfejsowania między systemami pracującymi w przedsiębiorstwie, a także ze stosowania nowych dróg powiązania przedsiębiorstwa ze światem zewnętrznym. W związku z tym, że każde z wymienionych tu działań może naruszyć bezpieczeństwo cybernetyczne, niezbędne jest okresowe powtarzanie opisanego procesu.

Można się spodziewać, że w podobnym stopniu, jak stopień zaawansowania i poprawność wdrożenia systemów nadzoru stanu technicznego majątku rzutuje na koszty ponoszone przez przedsiębiorstwo na rzecz firm ubezpieczeniowych (asekuracja na okoliczność awarii majątku produkcyjnego, asekuracja na okoliczność strat produkcyjnych spowodowanych uszkodzeniem majątku etc.), także poprawność wdrożenia systemów zmniejszających ryzyko zagrożeń cybernetycznych będzie wpływać na ponoszone w przyszłości koszty asekuracji.

6. Certyfikacja Achillesa dla systemów nadzoru

Pierwszym warunkiem zapewnienia wymaganego poziomu bezpieczeństwa cybernetycznego dla systemów wykorzystywanych na rzecz nadzoru stanu technicznego majątku produkcyjnego jest stosowanie rozwiązań, które zostały zaprojektowane zgodnie z wymaganiami zapewniającymi określony poziom tego bezpieczeństwa. W tym przypadku najlepiej jest wymagać przedstawienia stosownego certyfikatu potwierdzającego spełnienie wymagań.

Certyfikatem cieszącym się powszechnym uznaniem jest tzw. certyfikat Achillesa [7]. Przyznawaniem takiego certyfikatu zajmują się wybrane organizacje, które posiadają doświadczenie zarówno w zakresie wymogów dla zapewnienia bezpieczeństwa, jak i wyrafinowanych metod jego naruszania. Taką wiodącą organizacją jest WURLDTECH.

Drugim warunkiem jest wdrażanie systemów nadzoru stanu technicznego majątku produkcyjnego w sposób zgodny z wymaganiami opisanymi w certyfikacie Achillesa. Bowiem rzecz nie w zabieganiu o stosowanie systemów certyfikowanych, ale przede wszystkim systemów, które są wdrożone w sposób nienaruszający wymagań certyfikacji. Różne systemy nadzoru stanu technicznego zapewniają wymogi bezpieczeństwa cybernetycznego w zróżnicowany sposób. I tak w przypadku pokazanym na rys. 5 sposób zabezpieczenia kasety warunkujący możliwość przeprowadzenia jej rekonfiguracji może być jednak pokonany poprzez sabotaż wewnątrzzakładowy, tzn. ktoś, kto nie posiada „klucza fizycznego", może dokonać takiej przeróbki „zamka", że przeprogramowanie kasety stanie mu się mimo wszystko dostępne. Dla SYSTEMU 3500 Certyfikat Achillesa formułuje zatem dodatkowe wymogi na okoliczność pełnego bezpieczeństwa cybernetycznego przy dokonywaniu różnych połączeń i wymiany danych między różnymi systemami.

Natomiast w przypadku rodziny systemów nadzoru stanu technicznego ADAPT [15] nie są już potrzebne ani fizyczny klucz, ani stosowanie dodatkowych modemów, bowiem posiadają one tak silną konstrukcję na okoliczność bezpieczeństwa cybernetycznego, że certyfikat Achillesa nie wymaga w stosunku do nich stosowania żadnych dodatkowych zabezpieczeń (tak jak to jest np. wymagane w przypadku wireless HART dla strefy 1).

W przeszłości obserwowane było w kraju postępowanie typowe dla przysłowiowego wylewania dziecka z kąpielą. I tak w końcu lat 90. XX w., kiedy w Polsce, w wiodących przedsiębiorstwach, pracowało już co najmniej kilkanaście dużych systemów diagnostyki stanu technicznego, wykorzystujących dla dostępu na odległość linie telefoniczne z numerami dostępowymi do modemów współpracujących z serwerami systemów diagnostyki, zaczęto masowo usuwać te modemy celem uniknięcia niekontrolowanego dostępu do sieci zakładowych wykorzystywanych zadaniowo szerzej niż tylko jako sieć diagnostyczna. W tym samym czasie w krajach wyżej rozwiniętych pracowało dużo systemów diagnostyki zapewniających online'owy dostęp odległy, natomiast na wejściu do sieci zakładowej stosowane były odpowiednie zapory sieciowe, gwarantujące wystarczające bezpieczeństwo cybernetyczne przedsiębiorstwa.

Współcześnie, kierując się podobnym jak w przeszłości przesłaniem bezpieczeństwa, w jednym z dużych krajowych przedsiębiorstw zaczęto eliminować wdrożone interfejsowanie cyfrowe między systemami monitorowania i zabezpieczeń stanu technicznego (*nota bene* posiadającymi certyfikat Achillesa) a komponentami DCS pracującymi na rzecz procesu. Historyczną alternatywą do komunikacji cyfrowej jest analogowe połączenie między systemami. W tym przypadku wszystkie kanały systemu monitorowania i zabezpieczeń muszą posiadać wyjścia analogowe. Aby zrealizować transmisję analogową z systemu monitorowania stanu, należy najpierw wykonać konwersję cyfrowo-analogową, po czym przekazywane przewodami sygnały analogowe będą podlegać na wejściu do modułu DCS kolejnej konwersji, tym razem analogowo-cyfrowej. Taka forma interfejsowania jest archaiczna, kosztowna, realizuje funkcję przekazywania danych na poziomie minimalnym, bowiem dla każdego czujnika drgań w profesjonalnym systemie monitorowania stanu technicznego wykonywany jest nie jeden, ale co najmniej kilka pomiarów (w systemach bardziej zaawansowanych – nawet do 20 pomiarów) oraz dodatkowo, z systemu nadzoru do DCS, przekazywanych może być dla każdego kanału pomiarowego kilka danych binarnych, które są użyteczne dla operatorów. Transmisja wszystkich wymienionych pomiarów i danych

binarnych dla wielu kanałów w systemie monitorowania stanu technicznego może być zrealizowana drogą cyfrową z pomocą pojedynczego połączenia, natomiast droga analogowa ogranicza się do pojedynczego pomiaru dla każdego kanału.

W opisanym powyżej przypadku uwsteczniania sposobu interfejsowania między systemami problemem wydaje się być brak wystarczającej wiedzy technicznej specjalistów tego przedsiębiorstwa, w jaki sposób systemy nadzoru stanu technicznego winny być interfejsowane z DCS, aby wymagany poziom bezpieczeństwa cybernetycznego nie był naruszony.

7. Potrzeba zapisów w dokumentach typu SiWZ

Jeśli problematyka nadzoru stanu technicznego jest traktowana w przedsiębiorstwie poważnie, to w przypadku formułowania dokumentów w zakresie nadzoru stanu technicznego dla kolejnej inwestycji (nie ma znaczenia, czy jest to jedynie pojedyncza maszyna, czy też duża instalacja) winny być sformułowane, po pierwsze, wymagania standaryzacji dla dostarczanego systemu nadzoru, a po drugie, postawione wymogi na okoliczność oczekiwanego poziomu zapewnienia bezpieczeństwa cybernetycznego. Podobne wymagania winny być sformułowane w przypadku inwestycji mających na celu unowocześnienie systemu monitorowania i zabezpieczeń i/lub systemu diagnostyki.

W przypadku przedsiębiorstw, które posiadają zaszłości w zakresie wdrożonych już systemów nadzoru stanu technicznego i posiadają wdrożony jakiś dostatecznie nowoczesny i satysfakcjonujący standard, celowe jest postawienie wymogu dostosowania się do tego standardu. Natomiast w przypadku przedsiębiorstw, które dotychczas nie wykorzystywały na szerszą skalę systemów nadzoru, a dla maszyn i urządzeń mających być dostarczonymi w ramach procesu inwestycyjnego planują realizację utrzymania ruchu, bazując na ich stanie technicznym, winien być sformułowany wymóg zrealizowania dostaw w ramach jednego standardu. Celowe jest w tym przypadku wskazanie kilku systemów dostępnych na rynku, które z pozycji inwestora są oceniane jako technicznie wystarczająco nowoczesne[5], a dla wykonawcy inwestycji stanowią egzemplifikację oczekiwań inwestora.

W zakresie zapewnienia bezpieczeństwa cybernetycznego mogą być postawione wymagania bardziej szczegółowe, w tym również w zakresie oczekiwanych certyfikatów dla wdrażanych rozwiązań systemowych na rzecz nadzoru stanu technicznego środków produkcji: dla maszyn krytycznych może być wymagana np. dostawa systemu nadzoru posiadającego opisany powyżej certyfikat Achillesa.

8. Zakończenie

Naruszenie bezpieczeństwa cybernetycznego może zaistnieć poprzez różne elementy systemu nadzoru stanu technicznego.

Stopień hipotetycznego zagrożenie jest uzależniony od uwzględnienia różnych form zagrożenia na etapie projektowania i konstruowania rozwiązania systemowego dedykowanego nadzorowi stanu oraz od poprawności jego wdrożenia. W artykule omówiono dostępne standardy, które mogą być pomocne w projektowaniu i we wdrażaniu rozwiązań bardziej bezpiecznych. Dla przykładowo wybranych produktów omówiono dodatkowe wymogi niezbędne dla spełnienia certyfikatu Achillesa. Wskazano na celowość wprowadzenia stosownych zapisów w dokumentach przetargowych, zarówno chroniących inwestora przed przypadkowymi dostawami komponentów systemu nadzoru, jak również zabezpieczających go na okoliczność bezpieczeństwa cybernetycznego.

Gdyby dla irańskich wirówek nie wykorzystywano w celu nadzoru stanu technicznego komponentów DCS, a stosowane były systemy o właściwościach podobnych do posiadanych przez system pokazany przykładowo na rys. 5, to nigdy nie doszłoby do opracowania STUXneta oraz do jego z sukcesem przeprowadzonych destrukcji. Nie miałyby także szansy powodzenia niektóre inne zakończone sukcesem ataki wspomniane w tym artykule.

Przypisy

1. BSI = *Bundesamt für Sicherheit in der Informationstechnik*.
2. Wciąż jeszcze szereg przedsiębiorstw nie korzysta z narzędzi umożliwiających synchronizację czasu na bazie sygnału radiowego.
3. ETSI = *European Telecommunications Standards Institute.*
4. TC CYBER = *Cyber Security Technical Committee*.
5. Znane są przypadki dostawy nowych maszyn (także dla inwestycji realizowanych w Polsce), kiedy to firma realizująca inwestycję dostarczyła maszynę wyposażoną w system monitorowania i zabezpieczeń, który już kilka lat wcześniej został wycofany z produkcji, natomiast inwestor przechodził nad tym faktem do porządku dziennego. Systemy nadzoru stanu technicznego są zastępowane przez nowe produkty z kilku przyczyn: (i) brak dostępności do komponentów, które są niezbędne do ich produkcji i serwisowania; (ii) pojawienie się nowych standardów, których wdrożenie dla jakiegoś produktu (tu: systemu nadzoru) wymagałoby przyprowadzenia bardzo głębokiej jego rekonstrukcji i w konsekwencji zaprojektowanie nowego systemu jest tańsze niż modernizacja tego dotychczas produkowanego.

   Powyższe nie oznacza jednak, że systemy wprowadzone do sprzedaży wiele lat temu nie mogą być wciąż nienowoczesne. W przypadku niektórych dużych i mocno rozpowszechnionych systemów ich producenci decydują się na głębokie rekonstrukcje. Przykładem może być SYSTEM 3500 [13], który przechodzi okresowe rekonstrukcje stymulowane przez (i) dostępność na rynku nowszej bazy komponentów wykorzystywanych do produkcji systemu; (ii) wprowadzanie nowych monitorów dla nowych metod monitorowania i wykorzystywanych w związku z tym nowych typów czujników; (iii) dostosowywanie konstrukcji do wymagań nowych standardów (jak np. dyrektywa RoHS); (iv) unowocześnianie sposobu interfejsowania ze środowiskiem tak w połączeniach z DCS, jak i z systemami diagnostyki, również ze względu na potrzeby zapewnienia wymogów bezpieczeństwa cybernetycznego i uzyskania na tę okoliczność certyfikacji Achillesa.

Literatura

[1] Nowicki R.: *Nadzór stanu technicznego agregatów z napędami elektrycznymi – wprowadzenie do tematyki*. „Napędy i Sterowanie" 10/2013.

[2] Nowicki R.: *Cybersecurity for condition management systems of production assets*. The Global Summit on Chemical Safety and Security CHEMMS 2016, Kielce, Poland, 18–20 APR 2016, prezentacja konferencyjna.

[3] Repository for Industrial Security Incidents, www.securityincidents.org.

[4] Berger R.: *CYBER-SECURITY: Managing threat scenarios in manufacturing companies*, THINK ACT, CYBER-SECURITY, MARCH 2015.

[5] Abramczyk A.: *Badanie rynku: Cyberbezpieczeństwo.* „Inżynieria i Utrzymanie Ruchu" 4/2016.

[6] Manhattan U.S. Attorney Announces Charges Against Seven Iranians (…), 24-03-2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

[7] Cyber security certification becomes a focus of process security, Asian Engineer, 21st FEB 2013

[8] Wasiak A.: *Utrzymanie ruchu w dobre ręce oddam.* „Inżynieria & Utrzymanie Ruchu" 2/2012.

[9] Nowicki R., Pappas Y.: *Intelligent maintenance support of hydro station asset management*. Proceedings of International Conf. OCT 29–31, 2012, Bilbao, Spain.

[10] Nowicki R., Bate M.: *Programowe rozpoznawanie anomalii pracy agregatów napędzanych silnikami elektrycznymi*. „Napędy i Sterowanie" 12/2013.

[11] ANSI/ISA 99.01.01 – 2007-3.2.116: Security zone: grouping of logical and physical assets that share common security requirements.

[12] Byres E.: *Using ANSI/ISA-99 standards to improve control system security*, Published by IEB Media GbR.

[13] Boyer L.: *The 3500 Series Machinery Protection System*, ORBIT Vol. 31, No.3, OCT 2011, p. 9–13.

[14] Nowicki R.: *A Way for a better alarm management*. Water Power & Dam Construction, MAY 2016, p. 30–32.

[15] Nowicki R.: *Nadobroty: skutki, systemy detekcji i zabezpieczenia*. „Napędy i Sterowanie" 10/2015.

dr inż. Ryszard Nowicki – e-mail: Ryszard.Nowicki@ge.com

artykuł recenzowany