OSDP

NOWY STANDARD W SYSTEMACH KONTROLI DOSTĘPU

Andrzej TOMCZAK

W lutym 2019 r. została zainicjowana w PKN ankieta projektu przyszłej normy europejskiej, która wprowadza normę międzynarodową IEC 60839-11-5 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-5: Elektroniczne systemy kontroli dostępu – Protokół komunikacyjny OSDP*. Warto zainteresować się tym, co do branży elektronicznych systemów kontroli dostępu (SKD) wnosi nowy standard. W trakcie pisania artykułu wykorzystano m.in. materiały firm: HID Global oraz IFSEC Global.

Temat zmian w sposobie komunikacji pomiędzy czytnikami a centralami (kontrolerami) w systemach KD był już wielokrotnie poruszany na łamach SEC&AS[1]. Na pewno można przyjąć, że jeżeli dla nowego standardu komunikacji powstała norma międzynarodowa, to należy OSDP traktować bardzo poważnie. Przez ostatnie 30 lat branża SKD zmieniała się dość powoli. Czytniki kart magnetycznych, które królowały w latach 80. i 90. XX w., nie tak dawno na stałe zniknęły z naszego krajobrazu. Natomiast w zakresie komunikacji pomiędzy czytnikami a centralami (kontrolerami) w latach 90. zaczęły dominować interfejsy wykorzystujące protokół Wieganda (D0/D1), które zostały zaimplementowane do komunikacji z większością typów czytników wykorzystujących technologię radiową (RFID). Interfejs Wieganda został przyjęty jako podstawowe rozwiązanie do systemów KD w 1996 r., wraz z opublikowaniem jego kompletnej specyfikacji przez Security Industry Association (SIA)[2]. Nowe zagrożenia, szczególnie związane z cyberprzestępczością, narzuciły konieczność rozstania się z tym jednokierunkowym, niekodowanym standardem komunikacji. Kilka lat temu dzięki współpracy firm pod przewodnictwem HID Global na potrzeby komunikacji wewnątrz systemów KD powstał nowy, dwukierunkowy, szyfrowany, otwarty protokół komunikacyjny – Open Supervised Device Protocol (OSDP).

OTWARTY, BEZPIECZNY STANDARD

Zacznijmy od przypomnienia i porównania poprzednio stosowanych w SKD otwartych protokołów komu-

[1] A. Tomczak: *Zwrot w podejściu producentów do systemów kontroli dostępu.* SEC&AS, nr 4/2017, s. 21–24; A. Tomczak: *Systemy kontroli dostępu w obiektach infrastruktury krytycznej zgodne z polskimi normami*. SEC&AS, nr 6/2017, s. 10–14; A. Tomczak: *Systemy kontroli bezpieczne czy nie? Czy wiesz, że normy od blisko 5 lat zalecają stosowanie szyfrowania?.* Wykład PISA – Securex 2018. SEC&AS, nr 3/2018, s. 10–14.

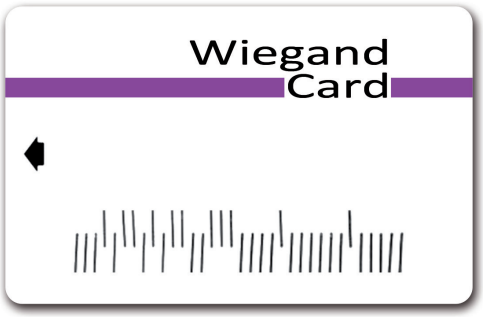
[2] Security Industry Association (SIA) – amerykańska organizacja branży security, zrzeszająca blisko 1000 firm.

nikacyjnych. Standard Wieganda i *clock-and-data* (wykorzystywany w przypadku komunikacji z czytnikami kart magnetycznych) mają ze sobą wiele wspólnego. Po pierwsze, służą do podłączenia jednego czytnika do jednego wejścia centrali (kontrolera), czyli stosuje się komunikację punkt–punkt, co de facto oznacza konieczność łączenia czytników w tzw. gwiazdę. Do tego w obu przypadkach jest to jednokierunkowa, nieszyfrowana komunikacja szeregowa, wykorzystująca do transmisji dwie żyły przewodu łączącego czytnik z wejściem centrali (kontrolera) SKD, opisywane np. jako D0, D1 i masa, oznaczana np. jako GND. Aby umożliwić działanie czytnika potrzebna jest jeszcze kolejna żyła, podająca napięcie zasilające. System nie może zażądać przesłania jakichkolwiek danych z czytnika, a w przypadku konieczności wysyłania danych do czytnika, np. do sterowania diodami LED, należy zastosować dodatkowe żyły przewodu. Komunikacja jednokierunkowa ma wiele wad – za pomocą interfejsu Wieganda nie można sprawdzić stanu czytnika czy też na ten stan wpływać, jedynie można czekać na moment, kiedy użytkownik stwierdzi, że coś nie jest w porządku. Nie można również wykryć, że ktoś podpiął się do magistrali i atakuje system metodą „man in the middle", opisaną szerzej w jednym z poprzednich numerów SEC&AS[3]. Kolejną słabością jest wymóg, aby urządzenia odbierające informację od czytnika były zawsze w pełnej gotowości w oczekiwaniu na niezapowiadaną transmisję danych. Nie można też wykorzystywać podłączeń magistralowych ze względu na brak kontroli nad przepływem danych, a w przypadku bardzo prawdopodobnych kolizji – niemożność zażądania powtórnej transmisji.

Skąd w ogóle wziął się protokół Wieganda? Pod koniec lat 70. John Wiegand zrewolucjonizował przemysł systemów kontroli dostępu, wykorzystując pomysły, które wynikały z odkrycia efektu skokowej zmiany namagnesowania przewodników o specjalnej konstrukcji, pod wpływem zmiany pola elektromagnetycznego, nazwanych od jego nazwiska efektem Wieganda. Na bazie tego odkrycia powstała karta identyfikacyjna, tzw. karta Wieganda, w czasie wytwarzania której zatapiano w laminacie ciąg co najmniej 26 odpowiednio ułożonych krótkich drucików o specjalnej konstrukcji, generujących zaprogramowany fabrycznie kod w momencie przeciągnięcia identyfikatora (rys. 1) w polu elektromagnetycznym, wytwarzanym w czytniku (rys. 2). Rozwiązanie to przewyższało technicznie uprzednio stosowane karty magnetyczne, ze względu na: trwałość, odporność na ścieranie, niemożliwość rozmagnesowania oraz samodzielnego zaprogramowania i przeprogramowania – a więc olbrzymią trudność podrobienia. Karty były kodowane w czasie produkcji w fabryce, co jednak negatywnie wpływało na ich cenę. Mimo że karty Wieganda były dużo lepsze i bezpieczniejsze niż karty magnetyczne, nie zdobyły one polskiego rynku, zwykle zwracającego większą uwagę na cenę niż bezpieczeństwo rozwiązań.

Wiegand zastosował specjalny interfejs do transmisji danych z czytnika, nazywany potem interfejsem Wieganda, dzięki któremu można było transmitować informacje identyfikujące użytkownika na odległość dochodzącą nawet do 150 m długości przewodu. W tamtych czasach był to ogromny skok jakościowy, ponieważ uprzednio stosowane rozwiązania pozwalały podłączać czytniki za pomocą przewodów o maksymalnej długości do ok. 20 m – wyjątkiem była stosowana przez szwedzką firmę APTUS transmisja oparta na telefonicznym standardzie DTMF, której zasięg określano na ok. 100 m. Na przełomie wieku tylko firma COTAG uzyskiwała większe odległości umiejscowienia czytników od central (kontrolerów), które wynosiły nawet do 300 m długości przewodu. Ponieważ ta transmisja była dedykowana tylko do firmowego systemu GRANTA, siłą rzeczy nie mogła się rozpowszechnić wśród innych producentów. Natomiast otwarty protokół Wieganda na dekady zadomowił się w branży SKD.

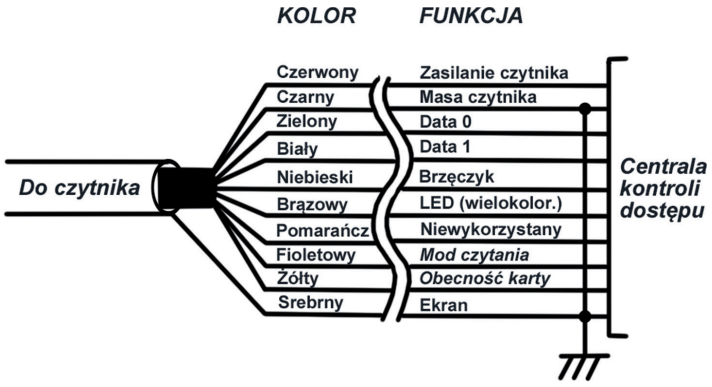
Jak już wiadomo, pomimo szerokiego stosowania protokół Wieganda ma wiele ograniczeń i nie jest bezpieczny. Nie ma szyfrowania, co daje hakerom możliwość przechwycenia przesyłanych informacji lub podłożenia spreparowanych danych w celu oszukania centrali (kontrolera). Oprócz tego szybkość transferu danych jest zbyt mała do zastosowania aktualnego



Rys. 1. Poglądowo pokazana konstrukcja karty Wieganda – w rzeczywistości ciąg zalaminowanych w karcie drucików nie jest widoczny

Rys. 2. Czytnik kart Wieganda wyprodukowany w 1993 r. w amerykańskiej firmie Sensor Engineering – w czasie odczytu kartę przesuwało się poziomo

[3] A. Tomczak: *Systemy kontroli bezpieczne czy nie? Czy wiesz, że normy od blisko 5 lat zalecają stosowanie szyfrowania?*. Wykład PISA – Securex 2018. SEC&AS, nr 3/2018, s. 10–14.

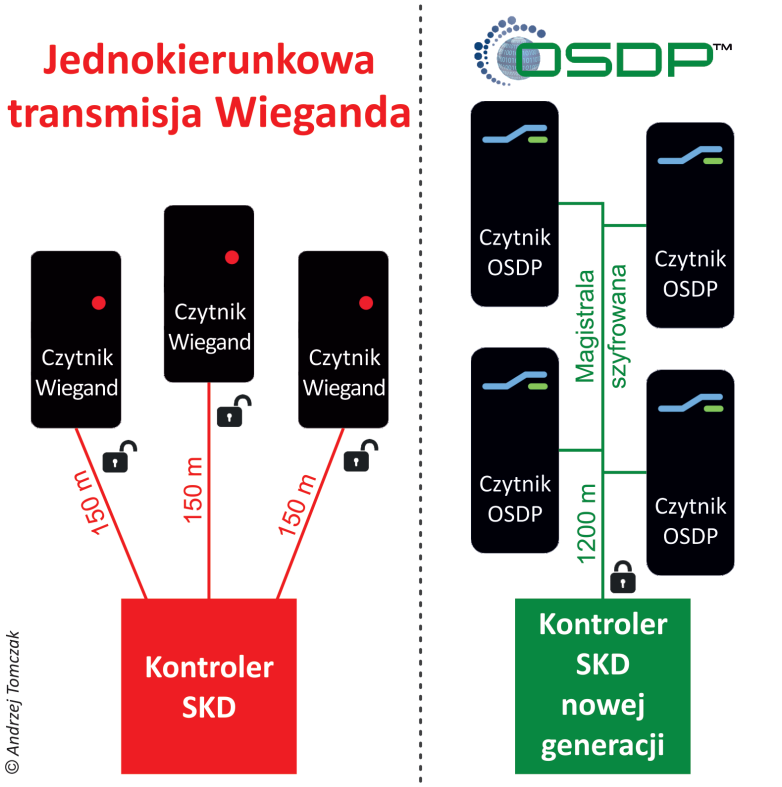


Rys. 3. Przykładowe pełne okablowanie czytnika z interfejsem Wieganda

modelu identyfikacji PIV (ang. *Personal Identity Verification*), który wymaga transmisji ponad 200 bitów informacji identyfikacyjnych. Do wad należą również: brak możliwości zdalnego zarządzania czytnikami, konieczność łączenia czytników w tzw. gwiazdę, zasięg transmisji do 150 m, potrzeba stosowania dodatkowych żył przewodu do sterowania funkcjami czytnika. Standardowy przewód wykorzystywany do podłączenia czytnika za pomocą interfejsu Wieganda wymaga zastosowania od 6 do 9–10 żył (rys. 3).

Wszystkie powyżej wymienione ograniczenia spowodowały konieczność wypracowania nowego standardu komunikacji pomiędzy czytnikami a centralami (kontrolerami) SKD. Co prawda niektóre firmy wdrożyły własne sposoby komunikacji dwukierunkowej, ale hermetyczność tych rozwiązań nie pozwoliła na ich rozpowszechnienie. Dopiero porozumienie firm HID Global i Mercury Security Corp. pozwoliło na wypracowanie w 2008 r. nowego protokołu komunikacji, pod nazwą OSDP (ang. *Open Supervised Device Protocol*), który został w 2011 r. przyjęty jako standard SIA. Organizacja stworzyła grupy robocze OSDP, otwarte dla wszystkich członków, i mogła finansować kontynuację prac nad tym standardem dzięki pochodzącym od nich składkom.

OSDP jest protokołem interfejsów komunikacyjnych urządzeń peryferyjnych, takich jak czytniki i kontrolery SKD oraz inne urządzenia elektronicznych systemów zabezpieczeń. Oczekuje się, że całkowicie zastąpi leciwy protokół Wieganda w aplikacjach wymagających komunikacji dwukierunkowej, szyfrowania oraz transmisji większej ilości danych, szczególnie do komunikacji z kartami elektronicznymi. Bezpieczny protokół SCP (ang. *Secure Channel Protocol*), wykorzystywany w OSDP, wspiera przemysłowy, magistralowy standard komunikacji szeregowej RS-485, ale może również być rozszerzony o komunikację opartą na protokole IP. Aktualnie najszerzej wspierana jest wersja OSDP dla komunikacji szeregowej, która została zaimplementowana przez wielu producentów systemów KD oraz dostawców czytników. Dominacja rozwiązań opartych na transmisji szeregowej wynika m.in. z tego, iż wymogi dotyczące przepustowości kanałów w systemach kontroli dostępu nie są tak wysokie jak w telewizji IP, z reguły nie ma więc potrzeby godzenia się na niedogodności i kompromisy, jakie wymusza stosowanie technologii sieci komputerowych. Zaś komunikacja przemysłowa RS-485 jest bardzo odporna na zakłócenia, pozwala podłączyć do 32 urządzeń pracujących na jednej magistrali, której długość przewodów, bez replikacji, może dochodzić nawet do 1500 m (standard określa tę długość na ok. 1200 m). W przypadku sieci komputerowych odległość do punktu aktywnego w przypadku okablowania miedzianego wynosi tylko 100 m, a do tego dochodzą specyficzne dla systemów zabezpieczeń wymagania stawiane zasilaniu urządzeń, często bardzo trudne do zaimplementowania w przypadku sieciowych urządzeń aktywnych, co było już szeroko opisywane w SEC&AS[4].



© Andrzej Tomczak

Rys. 4. Zasady podłączania czytników w przypadku stosowania protokołów Wieganda i OSDP wykorzystującego transmisję szeregową RS-485

KOMUNIKACJA DWUKIERUNKOWA

Przemysł SKD dobrze przyjął nowy standard, ponieważ jest on znacznie korzystniejszy i bezpieczniejszy od dotychczas stosowanego. Wykorzystanie OSDP z SCP przyczynia się do poprawy bezpieczeństwa systemów oraz zwiększa możliwości w zakresie integracji. Dzięki wykorzystaniu OSDP możliwe są: konfiguracja i zdalna kontrola czytników, ich „odpytywanie" w razie wystą-

[4] W. Kessler: *Stosowanie sieciowych systemów zabezpieczeń w obiektach IK i nie tylko…* SEC&AS, nr 5/2018, s. 56–59; A. Tomczak: *Zasilanie sieciowych systemów zabezpieczeń na cenzurowanym*. SEC&AS, nr 5/2018, s. 72–76.

pienia takiej konieczności, a także nadzór nad kanałem komunikacji. Przyczynia się to do zmniejszenia kosztów uruchamiania i zarządzania oraz zwiększenia niezawodności systemu – OSDP, w odróżnieniu od protokołów Wieganda i *clock-and-data*, umożliwia monitorowanie stanu czytników oraz kanału komunikacji. Pozwala to na natychmiastowe wykrycie uszkodzenia czytnika, usunięcia z systemu, jak również jego sabotowania. W przypadku komunikacji szeregowej wszystkie sygnały są transmitowane za pośrednictwem dwużyłowej magistrali – czyli razem z zasilaniem do czytnika doprowadza się przewód czterożyłowy. W przypadku poprzednio stosowanych protokołów komunikacji do czytnika trzeba było doprowadzić przewód składający się z co najmniej 6, a często nawet 10 żył. Do tego RS-485 pozwala na magistralowe łączenie czytników, co jeszcze bardziej upraszcza instalację (rys. 4). Przykładowo, do czytników obsługujących wejście i wyjście jednego przejścia kontrolowanego wystarczy doprowadzić jeden przewód czterożyłowy (wcześniej musiały być to dwa przewody, co najmniej 6-żyłowe). Z tego wynika, że przy zastosowaniu OSDP koszty okablowania stają się niższe.

W OSDP zastosowano silne szyfrowanie z uwierzytelnianiem, dzięki któremu komunikacja z czytnikami jest bardzo bezpieczna. Protokół SCP został opracowany przez organizację GlobalPlatform, która zajmuje się rozwijaniem i tworzeniem standardów w zakresie bezpieczeństwa aplikacji wykorzystywanych w przemyśle m.in. dla kart elektronicznych. W celu rozpoczęcia sesji komunikacyjnej, wykorzystującej Secure Channel Protocol, pomiędzy czytnikiem a centralą (kontrolerem) musi nastąpić wzajemne uwierzytelnienie z wykorzystaniem zestawu kluczy ustalonych dla danej sesji. W przypadku niepowodzenia połączenie zostaje zerwane, a klucze zniszczone. HID Global był jednym z pierwszych producentów wspierających w swoich czytnikach protokół OSDP z SCP, jako elementu platformy iCLASS SE. Produkcję czytników wykorzystujących nowy protokół wdrożyły też inne fabryki. Również poważni producenci systemów KD zaczęli implementować ten standard w swoich urządzeniach.

Dostępność standardu oraz produkowanie urządzeń komunikujących się za pomocą tego protokołu przez największego dostawcę czytników KD, jakim jest HID Global, jest gwarancją tego, że OSDP bardzo szybko opanuje rynek systemów kontroli dostępu, a udział urządzeń wykorzystujących komunikację opartą na protokole Wieganda będzie się systematycznie zmniejszał.

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym, redaktor naczelny SEC&AS