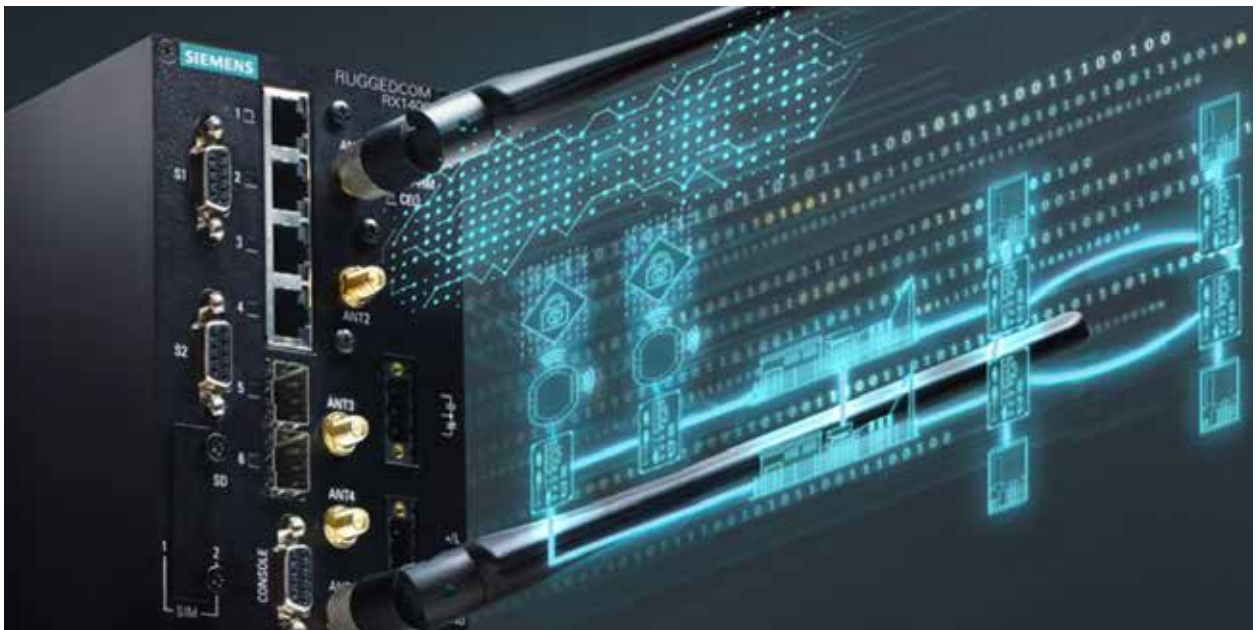
Andrzej Cieślak, Ekspert ds. Bezpieczeństwa i Komunikacji Przemysłowej,
CCIE #48567, MSc Ethical Hacking & Computer Security, SCPIN, CCDP, CCNP Sec,
CCNA Industrial, ISO 27001 Auditor, Prince 2 Practitioner, NSA Recognition
FIRMA: Dynacon sp. z o.o.

Piotr Jaskólski,
Product Manager Siemens RUGGEDCOM.
FIRMA: Siemens Sp. z o.o.

Nowa era
komunikacji przemysłowej

Zakłady wytwarzające jakiekolwiek dobra konsumpcyjne, opierające swoją produkcję na standardach przemysłu procesowego, zderzają się z zagadnieniami wymiany informacji na masową skalę, wymiany danych pomiędzy światem biznesu oraz połączeniami pomiędzy OT (Operation Technology/Technologia Operacyjna), ICT (Information and Communication Technolog /Technologia Informacyjna i Komunikacyjna) i IT (Information Technology/Technologia Informacyjna). Jak optymalnie podejść do budowy skutecznej strategii komunikacji w przemyśle? Jak wybrać właściwą technologię i ją wdrożyć? W końcu jak eksploatować i utrzymywać wypracowany poziom jakości i skuteczności wymiany danych w środowisku OT?



Poruszane zagadnienie jest osadzone w środowisku przemysłowym i jako takie wymaga niezależnego podejścia i obsługi. Większość projektów dotyczących modernizacji czy implementacji nowych sieci przemysłowych oparte jest o środowisko IT. Dla systemów sterowania prace te oparte są o wysoce izolowane i specjalistyczne rozwiązania sygnalizacyjne. Konieczność łączenia i zarazem izolacji tych stref materializuje, obserwowane w coraz większej skali przenikanie, czy wręcz wprost przeszczepianie niemodyfikowanych rozwiązań IT, do przemysłowych środowisk przesyłu danych. Rozumienie rozpoznanych różnic pomiędzy światem IT, ICT i OT jest uważane za pierwszy skuteczny i bezpieczny krok w doborze strategii i tym samym odpowiedzi na postawione na wstępie pytania. Różnice te efektywnie ujęto w m.in. dokumentach NIST.

Spojrzenie na świat ICS (Industrial Control Systems/Przemysłowe Systemy Sterowania) jako środowisko kontrolujące świat fizyczny, a na świat IT jako środowisko zarządzające danymi, ułatwia interpretację zasadniczych różnic. Usługi ICS mają wiele cech różniących się od tradycyjnych systemów IT, w tym różne rodzaje ryzyka i priorytety. Systemy ICS mają różne wymagania dotyczące wydajności i niezawodności, a także korzystają z systemów operacyjnych i aplikacji, które mogą być uznane za niekonwencjonalne w typowym środowisku sieci IT. Zabezpieczenia muszą być implementowane w sposób zapewniający integralność systemu podczas normalnych operacji, a także podczas sytuacji kryzysowych.

Początkowo system ICS miał niewielkie podobieństwo do systemów IT, ponieważ systemy ICS były izolowanymi systemami z zastrzeżonymi protokołami kontrolnymi, wykorzystującymi specjalistyczny sprzęt i oprogramowanie. Powszechnie dostępne, tanie urządzenia Ethernet i protokół internetowy (IP) zastępują obecnie starsze, zastrzeżone technologie, co zwiększa możliwości luk w zabezpieczeniach i incydentów związanych ze stabilnością rozwiązań czy cyberprzestępczością. Ponieważ ICS przyjmuje rozwiązania IT (jedynie opisywane jako OT), które są projektowane i wdrażane przy użyciu standardowych komputerów, systemów operacyjnych i protokołów sieciowych, zaczynają przypominać systemy IT. Ta integracja obsługuje nowe możliwości dzięki IT, ale zapewnia również znacznie mniej izolacji dla ICS od świata zewnętrznego niż systemy wcześniejsze.

Biorąc pod uwagę istotny aspekt środowiska systemów technologicznych w tym systemów sterowania w kontekście np. infrastruktury krytycznej, należy rozważyć zastosowanie rekomendacji wynikającej wprost z zapisów dokumentu NIST 800.82 rev 2.

Podczas gdy rozwiązania bezpieczeństwa zostały opracowane w celu radzenia sobie z tymi problemami bezpieczeństwa w typowych systemach IT, należy wprowadzić specjalne środki ostrożności przy wprowadzaniu tych samych rozwiązań do środowisk ICS. W niektórych przypadkach potrzebne są nowe rozwiązania komunikacji, bezpieczeństwa oraz szkoleń dostosowane do środowiska ICS.

Systemy ICS są na ogół krytyczne czasowo, z kryterium dopuszczalnych poziomów opóźnienia i fluktuacji dyktowanych przez poszczególne instalacje. Niektóre systemy wymagają deterministycznych odpowiedzi. Wysoka przepustowość zazwyczaj nie jest niezbędna w przypadku usługi ICS. W przeciwieństwie do tego systemy IT zazwyczaj wymagają dużej przepustowości i zazwyczaj mogą wytrzymać pewien poziom opóźnień i fluktuacji. Istnieją systemy IT biorące pod uwagę względy wartości czasowej,

ale wiele systemów IT tego nie robi. Systemy te, które modelują przestrzeń problemową, w której czas nie jest czynnikiem, są ściśle kombinatoryczne. ICS i systemy IT, które zawierają czas jako zmienną, są sekwencyjne. Układy sekwencyjne często mają wymagania dotyczące czasu i jego synchronizacji. W przypadku niektórych usług ICS bardzo ważny jest automatyczny czas odpowiedzi. Niektóre usługi ICS opierają się na systemach operacyjnych czasu rzeczywistego (RTOS), w których czas rzeczywisty odnosi się do wymogów terminowości.

Wiele procesów w ICS ma charakter ciągły. Nieoczekiwane wyłączenia systemów kontrolujących procesy przemysłowe są niedopuszczalne. Wyczerpujące testy przed wprowadzeniem zmian są niezbędne dla zapewnienia wysokiej dostępności (tj. niezawodności) dla usługi ICS. Systemy kontroli często nie mogą być łatwo zatrzymane i uruchomione bez wpływu na produkcję. W związku z tym stosowanie typowych strategii informatycznych, takich jak ponowne uruchomienie komponentu, jest zwykle niedopuszczalnym rozwiązaniem. Niektóre usługi wykorzystują nadmiarowe składniki, często działające równolegle, aby zapewnić ciągłość, gdy podstawowe komponenty są niedostępne co wymusza zastosowanie specyficznej architektury sieci, która nie jest wspierana przez systemy IT.

ICS i ich systemy czasu rzeczywistego są często systemami z ograniczonymi zasobami, które nie obejmują typowych współczesnych możliwości bezpieczeństwa informatycznego. W starszych systemach często brakuje zasobów wspólnych dla nowoczesnych systemów informatycznych. Wiele systemów może nie mieć pożądanych funkcji, w tym możliwości szyfrowania, rejestrowania błędów i ochrony hasłem. Te rozwiązania ICS mogą nie tolerować typowych praktyk bezpieczeństwa IT. Nieuzasadnione ich użycie może spowodować niedostępność i zakłócenia w czasie. W przypadku chęci modernizacji komponentów ICS możemy spotkać się z zagadnieniem braku wymaganych zasobów, które spełniłyby wymagania aktualnie stosowanych zabezpieczeń, zatem dodawanie funkcji może nie być możliwe.

Protokoły komunikacyjne i media używane przez środowiska ICS do sterowania urządzeniami obiektowymi i komunikacji wewnątrz-procesowej zwykle zasadniczo różnią się od większości protokołów informatycznych.

Zarządzanie zmianą ma kluczowe znaczenie dla utrzymania integralności systemów informatycznych i kontrolnych. Niezaktualizowane oprogramowanie stanowi jedną z największych luk w zabezpieczeniach danego systemu. Aktualizacje oprogramowania w systemach IT, w tym poprawki zabezpieczeń, są zazwyczaj stosowane w odpowiednim czasie, w oparciu o odpowiednią politykę bezpieczeństwa i procedury. Ponadto procedury te są często zautomatyzowane za pomocą narzędzi serwerowych. Aktualizacje oprogramowania systemów ICS nie zawsze mogą być wdrożone zgodnie z wymaganiami producentów poszczególnych komponentów, ponieważ te aktualizacje muszą być dokładnie przetestowane przez dostawcę aplikacji systemów sterowania i głównego operatora przed wdrożeniem, a niedostępności komponentów ICS muszą być zaplanowane z wyprzedzeniem. System ICS może również wymagać ponownej walidacji w ramach procesu aktualizacji. Innym problemem jest to, że wiele usług ICS wykorzystuje starsze wersje systemów operacyjnych, które nie są już obsługiwane przez integratora. W związku z tym dostępne poprawki mogą nie mieć zastosowania. Zarządzanie zmianami dotyczy również sprzętu i oprogramowania układowego. Proces zarządzania zmianami, gdy jest stosowany do ICS, wymaga starannej oceny przez ekspertów OT pracujących w powiązaniu z personelem bezpieczeństwa i IT. Bezpośrednie stosowanie systemów zarządczych ze świata IT może być katastrofalne w skutkach.

Podsumowując, systemy ICS często różnią się znacznie od odpowiedników IT, wymagając różnych zestawów umiejętności, doświadczenia i poziomu wiedzy specjalistycznej. Sieci przemysłowe są zwykle zarządzane przez inżynierów OT, a nie przez personel IT. Założenia, że różnice nie są znaczące, mogą mieć katastrofalne konsekwencje. Dodatkowo różnice operacyjne i źródła ryzyk między systemami ICS a systemami informatycznymi stwarzają potrzebę zwiększenia złożoności w kontekście komunikacji, cyberbezpieczeństwa i strategii operacyjnych. Interdyscyplinarny zespół inżynierów OT, operatorów systemów sterowania i specjalistów ds. Bezpieczeństwa IT musi ściśle współpracować, aby zrozumieć możliwe konsekwencje instalacji, działania i utrzymania rozwiązań bezpieczeństwa w połączeniu z działaniem systemu sterowania. Specjaliści IT pracujący z ICS muszą zrozumieć wpływ niezawodności technologii komunikacji i bezpieczeństwa informacji przed wdrożeniem. Niektóre systemy operacyjne i aplikacje działające w systemie ICS mogą nie działać poprawnie z dostępnymi komercyjnie rozwiązaniami komunikacji i cyberbezpieczeństwa IT ze względu na wyspecjalizowane architektury środowiskowe ICS. Stosowanie rozwiązań projektowanych dla OT i „rozumiejących" specyfikę i wymagania środowisk ICS (m.in. SIEMENS RUGGEDCOM i DYNACON) o wysokim współczynniku adaptacyjności i elastyczności (np. wymienne moduły komunikacyjne na gorąco, szerokie spektrum technologii uruchamianych na platformach RUGGEDCOM, dedykowane systemy autonomicznego zarządzania i reakcji na zdarzenia cyberbezpieczeństwa - DYNACON A.R.I.C Network Defence System, czy IDCS AIN® uruchamiane bezpośrednio na urządzeniach RUGGEDCOM, zgodność z rygorystycznymi normami przemysłowymi m.in. IEC 61850, IEC 1613, IEC 61000-6-2, IEC 61800-3, NEMA TS-2, EN 50155, itd.), **znacząco podnosi poziom skuteczności, stabilności i efektywności dla systemów OT wymagających przesyłu danych.** □