Ochrona informacji sterującej w sieciach i systemach przemysłowych – propozycja podstaw edukacyjnych

Krzysztof LIDERMAN

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono problematykę nauczania zagadnień bezpieczeństwa dla przemysłowych systemów sterowania. Po zwięzłym scharakteryzowaniu we wstępie sieci i systemów przemysłowych, w kolejnych punktach krótko opisano podstawowe dla tego obszaru problemowego normy i standardy (IEC 62443 oraz *CIS Critical Security Controls for Effective Cyber Defense*), framework MITRE ATT&CK oraz zbiór „dobrych praktyk" opublikowany przez *Bundesamt für Sichercheit in der Informationstechnik*.

SŁOWA KLUCZOWE: przemysłowe systemy sterowania, IEC 62443, CAG/CIS, MITRE ATT&CK, „dobre praktyki" dla przemysłowych systemów sterowania

1. Wstęp

Eksploatowane we współczesnych organizacjach i – ujmując problem szerzej – infrastrukturze państwowej systemy: transportowe, komunikacyjne, magazynowe i produkcyjne, muszą być *nadzorowane* oraz w części przypadków, dotyczy to głównie systemów produkcji, *sterowane*. Zadania te są realizowane za pomocą przemysłowych systemów sterowania, na które składają się m.in. sieci SCADA (ang. *Supervisory Control And Data Acquisition*), DCS (ang. *Distributed Control Systems*) oraz ich elementy składowe w postaci sterowników programowalnych PLC (ang. *Programmable Logic Controllers*) [5].

Przemysłowe systemy sterowania (ang. *Industrial Control System* – ICS)[1] rozwijały się w zasadzie oddzielnie od teleinformatycznych (biurowych) sieci komputerowych. To oddzielenie, brak połączeń pomiędzy różnymi ICS, stosowanie specjalizowanego sprzętu i protokołów, wydzielonych kanałów komunikacyjnych oraz zwykle dobra ochrona fizyczna centrów sterowania powodowały, że problemy nękające biurowe sieci informatyczne związane z działaniami różnego rodzaju intruzów, możliwościami propagacji niekorzystnych efektów pomiędzy różnymi, połączonymi sieciami, podatność na ataki typu Denial of Services itp. nie dotyczyły praktycznie sieci przemysłowych.

Jednak od lat 90. XX wieku zaczął się zarysowywać trend[2] łączenia wydzielonych dotąd ICS z sieciami biurowymi oraz stosowanie do ICS rozwiązań z „klasycznych" sieci biurowych (komercyjnych systemów operacyjnych i sprzętu komputerowego) oraz wykorzystanie Internetu (protokołu IP) jako medium komunikacyjnego. Wymienione fakty złożyły się na nowy jakościowo obraz współczesnych sieci przemysłowych – pojawiły się w nich nowe problemy z zapewnianiem bezpieczeństwa o tym, że są to zagadnienia istotne dla żywotnych interesów nie tylko poszczególnych firm czy organizacji, ale także państwa, świadczą już wczesne publikacje o tej tematyce i podejmowane działania:

– opublikowane po raz pierwszy we wrześniu 2007 roku rekomendacje NIST (*National Institute of Standards and Technology*) [30],
– przyjęcie przez NERC (*North American Electric Reliability Corporation*) w 2008 roku ośmiu standardów z zakresu „cybersecurity" i ochrony infrastruktury krytycznej (patrz też rozdział 4.3 oraz przypisy dolne z linkami w tym rozdziale) oraz opracowanie [29] listy dziesięciu najgroźniejszych podatności dla ICS wraz ze wskazaniem sposobów ich minimalizacji;
– powołanie w USA, w ramach U.S. Department of Homeland Security, przemysłowego zespołu reagowania (ICS-CERT − *Industrial Control Systems Cyber Emergency Response Team*)[3]. Obecnie na swoich stronach internetowych[4] ICS-CERT prezentuje nie tylko specyfikacje aktualnych

[1] W literaturze anglojęzycznej jest też często używane określenie *Operational Technology* (OT).

[2] Głównie pod wpływem czynników ekonomicznych i nowych koncepcji zarządzania biznesem, w których kadra zarządzająca w celu podwyższenia efektywności i konkurencyjności swoich organizacji korzysta z danych na temat produkcji dostępnych w systemach automatyki.

[3] https://www.us-cert.gov/control_systems/ics-cert/

[4] https://www.us-cert.gov/ics/Recommended-Practices

zagrożeń i podatności wykrytych w systemach przemysłowych, ale także obszernie opisane zalecane praktyki zabezpieczania takich systemów [34].

Najnowsze dane statystyczne pokazują[5], że sieci przemysłowe i przemysłowe systemy sterowania w szczególności mogą być stosunkowo łatwym celem dla intruzów, ponieważ:

- 40% instalacji przemysłowych ma co najmniej jedno bezpośrednie połączenie z Internetem;
- w 53% instalacji przemysłowych używa się przestarzałych systemów Windows, takich jak Windows XP;
- w 69% instalacji przemysłowych używa się nieszyfrowanych haseł do dostępu do ICS;
- 57% instalacji przemysłowych nie ma zainstalowanego oprogramowania antywirusowego z funkcją automatycznej aktualizacji baz sygnatur;
- 16% instalacji przemysłowych ma co najmniej jeden bezprzewodowy punkt dostępowy;
- 84% instalacji przemysłowych ma co najmniej jedno urządzenie z dostępem zdalnym.

W specyfikacjach systemów sterowania używane są często określenia: „czasu rzeczywistego" (ang. *real-time systems*) oraz „systemy wbudowane" (ang. *embedded systems*), wskazujące dokładniej typ systemu sterowania [10], [11]. Zgodnie z definicją IEEE/ANSI Std 729: „ (…) *komputerowym systemem czasu rzeczywistego nazywamy system komputerowy, w którym obliczenia są wykonywane współbieżnie z procesem zewnętrznym (otoczenia) w celu sterowania, nadzorowania lub terminowego reagowania na zdarzenia występujące w tym procesie (otoczeniu)*". Jeżeli oprogramowanie systemu sterowania jest zapisane w pamięci stałej stanowiącej część urządzenia sterującego (tzn. jego zmiana wiąże się z wymianą bądź przeprogramowaniem pamięci PROM), to o takim systemie sterowania mówi się, że jest „wbudowany"[6].

Współczesne środowisko ICS może mieć wbudowanych wiele urządzeń połączonych poprzez protokół IP. Tym urządzeniom brakuje zwykle mocy obliczeniowej do obsługi zabezpieczeń użytkowanych w tradycyjnych systemach informacyjnych. Poza tym używa się w nich specjalizowanego firmware, systemów operacyjnych czasu rzeczywistego oraz firmowych

[5] Patrz np. raport firmy CyberX za rok 2019 dostępny pod: https://cyberx-labs.com/resources/risk-report-2019/ (dostęp 22.05.2020). Dane opracowano na podstawie badania ponad 850 podmiotów z całego świata.

[6] W przypadku instalacji systemów wbudowanych na platformach pływających, latających lub jeżdżących używa się często określenia „systemy pokładowe".

(prawnie zastrzeżonych) protokołów, takich jak Profibus, COTP, TPKT Modbus, czy EtherNet/IP. W odróżnieniu od systemów informacyjnych, pierwszoplanowym zadaniem z zakresu bezpieczeństwa dla systemu składającego się z takich urządzeń jest utrzymanie jego integralności i dostępności, a nie zapewnienie ochrony danych i prywatności.

Zagadnienia bezpieczeństwa ICS związane z przesyłaniem sygnałów sterujących i danych produkcyjnych, w zasadzie od początku ich zaistnienia, są dowiązywane do problemów bezpieczeństwa infrastruktury krytycznej[7], a ostatnio także do modnej tematyki łańcucha dostaw [15]. Ma to odzwierciedlenie w tworzonych rozwiązaniach prawnych, publikacjach naukowych, szkoleniach itp. Przykład takiego podejścia daje chociażby ENISA (*European Union Agency for Network and Information Security*). ENISA w 2014 roku ustanowiła grupę zainteresowanych stron dla problematyki sieci przemysłowych (*ICS Stakeholder Group*). Jej celem jest dostarczenie użytkownikom i ekspertom od ICS/SCADA platformy wymiany poglądów oraz możliwości opracowywania i rozpowszechniania nowych idei podnoszących poziom bezpieczeństwa przemysłowego w UE[8]. Przykłady takich opracowań eksperckich to [13] i [14]. Pierwsze z nich dotyczy wyzwań i rekomendacji związanych z Industry 4.0 Cybersecurity. Drugie z kolei, oprócz przeglądu publikacji i przedsięwzięć ENISY (do roku 2015) w dziedzinie ICS, zawiera wyniki oceny[9] ośmiu krajów UE (w tym Polski) pod względem dojrzałości wdrożonych w infrastrukturze krytycznej państwa rozwiązań z zakresu bezpieczeństwa przemysłowego.

Wzmiankowane powyżej zagadnienia były także przedmiotem zainteresowania już przed ponad dwunastoma latami w ówczesnym Instytucie Automatyki i Robotyki[10] Wydziału Cybernetyki WAT (patrz np. [6]-[9]). Można zatem powiedzieć, że niniejszy artykuł jest powrotem po długiej przerwie do analizowanych kiedyś zagadnień, przy czym powrót ten wiąże się m.in. z przeświadczeniem autora, że opisywane tu zagadnienia powinny zostać włączone do procesu dydaktycznego w obszerniejszym niż dotąd zakresie, szczególnie na takich specjalnościach, jak „bezpieczeństwo systemów teleinformatycznych", „cyberobrona" czy „bezpieczeństwo cybernetyczne". Wiedza przekazywana studentom powinna obejmować:

[7] Patrz np. standardy NERC-CIP (CIP − *Critical Infrastructure Protection*) oraz [32].

[8] *Terms of reference for an ENISA ICS Security Stakeholder Group* − https://resilience.enisa.europa.eu/ics-security/EICSSGTermsofReference.pdf

[9] Ocena bazowała na dziewięciu kryteriach, przydzielonych (po trzy) do trzech grup: prawo lokalne, wsparcie operatorów usług krytycznych przez państwo, lokalne warunki eksploatacji i rozwoju systemów ICS-SCADA.

[10] Obecnie Instytut Teleinformatyki i Cyberbezpieczeństwa.

1. **Zalecenia normatywne**, które powinny być dla inżyniera podstawowymi elementami ukierunkowującymi jego działania przy projektowaniu, konstrukcji, wdrażaniu i ocenie rozwiązań i produktów, w tym przypadku z zakresu bezpieczeństwa *Operational Technology*. Jako podstawę proponuje się zapoznanie studentów z normą IEC 62443 oraz *The CIS Critical Security Controls for Effective Cyber Defense* (w wersji dla sieci i systemów przemysłowych).
2. Znajomość **sposobów realizacji celowych zagrożeń**[11] dla infrastruktury przemysłowej, w tym jej zasobów informacyjnych (w szczególności danych produkcyjnych i sterujących) oraz **znajomość metod i narzędzi** umożliwiających skuteczne przeciwdziałanie takim realizacjom. Jako podstawę proponuje się zapoznanie studentów z rozbudowanym frameworkiem MITRE ATT&CK w wersji dla sieci i systemów przemysłowych. Narzędzie to jest obecnie podstawą działań w zakresie bezpieczeństwa informacyjnego prowadzonych przez wiele uznanych firm z branży „bezpieczeństwa".
3. Tak zwane **„dobre praktyki"** opracowane przez uznane organizacje oraz stosowane i doskonalone w praktyce na całym świecie przez firmy zajmujące się zabezpieczeniem zasobów informacyjnych. Jako podstawę proponuje się zapoznanie studentów z „dobrymi praktykami" dotyczącymi zabezpieczania sieci i systemów przemysłowych, opublikowanymi [16] przez *Bundesamt für Sichercheit in der Informationstechnik*.

Wymienione trzy elementy nauczania: norma IEC 62443 oraz standard *The CIS Critical Security Controls for Effective Cyber Defense*, MITRE ATT&CK w wersji dla sieci i systemów przemysłowych oraz „dobre praktyki" opracowane przez *Bundesamt für Sichercheit in der Informationstechnik* są przedstawione w kolejnych rozdziałach niniejszego artykułu.

2. Normy, standardy i zbiory „dobrych praktyk" dotyczące bezpieczeństwa sieci przemysłowych

Zamieszczona w pracy [2] tabela nr 8: *Top 10 Regulations, Standards, Best Practices Used* przedstawia następujący ranking (z prawej strony procent respondentów, którzy wskazali dany standard, regulację lub zbiór dobrych praktyk):

1. NIST CSF (Cyber Security Framework)	38.1%
2. ISO 27000 series	32.0%

[11] Potocznie nazywanych atakami.

3. **NIST 800-53**	31.4%
4. **NIST 800-82**	30.9%
5. **ISA/IEC 62443**	30.4%
6. CIS Critical Security Controls	29.9%
7. **NERC CIP**	23.7%
8. GDPR	15.5%
9. C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10. NIS Directive (EU)	8.3%.

Badaniem objęto 338 respondentów, przy czym większość (ok. 70%) pochodziła z USA i Kanady i ten fakt należy mieć na uwadze przy dyskusji popularności konkretnych regulacji, standardów czy zbiorów dobrych praktyk. Warto też zauważyć, że do jednego worka wrzucono opracowania o różnych profilach:

- NIST CSF [36] jest opracowaną przez organ standaryzacyjny USA, w odpowiedzi na regulacje prawne administracji rządowej, ogólną metodyką zabezpieczania infrastruktury krytycznej państwa w zakresie „cybersecurity". W jej ramach ICS są jednym z zabezpieczanych elementów[12].
- Seria ISO 27000 dotyczy bezpieczeństwa informacji w systemach informacyjnych, w tym budowania systemów zarządzania bezpieczeństwem informacji (SZBI). Nie dotyczy bezpośrednio ICS.
- NIST 800-53 [31] jest standardem zawierającym zbiór zalecanych przez NIST zabezpieczeń i metodykę ich wdrożenia w systemach informacyjnych. Do ICS standard ten stosuje się przez dodatkowe uregulowania (NIST 800-82 [30]).
- CIS Critical Security Controls są zbiorem 20 dobrych praktyk zabezpieczania systemów informatycznych przed atakami (tylko!). Nie odnoszą się bezpośrednio do ICS – sposób zastosowania tych zaleceń do ICS jest podany w [35][13].
- NIS Directive (EU) jest dyrektywą europejską mającą na celu usprawnienie współpracy (przede wszystkim międzynarodowej) w zakresie incydentów dotyczących infrastruktury krytycznej. Nie odnosi się bezpośrednio do ICS.

[12] W oryginalnej publikacji [36] zapisano: (…) *The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on* information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), *or connected devices more generally, including the* Internet of Things (IoT).

[13] Patrz też część 5 tego artykułu.

- GDPR (*General Data Protection Regulation*), czyli po polsku RODO, dotyczy tylko jednej kategorii informacji – danych osobowych, które w systemach ICS mają marginalne znaczenie.
- **Tylko ISA/IEC 62443, NIST 800-82, NERC CIP dotyczą w całości i bezpośrednio ICS** (ten ostatni zbiór standardów jest ukierunkowany na ICS w elektroenergetyce).

W rozdz. 2.1 przedstawiono krótką charakterystykę serii norm IEC 62443, ponieważ to one obecnie stanowią światowy standard w dziedzinie bezpieczeństwa sieci i systemów przemysłowych oraz dlatego, że w tabeli 1 jest pokazane mapowanie zaleceń BSI na zalecenia tej serii norm. W rozdz. 2.2 z kolei scharakteryzowano *CIS Critical Security Controls* w wydaniu „przemysłowym".

2.1. Seria norm IEC 62443

Mająca za podstawę serię standardów ISA99 norma ISA/IEC 62443 jest normą wieloelementową [17]-[28] (patrz rys. 5; IACS – ang. *Industrial Automation and Control Systems*)[14]. Jej elementy układają się w następujące cztery „serie":

– Seria 1 zawiera wyjaśnienie używanych terminów, koncepcji oraz proponowane miary „bezpieczeństwa".
– Seria 2 dotyczy bezpieczeństwa czynności operacyjnych i eksploatacji.
– Seria 3 zawiera proponowane poziomy ochrony IACS oraz standaryzuje realizację zadań bezpieczeństwa dla OEM i integracji elementów przygotowywanych na zamówienie klienta.
– Seria 4 dotyczy „bezpiecznego" cyklu życia produktów, takich jak przełączniki, sterowniki, zapory sieciowe itp. oraz technicznych wymagań bezpieczeństwa dla tych produktów.

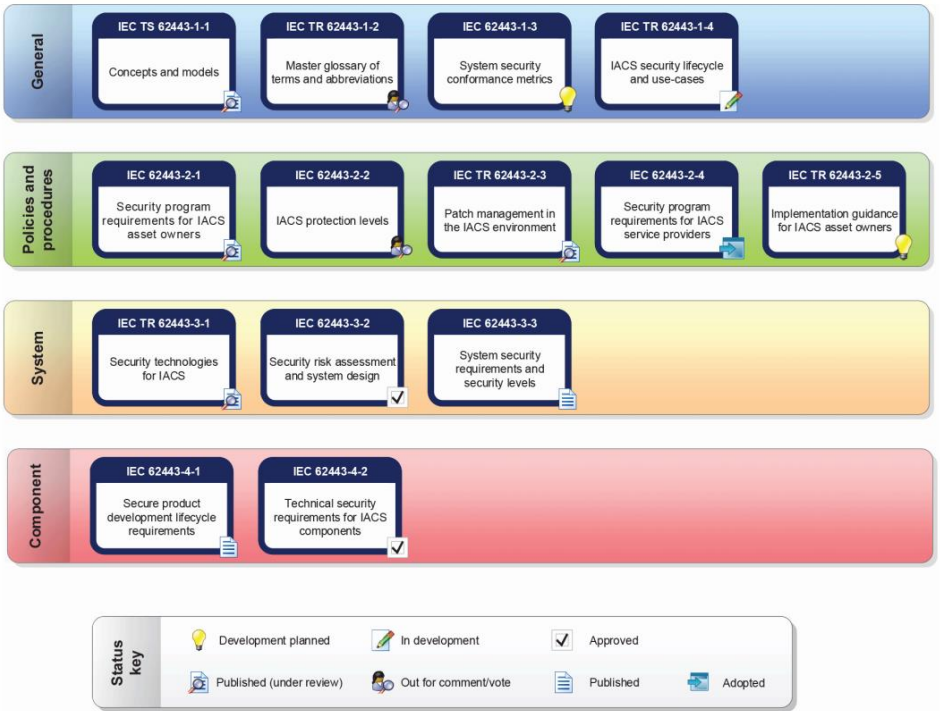
Polski Komitet Normalizacyjny wydał dotychczas (stan na maj 2020) następujące normy polskie serii IEC 62443[15]:

1. **PN-EN IEC 62443-4-1:2018-06 –** wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-1: *Wymagania cyklu rozwoju dotyczące tworzenia bezpiecznego produktu*.

   W tej części normy podano wymagania dla bezpiecznego procesu wytwarzania produktów wykorzystywanych w systemach sterowania i automatyki przemysłowej. Zdefiniowano bezpieczny proces tworzenia

[14] Ułatwia to np. jej aktualizację.
[15] Ale jak widać, nie przetłumaczono tych norm (oprócz tytułów) na język polski!

i rozwoju (SDL) oraz podano definicje wymagań bezpieczeństwa, bezpiecznego projektowania i bezpiecznego wdrożenia (wraz z wytycznymi dla procesów: kodowania, weryfikacji i walidacji, obsługi błędów i wprowadzania poprawek oraz wycofania produktu z użycia). Te wymagania mogą być stosowane do nowych lub istniejących projektów rozwojowych, obsługi i utylizacji sprzętu, programów lub oprogramowania produktów nowych lub istniejących. Wymagania te dotyczą projektantów i serwisantów produktów, nie dotyczą użytkowników produktów. Pełny wykaz wymagań jest podany w załączniku B normy.



Rys. 1. Stan procesu wydawniczego norm serii 62443 na koniec roku 2019 (za IEC 62443-4-2:2019)

2. **PN-EN IEC 62443-4-2:2019-08** – wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-2: *Wymagania techniczne bezpieczeństwa dla komponentów IACS*.

   W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla komponentów systemów sterowania powiązane z siedmioma podstawowymi

wymaganiami FR (*Foundational Requirement*)) opisanymi w IEC TS 62443-1-1[16]:

- FR-1 – identyfikacja i kontrola autoryzacji (IAC – *Identification and Authentication Control*),
- FR-2 – sterowanie użytkowe (UC – *Use Control*),
- FR-3 – nienaruszalność systemu (SI – *System Integrity*),
- FR-4 – poufność danych (DC – *Data Confidentiality*),
- FR-5 – ograniczenie przepływu danych (RDF – *Restricted Data Flow*),
- FR-6 – dokładna w czasie odpowiedź na zdarzenie (TRE – *Timely Response To Events*),
- FR-7 – dostępność zasobów (RA – *Resource Availability*).

Te wymagania są podstawą określania stopnia bezpieczeństwa systemu za pomocą tzw. poziomów bezpieczeństwa (SL – *Security Level*). Celem tej normy jest definicja przy użyciu kryteriów FR 1-7 bezpieczeństwa systemu sterowania na poziomie komponentu systemu sterowania (SL-C). Poziom bezpieczeństwa (SL-T) oraz poziom bezpieczeństwa osiągnięty (SL-A), nie są objęte zakresem tej normy.

3. **PN-EN IEC 62443-3-3:2020-01 –** wersja angielska: Przemysłowe sieci komunikacyjne − Bezpieczeństwo sieci i systemów − Część 3-3: *Wymagania dla systemu bezpieczeństwa i poziomów bezpieczeństwa*[17].

   W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla systemów sterowania przy użyciu kryteriów FR 1-7.

4. **PN-EN IEC 62443-2-4:2019-12 –** wersja angielska: Bezpieczeństwo w automatyce przemysłowej i systemach sterowania − Część 2-4: *Wymagania dla programu bezpieczeństwa dla dostawców usług IACS.*

   W tej normie określono wymagania bezpieczeństwa dla dostawców usług dla IACS, które to usługi mogą świadczyć np. podczas konserwacji systemów automatyki. Całość wymagań bezpieczeństwa spełnianych przez dostawcę usługi dla IACS jest nazywana *Programem Bezpieczeństwa*.

Zaproponowane w normie poziomy bezpieczeństwa (SL – ang. *Security Level*) to:

1. **SL 1** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji poprzez podsłuch lub przypadkową jej ekspozycję. Norma IEC 62443-3-3 specyfikuje

[16] Zawierającymi wymagania dla kompatybilności poziomów bezpieczeństwa SL-C (*Security Level-Control*).

[17] W oryginale: *system security requirements and security levels*. Czyli poprawnie powinno być: *wymagania na bezpieczeństwo systemu i poziomy bezpieczeństwa*.

37 wymagań, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.

2. **SL 2** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji słabo zmotywowanemu i mającemu ogólne umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu prostych metod i zaangażowaniu niewielkich środków. Norma IEC 62443-3-3 specyfikuje 23 wymagania, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.
3. **SL 3** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji średnio zmotywowanemu i mającemu ukierunkowane na IACS umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu zaawansowanych metod i zaangażowaniu średniej wielkości środków. Norma IEC 62443-3-3 specyfikuje 30 wymagań, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.
4. **SL 4** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji wysoce zmotywowanemu i mającemu ukierunkowane na IACS umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu zaawansowanych metod i zaangażowaniu dużych środków (zwykle będzie to podmiot instytucjonalny, np. wojsko lub służby państwowe).

Bardzo dobre wyjaśnienie praktycznego zastosowania koncepcji poziomów bezpieczeństwa jest zaprezentowane w pracy [1].

IEC 62443 *Cybersecurity Certification Programs* prowadzony jest w czterech kategoriach [3]:

1. Certyfikacji procesów – oceniane są procesy projektowania, integracji i testowania urządzeń i sieci ICS.
2. Certyfikacji urządzeń – oceniane są urządzenia, takie jak PLC, bramy sieciowe, zapory sieciowe, DCS.
3. Certyfikacji systemów – oceniane są złożone systemy zawierające różne urządzenia i sieci.
4. Certyfikacji osób:
   - certyfikat 1: *ISA/IEC 62443 Cybersecurity Fundamentals Specialist*;
   - certyfikat 2: *ISA/IEC 62443 Cybersecurity Risk Assessment Specialist*;
   - certyfikat 3: *ISA/IEC 62443 Cybersecurity Design Specialist*;
   - certyfikat 4: *ISA/IEC 62443 Cybersecurity Maintenance Specialist*.

Uzyskanie certyfikatów 1-4 uprawnia do tytułu *ISA/IEC 62443 Cybersecurity Expert*.

2.2. Zalecenia organizacyjne SANS

W 2008 roku administracja rządu USA (w tym m.in. *National Security Agency* oraz *SANS Institute*) w porozumieniu z członkami organizacji biznesowych opracowała zbiór zaleceń o nazwie *Consensus Audit Gudelines* (CAG). Zalecenia te zostały udostępnione publicznie przez instytut SANS w 2009 roku pod adresem *www.sans.org*. Przedstawiony w dokumencie CAG zbiór 20 zalecanych przedsięwzięć z zakresu ochrony przed działaniami intruzów (ang. *Critical Controls*) został uznany przez autorów opracowania za **minimalny, ale łatwy do szybkiego wdrożenia standard zabezpieczenia systemów i sieci komputerowych przed cyberatakami**[18]. Koncepcja CAG/CIS jest zbliżona do metodyki proponowanej przez NIST.

Najnowsza wersja CAG[19] to wersja 7.1. Od wersji 6.1 różni się zmianą miejsc niektórych zaleceń spośród pierwszej szóstki i zmianą nazwy zalecenia 17 na *Implement security Awareness and Training Programs*. Od wersji 6.0 zmieniła się nazwa dokumentu/projektu z *Consensus Audit Gudelines* (CAG) na *The CIS Critical Security Controls for Effective Cyber Defense*[20]. Udostępnianie kolejnych wersji artefaktów projektu odbywa się poprzez stronę *www.cisecurity.org*.

Dalej jest przedstawiona lista (wraz z tłumaczeniami) wszystkich punktów Critical Control dokumentu CAG v.6.1[21] (patrz też rys. 3 dla wersji 7.1). Liczby w nawiasach oznaczają liczbę zalecanych przedsięwzięć w ramach każdego z punktów[22].

1. *Inventory of Authorized and Unauthorized Devices* (6) – inwentaryzacja autoryzowanego i nieautoryzowanego sprzętu.
2. *Inventory of Authorized and Unauthorized Software* (4) – inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania.
3. *Secure Configurations for Hardware and Software* (7) – utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach.
4. *Continuous Vulnerability Assessment and Remediation* (8) – ciągłe monitorowanie podatności i ich minimalizowanie.

[18] CAG/CIS został wdrożony m.in. w norweskich elektrowniach – jest to obecnie standard uznany na całym świecie, stąd m.in. jego wybór do programu nauczania.

[19] W czasie przygotowywania niniejszego opracowania, tj. maj 2020 roku. Dostępna pod: https://learn.cisecurity.org/cis-controls-download. CAG jest też krótko opisany w rozdz. 6.1.3 w publikacji [4].

[20] CIS − *Center for Internet Security, Inc.*

[21] Punkty 1-10 dotyczą systemu, punkty 11-13 sieci, a punkty 14-20 aplikacji.

[22] W sumie daje to 149 punktów sprawdzeń do audytu zgodności.

5. *Controlled Use of Administrative Privileges* (9) – nadzór nad kontami administratorów i używaniem przywilejów administracyjnych.
6. *Maintenance, Monitoring, and Analysis of Audit Logs* (6) – utrzymanie, monitorowanie i analiza dzienników bezpieczeństwa.
7. *Email and Web Browser Protections* (8) – ochrona poczty elektronicznej i przeglądarek.
8. *Malware Defenses* (6) – ochrona przed programami i kodami złośliwymi.
9. *Limitation and Control of Network Ports* (6) – ograniczenie i kontrola portów, protokołów i usług sieciowych.
10. *Data Recovery Capability* (4) – zapewnianie zdolności do odzyskiwania danych.
11. *Secure Configurations for Network Devices* (7) – bezpieczna konfiguracja urządzeń sieciowych.
12. *Boundary Defense* (10) – stosowanie ochrony brzegowej.
13. *Data Protection* (9) – ochrona danych.
14. *Controlled Access Based on the Need to Know* (7) – kontrola dostępu na podstawie wiedzy koniecznej.
15. *Wireless Access Control* (9) – nadzór nad dostępem bezprzewodowym.
16. *Account Monitoring and Control* (14) – monitorowanie i kontrola kont użytkowników.
17. *Security Skills Assessment and Appropriate Training to Fill Gaps* (5) – ocena umiejętności personelu w zakresie bezpieczeństwa i odpowiednie szkolenia w celu eliminacji braków.
18. *Application Software Security* (9) – zapewnianie bezpieczeństwa aplikacji.
19. *Incident Response and Management* (7) – reagowanie na incydenty i zarządzanie incydentami.
20. *Penetration Tests and Red Team Exercises* (8) – wykonywanie testów penetracyjnych i ćwiczeń zespołów typu Red Team.

Publikacja [35] jest poradnikiem, jak zalecenia CIS przystosować do ICS. W publikacji tej każde z zaleceń (Critical Controls) jest jednolicie opisane. Na opis składają się zawsze trzy części: uzasadnienie stosowania (*Introduction*), zakres stosowania (*Applicability*) oraz dodatkowe wskazówki/ rozważania (*Considerations*). Przykład jest zamieszczony na rysunku 2.

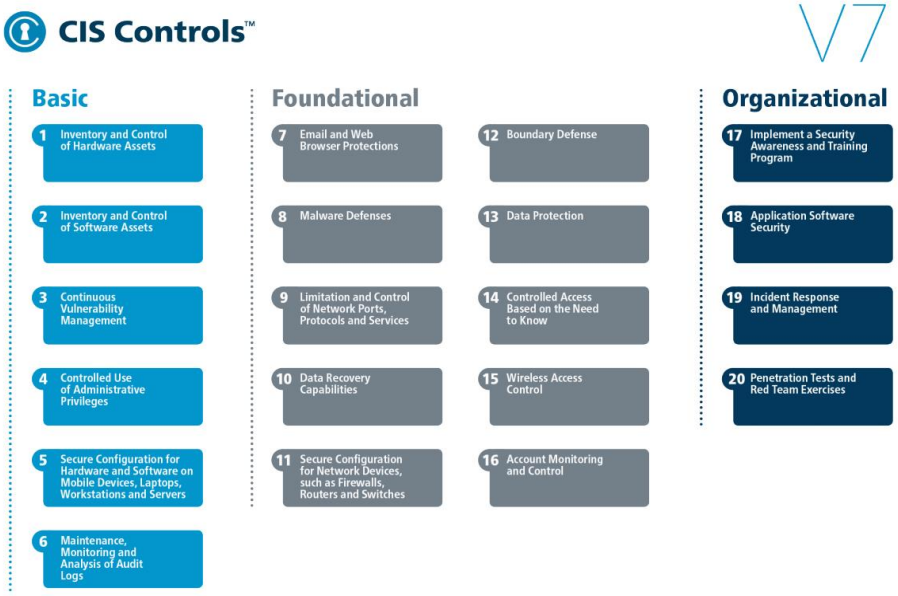
Każde zalecenie, traktowane także z innej perspektywy jako tzw. *punkt kontrolny*, zawiera wszystkie lub część przedstawionych dalej elementów, z których każdy opisuje pewne zagadnienia zabezpieczenia systemu w zakresie danego punktu kontrolnego lub wdrażania w organizacji zaleceń tego punktu:

CIS Control 11 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually these networks focus on availability and are architected with real-time performance and redundancy requirements. Attack vectors, however, remain the same. Unsecure services, poor firewall configurations, and default credentials remain issues.
Applicability	Due to the availability requirements associated with the ICS environments, Sub-Controls relating to network traffic may not be applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure firewalls are configured to deny by default. • If a location is unmanned or if critical process data flows through a perimeter device, ensure redundancy exists or device failure won't prevent this data from being received by its intended destination. If the management environment is sufficiently isolated, then multifactor authentication may not be required to manage network devices. Adding multifactor requirements can limit the use of vendor supplied network monitoring solutions.

Rys. 2. Przykład opisu zaleceń CIS w wersji dla ICS [35]

1. *How do Attackers Exploit the Absence of this Control?* – możliwy sposób wykorzystania przez intruza niezabezpieczonej podatności opisanej w danym punkcie.
2. *How to Implement, Automate, and Measure the Effectiveness of this Control?* – zalecenia odnośnie do minimalizowania danej podatności.
3. *Associated NIST Special Publication 800-53 Revision 3, Priority 1 Controls* – powiązania z dokumentami NIST.
4. *Associated NSA Manageable Network Plan Milestones and Network Security Tasks* – powiązania z dokumentami NSA.
5. *Procedures and Tools to Implement and Automate this Control* – opis możliwości wspomagania za pomocą narzędzi i przedsięwzięć organizacyjnych procesu zabezpieczania.
6. *Control xx Metric* – wymagania, jakie musi spełniać system, aby wypełniał założenia zawarte w danym punkcie.

7. *Control xx Test* – propozycje sprawdzeń, jakie muszą być przeprowadzone, aby ocenić implementację danego punktu CAG w praktyce biznesowej organizacji.
8. *Control xx Sensors, Measurements and Scoring* – propozycje sposobu realizacji i oceny sprawdzeń opisanych w punkcie Control xx Test.



Rys. 3. Zbiór zalecanych Critical Control w CAG v.7.1

3. Ataki na sieci i systemy przemysłowe

Podstawowy zbiór zagrożeń dla poprawnego działania sieci i systemów teleinformatycznych oraz sieci i systemów przemysłowych obejmuje:

1. Zagrożenia środowiskowe, tj. oddziaływanie:
   - ognia (np. pożary instalacji przemysłowych wywołanych uderzeniem pioruna),
   - wody (np. wylewy rzek powodujące podtopienia obiektów z infrastrukturą teleinformatyczną),
   - czynników mechanicznych (np. trzęsienia ziemi lub huragany niszczące infrastrukturę telekomunikacyjną),
   - czynników biologicznych (np. wirusów, powodujących braki w personelu obsługującym sieci i systemy teleinformatyczne i przemysłowe) itp.
2. **Zagrożenia celowymi** lub błędnymi **działaniami człowieka.**

3. Tak zwane „siły wyższe” inne niż zagrożenia środowiskowe (np. ustanowienie złych przepisów prawa przez ustawodawcę).

Wspomniane w tytule rozdziału „ataki” to forma realizacji zagrożenia celowymi działaniami człowieka. Cennym źródłem wiedzy o możliwościach ataków na zasoby informacyjne oraz sieci i systemy teleinformatyczne jest strona *https://attack.mitre.org/*[23]. Zawiera ona podstronę:

https://collaborate.mitre.org/attackics/index.php/Main_Page[24]

z tabelą podsumowującą **ataki na sieci i systemy przemysłowe** (jej fragment jest zamieszczony na rysunku 4). Na kolejnych podstronach są szczegółowe opisy:

- 81 technik ataków na systemy ICS;
- 17 narzędzi programowych używanych do ataków na systemy ICS (strona aktualizowana 02.01.2020);
- 10 ujawnionych grup atakujących systemy ICS (strona aktualizowana 02.01.2020).

Należy podkreślić, że opisywany framework (bo tak jest traktowany MITRE ATT&CK) dotyczy jedynie sposobów realizacji (czyli ataków) jednego typu zagrożenia – celowych działań ludzi.

Również w dodatku C (*Threat Sources, Vulnerabilities, and Incidents*) standardu NIST SP 800-82 rev. 2 zamieszczony jest opis 16 incydentów dotyczących ICS (w tym 8 ataków). Opis jest doprowadzony do roku 2013.

Dane statystyczne pokazują także [2], jak grupują się incydenty bezpieczeństwa dla ICS związane z działaniami ludzi (dane na rok 2019). Wyróżnia się incydenty związane z[25]:

1. Dostępem fizycznym (np. poprzez USB lub bezpośredni fizyczny dostęp do urządzenia, w szczególności do jego panelu sterującego) 56,3%.
2. Dostępem zdalnym (obejście zabezpieczeń wbudowanych w architekturę ICS) 40,6%.
3. Zaufanym dostępem zdalnym (dostęp zaufanego podmiotu bez naruszenia zabezpieczeń technicznych) 37,5%.
4. Działaniami serwisowymi i konsultacjami (skutki: nierozpoznane zmiany w konfiguracji) 34,4%.
5. Łańcuchem dostaw (np. oprogramowanie lub sprzęt niezgodne ze specyfikacjami) 18,8%.

[23] Dostęp 16.05.2020.

[24] Dostęp 16.05.2020; strona aktualizowana 04.03.2020.

[25] Podane na końcu każdego punktu wartości procentowe informują, jaki procent respondentów badania prowadzonego przez SANS wskazał na daną grupę.

The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View

Rys. 4. Fragment tabeli podsumowującej ataki na systemy ICS (ze strony https://collaborate.mitre.org/attackics/index.php/Main_Page).

4. Kompendium niemieckiego urzędu ds. bezpieczeństwa informacyjnego

Niemiecki urząd ds. bezpieczeństwa informacyjnego (BSI − *Bundesamt für Sichercheit in der Informationstechnik*; https://www.bsi.bund.de) wydał Kompendium [16], w którym, oprócz podstawowych zagadnień bezpieczeństwa ICS, w rozdziale 5 opisano 73 „najlepsze praktyki" w zakresie zapewniania bezpieczeństwa ICS rekomendowane przez ww. urząd. Praktyki te przyporządkowano do pięciu następujących grup:

1. Podstawowe przedsięwzięcia (ang. *first steps*; praktyki 1-6; rozdz. 5.2).
2. Procesy i zasady bezpieczeństwa (ang. *security-specific processes/policies*; praktyki 7-18; rozdz. 5.3).
3. Wybór (zakup) systemów i ich komponentów oraz związanych z nimi dostarczycieli usług serwisowych i integratorów (ang. *selection of the used systems and components as well as of the assigned service providers and integrators*; praktyki 19-30; rozdz. 5.4).
4. Bezpieczeństwo konstrukcyjne i fizyczne (ang. *constructional and physical securing*; praktyka 31; rozdz. 5.5).
5. Przedsięwzięcia techniczne (ang. *technical measures*; praktyki 32-73; rozdz. 5.6).

Te zalecenia zapisano w zwarty sposób w tabeli 7 Kompendium zatytułowanej: *Comparison of the best practices with IEC 62443, VDI/VDE*[26] *2182, NERC CIP*[27] *and DHS*[28] *Best Practices*. Zgodnie z tytułem, rekomendowane „najlepsze praktyki" BSI są w tej tabeli mapowane na zalecenia (nazywane tutaj też „najlepszymi praktykami") wymienionych norm i standardów. Tabela 1 to autorski wariant wspomnianej tabeli 7 z Kompendium, z własnymi komentarzami i mapowaniem na zalecenia normy IEC 62443.

[26] Verein Deutscher Ingenieure/Verband der Elektrotechnik Elektronik Informationstechnik.

[27] North American Electric Reliability Corporation Common Industrial Protocol.

[28] Department of Homeland Security.

Tab. 1. Zalecenia Bundesamt für Sichercheit in der Informationstechnik (BSI) z zakresu zabezpieczania sieci i systemów przemysłowych.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
1	Właściciele zasobów powinni ustanowić organizację zarządzania i kontrolowania ról i odpowiedzialności w zakresie bezpieczeństwa elementów ICS.	2-1 chapter A.3.2.3 2-1 chapter 4.3.2.3 2-1 chapter 4.3.2.3	Dotyczy wszystkich aktorów mających styczność z elementami ICS, np. dostawców produktów.
2	Zadbać o właściwe wytwarzanie i zarządzanie dokumentacją ICS.	2-1 chapter A.3.4.4 2-1 chapter 4.2.3.13	Należy opisać cykl życia dokumentacji.
3	Utworzyć SZBI dla informacji wykorzystywanych przez ICS.	Complete 2-1	**S**ystem **Z**arządzania **B**ezpieczeństwem **I**nformacji (SZBI).
4	Utrzymywać plan sieci (fizyczny i logiczny), na którym jest uwidocznione rozmieszczenie elementów ICS.	2-1 chapter A.3.4.2.3.3 2-1 chapter 4.2.3.5	
5	Utrzymywać w celu zapewnienia spójności listę eksploatowanego oprogramowania i listę plików konfiguracyjnych dla elementów ICS.	2-1 chapter 4.2.3.4 3-1 chapter 8.7	
6	Wytworzyć, utrzymywać i udostępniać zainteresowanym dokumentację operacyjną dla administratorów i użytkowników ICS.	2-1 chapter A.3.3.5	Ang. *Administration and user manual*.
7	Wdrożyć wewnętrzne zasady projektowania i integracji (z zakupionymi ICS) samodzielnie wytworzonego oprogramowania.	2-1 chapter 4.3.4.3.1 2-1 chapter 4.3.4.3.3 2-1 chapter 4.3.4.3.4 2-1 chapter 4.3.4.3.5	
8	Zadbać o bezpieczne wycofanie z użycia sprzętu.	2-1 chapter 4.3.3.3.9	Np. twardych dysków.
9	Chronić raporty audytowe.		
10	Właściciele zasobów, integratorzy i dostawcy powinni opracować i udokumentować odpowiednie procedury operacyjne.		Wytwarzania aplikacji, instalowania poprawek, konfigurowania itd.
11	Należy zarządzać zmianami.	2-1 chapter A.3.4.3.6 2-1 chapter 4.3.4.3.2	Np. osoba zalecająca zmianę nie powinna jej implementować
12	Zapewnić nadzór nad bezpieczeństwem i ciągłe monitorowanie stanu bezpieczeństwa.	2-1 chapter A.3.4.5 2-1 chapter 4.3.4.5 2-1 chapter 4.3.3.3.8	Ang. *Security monitoring*.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
13	Opracować i wdrożyć plan zapewniania biznesowej ciągłości działania.	2-1 chapter A.3.2.5 2-1 chapter A.3.4.3.8 2-1 chapter 4.3.2.5 2-1 chapter 4.3.4.3.9	Ang. *Business Continuity Plan* (BCP).
14	Dbać o regularne szkolenie personelu.	2-1 chapter A.3.2.4 2-1 chapter 4.3.2.4	
15	Właściwie zarządzać personelem, aby uniknąć związanych z nim naruszeń zasad bezpieczeństwa.	3-1 chapter 10.3, 2-1 chapter A.3.3.2 2-1 chapter 4.3.3.2	Ang. *Personnel security.*
16	Opracować i wdrożyć procedury zatrudniania, zmiany stanowiska i zwalniania pracowników.	2-1 chapter 4.3.3.2	
17	Przeprowadzać regularnie audyty bezpieczeństwa sieci i elementów ICS.	2-1 chapter A.3.4.2.5.4 2-1 chapter 4.2.3.10 2-1 chapter 4.4.2.2	
18	Testować komponenty (ICS) przed instalacją.	2-1 chapter A.3.4.3.5 2-1 chapter A.3.4.2.4.2 2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.1	
19	Włączyć do kontraktów z dostarczycielami produktów, zewnętrznymi właścicielami zasobów itp. klauzulę o zachowaniu tajemnicy.		Ang. *Non-disclosure agreement.*
20	Poinformować integratora systemu o obowiązujących wymaganiach bezpieczeństwa.	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	
21	Uwzględnić w analizie ryzyka specyfikację bezpieczeństwa dostarczoną przez integratora systemów ICS.	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	
22	Wymagać od produktów ICS odporności na błędy w oprogramowaniu i sprzęcie.	2-1 chapter A.3.4.2.4.2	W przypadku ujawnienia wady w trakcie działania produktu, musi on zachować się w ustalony sposób.
23	Nabywane produkty ICS muszą być wytworzone zgodnie z uznanymi/obowiązującymi standardami i umożliwiać współdziałanie z innymi produktami zgodnymi z tymi standardami.		Ang. *Compatibility.*

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
24	Sprzedający powinien dostarczyć produkt ICS z usuniętymi lub dezaktywowanymi funkcjami, które nie były wyspecyfikowane w zamówieniu.		Takie działanie musi być udokumentowane.
25	Dane dostępowe do komponentów ICS, po dostarczeniu przez sprzedającego, muszą być zmienione.	2-1chapter A.3.3.5.3.13	Patrz też 46.
26	Sprzedający powinien dostarczyć produkt z włączonymi funkcjami bezpieczeństwa, odpowiednio skonfigurowany oraz podać status zaktualizowania (ang. *patch status*).		Dostarczony produkt powinien być utwardzony (ang. *hardened*).
27	Wszystkie zainteresowane strony powinny przedstawić strategię długoterminowego zapewniania bezpieczeństwa instalacji przemysłowej.		
28	Nabywane komponenty ICS powinny być wyposażone w oprogramowanie antywirusowe lub powinny wspierać działanie takiego oprogramowania.		
29	**Musi być zachowana zgodność poziomów bezpieczeństwa ICS i systemu zdalnej obsługi tego ICS.**	2-1 chapter A.3.3.6.5.3 3-1 chapter 7.4	Patrz też 32 i 68 **BARDZO WAŻNE ZALECENIE!**
30	Muszą być sprecyzowane i zaimplementowane wymagania bezpieczeństwa dla urządzeń polowych		Urządzenia polowe (ang. *field devices*) – czujniki i elementy wykonawcze.
31	Zapewnić odpowiednią ochronę fizyczną komponentom ICS.	3-1 chapter 10.2 2-1 chapter A.3.3.3 2-1 chapter 4.3.3.3	Dotyczy budynków, pomieszczeń i szaf z urządzeniami.
32	Zapewnić segmentację sieci ICS.	2-1 chapter A.3.3.4 2-1 chapter A.3.4.2.3.3 2-4 chapter 4.3.3.4	Połączenia pomiędzy segmentami mogą być nawiązywane tylko od strony segmentu o wyższym poziomie ochrony.
33	Zabezpieczyć wszystkie zewnętrzne interfejsy do ICS.	2-1 chapter A.3.3.6.5.3	Patrz też: 2, 4, 29, 73.
34	Zaleca się statyczną konfigurację sieci.		
35	Wszystkie komponenty w jednym segmencie sieci powinny być zabezpieczone na tym samym poziomie.	2-1 chapter A.3.4.2.3.3	

Lp.	**Zalecane praktyki** (ICS Security Compendium v.1.23)	**Odpowiednik w normie IEC 62443**	**Komentarze**
36	Dążyć do niezależności operacji w poszczególnych segmentach ICS (utrata połączenia pomiędzy segmentami nie powinna mieć wpływu na produkcję lub wpływ powinien być minimalny).		
37	Poprawnie zabezpieczyć technologie bezprzewodowe używane w sieciach i systemach ICS.		
38	Do logicznej separacji segmentów sieci ICS używać sprzętowych zapór sieciowych.	3-1 chapter 6.2	Ang. *Firewalls.*
39	O ile to możliwe, na każdym komponencie ICS powinna być zainstalowana programowa zapora osobista.	3-1 chapter 6.3	Ang. *Host-based firewalls*.
40	Rozważyć użycie diód danych (ang. *Data diode; one-way gateway*).		
41	Zapewnić odpowiednią separację logiczną za pomocą VLAN-ów i separację fizyczną (na poziomie urządzeń) dla segmentów sieci z różnymi wymaganiami bezpieczeństwa.	3-1 chapter 6.4	
42	Rozważyć zaimplementowanie *Intrusion Detection System* (IDS) i/lub *Intrusion Prevention System* (IPS); zalecane jedynie dla dużych organizacji.	3-1 chapter 8.4	Na każdym urządzeniu ICS powinien być zainstalowany HIDS (*Host-IDS*).
43	Do realizacji zadań administrowania siecią lub zadań krytycznych ze względu na bezpieczeństwo używać tylko bezpiecznych protokołów (np. SSH, SFTP, HTTPS).		Lub protokołów dodatkowo zabezpieczonych kryptograficznie, np. SSL/TLS.
44	W sieciach ICS używać serwera DNS przeznaczonego do obsługi tylko tych sieci, odseparowanego od serwerów DNS z innych sieci (np. biurowych).		W celu utrzymania wysokiej dostępności, serwery DNS powinny być zdublowane.
45	Zapewnić synchronizację czasu (sygnałem czasu z zaufanego źródła).		Zalecane: Network Time Protocol lub IEEE 1588.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
46	Zaleca się usuwanie domyślnych kont i zmianę domyślnego hasła natychmiast po instalacji i sprawdzeniu poprawności działania urządzenia lub programu.	2-1 chapter 3.3.5.3.9 2-1 chapter 4.3.3.5.5 2-1 chapter 4.3.3.5.7 2-1chapter A.3.3.5.3.13	
47	Starać się przydzielić osobom obsługującym urządzenia ICS indywidualne konto w celu jednoznacznego rozliczania wykonanych czynności.	2-1 chapter A.3.3.5.3.7 2-1 chapter 4.3.3.5.2	W środowisku ICS jest to często niemożliwe.
48	Usunąć niepotrzebne oprogramowanie i usługi z komponentów ICS.		
49	Odpowiednio zmienić ustawienia domyślne.	2-1chapter A.3.3.5.3.13	
50	Dostroić do potrzeb konfigurację sprzętu.		Niepotrzebne porty USB, napędy CD/DVD itp. usunąć lub zablokować.
51	Zablokować nieograniczony dostęp do Internetu z poziomu sieci ICS.		
52	Opracować i wdrożyć procedurę aktualizacji i wgrywania poprawek do oprogramowania.	2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.7 2-1 chapter 4.3.4.5.3 2-1 chapter A.3.4.2.3.5	
53	Opracować i wdrożyć procedurę postępowania w przypadku zakończenia wsparcia produktu przez dostawcę.	2-1 chapter A.3.4.2.3.5	
54	Wybrać, na podstawie wyników analizy ryzyka, sposób i metodę uwierzytelniania w sieciach ICS użytkowników i usług.	2-1 chapter A.3.3.6 2-1 chapter 4.3.3.6 3-1 chapter 5.3 3-1 chapter 5.4 3-1 chapter 5.5 3-1 chapter 5.6 3-1 chapter 5.7 3-1 chapter 5.10	
55	Opracować zasady i wdrożyć procedury techniczne i organizacyjne posługiwania się hasłami.	3-1 chapter 5.9	
56	Zapobiegać nieautoryzowanemu dostępowi do systemu.		Każdy dostęp powinien być udokumentowany i rozliczalny: kto, co, kiedy.

Lp.	**Zalecane praktyki** (ICS Security Compendium v.1.23)	**Odpowiednik w normie IEC 62443**	**Komentarze**
57	W procesie autoryzacji uprawnienia przydzielać podmiotom zgodnie z zasadą „wiedzy koniecznej" i „minimalnego środowiska pracy".	2-1 chapter A.3.3.5 2-1 chapter A.3.3.7 2-1 chapter 4.3.3.5	Inna nazwa: zasada najmniejszych przywilejów.
58	Używać narzędzi/algorytmów kryptograficznych odpowiadających aktualnemu stanowi wiedzy w dziedzinie kryptologii.	3-1 chapter 7.2 3-1 chapter 7.3 3-1 chapter 7.4 3-1 chapter 5.2	
59	Jeżeli jest możliwa i dopuszczalna instalacja oprogramowania antywirusowego na komponentach ICS i dopuszcza to także dostawca produktu (ICS), to takie oprogramowanie należy zainstalować wraz z automatyczną aktualizacją sygnatur wirusów.	3-1 chapter 8.3 2-1 chapter 4.3.4.3.8	
60	Opracować i wdrożyć rozwiązania alternatywne, gdy nie można zainstalować oprogramowania antywirusowego.		Dotyczy to często sterowników, PLC, urządzeń polowych.
61	Bazując na rekomendacjach dostawcy oprogramowania antywirusowego i dostawcy produktu (ICS), zapewnić bezpieczną konfigurację oprogramowania antywirusowego.		Proces instalacji i konfiguracji powinien być udokumentowany dla każdego komponentu ICS.
62	Sygnatury wirusów dla oprogramowania antywirusowego nie powinny być pobierane bezpośrednio z Internetu tylko dystrybuowane przez centralny serwer (usługa dystrybucji sygnatur) umieszczony w DMZ.		
63	Zapewnić niezwłoczne pobieranie uaktualnionych baz sygnatur.	2-1 chapter A.3.4.2.4.2	
64	Rozważyć zastosowanie oprogramowania antywirusowego na zaporze sieciowej (*virus wall*, działający w warstwie 7) w celu sprawdzania ruchu pomiędzy sieciami pod kątem przenoszenia malwaru.		Application Level Gateway zwykle nie wspierają protokołów specyficznych dla ICS.
65	Dopuszczać do użytku tylko to oprogramowanie i tylko te jego działania (*behaviour*), które zostały wcześniej zaakceptowane (ang. *whitelisting*).		Nie jest to zamiennik oprogramowania antywirusowego!

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
66	Opracować i wdrożyć zasady postępowania z nośnikami wymiennymi.		Te zasady muszą być znane wszystkim pracownikom.
67	Wymienne pamięci przed ich zintegrowaniem z sieciami lub urządzeniami ICS sprawdzić na testowym komputerze, tzw. *quarantine PC*.		
68	Opracować i wdrożyć zasady używania notebooków w celach serwisowych.		
69	Aktywować hasło do BIOS-u i dopuszczać bootowanie tylko z wybranego medium na wszystkich urządzeniach ICS.		
70	Dezaktywować funkcję autorun na wszystkich urządzeniach ICS.		
71	Opracować i wdrożyć strategię i zasady wykonywania kopii bezpieczeństwa.	2-1 chapter 4.3.4.3.9	Proces wykonywania kopii bezpieczeństwa nie może mieć wpływu na produkcję.
72	Opracować i wdrożyć zasady przechowywania kopii bezpieczeństwa.	2-1 chapter A.3.4.3.8	
73	Uaktywnić odpowiednie dzienniki zdarzeń i zapisywać w nich monitorowane zdarzenia.	3-1 chapter 8.2 3-1 chapter 8.6 3-1 chapter 8.7 3-1 chapter 8.8 2-1 chapter 4.3.3.5.8 2-1 chapter 4.3.3.6.4	Dotyczy wszystkich dzienników zdarzeń na wszystkich mających je urządzeniach.

5. Podsumowanie

W artykule przedstawiono te elementy wiedzy techniczno-organizacyjnej, które, zdaniem autora, powinny być podstawą nauczania zagadnień bezpieczeństwa z zakresu sieci i systemów przemysłowych na studiach wyższych. Nauczanie powinno być uzupełnione o podstawowe zagadnienia dotyczące obowiązujących rozwiązań prawnych, takich jak ustawa *o Krajowym Systemie Cyberbezpieczeństwa* [33] (i towarzyszące jej rozporządzenia), która dotyczy operatorów usług kluczowych, czy RODO, żeby studenci mieli świadomość tego, jak nauczane zagadnienia techniczno-organizacyjne wpisują się w system prawny państwa. Należy

bowiem mieć na uwadze, że przy projektowaniu systemów zabezpieczeń, zapisy prawne, formalnie, są dla projektanta ograniczeniami projektowymi, które musi uwzględnić w specyfikacji wymagań projektowanego systemu.

Warto także podkreślić, że zabezpieczenie sieci przemysłowej powinno być elementem szerzej widzianego zabezpieczenia zakładu przemysłowego przed incydentami z zakresu bezpieczeństwa informacyjnego. Oznacza to na przykład, że dostawca zabezpieczeń dla sieci przemysłowej powinien umożliwiać ich integrację z rozwiązaniami nadrzędnymi typu SIEM (ang. *Security Information and Event Management*), w celu uzyskania jednolitego obrazu stanu bezpieczeństwa sieci i systemów teleinformatycznych (tzw. biurowych) oraz przemysłowych. Przekładając to na proces edukacji – nauczanie podstaw bezpieczeństwa informacyjnego powinno poprzedzać nauczanie bardziej specjalistycznych zagadnień, w tym tych związanych z ICS, co niestety nie zawsze ma miejsce w praktyce.

Literatura

1. DESRUISSEAUX D., *Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications*. Schneider Electric White Paper, 2018.
2. FILKINS B., WYLIE D.: *SANS 2019 State of OT/ICS Cybersecurity Survey*. ©2019 SANS™ Institute, June 2019.
3. GOBLE W., *Applying the Global Automation Standard IEC 62443 to protect against cyber threats*. Prezentacja. 2019.
4. LIDERMAN K.: *Bezpieczeństwo informacyjne*. *Nowe wyzwania*. WN PWN SA. Warszawa, 2017.
5. LIDERMAN K., *Bezpieczeństwo informacyjne*. WN PWN SA. Warszawa, 2012.
6. LIDERMAN K., *Ochrona informacji i obiektów w sieciach teleinformatycznych połączonych z systemami przemysłowymi – przegląd zagadnień*. Biuletyn IAiR WAT, nr 25, 2008, s. 85-107.
7. LIDERMAN K., ZIELIŃSKI Z.: *Ochrona informacji w połączonych sieciach przemysłowych i teleinformatycznych*. W: Huzar Z., Mazur Z. (red.): Zagadnienia bezpieczeństwa w systemach informacyjnych. WKŁ, Warszawa, 2008, s. 83-97.
8. LIDERMAN K., *Połączone sieci teleinformatyczne i sieci przemysłowe jako elementy infrastruktury krytycznej – zagrożenia i podstawowe standardy ochrony*. W: Cyberterroryzm – nowe wyzwania XXI wieku. Praca zbiorowa pod red. T. Jemioły, J. Kisielnickiego, K. Rajchela, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa, 2009, s. 244-260.

9. LIDERMAN K., *Audyt bezpieczeństwa sieci teleinformatycznych połączonych z systemami przemysłowymi − wytyczne do modyfikacji metodyki LP-A*. W: Zieliński Z. (red.): Systemy czasu rzeczywistego. Postępy badań i zastosowania. WKŁ, Warszawa, 2009, s. 299-308.
10. SZMUC T., MOTET G.: *Specyfikacja i projektowanie oprogramowania czasu rzeczywistego*. CCATIE, Katedra Automatyki AGH, Kraków, 1998.
11. ŻURAKOWSKI Z., *Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem*. Informatyka, nr 3, 1995, s. 20-28.
12. *21 Steps to Improve Cyber Security of SCADA Networks*. Office of Energy Assurance, U.S. Department of Energy. http://www.oe.netl.doe.gov/docs/prepare /21stepsbooklet.pdf (dostęp 16.05.2020).
13. ENISA: *Industry 4.0 Cybersecurity: Challenges&Recommendations*. May, 2019.
14. ENISA: *Analysis of ICS-SCADA Cyber Security Maturity Levels In Critical Sectors*. 2015.
15. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. U.S. GAO, 2004. http://www.gao.gov/new.items/d04354.pdf (dostęp 16.05.2020).
16. *ICS Security Compendium*. V. 1.23. Federal Office for Information Security (BSI). Germany, 2013.
17. IEC 62443-1-1: *Industrial communication networks - Network and system security – Part 1-1*: *Terminology, concepts and models* (IEC/TR 62443-1-1:2009).
18. ISA-62443-1-2: *Security for industrial automation and control systems – Master Glossary*. Draft 1. Edit 5. August, 2014 (ISA-TR62443-1-2).
19. ISA-62443-1-3: *Security for industrial automation and control systems – Part 1-3: Cyber security system conformance metrics*. Draft 1. Edit 19. October, 2015.
20. ISA-62443-2-1: *Security for industrial automation and control systems: Part 2-1: Industrial automation and control system security management system*. Draft 7. Edit 5. November 9, 2015.
21. ISA-62443-2-2: *Security for industrial automation and control systems: Implementation Guidance for and IACS Security Management System*. Draft 1. Edit 4. April, 2013.
22. IEC 62443-2-3: *Security for industrial automation and control systems: Part 2-3: Patch Management in IACS environment* (IEC /TR 62443-2-3:2015).
23. IEC 62443-2-4: *Security for industrial automation and control systems: Part 2-4: Security program requirements for IACS providers* (IEC 62443-2-4:2015).
24. ISA-62443-3-2: *Security for industrial automation and control systems: Security risk assessment for system design*. Draft 6. Edit 3. August 5, 2015.

25. IEC 62443-3-3: *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (IEC 62443-3-3: 2013).
26. IEC/NP 62443-4-1 *Industrial communication networks – Network and system security – Part 4-1: Product development requirements based on ISA-62443-04-01*. Draft 1. Edit 9. April, 2013.
27. ISA-62443-4-1 *Security for industrial automation and control systems Part 4-1: Secure product development life – cycle requirements*. Draft 3. Edit 11. March, 2016.
28. ISA-62443-4-2 *Security for industrial automation and control systems*. *Technical security requirements for IACS components.* Draft 2. Edit 4. July 2, 2015.
29. NERC: *Top 10 vulnerabilities of control systems and their associated mitigations*. 2006.
30. NIST Special Publication 800-82 Rev. 2: *Guide to Industrial Control Systems (ICS) Security*. May, 2015.
31. NIST Special Publication 800-53 Rev. 5: *Security and Privacy Controls for Federal Information Systems and Organizations*. August, 2017.
32. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z dn. 21.05.07).
33. Ustawa z dnia 5 lipca 2018 r. *o Krajowym Systemie Cyberbezpieczeństwa* (Dz. U. 1560).
34. US Industrial Control Systems Cyber Emergency Response Team: *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. September, 2016.
35. *Implementation Guide for Industrial Control Systems*. Version 7. CIS Controls™ https://www.cisecurity.org/controls/ (dostęp 22.05.2020).
36. NIST: *Framework for Improving Critical Infrastructure Cybersecurity* v.1.1. April 16, 2018. https://doi.org/10.6028/NIST.CSWP.04162018 (dostęp 22.05.2020).

ICS security – subject content proposal

ABSTRACT: The paper considers the issue of ICS security teaching. A brief ICS characteristic is given in the introduction. Background chapters present basic norms and standards (e.g.: IEC 62443 and *CIS Critical Security Controls for Effective Cyber Defense*), framework MITRE ATT&CK, as well as a set of „best practices" published by *Bundesamt für Sichercheit in der Informationstechnik*. The considered problem under is based on these elements.

KEYWORDS: Industrial Control System (ICS), IEC 62443, MITRE ATT&CK Framework, „best practices" for Operational Technology (OT)

Praca wpłynęła do redakcji: 16.06.2020 r.