Załącznik nr 6 – Wymogi Bezpieczeństwa dla LZO.

1. Bezpieczeństwo w Cyklu Życia LZO

SLC-1.1	Certyfikowany System Zarządzania Bezpieczeństwem
opis wymagania	Producent oraz wykonawca (dostawca) muszą posiadać i utrzymywać certyfikowany na zgodność z normą ISO/IEC 27001 system zarządzania bezpieczeństwem informacji. W przypadku Producenta zakres certyfikacji musi jawnie obejmować procesy projektowania, rozwoju oprogramowania, produkcji, inicjalizacji i utrzymania urządzeń. W przypadku Wykonawcy (jeśli nie jest Producentem), zakres musi obejmować procesy logistyki, bezpiecznego dostarczania oraz konfiguracji systemów AMI.
dyskusja	Certyfikat ISO/IEC 27001 jest formalnym, uznawanym międzynarodowo dowodem na to, że producent oraz wykonawca stosują najlepsze praktyki w zakresie zarządzania bezpieczeństwem informacji. Wymóg ten, zapewnia, że bezpieczeństwo jest integralną częścią całej organizacji i wszystkich procesów związanych z produktem, a nie tylko cechą samego urządzenia. Obejmując cały cykl życia, od projektu po utrzymanie, minimalizuje się ryzyko wystąpienia podatności na każdym etapie.
kryterium weryfikacji	Przedstawienie ważnego certyfikatu ISO/IEC 27001 wydanego przez akredytowaną jednostkę certyfikującą. Zakres certyfikacji (Statement of Applicability) musi jednoznacznie potwierdzać objęcie wszystkich wymienionych procesów (projektowania, rozwoju, produkcji i utrzymania urządzeń AMI), właściwych dla roli danego podmiotu w projekcie AMI.

SLC-1.2	Udokumentowany i Weryfikowalny Bezpieczny Cykl Rozwoju Oprogramowania
opis wymagania	Producent musi posiadać i stosować udokumentowany, bezpieczny cykl rozwoju oprogramowania (SSDLC). Proces ten musi obejmować co najmniej: analizę statyczną i dynamiczną kodu, zarządzanie komponentami oprogramowania (np. poprzez Software Bill of Materials - SBOM) oraz posiadać formalny proces zarządzania podatnościami. Całość dokumentacji musi być dostępna do weryfikacji. Każda wersja oprogramowania i firmware'u musi być jednoznacznie identyfikowalna (np. poprzez numer wersji i datę wydania), a każdy obraz

	oprogramowania powinien posiadać unikalną kryptograficzną wartość skrótu (hash).
dyskusja	Bezpieczeństwo "by design" jest fundamentalną zasadą nowoczesnego cyberbezpieczeństwa. Wymóg posiadania i stosowania SSDLC przenosi odpowiedzialność za bezpieczeństwo na najwcześniejszy etap – projektowania i tworzenia oprogramowania. Zapewnia to, że luki w zabezpieczeniach są identyfikowane i eliminowane, zanim produkt trafi na rynek, a nie dopiero w fazie eksploatacji. Ze względu na ochronę własności intelektualnej oraz poufność technologiczną, weryfikacja artefaktów procesu może odbywać się w kontrolowanych warunkach, np. w trakcie audytu lokalnego u producenta, lub pod NDA.
kryterium weryfikacji	Producent przedstawi dokumentację opisującą proces SSDLC. Dokumentacja będzie zawierać opis stosowanych narzędzi (SAST, DAST), procedur zarządzania zależnościami (SBOM), politykę reagowania na podatności oraz sposób identyfikacji i wersjonowania komponentów (wraz z przykładami oznaczeń wersji i hashy). Przedstawione zostaną raporty z narzędzi SAST/DAST oraz dokument SBOM dla dostarczanego oprogramowania.

SLC-1.3	**Bezpieczne Praktyki Inżynierii Oprogramowania**
opis wymagania	Proces rozwoju oprogramowania musi być oparty na uznanych standardach bezpiecznego kodowania adekwatnych do platformy sprzętowej (np. CERT C, MISRA C 2023). Producent musi stosować narzędzia do statycznej (SAST) i dynamicznej (DAST) analizy kodu w celu eliminacji podatności oraz utrzymywać bezpieczny system zarządzania konfiguracją i wersjonowaniem oprogramowania.
dyskusja	Bezpieczeństwo "by design" jest fundamentalną zasadą nowoczesnego cyberbezpieczeństwa, wymaganą przez unijne regulacje, takie jak Cyber Resilience Act. Stosowanie narzędzi SAST i DAST pozwala na automatyczne wykrywanie powszechnych błędów programistycznych i podatności na wczesnym etapie rozwoju, co znacząco obniża koszty ich naprawy i ryzyko ich wykorzystania w środowisku produkcyjnym. Bezpieczne zarządzanie wersjami jest kluczowe dla zapewnienia integralności i identyfikowalności oprogramowania. Wskazane w wymogu standardy (MISRA, CERT) mają charakter przykładowy; producent jest zobowiązany wykazać stosowanie profesjonalnej metodyki kodowania adekwatnej do platformy sprzętowej.

kryterium weryfikacji	Producent przedstawi dokumentację opisującą proces bezpiecznego rozwoju oprogramowania (SSDLC). Dokumentacja będzie zawierać opis stosowanych standardów kodowania, narzędzi (SAST, DAST) oraz procedur zarządzania konfiguracją. Przedstawione zostaną zanonimizowane raporty z narzędzi SAST/DAST potwierdzające ich stosowanie w praktyce.

SLC-1.4	**Zarządzanie Łańcuchem Dostaw Komponentów**
opis wymagania	Producent musi stosować udokumentowany proces oceny i kwalifikacji komponentów zewnętrznych (sprzętu i oprogramowania). Komponenty mogą być użyte tylko, jeśli ich pochodzenie i integralność są potwierdzone (np. podpis cyfrowy, certyfikat dostawcy, zweryfikowane repozytorium, identyfikowalność komponentów sprzętowych).
dyskusja	Nowoczesne urządzenia składają się z wielu komponentów od różnych dostawców, co tworzy złożony łańcuch dostaw. Atak na ten łańcuch jest jednym z najpoważniejszych zagrożeń. Wymóg ten, podkreślany w Dyrektywie NIS2, zmusza producenta do wzięcia odpowiedzialności za bezpieczeństwo całego produktu, a nie tylko części, które sam wytworzył. Stosowanie np. Software Bill of Materials (SBOM) oraz Hardware Bill of Materials (HBOM) jest dobrą praktyką w tym zakresie. Weryfikacja techniczna (HBOM) powinna koncentrować się na elementach o wysokim ryzyku, czyli komponentach posiadających logikę cyfrową. Ze względu na ochronę własności intelektualnej oraz poufność technologiczną, dokumentacja HBOM/SBOM udostępniana jest pod NDA.
kryterium weryfikacji	Producent przedstawi udokumentowaną procedurę oceny i kwalifikacji dostawców oraz komponentów firm trzecich (software i hardware). Procedura musi opisywać sposób weryfikacji integralności (np. sprawdzanie sum kontrolnych, podpisów cyfrowych, certyfikaty dostawcy, identyfikowalność komponentów sprzętowych) oraz autentyczności komponentów. Na żądanie, producent udostępni listę komponentów firm trzecich (SBOM i HBOM) wraz z dowodami ich weryfikacji.

SLC-1.5	**Audytowalność Procesów Bezpieczeństwa**
opis wymagania	Producent oraz wykonawca (dostawca) urządzenia zgadzają się na okresowy audyt procesów bezpieczeństwa swojej organizacji.

dyskusja	Zapewnienie bezpieczeństwa infrastruktury AMI jest wspólną odpowiedzialnością producenta oraz wykonawcy (dostawcy) i operatora. Aby OSD mógł skutecznie zarządzać ryzykiem w całym cyklu życia systemu, musi mieć możliwość weryfikacji, czy procesy bezpieczeństwa deklarowane przez producenta oraz wykonawcę (dostawcę) są faktycznie i konsekwentnie stosowane. Wymóg ten formalizuje prawo OSD do przeprowadzania audytów, co jest standardową praktyką w zarządzaniu bezpieczeństwem łańcucha dostaw dla infrastruktury krytycznej. Audyt odbywa się w siedzibie producenta wykonawcy (dostawcy), pod NDA. Osoby audytujące muszą posiadać certyfikat Lead Auditor ISO/IEC 27001 oraz doświadczenie w audytowaniu systemów OT/AMI.
kryterium weryfikacji	Producent oraz wykonawca (dostawca) w ramach umowy zagwarantuje OSD (lub wskazanej przez niego, upoważnionej stronie trzeciej) prawo do przeprowadzania okresowych audytów procesów bezpieczeństwa wymienionych w wymaganiach SLC-1.1, SLC-1.2, SLC-1.3, SLC-1.4 oraz SLC-5.1. Zakres i częstotliwość audytów będą określone w umowie, a ich celem będzie weryfikacja zgodności faktycznie stosowanych praktyk z przedstawioną dokumentacją.

SLC-2.1	**Zaufany Moduł Sprzętowy i Bezpieczny Rozruch**
opis wymagania	Urządzenie musi być wyposażone w mechanizm bezpiecznego uruchamiania, który uniemożliwia start systemu z nieautoryzowanym oprogramowaniem. Weryfikacja integralności i autentyczności oprogramowania musi odbywać się przy użyciu wbudowanego, zaufanego elementu sprzętowego przechowującego klucz producenta.
dyskusja	Modyfikacja oprogramowania jest jednym z najpoważniejszych wektorów ataku. Bezpieczny rozruch zaimplementowany w sprzęcie gwarantuje, że na urządzeniu uruchamiane jest wyłącznie autentyczne, podpisane przez producenta oprogramowanie. Chroni to przed instalacją złośliwego kodu, który mógłby manipulować danymi pomiarowymi lub zakłócać pracę sieci. Wbudowany zaufany element sprzętowy - należy rozumieć jako dedykowany układ (np. TPM, HSM) lub funkcjonalność mikrokontrolera (np. TrustZone), przy założeniu spełnienia wymogu trwale wyłączonych interfejsów serwisowych modułu mikrokontrolera (ACC-4.3). Mechanizmy bezpiecznego rozruchu opisane w wymaganiach INT-2.2, INT-2.3.
kryterium weryfikacji	Proces uruchamiania urządzenia zakończy się niepowodzeniem (np. urządzenie przejdzie w stan błędu i nie uruchomi głównej aplikacji), jeśli którakolwiek część oprogramowania (firmware, bootloader, system operacyjny, aplikacja) nie przejdzie pomyślnie weryfikacji podpisu cyfrowego. Próba

	uruchomienia niepodpisanego obrazu oprogramowania musi zostać zablokowana. Zdarzenie nieudanego rozruchu zostanie zapisane w dzienniku zdarzeń (np. z wykorzystaniem mechanizmu bootloadera).

SLC-3.1	**Uwierzytelnienie i Weryfikacja Integralności Aktualizacji**
opis wymagania	Każdy pakiet aktualizacyjny (oprogramowanie układowe) musi być podpisany cyfrowo przez producenta. Urządzenie musi bezwzględnie zweryfikować ten podpis przed rozpoczęciem instalacji. Aktualizacje bez ważnego podpisu cyfrowego muszą zostać odrzucone. Proces aktualizacji oprogramowania układowego urządzenia (firmware update) może być zainicjowany wyłącznie przez uwierzytelnione konto z przypisaną rolą o uprawnieniach administracyjnych (np. asocjacja management).
dyskusja	Proces zdalnej aktualizacji, choć niezbędny do utrzymania bezpieczeństwa, stwarza ryzyko wgrania złośliwego oprogramowania. Wymóg weryfikacji podpisu cyfrowego gwarantuje, że urządzenie akceptuje aktualizacje pochodzące wyłącznie z autoryzowanego źródła (producenta). Jednocześnie, ograniczenie możliwości inicjowania aktualizacji do roli administratora (np. asocjacja management) zapobiega nieautoryzowanym próbom wgrania oprogramowania, nawet jeśli atakującemu udałoby się obejść inne zabezpieczenia.
kryterium weryfikacji	Urządzenie odrzuci i nie zainstaluje pakietu aktualizacyjnego, którego podpis cyfrowy jest nieprawidłowy, uszkodzony lub pochodzi od niezaufanego wystawcy podpisu cyfrowego. Zdarzenie nieudanej weryfikacji zostanie zapisane w dzienniku zdarzeń bezpieczeństwa. Inicjowanie aktualizacji będzie możliwe tylko z konta z rolą o uprawnieniach administracyjnych (np. asocjacja management).

SLC-3.2	**Ochrona przed Wycofaniem Wersji**
opis wymagania	Urządzenie musi implementować mechanizm uniemożliwiający instalację wersji oprogramowania starszej niż aktualnie zainstalowana, z wyjątkiem sytuacji autoryzowanych przez OSD.
dyskusja	Atakujący mogą próbować zainstalować starszą wersję oprogramowania, która zawiera znaną i już załataną podatność, aby ją wykorzystać. Mechanizm

	ochrony przed wycofaniem wersji (tzw. anti-rollback) blokuje ten wektor ataku, zapewniając, że na urządzeniu zawsze działa wersja oprogramowania co najmniej tak samo bezpieczna jak poprzednia.
kryterium weryfikacji	Próba instalacji pakietu aktualizacyjnego z numerem wersji niższym niż wersja aktualnie działająca na urządzeniu jest domyślnie odrzucana. Urządzenie zapisze to zdarzenie w dzienniku zdarzeń bezpieczeństwa. Jeśli określono tak w zamówieniu, urządzenie musi umożliwiać wymuszenie powrotu do wersji poprzedniej (N-1) poprzez specjalnie autoryzowane polecenie systemowe OSD.

SLC-3.3	**Bezpieczna Aktualizacja Oprogramowania**
opis wymagania	Urządzenie musi realizować proces aktualizacji oprogramowania w sposób, w którym nowa wersja oprogramowania jest aktywowana wyłącznie po pomyślnej weryfikacji integralności i kompletności. W przypadku błędu aktualizacji (np. błąd transmisji, przerwanie zasilania, niezgodność sum kontrolnych), nowa wersja nie może zostać aktywowana, a urządzenie musi kontynuować pracę na ostatniej znanej, stabilnej wersji oprogramowania.
dyskusja	Proces aktualizacji jest operacją krytyczną. Błąd w jego trakcie nie może prowadzić do trwałego uszkodzenia urządzenia. Urządzenie musi zapewniać ciągłość działania i odporność systemu na nieprzewidziane problemy, co jest kluczowe w infrastrukturze o długim cyklu życia.
kryterium weryfikacji	Symulacja nieudanej aktualizacji (np. poprzez przerwanie zasilania w jej trakcie) musi spowodować, że po ponownym uruchomieniu urządzenie będzie kontynuować normalną pracę. Urządzenie zapisze to zdarzenie w dzienniku zdarzeń.

SLC-3.4	**Zakres Aktualizacji Oprogramowania**
opis wymagania	Urządzenie musi mieć zapewnioną możliwość aktualizacji kluczowych komponentów oprogramowania, zarówno lokalnie, jak i zdalnie.
dyskusja	Zapewnienie możliwości aktualizacji kluczowych komponentów oprogramowania jest fundamentem długoterminowego bezpieczeństwa. Umożliwia to reagowanie na nowo odkryte podatności oraz adaptację do zmieniających się standardów (np. kryptograficznych). W przypadku urządzeń o architekturze oprogramowania typu "monolitycznego", wymóg ten realizowany jest poprzez możliwość wymiany całego obrazu

	oprogramowania (firmware), w którym zaimplementowano zaktualizowane kluczowe komponenty oprogramowania. Wymóg uwzględnia, że w LZO aktualizacja często polega na podmianie całego obrazu zawierającego poprawione komponenty, przy zachowaniu obostrzeń metrologicznych (WELMEC).
kryterium weryfikacji	Producent musi zapewnić możliwość zdalnej i lokalnej aktualizacji wszystkich kluczowych komponentów oprogramowania układowego urządzenia. Dokumentacja musi potwierdzać, że architektura pozwala na podmianę tych funkcjonalności w ramach procesu aktualizacji oprogramowania.

SLC-4.1	**Udokumentowany Proces Zarządzania Podatnościami**
opis wymagania	Producent musi wdrożyć i utrzymywać formalny proces zarządzania podatnościami, zgodny z normami np. ISO/IEC 29147 i ISO/IEC 30111, przez cały zdefiniowany okres wsparcia technicznego urządzenia. Proces musi obejmować proaktywne monitorowanie komponentów pod kątem nowo odkrytych luk, ocenę ryzyka i terminowe dostarczanie poprawek bezpieczeństwa zgodnie ze zdefiniowanymi ramami czasowymi.
dyskusja	Żadne oprogramowanie nie jest wolne od błędów, a nowe podatności są odkrywane nieustannie. Posiadanie sformalizowanego proaktywnego procesu reagowania na nie jest kluczowe dla utrzymania bezpieczeństwa przez cały, długi cykl życia licznika. Jest to fundamentalny wymóg unijnego Aktu o cyberodporności (CRA). Zapewnia to, że wykryte luki będą systematycznie analizowane i łatane w czasie z uwzględnieniem czasu niezbędnego na procesy certyfikacji w Jednostkach Notyfikowanych.
kryterium weryfikacji	Producent przedstawi publicznie dostępną politykę ujawniania podatności (Vulnerability Disclosure Policy) oraz wewnętrzną procedurę zarządzania podatnościami. Procedura musi definiować ramy czasowe (SLA) dla dostarczania poprawek w zależności od poziomu krytyczności luki (np. na podstawie CVSS) i uwzględniać czas niezbędny na procesy certyfikacji w Jednostkach Notyfikowanych.

SLC-5.1	**Bezpieczne Środowisko Produkcyjne i Inicjalizacja**
opis	Proces inicjalizacji urządzenia (provisioningu), w tym wgrywanie unikalnych poświadczeń kryptograficznych, musi odbywać się w fizycznie i logicznie

wymagania	zabezpieczonym, kontrolowanym i audytowalnym środowisku produkcyjnym.
dyskusja	Inicjalizacja to moment, w którym urządzeniu nadawana jest jego unikalna, cyfrowa tożsamość (klucze, certyfikaty). Kompromitacja tego procesu mogłaby doprowadzić do sklonowania urządzeń lub kradzieży kluczy głównych, co podważyłoby bezpieczeństwo całego systemu.
kryterium weryfikacji	Producent przedstawi dowody na zabezpieczenie środowiska produkcyjnego, np. w ramach certyfikacji ISO/IEC 27001 (zgodnie z SLC-1.1). Dokumentacja musi opisywać środki kontroli dostępu fizycznego i logicznego do linii produkcyjnej oraz procedury audytu procesu wgrywania poświadczeń. Musi istnieć możliwość prześledzenia, jakie poświadczenia i kiedy zostały wgrane do danego urządzenia.

SLC-6.1	**Projektowanie z Myślą o Przyszłości**
opis wymagania	Urządzenie musi posiadać rezerwy mocy obliczeniowej i pamięci, aby w przyszłości możliwa była aktualizacja algorytmów kryptograficznych i protokołów komunikacyjnych na nowsze, bezpieczniejsze wersje, bez konieczności fizycznej wymiany sprzętu.
dyskusja	Cykl życia licznika wynosi 15-20 lat. W tym czasie obecne standardy kryptograficzne mogą okazać się niewystarczające. Zapewnienie rezerw sprzętowych umożliwia zdalne podniesienie poziomu bezpieczeństwa w przyszłości i zapobiega powstawaniu długu technologicznego.
kryterium weryfikacji	Dokumentacja techniczna urządzenia musi wykazać, że urządzenie posiada min. 15% rezerwy zasobów (pamięć Flash/RAM, CPU) w stosunku do wersji bazowej, umożliwiającej wdrożenie SS2 (np. AES-256) bez wymiany sprzętu. Producent dostarcza dowody (np. testy wydajnościowe lub deklaracje) potwierdzające rezerwę zasobów.

2. Silna Kryptografia

CRY-1.1	**Zatwierdzone Algorytmy Kryptograficzne**
opis wymagania	Dozwolone jest stosowanie wyłącznie publicznie znanych, sprawdzonych i uważanych za bezpieczne na moment dostawy algorytmów kryptograficznych.

dyskusja	Wymóg opierania się na uznanych, międzynarodowych standardach zapewnia, że zastosowane mechanizmy są odporne na znane ataki i zostały gruntownie przeanalizowane przez społeczność kryptograficzną. Wymagania minimalne: • szyfrowanie symetryczne – np. AES-128 bit • kryptografia klucza publicznego – np. ECC z kluczem 256 bit funkcje skrótu – np. SHA-256
kryterium weryfikacji	Analiza dokumentacji i testy komunikacji wykażą, że urządzenie do realizacji funkcji bezpieczeństwa (szyfrowanie, podpisy) wykorzystuje wyłącznie algorytmy i parametry (długości kluczy, krzywe) zgodne z podaną specyfikacją.

CRY-1.2	**Możliwość Aktualizacji Mechanizmów Kryptograficznych**
opis wymagania	Architektura oprogramowania musi umożliwiać w przyszłości aktualizację lub wymianę bibliotek i algorytmów kryptograficznych na nowsze, bezpieczniejsze wersje poprzez zdalną i lokalną aktualizację oprogramowania.
dyskusja	Jest to rozwinięcie wymogu SLC-6.1 ("Projektowanie z myślą o przyszłości"). W perspektywie 15-20 lat eksploatacji licznika, obecnie stosowane algorytmy kryptograficzne mogą zostać uznane za niebezpieczne. Możliwość ich zdalnej i lokalnej aktualizacji jest kluczowa dla utrzymania długoterminowego bezpieczeństwa. W przypadku urządzeń o architekturze oprogramowania typu "monolitycznego", wymóg ten realizowany jest poprzez możliwość wymiany całego obrazu oprogramowania (firmware), w którym zaimplementowano zaktualizowane funkcje kryptograficzne. Pozwala to na uniknięcie ograniczeń związanych z brakiem dynamicznych bibliotek w prostych systemach czasu rzeczywistego.
kryterium weryfikacji	Dokumentacja architektury oprogramowania musi wykazać, że funkcje kryptograficzne są zaimplementowane w kodzie źródłowym w sposób umożliwiający ich modyfikację i aktualizację w ramach nowego wydania oprogramowania. Producent musi zademonstrować (np. w środowisku testowym lub poprzez dokumentację procesu) możliwość przeprowadzenia aktualizacji, która zmienia lub podnosi parametry/wersję używanych algorytmów kryptograficznych.

CRY-2.1	**Kryptograficznie Bezpieczny Generator Liczb Losowych**

opis wymagania	Urządzenie musi być wyposażone w kryptograficznie bezpieczny generator liczb losowych, który jest źródłem entropii dla wszystkich operacji kryptograficznych.
dyskusja	Jakość i nieprzewidywalność liczb losowych jest fundamentem bezpieczeństwa wszystkich operacji kryptograficznych, takich jak generowanie kluczy czy tworzenie wektorów inicjalizacyjnych. Użycie słabego generatora czyni nawet najsilniejsze algorytmy bezużytecznymi.
kryterium weryfikacji	Producent dostarczy dokumentację techniczną wykorzystywanego mikrokontrolera (MCU) lub dedykowanego układu bezpieczeństwa, potwierdzającą obecność sprzętowego Kryptograficznie Bezpiecznego Generatora Liczb Losowych (TRNG/CSPRNG) zgodnego z aktualnymi standardami (np. NIST SP 800-90A/B/C lub BSI AIS 20/31). Producent złoży deklarację, że Kryptograficznie Bezpieczny Generator Liczb Losowych jest wykorzystywany we wszystkich operacjach kryptograficznych wymagających entropii.

CRY-3.1	**Unikalność Kluczy Kryptograficznych dla Urządzenia**
opis wymagania	Każdy licznik musi posiadać swój własny, unikalny zestaw kluczy kryptograficznych. Zabrania się stosowania kluczy domyślnych, wspólnych dla grupy urządzeń (grupowych) lub generowanych w sposób przewidywalny.
dyskusja	Użycie tych samych kluczy w wielu urządzeniach stwarza ogromne ryzyko systemowe – kompromitacja jednego urządzenia prowadzi do kompromitacji całej grupy. Unikalne klucze dla każdego licznika zapewniają, że skutki ewentualnego złamania zabezpieczeń są ograniczone tylko do jednego urządzenia.
kryterium weryfikacji	Analiza certyfikatów cyfrowych (lub kluczy publicznych) pozyskanych z co najmniej dwóch różnych urządzeń musi wykazać, że są one unikalne. Producent musi dostarczyć dowody w ramach audytu procesu produkcyjnego (provisioningu), że każde urządzenie jest inicjalizowane unikalnym zestawem kluczy kryptograficznych, w tym unikalnym kluczem głównym (Master Key). Wykazane zostanie, że klucze nie są w prosty sposób generowane z publicznie znanych identyfikatorów (np. numeru seryjnego), co mogłoby uczynić je przewidywalnymi.

CRY-3.2	**Zarządzanie Cyklem Życia Kluczy**

opis wymagania	Urządzenie musi wspierać współprace w ramach pełnego cyklu życia kluczy, obejmującego ich bezpieczne generowanie, dystrybucję, przechowywanie, zdalną i lokalną rotację (wymianę) oraz bezpieczne usuwanie. Wszelkie klucze tymczasowe muszą być usuwane po użyciu. Współpraca w ramach cyklu życia kluczy musi być możliwa do realizacji przez funkcjonalności wbudowane w licznik lub inne aplikacje do obsługi i współpracy z urządzeniem (klasy KMS).
dyskusja	Klucze kryptograficzne powinny być regularnie zmieniane (rotowane), aby ograniczyć czas ich ewentualnego wykorzystania po kradzieży. Urządzenie musi posiadać bezpieczne, zautomatyzowane mechanizmy do zarządzania kluczami przez cały okres jego eksploatacji. Bezpieczne usuwanie w kontekście licznika oznacza nadpisywanie kluczy sesyjnych w pamięci RAM po zakończeniu sesji oraz unieważnianie (nadpisywanie) starych kluczy w pamięci nieulotnej po pomyślnym przeprowadzeniu procesu rotacji na nowe klucze.
kryterium weryfikacji	Urządzenie musi udostępniać bezpieczne funkcje (np. w ramach protokołu DLMS/COSEM) pozwalające autoryzowanemu administratorowi na zdalną i bezpieczną wymianę (rotację) kluczy sesyjnych i aplikacyjnych. Testy potwierdzą, że po pomyślnej wymianie klucza stary klucz jest nieaktywny, a klucze tymczasowe (sesyjne) są usuwane z pamięci operacyjnej po zamknięciu sesji komunikacyjnej.

CRY-3.3	**Wsparcie dla Zewnętrznych Systemów Zarządzania Kluczami**
opis wymagania	Urządzenie musi wspierać mechanizmy umożliwiające bezpieczną współpracę z zewnętrznymi systemami zarządzania kluczami (KMS). Musi istnieć możliwość zdalnego inicjowania operacji cyklu życia kluczy (np. generowanie nowej pary kluczy, żądanie podpisania certyfikatu, instalacja nowego certyfikatu lub wymiana kluczy symetrycznych) przy użyciu standardowych mechanizmów protokołu komunikacyjnego (np. Security Suite 1 lub 2 w DLMS/COSEM).
dyskusja	W dużej skali ręczne zarządzanie kluczami jest niepraktyczne i podatne na błędy. Licznik musi umożliwić automatyzację procesów zarządzania tożsamością i kluczami poprzez standardowe funkcje protokołu (np. obiekty i metody DLMS), co pozwala systemom klasy KMS na zdalne egzekwowanie polityk rotacji i unieważniania certyfikatów bez udziału personelu technicznego w terenie.
kryterium weryfikacji	Producent udokumentuje wspierane metody zdalnego zarządzania kluczami zgodnie ze standardem DLMS/COSEM. Przeprowadzone zostaną testy funkcjonalne potwierdzające, że urządzenie jest w stanie poprawnie przetworzyć żądanie odnowienia certyfikatu zainicjowane

	przez system centralny, generując nową parę kluczy lub odnowienia certyfikatu (jeśli dotyczy) zainicjowane przez system nadrzędny.

CRY-4.1	Sprzętowa Ochrona Kluczy Krytycznych
opis wymagania	Klucze prywatne urządzenia oraz wszelkie klucze główne (master keys) muszą być generowane, przechowywane i wykorzystywane w ramach chronionego sprzętowo, izolowanego środowiska (np. Secure Element, Trusted Execution Environment), które uniemożliwia ich odczytanie lub skopiowanie w postaci jawnej.
dyskusja	Klucze prywatne i główne są najbardziej krytycznymi sekretami urządzenia. Ich kompromitacja pozwala na podszywanie się pod urządzenie lub deszyfrację komunikacji. Izolacja sprzętowa zapewnia, że klucze nigdy nie opuszczają bezpiecznego środowiska w postaci jawnej. Wymóg ten może być realizowany zarówno przez dedykowane, zewnętrzne układy (Secure Element), jak i przez wbudowane funkcjonalności nowoczesnych mikrokontrolerów (np. TrustZone), przy założeniu spełnienia wymogu trwale wyłączonych interfejsów serwisowych modułu mikrokontrolera (ACC-4.3).
kryterium weryfikacji	Wykazane zostanie (np. poprzez analizę dokumentacji projektowej i testy penetracyjne), że nie istnieje żadna funkcja programistyczna (API) ani interfejs fizyczny, który pozwalałby na bezpośredni odczyt lub eksport kluczy prywatnych/głównych z chronionego środowiska. Operacje kryptograficzne wykorzystujące te klucze (np. podpisywanie) muszą być wykonywane wewnątrz tego środowiska.

CRY-5.1	Tożsamość Cyfrowa Oparta na Certyfikatach
opis wymagania	Licznik zdalnego odczytu nawiązujący bezpośrednie połączenie z systemem centralnym musi posiadać unikalną tożsamość cyfrową potwierdzoną certyfikatem standardu X.509, zgodnie ze standardem DLMS/COSEM Security Suite 1 lub wyższym. Certyfikat musi zostać wydany przez zaufane Centrum Certyfikacji (CA) w ramach dedykowanej dla AMI infrastruktury klucza publicznego (PKI). W przypadku komunikacji za pośrednictwem urządzeń pośredniczących (np. koncentratorów danych) lub technologii o krytycznie niskiej przepustowości, dopuszcza się stosowanie mechanizmów bezpieczeństwa opartych na kryptografii symetrycznej (Security Suite 0), o ile zostanie zapewnione bezpieczeństwo end-to-end na poziomie aplikacyjnym zgodnie z wytycznymi OSD.

dyskusja	W systemie obejmującym miliony urządzeń, certyfikaty cyfrowe są jedynym skalowalnym i wiarygodnym sposobem na zarządzanie tożsamością i budowanie zaufania. Wymóg ten ma charakter fundamentalny – ustanawia on, że każde urządzenie *jest* unikalną, kryptograficznie weryfikowalną jednostką. Jest to warunek konieczny do realizacji wymogów proceduralnych, takich jak COM-2.1, który definiuje, w jaki sposób ta tożsamość *jest używana* do wzajemnego uwierzytelniania kanału komunikacyjnego (np. w ramach sesji TLS). Pozwalają one na silne, wzajemne uwierzytelnienie między licznikiem a systemem centralnym, co jest fundamentem bezpiecznej komunikacji i uniemożliwia ataki typu Man-in-the-Middle.
kryterium weryfikacji	Każde urządzenie jest fabrycznie wyposażone w unikalny certyfikat (np. X.509), podpisany przez zaufany urząd certyfikacji. Urządzenie wykorzystuje ten certyfikat do uwierzytelnienia się w systemie centralnym (np. podczas nawiązywania sesji TLS).

3. Bezpieczeństwo Komunikacji

COM-1.1	**Zabezpieczenie End-to-End na Poziomie Aplikacji**
opis wymagania	Bezpośrednia komunikacja między licznikiem a systemem centralnym musi być zabezpieczona na poziomie warstwy aplikacyjnej (np. z użyciem DLMS/COSEM Security Suite 1 lub 2), zapewniając poufność i integralność danych na całej ścieżce, niezależnie od zabezpieczeń stosowanych w niższych warstwach sieciowych. W przypadku komunikacji za pośrednictwem urządzeń pośredniczących (np. koncentratorów danych) lub technologii o krytycznie niskiej przepustowości, dopuszcza się stosowanie mechanizmów bezpieczeństwa opartych na kryptografii symetrycznej (Security Suite 0), o ile zostanie zapewnione bezpieczeństwo end-to-end na poziomie aplikacyjnym zgodnie z wytycznymi OSD.
dyskusja	Zabezpieczenia na niższych warstwach (np. w sieci komórkowej) mogą być niewystarczające lub poza kontrolą operatora. Szyfrowanie na poziomie aplikacji gwarantuje, że dane są chronione od momentu opuszczenia licznika aż do dotarcia do systemu centralnego, a żadne systemy pośredniczące (np. koncentratory) nie mają do nich dostępu w jawnej postaci. Szyfrowanie na poziomie aplikacji gwarantuje, że dane są chronione od momentu wygenerowania w liczniku aż do ich przetworzenia w systemie HES. Kluczowym aspektem jest rola licznika jako punktu końcowego (terminatora) sesji aplikacyjnej. Oznacza to, że żadne urządzenie pośredniczące (np. koncentrator PLC, modem komunikacyjny czy serwer VPN) nie może mieć dostępu do danych w formie jawnej. Wymóg ten koncentruje się na protokole i logicznej ścieżce danych; techniczna izolacja procesów kryptograficznych od

	stosu komunikacyjnego jest uregulowana komplementarnie w wymogu CRY-4.1.
kryterium weryfikacji	Analiza ruchu sieciowego wykaże, że zawartość protokołu aplikacyjnego (np. DLMS) jest zaszyfrowana, nawet jeśli komunikacja odbywa się wewnątrz tunelu VPN/IPsec.

COM-2.1	**Wzajemne Uwierzytelnianie Kanału Komunikacyjnego**
opis wymagania	Każda bezpośrednia sesja komunikacyjna z systemem centralnym musi być poprzedzona silnym, wzajemnym uwierzytelnieniem obu stron, opartym na certyfikatach cyfrowych (np. Security Suite 1 lub 2). W przypadku komunikacji za pośrednictwem urządzeń pośredniczących (np. koncentratorów danych) lub technologii o krytycznie niskiej przepustowości, dopuszcza się stosowanie mechanizmów bezpieczeństwa opartych na kryptografii symetrycznej (Security Suite 0), o ile zostanie zapewnione bezpieczeństwo end-to-end na poziomie aplikacyjnym zgodnie z wytycznymi OSD.
dyskusja	Samo szyfrowanie nie jest zabezpieczeniem wystarczającym. Konieczne jest, aby obie strony komunikacji miały pewność co do tożsamości swojego rozmówcy. Wzajemne uwierzytelnienie za pomocą certyfikatów uniemożliwia atakującemu podszycie się pod system lub pod urządzenie.
kryterium weryfikacji	Nawiązanie bezpośredniej sesji komunikacyjnej (np. TLS) powiedzie się tylko wtedy, gdy zarówno serwer przedstawi ważny certyfikat, któremu ufa licznik, jak i licznik przedstawi ważny certyfikat, któremu ufa serwer. Próba nawiązania połączenia z serwerem z nieprawidłowym certyfikatem zostanie odrzucona i odnotowana w dzienniku zdarzeń.

COM-3.1	**Ochrona przed Atakami Powtórzeniowymi**
opis wymagania	Protokół komunikacyjny musi implementować mechanizm ochrony przed atakami powtórzeniowymi, np. poprzez stosowanie unikalnych, rosnących numerów sekwencyjnych w wiadomościach lub jednorazowych wartości kryptograficznych.
dyskusja	Atak typu replay polega na przechwyceniu i ponownym wysłaniu legalnej wiadomości w celu wywołania niepożądanej akcji. Skuteczna ochrona przed

	takimi atakami jest kluczowa dla zapewnienia integralności i niezaprzeczalności operacji.
kryterium weryfikacji	Przechwycenie i ponowne wysłanie tej samej, ważnej kryptograficznie wiadomości do urządzenia musi zostać przez nie odrzucone. Zdarzenie odrzucenia powtórzonej wiadomości zostanie zapisane w dzienniku zdarzeń.

COM-3.2	**Walidacja Poleceń**
opis wymagania	Urządzenie musi walidować wszystkie otrzymane dane i polecenia pod kątem ich poprawności składniowej i semantycznej. Niewłaściwe lub nieznane komendy muszą być ignorowane, odrzucane.
dyskusja	Wysyłanie do urządzenia niepoprawnie sformatowanych lub nieoczekiwanych danych (fuzzing) jest popularną techniką wyszukiwania luk w oprogramowaniu. Rygorystyczna walidacja wszystkich danych wejściowych chroni przed atakami typu buffer overflow i innymi błędami parsowania, które mogłyby prowadzić do niestabilności lub kompromitacji urządzenia.
kryterium weryfikacji	Wysłanie do urządzenia serii celowo zniekształconych lub niepoprawnych składniowo poleceń (fuzzing) nie może spowodować jego awarii, restartu ani przejścia w stan niebezpieczny. Urządzenie musi odrzucić takie polecenia i kontynuować normalną pracę.

4. Kontrola Dostępu

ACC-1.1	**Wymóg Uwierzytelnienia dla Wszystkich Interfejsów**
opis wymagania	Dostęp do wszystkich interfejsów dostępowych urządzenia (zdalnych WAN i lokalnych, np. portu optycznego) musi być bezwzględnie poprzedzony pomyślnym procesem silnego uwierzytelnienia. Dostęp anonimowy jest niedozwolony, z wyłączeniem: • asocjacji typu „Public Client” w standardzie DLMS/COSEM (ograniczonej wyłącznie do odczytu podstawowych informacji o urządzeniu niezbędnych do nawiązania sesji), • interfejsu służącego do komunikacji z infrastrukturą sieci domowej (ISD), o ile pracuje on wyłącznie w trybie jednostronnej publikacji danych (push).

dyskusja	Każdy interfejs dostępowy bez uwierzytelnienia stanowi otwartą bramę dla potencjalnych atakujących. Wymóg silnego uwierzytelnienia na każdym punkcie dostępu jest podstawową zasadą bezpieczeństwa, która zapewnia, że tylko uprawnione podmioty mogą wchodzić w interakcję z urządzeniem. Interfejs ISD, ze względu na swoją specyfikę (brak możliwości inicjowania komunikacji w stronę licznika przez użytkownika), nie jest traktowany jako interfejs dostępowy w rozumieniu tego wymogu.
kryterium weryfikacji	Próba wykonania jakiejkolwiek operacji (poza podstawową identyfikacją w ramach asocjacji publicznej) na dowolnym interfejsie dostępowym bez uprzedniego pomyślnego uwierzytelnienia musi zostać odrzucona przez urządzenie.

ACC-2.1	**Ochrona przed Atakami Siłowymi**
opis wymagania	Interfejsy dostępowe muszą implementować mechanizm ochrony przed atakami siłowymi, polegający na czasowym zablokowaniu dostępu po przekroczeniu zdefiniowanej, konfigurowalnej liczby nieudanych prób logowania. Zdarzenie musi być logowane.
dyskusja	Ataki siłowe, polegające na próbie odgadnięcia hasła lub klucza, są powszechnym zagrożeniem. Mechanizm czasowej blokady znacząco spowalnia i utrudnia taki atak, zwiększając jego koszt i prawdopodobieństwo wykrycia.
kryterium weryfikacji	Po przekroczeniu skonfigurowanej liczby nieudanych prób uwierzytelnienia na danym interfejsie, urządzenie musi przestać odpowiadać na kolejne próby przez zdefiniowany okres czasu. Każda nieudana próba musi zostać zapisana w dzienniku zdarzeń.

ACC-3.1	**Implementacja Modelu Separacji Uprawnień**
opis wymagania	Urządzenie musi implementować granularny model kontroli dostępu oparty na asocjacjach (zgodnie ze standardem DLMS/COSEM), lub równoważny mechanizm separacji uprawnień (np. RBAC). Każdej uwierzytelnionej tożsamości musi być przypisany jednoznacznie określony zestaw uprawnień, zgodny z zasadą minimalnych przywilejów.
dyskusja	Przypisywanie uprawnień poszczególnym użytkownikom jest nieefektywne i podatne na błędy. Zastosowanie zorganizowanego modelu uprawnień – np. opartego na rolach, poziomach dostępu lub grupach funkcji – umożliwia logiczne

	grupowanie przywilejów, upraszcza zarządzanie i zapewnia stosowanie zasady minimalnych przywilejów. Każdy poziom lub rola ma dostęp wyłącznie do funkcji niezbędnych do wykonywania przypisanych zadań.
kryterium weryfikacji	Uwierzytelniona asocjacja może wykonywać wyłącznie operacje dozwolone w ramach przydzielonego jej zakresu uprawnień (np. roli, poziomu dostępu lub profilu funkcji). Próba wykonania operacji wykraczającej poza ten zakres musi zostać odrzucona i zarejestrowana w dzienniku zdarzeń.

ACC-3.2	**Zestaw Poziomów Uprawnień**
opis wymagania	Urządzenie musi wspierać możliwość definiowania odrębnych poziomów uprawnień lub równoważnych ról użytkowników. Muszą istnieć co najmniej dwa predefiniowane poziomy uprawnień lub predefiniowane równoważne role użytkowników: • administracyjny (pełny dostęp, konfiguracja, aktualizacje), • publiczny (wyłącznie odczyt podstawowych informacji o urządzeniu niezbędnych do nawiązania sesji).
dyskusja	Ujednolicenie minimalnego zestawu poziomów dostępu lub ról użytkowników zwiększa interoperacyjność i umożliwia spójne zarządzanie uprawnieniami w całym systemie AMI. Takie rozróżnienie odzwierciedla typowych uczestników interakcji z licznikiem (administrator, użytkownik końcowy, inne poziomy) i wspiera egzekwowanie zasady minimalnych przywilejów.
kryterium weryfikacji	Dokumentacja urządzenia musi opisywać zaimplementowane poziomy uprawnień, role lub inne mechanizmy autoryzacji oraz przypisane im funkcje. Testy funkcjonalne muszą potwierdzić, że: • urządzenie rozróżnia co najmniej dwa poziomy dostępu lub równoważne profile użytkowników, • każdy poziom posiada zakres uprawnień zgodny z opisem, • istnieje możliwość definiowania dodatkowych poziomów dostępu i przydzielania im zakresu uprawnień • próby wykonania operacji wykraczających poza przydzielony poziom są odrzucane i rejestrowane w dzienniku zdarzeń.

ACC-3.3	**Dokumentacja Kont Użytkowników**

opis wymagania	Wszystkie zaimplementowane w liczniku konta użytkowników, w tym konta serwisowe, muszą być udokumentowane i przedstawione w specyfikacji urządzenia.
dyskusja	Ukryte lub nieudokumentowane konta stanowią poważne ryzyko bezpieczeństwa. Wymóg pełnej dokumentacji wszystkich kont zapewnia transparentność i umożliwia audytorom weryfikację, czy nie istnieją żadne nieautoryzowane punkty dostępu. Wymogi precyzowane dla kont mają na celu zabezpieczenie przed implementacją niebezpiecznych mechanizmów wykraczających poza standard DLMS (konta inżynierskie, hasła). W ramach DLMS konta nie występują.
kryterium weryfikacji	Lista kont użytkowników (jeśli istnieją) uzyskana z urządzenia (np. poprzez interfejs administracyjny) musi być w 100% zgodna z listą przedstawioną w dokumentacji technicznej produktu.

ACC-4.1	**Minimalizacja Powierzchni Ataku**
opis wymagania	Wszystkie nieużywane i zbędne z punktu widzenia funkcjonalności porty fizyczne, protokoły sieciowe i usługi programowe muszą być domyślnie wyłączone.
dyskusja	Każda aktywna usługa czy otwarty port stanowi potencjalny punkt wejścia dla atakującego (tzw. powierzchnię ataku). Minimalizacja tej powierzchni poprzez wyłączenie wszystkiego, co nie jest absolutnie niezbędne do działania, jest jedną z podstawowych zasad utwardzania systemów.
kryterium weryfikacji	Skanowanie portów i analiza konfiguracji urządzenia w stanie fabrycznym musi wykazać, że aktywne są wyłącznie te usługi i porty, które zostały zdefiniowane jako niezbędne w dokumentacji produktu.

ACC-4.2	**Możliwość Dezaktywacji Interfejsów**
opis wymagania	Operator musi mieć możliwość zdalnej i lokalnej dezaktywacji poszczególnych interfejsów komunikacyjnych na zdefiniowany okres czasu.
dyskusja	Posiadanie możliwości dynamicznego włączania i wyłączania interfejsów daje operatorowi elastyczność w zarządzaniu bezpieczeństwem. W przypadku wykrycia zagrożenia lub braku potrzeby biznesowej, dany interfejs (np. HAN dla

	odbiorcy) może zostać tymczasowo wyłączony, co dodatkowo redukuje powierzchnię ataku.
kryterium weryfikacji	Autoryzowany administrator musi być w stanie za pomocą polecenia zdalnego lub lokalnego wyłączyć, a następnie ponownie włączyć wybrany interfejs komunikacyjny. Stan interfejsu (aktywny/nieaktywny) musi być poprawnie raportowany przez urządzenie.

ACC-4.3	**Trwałe Wyłączenie Interfejsów Debugowania**
opis wymagania	Wszelkie fizyczne i logiczne interfejsy deweloperskie i diagnostyczne (np. JTAG, porty szeregowe z dostępem do powłoki systemowej) muszą być trwale i nieodwracalnie wyłączone w urządzeniach przeznaczonych do eksploatacji.
dyskusja	Interfejsy debugowania dają niemal nieograniczony dostęp do wnętrza urządzenia i pozwalają na obejście większości zabezpieczeń. Ich pozostawienie w wersji produkcyjnej jest niedopuszczalnym ryzykiem. Trwałe wyłączenie (np. poprzez przepalenie bezpieczników eFuse w mikrokontrolerze) jest standardową praktyką bezpieczeństwa dla LZO. Mechanizmy ewentualnych napraw u producenta muszą opierać się na autoryzowanych i bezpiecznych procesach (np. bootloader serwisowy), a nie na interfejsach sprzętowych..
kryterium weryfikacji	Inspekcja fizyczna i testy elektroniczne urządzenia nie mogą wykazać obecności aktywnych sygnałów na pinach odpowiadających za interfejsy debugowania. Próby połączenia z takimi interfejsami muszą zakończyć się niepowodzeniem.

ACC-5.1	**Zarządzanie Hasłami**
opis wymagania	Uwierzytelnianie do wszystkich interfejsów oparte na hasłach muszą spełniać następujące wymagania: • Hasła fabryczne muszą być unikalne dla każdego urządzenia i wymuszać zmianę przy pierwszym logowaniu. • Musi istnieć możliwość zdefiniowania polityki złożoności haseł (minimalna długość, wymagane klasy znaków) oraz polityki starzenia się haseł (maksymalny okres ważności, historia haseł). Możliwa do zdefiniowania polityka haseł musi odpowiadać obecnie stosowanym standardom bezpieczeństwa. • Hasła muszą być przesyłane wyłącznie zaszyfrowanymi kanałami. • System nie może ujawniać, czy błąd logowania dotyczył nazwy użytkownika

	czy hasła. • Zmiana hasła musi generować wpis w dzienniku zdarzeń.
dyskusja	Słabe hasła lub ich niewłaściwe przechowywanie i przesyłanie to jedne z najczęstszych przyczyn naruszeń bezpieczeństwa. Wprowadzenie kompleksowych wymagań dotyczących zarządzania hasłami znacząco podnosi odporność na ataki polegające na ich odgadywaniu lub przechwyceniu. Wymóg zabezpieczający przed implementacją niebezpiecznych mechanizmów wykraczających poza standard DLMS (konta inżynierskie, hasła). W ramach DLMS spełniony.
kryterium weryfikacji	Jeśli urządzenie korzysta z uwierzytelniania opartego na hasłach, to testy funkcjonalne muszą potwierdzić, że: • Po zalogowaniu domyślnym hasłem system wymusza jego zmianę. • Istnieje interfejs administracyjny do konfiguracji reguł złożoności. • Analiza ruchu sieciowego potwierdzi, że hasła są przesyłane w formie zaszyfrowanej. • Komunikat błędu jest generyczny (np. "Nieprawidłowe dane logowania"). • Zmiana hasła jest odnotowywana w dzienniku zdarzeń.

ACC-5.2	**Mechanizmy Wylogowania i Blokady Sesji**
opis wymagania	Urządzenie musi implementować mechanizm automatycznego wylogowania (lub zablokowania) sesji o podwyższonych uprawnieniach (np. administracyjnej, serwisowej) po upływie konfigurowalnego okresu bezczynności.
dyskusja	Pozostawienie aktywnej, uprzywilejowanej sesji bez nadzoru stwarza ryzyko jej nieautoryzowanego przejęcia przez osoby trzecie. Automatyczne wylogowanie po okresie bezczynności jest podstawowym środkiem zaradczym, zgodnym z zasadą minimalizacji okna czasowego ataku. Jest to standardowa funkcja bezpieczeństwa w dojrzałych systemach IT/OT.
kryterium weryfikacji	Po upływie skonfigurowanego czasu bezczynności na interfejsie lokalnym lub zdalnym, sesja użytkownika musi zostać automatycznie zakończona. Każda kolejna operacja wymagająca uprawnień musi wymagać ponownego uwierzytelnienia.

5. Ochrona Integralności

INT-1.1	Ochrona Integralności Danych Przechowywanych
opis wymagania	Krytyczne dane przechowywane w pamięci nieulotnej (dane pomiarowe, takie jak bieżące stany liczydeł energii, klucze uwierzytelniające i szyfrujące, logi) muszą być zabezpieczone mechanizmami kryptograficznymi (np. kodami uwierzytelniającymi MAC lub sumami kontrolnymi) w celu weryfikacji ich integralności. Ochroną integralności objęte są następujące kategorie danych: dane pomiarowe i rozliczeniowe, klucze kryptograficzne, konfiguracja bezpieczeństwa, dzienniki zdarzeń.
dyskusja	Zapewnienie, że dane zapisane w pamięci nie zostały zmienione (celowo lub przypadkowo) jest kluczowe dla wiarygodności całego systemu. Mechanizmy kryptograficzne, takie jak MAC, działają jak cyfrowa plomba, która pozwala w każdej chwili zweryfikować nienaruszalność danych.
kryterium weryfikacji	Celowa modyfikacja bloku chronionych danych w pamięci (np. za pomocą narzędzi deweloperskich) musi zostać wykryta przez urządzenie podczas następnej próby odczytu tych danych. Wykrycie naruszenia integralności musi zostać zarejestrowane w dzienniku zdarzeń.

INT-1.2	Ochrona przed Informacjami Pozostałymi
opis wymagania	Pamięć tymczasowa (np. bufory) używana do przechowywania kluczy kryptograficznych lub innych danych wrażliwych musi być bezpiecznie czyszczona (nadpisywana) natychmiast po zakończeniu operacji.
dyskusja	Pozostawienie wrażliwych danych w pamięci po zakończeniu operacji stwarza ryzyko, że mogą one zostać odczytane przez późniejsze, mniej uprzywilejowane procesy. Bezpieczne czyszczenie pamięci eliminuje to zagrożenie.
kryterium weryfikacji	W przypadku przekazania przez producenta kopii licznika z celowo niezabezpieczonym interfejsem deweloperskim, analiza na podstawie zrzutu pamięci urządzenia po wykonaniu operacji kryptograficznej. Analiza nie może ujawnić żadnych fragmentów użytych kluczy sesyjnych ani innych danych. wrażliwych w postaci jawnej. W przypadku braku możliwości przekazania przez producenta kopii licznika z celowo niezabezpieczonym interfejsem deweloperskim, analiza na podstawie przedstawionej dokumentacji SBOM i HBOM w kontekście zastosowanych rozwiązań i sposobu ich wdrożenia. Muszą istnieć udokumentowane możliwości techniczne do wdrożenia mechanizmu ochrony przed informacjami pozostałymi i pisemna deklaracja producenta o wdrożeniu tego mechanizmu.

INT-2.1	Logiczna Separacja Funkcji i Odporność na DoS
opis wymagania	Architektura oprogramowania musi zapewniać silną, logiczną separację pomiędzy komponentami metrologicznymi a komunikacyjnymi. Atak typu DoS/DDoS na interfejs komunikacyjny nie może wpłynąć na ciągłość i poprawność funkcji pomiarowych.
dyskusja	Kompromitacja modułu komunikacyjnego nie może zagrażać podstawowej funkcji urządzenia, czyli pomiarowi energii. Logiczna separacja gwarantuje, że nawet w przypadku udanego ataku na część sieciową, część metrologiczna pozostaje nienaruszona i działa poprawnie.
kryterium weryfikacji	Przeprowadzenie ataku DoS (np. zalewanie portów) na interfejs komunikacyjny urządzenia nie może spowodować zatrzymania ani zakłócenia procesu pomiaru i rejestracji zużycia energii. Po ustaniu ataku, funkcje komunikacyjne muszą powrócić do normalnego działania.

INT-2.2	Bezpieczny Powrót do Pracy po Awarii
opis wymagania	Urządzenie musi zachować bezpieczny stan w przypadku wystąpienia awarii (np. błąd samotestowania, błąd funkcji kryptograficznej). Po awarii urządzenie musi powrócić do ostatniego znanego bezpiecznego stanu, nie może ujawnić informacji poufnych ani pozwolić na obejście kontroli dostępu.
dyskusja	Awaria urządzenia nie może tworzyć luki w zabezpieczeniach. Zasada "fail-secure" gwarantuje, że w przypadku błędu, urządzenie automatycznie przejdzie w stan maksymalnego bezpieczeństwa (np. zablokuje dostęp), zamiast "zawiesić się" w stanie otwartym. Awaria urządzenia nie może ujawniać informacji poufnych takich jak klucze kryptograficzne, lub dane uwierzytelniające. Awaria urządzenia nie może także wpływać na bezpieczeństwo innych elementów systemu.
kryterium weryfikacji	Symulacja awarii krytycznego komponentu (np. utrata komunikacji z modułem kryptograficznym) musi spowodować, że urządzenie przejdzie w zdefiniowany stan awaryjny. Po restarcie urządzenie musi uruchomić się w bezpiecznej konfiguracji, a analiza logów nie może wykazać wycieku żadnych danych wrażliwych.

INT-2.3	Samotestowanie przy Starcie
opis wymagania	Urządzenie musi przeprowadzać autotesty kluczowych funkcji bezpieczeństwa (np. mechanizmów kryptograficznych, generatora liczb losowych) podczas procesu uruchamiania w celu weryfikacji ich poprawnego działania. W przypadku wykrycia błędu autotestu urządzenie musi: kontynuować funkcję pomiarową, zarejestrować zdarzenie w dzienniku zdarzeń, wysłać alarm do systemu HES, zasygnalizować stan błędu lokalnie. Urządzenie pozostające w stanie błędu autotestu funkcji bezpieczeństwa wymaga interwencji lokalnej (wymiany).
dyskusja	Zapewnienie, że podstawowe mechanizmy bezpieczeństwa działają poprawnie przy każdym uruchomieniu, jest kluczowe dla utrzymania zaufania do urządzenia. Autotesty pozwalają na wczesne wykrycie awarii sprzętowych lub uszkodzeń oprogramowania, które mogłyby osłabić zabezpieczenia. Każde uszkodzenie modułów bezpieczeństwa musi zostać wykryte podczas następnego restartu urządzenia.
kryterium weryfikacji	Celowe uszkodzenie (na poziomie oprogramowania) jednego z modułów bezpieczeństwa (np. biblioteki AES) musi zostać wykryte podczas następnego restartu urządzenia. Urządzenie musi zasygnalizować błąd i nie kontynuować normalnego uruchamiania.

INT-3.1	Wykrywanie Otwarcia Obudowy i Osłony Zacisków
opis wymagania	Urządzenie musi być wyposażone w czujniki fizyczne wykrywające i rejestrujące co najmniej następujące zdarzenia: otwarcie obudowy licznika (z wyjątkiem obudów liczników nierozbieralnych), otwarcie osłony zacisków przyłączeniowych oraz otwarcie osłony modułu komunikacyjnego - jeśli dotyczy (nie dotyczy liczników z modułem komunikacyjnym zintegrowanym). Każde takie zdarzenie musi zostać niezwłocznie zarejestrowane i zaraportowane.
dyskusja	Wykrywanie prób fizycznej ingerencji jest pierwszą linią obrony przed manipulacją. Rejestrowanie i alarmowanie o otwarciu obudowy pozwala na szybką reakcję na potencjalne próby oszustwa lub sabotażu.
kryterium weryfikacji	Fizyczne otwarcie osłony zacisków, modułu komunikacyjnego (jeśli dotyczy) lub obudowy, musi skutkować natychmiastowym zapisaniem zdarzeń w dzienniku bezpieczeństwa. Zdarzenia te muszą zawierać dokładny znacznik czasu.

INT-4.1	Wykrywanie Pola Magnetycznego
opis wymagania	Urządzenie musi być wyposażone w czujnik wykrywający próby manipulacji z użyciem zewnętrznego pola magnetycznego. Wykrycie takiego pola musi zostać niezwłocznie zarejestrowane i zaraportowane.
dyskusja	Magnesy neodymowe mogą być używane do prób zakłócenia pracy elektronicznych komponentów pomiarowych. Dedykowany czujnik pozwala na wykrycie takich prób i stanowi środek odstraszający.
kryterium weryfikacji	Zbliżenie do licznika magnesu (o zdefiniowanej sile pola) musi spowodować zapisanie zdarzenia w dzienniku bezpieczeństwa oraz wysłanie alarmu do systemu centralnego.

6. Rejestrowanie i Audyt

LOG-1.1	Zakres Rejestrowanych Zdarzeń Bezpieczeństwa
opis wymagania	Urządzenie musi rejestrować w dedykowanym dzienniku zdarzeń bezpieczeństwa wszystkie zdarzenia istotne z punktu widzenia bezpieczeństwa. Minimalny zestaw zdarzeń obejmuje: • udane próby uwierzytelnienia, • zadziałanie mechanizmu ochrony przed atakami siłowymi, • zmiany konfiguracji bezpieczeństwa, • aktualizacje oprogramowania (udane i nieudane) – przesłanie, weryfikacja i aktywacja firmware, • wykryte próby manipulacji fizycznej, • błędy integralności oprogramowania (np. nieudany bezpieczny rozruch), • błędy funkcji kryptograficznych, • zmiany czasu systemowego, • reset urządzenia, • błędy krytyczne systemu. Retencja rejestrowanych zdarzeń na poziomie centralnym wynosi minimum 12 miesięcy dla wszystkich zdarzeń, na poziome lokalnym: min. 90 dni dla zdarzeń krytycznych/wysokich, oraz min. 30 dla zdarzeń niskich,
dyskusja	Kompletny i szczegółowy dziennik zdarzeń jest niezbędnym narzędziem do monitorowania stanu bezpieczeństwa systemu, wykrywania anomalii i incydentów oraz prowadzenia dochodzeń po incydencie. Zdefiniowanie

	minimalnego, standardowego zestawu logowanych zdarzeń zapewnia spójność i użyteczność danych w całym systemie AMI.
kryterium weryfikacji	Wykonanie każdej z wymienionych w opisie operacji (np. nieudane logowanie, aktualizacja firmware) musi skutkować pojawieniem się odpowiedniego, szczegółowego wpisu w dzienniku zdarzeń.

LOG-1.2	**Szczegółowość Wpisu w Dzienniku Zdarzeń**
opis wymagania	Każdy wpis w dzienniku zdarzeń musi zawierać co najmniej: • dokładny znacznik czasu, • typ zdarzenia, • identyfikator podmiotu inicjującego zdarzenie (jeśli dotyczy), • wynik operacji (sukces/porażka), (jeśli dotyczy), • interfejs, na którym zdarzenie miało miejsce (jeśli dotyczy).
dyskusja	Aby logi były użyteczne, muszą zawierać wystarczająco dużo informacji kontekstowych. Zdefiniowanie minimalnego zestawu atrybutów dla każdego wpisu gwarantuje, że zarejestrowane zdarzenia będą zrozumiałe i możliwe do skorelowania podczas analizy.
kryterium weryfikacji	Analiza wpisów w dzienniku zdarzeń musi potwierdzić, że każdy z nich zawiera wszystkie wymagane pola, a ich treść jest zgodna z faktycznie wykonaną operacją.

LOG-2.1	**Ochrona Dziennika Zdarzeń przed Modyfikacją**
opis wymagania	Dziennik zdarzeń musi być chroniony przed nieautoryzowaną modyfikacją i usunięciem. Możliwe powinno być wyłącznie dodawanie nowych wpisów. Próba modyfikacji lub usunięcia istniejących wpisów musi zostać zablokowana i sama w sobie zarejestrowana jako zdarzenie bezpieczeństwa (jeśli to technicznie możliwe).
dyskusja	Wiarygodność dziennika zdarzeń zależy od jego integralności. Atakujący często próbują zacierać swoje ślady poprzez modyfikację lub kasowanie logów. Mechanizm "write-only" (lub "append-only") jest podstawowym środkiem ochrony, zapewniającym, że historia zdarzeń pozostaje nienaruszona.
kryterium	Próba modyfikacji lub usunięcia wpisu w pamięci, w której przechowywany jest

weryfikacji	dziennik zdarzeń, musi zostać wykryta przez mechanizmy integralności urządzenia. Nie może istnieć żadna funkcja API pozwalająca na edycję istniejącego wpisu.

LOG-2.2	**Autoryzowany Dostęp do Dziennika Zdarzeń**
opis wymagania	Dostęp do odczytu, i usuwania wpisów w dzienniku zdarzeń musi być kontrolowany i ograniczony do autoryzowanych ról (zgodnie z modelem separacji uprawnień). Modyfikacja istniejących wpisów jest zabroniona (wyjątek mogą stanowić uzasadnione operacje administracyjne). Dziennik aktualizacji oprogramowania oraz dzienniki objęte prawną kontrolą metrologiczną są nieusuwalne w warunkach polowych, a operacje na tych dziennikach są możliwe wyłącznie w warunkach laboratoryjnych. Każda operacja wyczyszczenia pozostałych dzienników, wykonana przez uprawnioną rolę, musi być zarejestrowana w dzienniku zdarzeń bezpieczeństwa.
dyskusja	Chociaż modyfikacja pojedynczych wpisów jest zabroniona (LOG-2.1), mogą istnieć uzasadnione operacje administracyjne, takie jak wyczyszczenie całego dziennika podczas serwisu. Wymóg ten zapewnia, że takie operacje mogą być wykonane tylko przez najbardziej uprzywilejowane role i sama ta czynność jest również rejestrowana.
kryterium weryfikacji	Użytkownik z rolą o niższych uprawnieniach nie może mieć dostępu do funkcji odczytu lub czyszczenia dziennika bezpieczeństwa. Próba wykonania takiej operacji musi zostać zablokowana i zarejestrowana.

LOG-3.1	**Pojemność i Zarządzanie Dziennikiem Zdarzeń**
opis wymagania	Urządzenie musi posiadać nieulotną pamięć wystarczającą do przechowania konfigurowalnego, określonego minimum ostatnich zdarzeń bezpieczeństwa, zarządzaną według następujących zasad: • Dziennik zdarzeń bezpieczeństwa oraz dzienniki operacyjne działają w trybie bufora cyklicznego zapewniającej przechowywanie zdarzeń z okresu nie krótszego niż 90 dni przy nominalnym obciążeniu urządzenia. Po zapełnieniu bufora, najstarsze wpisy muszą być nadpisywane przez najnowsze (mechanizm FIFO). • Dziennik aktualizacji oprogramowania oraz dzienniki objęte prawną kontrolą metrologiczną działają w trybie zapisu jednokierunkowego - bez mechanizmu FIFO. Po zapełnieniu dziennika wykonanie kolejnej aktualizacji jest blokowane, zgodnie z wymaganiami WELMEC Guide 7.2. Wyczyszczenie

	tych dzienników jest możliwe wyłącznie w warunkach laboratoryjnych.
dyskusja	Zapewnienie odpowiedniej pojemności dziennika jest kluczowe dla możliwości analizy zdarzeń z rozsądnego okresu. Mechanizm bufora cyklicznego jest standardową i bezpieczną metodą zarządzania ograniczoną pamięcią, gwarantującą, że najnowsze zdarzenia są zawsze dostępne.
kryterium weryfikacji	Po wygenerowaniu zdarzeń bezpieczeństwa, które przekraczają minimalną skonfigurowaną ilość, najstarsze (pierwsze) zdarzenie musi zostać nadpisane, a w dzienniku musi znajdować się określona w konfiguracji minimalna liczba najnowszych zdarzeń.

LOG-4.1	**Synchronizacja Czasu**
opis wymagania	Urządzenie musi implementować bezpieczny mechanizm synchronizacji czasu (np. z wykorzystaniem komunikatów DLMS/COSEM), aby zapewnić dokładność i wiarygodność znaczników czasu we wszystkich dziennikach zdarzeń.
dyskusja	Dokładne i zsynchronizowane znaczniki czasu są niezbędne do korelacji zdarzeń pomiędzy różnymi urządzeniami i systemami podczas analizy incydentów. Niewiarygodny czas uniemożliwia odtworzenie chronologii ataku.
kryterium weryfikacji	Urządzenie musi odrzucać próby ustawienia czasu pochodzące z nieuwierzytelnionych źródeł. Zmiana czasu systemowego musi być możliwa wyłącznie dla autoryzowanych ról i musi być rejestrowana w dzienniku zdarzeń (udana lub nieudana). Testy wykażą, że urządzenie utrzymuje poprawny czas zgodnie ze skonfigurowanym, zaufanym źródłem.

LOG-5.1	**Alarmowanie o Zdarzeniach Krytycznych**
opis wymagania	Wybrane, krytyczne zdarzenia bezpieczeństwa (np. wykrycie manipulacji fizycznej, wielokrotne nieudane logowanie, otwarcie pokrywy modułu komunikacyjnego z wyjątkiem liczników zintegrowanych) muszą powodować wysłanie komunikatu alarmowego.
dyskusja	Samo logowanie zdarzeń nie wystarczy; w przypadku krytycznych incydentów konieczna jest natychmiastowa reakcja. Mechanizm alarmowania zapewnia, że operator systemu jest niezwłocznie informowany o potencjalnych zagrożeniach,

	co pozwala na podjęcie odpowiednich działań.
kryterium weryfikacji	Wywołanie zdarzenia zdefiniowanego jako krytyczne (np. otwarcie obudowy – jeśli dotyczy) musi skutkować nie tylko zapisem w logu, ale również natychmiastowym zainicjowaniem wysłania odpowiedniego komunikatu alarmowego do systemu HES.

7. Bezpieczeństwo Fizyczne

PHY-1.1	**Możliwość Plombowania**
opis wymagania	Obudowa licznika (z wyjątkiem liczników posiadających nierozbieralną obudowę) oraz osłona zacisków muszą być skonstruowane w sposób umożliwiający ich zaplombowanie. Konstrukcja musi uniemożliwiać dostęp do wnętrza urządzenia lub do zacisków bez zerwania lub widocznego uszkodzenia plomby.
dyskusja	Plomba jest podstawowym, wizualnym środkiem odstraszającym i dowodowym, świadczącym o próbie nieautoryzowanej ingerencji fizycznej. Jest to fundamentalny wymóg bezpieczeństwa fizycznego.
kryterium weryfikacji	Inspekcja fizyczna urządzenia musi potwierdzić istnienie dedykowanych punktów do założenia plomb. Próba zdjęcia obudowy lub osłony zacisków bez usunięcia plomby musi być niemożliwa bez jej widocznego zniszczenia.

PHY-2.1	**Ochrona Lokalnych Portów Serwisowych**
opis wymagania	Fizyczne interfejsy komunikacyjne z wyjątkiem portu optycznego, muszą być umieszczone w lokalizacji, która wymaga zdjęcia zaplombowanej osłony (np. osłony zacisków), aby uzyskać do nich dostęp.
dyskusja	Interfejsy komunikacyjne stanowią potencjalny wektor ataku. Umieszczenie ich za zaplombowaną osłoną zapewnia, że dostęp do nich jest możliwy tylko dla autoryzowanego personelu i każda taka interwencja pozostawia fizyczny ślad (zerwanej plomby). Port optyczny, ze względu na praktyki operacyjne związane z jego stosowaniem, może nie być objęty tą dodatkową ochroną.
kryterium weryfikacji	Inspekcja fizyczna urządzenia musi potwierdzić, że wszystkie fizyczne interfejsy komunikacyjne z wyjątkiem portu optycznego nie są dostępne z zewnątrz bez

	uprzedniego zdjęcia osłony zacisków.

PHY-3.1	Odporność Obudowy
opis wymagania	Obudowa urządzenia musi zapewniać ochronę przed podstawowymi próbami siłowej ingerencji oraz spełniać odpowiednie normy dotyczące urządzeń elektrycznych w zakresie ochrony przed czynnikami środowiskowymi.
dyskusja	Obudowa stanowi pierwszą barierę fizyczną chroniącą wrażliwe komponenty elektroniczne wewnątrz licznika. Musi być ona wystarczająco solidna, aby utrudnić proste, siłowe próby dostępu do wnętrza.
kryterium weryfikacji	Dokumentacja produktu musi potwierdzać zgodność z odpowiednimi normami (np. dotyczącymi stopnia ochrony IP i IK). Inspekcja wizualna musi potwierdzić solidność konstrukcji i brak oczywistych słabości.

Słownik Skrótów (PL–EN)

Skrót	Nazwa angielska	Nazwa polska
Standardy, normy, certyfikacje		
ISO/IEC 27001	Information Security Management System	System Zarządzania Bezpieczeństwem Informacji
ISO/IEC 29147	Vulnerability Disclosure	Ujawnianie podatności
ISO/IEC 30111	Vulnerability Handling Processes	Procesy obsługi podatności
NIST SP 800-90A	Recommendation for Random Number Generation	Rekomendacja dotycząca generatorów liczb losowych
BSI AIS 20/31	Requirements for Random Number Generators	Wymagania dla generatorów liczb losowych
IP / IK	Ingress Protection / Impact Protection	Stopień ochrony przed wnikaniem / ochrona mechaniczna
NDA	Non-Disclosure Agreement	Umowa o zachowaniu poufności
Modele, procesy i metodologia		
SSDLC	Secure Software Development Life Cycle	Bezpieczny cykl życia rozwoju oprogramowania
SAST	Static Application Security Testing	Statyczne testy bezpieczeństwa aplikacji
DAST	Dynamic Application Security Testing	Dynamiczne testy bezpieczeństwa aplikacji
SBOM	Software Bill of Materials	Wykaz komponentów oprogramowania
HBOM	Hardware Bill of Materials	Wykaz komponentów sprzętowych
SLA	Service Level Agreement	Umowa poziomu usług
CRA	Cyber Resilience Act	Akt o Cyberodporności
DoS / DDoS	Denial of Service / Distributed Denial of Service	Atak odmowy usługi / rozproszony atak odmowy usługi
FIFO	First-In, First-Out	Bufor cykliczny, pierwsze weszło –

		pierwsze wychodzi
RBAC	Role-Based Access Control	Kontrola dostępu oparta na rolach
KMS	Key Management System	System zarządzania kluczami
Bezpieczeństwo i kryptografia		
AES	Advanced Encryption Standard	Zaawansowany standard szyfrowania
ECC	Elliptic Curve Cryptography	Kryptografia krzywych eliptycznych
SHA-256	Secure Hash Algorithm	Algorytm skrótu SHA-256
MAC	Message Authentication Code	Kod uwierzytelniający wiadomość
TLS	Transport Layer Security	Bezpieczeństwo warstwy transportowej
VPN	Virtual Private Network	Wirtualna sieć prywatna
IPsec	Internet Protocol Security	Zabezpieczenia protokołu IP
PKI	Public Key Infrastructure	Infrastruktura klucza publicznego
X.509	Standard X.509	Standard certyfikatów cyfrowych
SE	Secure Element	Bezpieczny element sprzętowy
TEE	Trusted Execution Environment	Zaufane środowisko wykonawcze
HSM	Hardware Security Module	Sprzętowy moduł bezpieczeństwa
TPM	Trusted Platform Module	Moduł zaufanej platformy
TRNG / CSPRNG	True / Cryptographically Secure Random Number Generator	Sprzętowy / kryptograficznie bezpieczny generator liczb losowych
Master Key	Master Key	Klucz główny
Komunikacja i protokoły		
DLMS/COSEM	Device Language Message Specification / Companion Specification for Energy Metering	Specyfikacja komunikacji i modelu danych dla liczników energii
PLC	Power Line Communication	Komunikacja po liniach energetycznych
HES	Head-End System	System nadrzędny (centrala AMI)

WAN	Wide Area Network	Sieć rozległa
HAN	Home Area Network	Sieć domowa
EST	Enrollment over Secure Transport	Rejestracja certyfikatów przez bezpieczny transport
Sprzęt i architektura systemów		
MCU	Microcontroller Unit	Mikrokontroler
FLASH	Flash Memory	Pamięć nieulotna (flash)
RAM	Random Access Memory	Pamięć operacyjna
CPU	Central Processing Unit	Jednostka centralna procesora
TrustZone	ARM TrustZone	Technologia izolacji sprzętowej (strefa zaufana)
Infrastruktura energetyczna i systemy licznika		
AMI	Advanced Metering Infrastructure	Zaawansowana infrastruktura pomiarowa
OSD	Distribution System Operator	Operator systemu dystrybucyjnego
LZO	Licznik zdalnego odczytu	Remote Reading Meter
HES	Head-End System	System nadrzędny AMI
Firmware	Firmware	Oprogramowanie układowe licznika
Bootloader	Bootloader	Program rozruchowy
Organizacje i regulacje		
NIS2	Network and Information Security Directive 2	Dyrektywa UE NIS2
BSI	German Federal Office for Information Security	Federalny Urząd ds. Bezpieczeństwa Informacji (Niemcy)
NIST	National Institute of Standards and Technology	Narodowy Instytut Standaryzacji i Technologii (USA)