INFRASTRUKTURY KRYTYCZNE w elektroenergetyce

Adam KLimpel

Krzysztof Lipko

USTAWA 590

z dnia 26 kwietnia 2007 r.

o zarządzaniu kryzysowym

Ustawa definiuje Infrastrukturę krytyczną jako cyt:

„ - należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz zapewnienia sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.”

USTAWA 590

„Infrastruktura krytyczna obejmuje systemy:

a) **zaopatrzenia w energię** i paliwa,

b) łączności i sieci teleinformatycznych,

c) finansowe,

d) zaopatrzenia w żywność i wodę,

e) ochrony zdrowia,

f) transportowe i komunikacyjne,

g) ratownicze,

h) zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych;”

USTAWA 590

Ochrona infrastruktury krytycznej – należy przez to rozumieć zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie;

Zadania z zakresu ochrony infrastruktury krytycznej obejmują:

1) gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej;
2) przygotowywanie i aktualizację planów ochrony infrastruktury krytycznej;
3) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
4) zapewnienie możliwości odtworzenia infrastruktury krytycznej;
5) współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Bezpieczeństwo Infrastruktur Krytycznych

W dniu 4 kwietnia br. w **Ministerstwie Spraw Wewnętrznych i Administracji** odbyło się pierwsze międzyresortowe spotkanie poświęcone ochronie infrastruktury krytycznej.

Celem spotkania było przedstawienie, przygotowanego w Departamencie Zarządzania Kryzysowego i Spraw Obronnych MSWiA projektu założeń do **Krajowego Planu Ochrony Infrastruktury Krytycznej** oraz wypracowanie dalszych metod pracy nad przedmiotowym dokumentem.

W spotkaniu udział wzięli przedstawiciele Kancelarii Prezesa Rady Ministrów, ministerstw i agencji.

Przedstawiono projekt założeń do **Krajowego Planu Ochrony Infrastruktury Krytycznej** oraz informację o działaniach w zakresie ochrony infrastruktury krytycznej podejmowane na forum Unii Europejskiej. Przedstawiono również koncepcje współpracy pomiędzy administracją publiczną a **operatorami infrastruktury krytycznej**, reprezentującymi sektor prywatny

KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 12.12.2006, KOM(2006) 787 wersja ostateczna,2006/0276 (CNS).

DYREKYWA RADY

w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony.

- w czerwcu 2004 r. Rada Europejska wezwała do przygotowania ogólnej strategii ochrony infrastruktur krytycznych,
- w dniu 20 października 2004 r. Komisja przyjęła komunikat w sprawie ochrony infrastruktury krytycznej,
- w dniu 17 listopada 2005 r. Komisja przyjęła zieloną księgę w sprawie europejskiego programu ochrony infrastruktury krytycznej
- w grudniu 2005 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wezwała Komisję do przygotowania wniosku legislacyjnego dotyczącego **europejskiego programu ochrony infrastruktury krytycznej** (EPOIK).

Bezpieczeństwo Infrastruktur Krytycznych

Program ten powinien zakładać ochronę wszechstronną, traktując jednak przeciwdziałanie zagrożeniom terrorystycznym jako priorytet. Zgodnie z takim podejściem w procesie ochrony infrastruktury należy uwzględniać zagrożenia wywołane działalnością człowieka, zagrożenia technologiczne i klęski żywiołowe, największą uwagę poświęcając jednak zagrożeniom terrorystycznym

Komisja Europejska decyzją C/2006/5025 z dnia 26 października 2006 w tym o finansowaniu Projektu Pilotażowego w ramach niniejszego projektu możliwych jest 6 tematyk finansowania:

- Wzmocnienie działań związanych z ochroną infrastruktury krytycznej,
- Odporność i podatność infrastruktury krytycznej, włączając rozwój, metodologii,
- Strategia zmniejszenia ryzyka i ocena zagrożeń dla infrastruktury krytycznej,
- Rozwój planów na wypadek sytuacji kryzysowej,
- Rozwój wspólnych standardów bezpieczeństwa i innowacyjnych technologii dla ochrony infrastruktury krytycznej,
- Międzynarodowe projekty, angażujące przynajmniej 2 państwa członkowskie lub państwo członkowskie i kandydujące.

Bezpieczeństwo Infrastruktur Krytycznych

Infrastruktury krytyczne rozwijały się spontanicznie i niezależnie – obecnie trzeba prowadzić analizy kompleksowo uwzględniając występujące między nimi współzależności.

W analizach podkreślana jest współzależność między poszczególnymi infrastrukturami – atak na jedną z infrastruktur mógłby lawinowo rozszerzyć się na inne

System Elektroenergetyczny uznawany jest za infrastrukturę najbardziej krytyczną, ponieważ wszystkie pozostałe są w pełni od niej zależne.

Jednocześnie systemy elektroenergetyczne i infrastrukturę telekomunikacyjną uważa się za najbardziej podatne na sabotaż i atak na drodze elektronicznej.

W ostatnich latach w Stanach Zjednoczonych i w szeregu krajów Europy Zachodniej podjęto prace mające na celu dokonanie analizy tych zależności miedzy infrastrukturami krytycznymi.

Bezpieczeństwo Infrastruktur Krytycznych - UE

W dniach 27-28 września 2007 r. pod egidą Komisji Europejskiej w Amsterdamie odbyło się spotkanie z udziałem:

UCTE, ETSO, JRC, TREN – temat: „**CIP Electricity Power Grid”**

Główne aspekty Dyrektywy:

- ECI (Europejskie Infrastruktury Krytyczne) oznacza te Infrastruktury Krytyczne, których przerwanie funkcjonowania, lub uszkodzenie może mieć poważny wpływ na dwa lub więcej Kraje członkowskie, lub na pojedynczy kraj jeśli Infrastruktura Krytyczna jest zlokalizowana w innym kraju członkowskim,
- Komisja wraz z Krajami członkowskimi i właściwymi interesariuszami opracowuje kryteria przekrojowe i sektorowe dla identyfikacji ECI,
- Kryteria są opracowywane na podstawie dotkliwości zakłóceń czy uszkodzeń Infrastruktur Krytycznych,
- Kraje członkowskie identyfikują ECI i uzgadniają końcową listę ECI,
- Właściciele/Operatorzy ECI wyznaczonych jako ECI określają Operatorskie Plany Bezpieczeństwa (OSP) oraz wyznaczają Koordynatora Bezpieczeństwa.

Bezpieczeństwo Infrastruktur Krytycznych

UCTE, ETSO, JRC, TREN – „**CIP Electricity Power Grid”**

Struktura EPCIP będzie zawierała:

- Dyrektywę
- Plan działania EPCIP, Sieć Informacji Ostrzegawczych Infrastruktur Krytycznych (CIWIN), grupy ekspertów CIP na poziomie EU, procesy wymiany informacji oraz identyfikacji i analiz
- Wsparcie dla Krajów Członkowskich odnośnie Narodowych Infrastruktur Krytycznych (NCI) które mogą być opcjonalnie używane przez poszczególne Kraje Członkowskie,
- Planowanie odstawień,
- Towarzyszące środki finansowe a w szczególności proponowany Program UE „Zapobieganie, przygotowanie i zarządzanie konsekwencjami terroryzmu i innym ryzykom związanym z bezpieczeństwem” dla okresu lat 2007 - 2013
- Współpraca, wymiana informacji

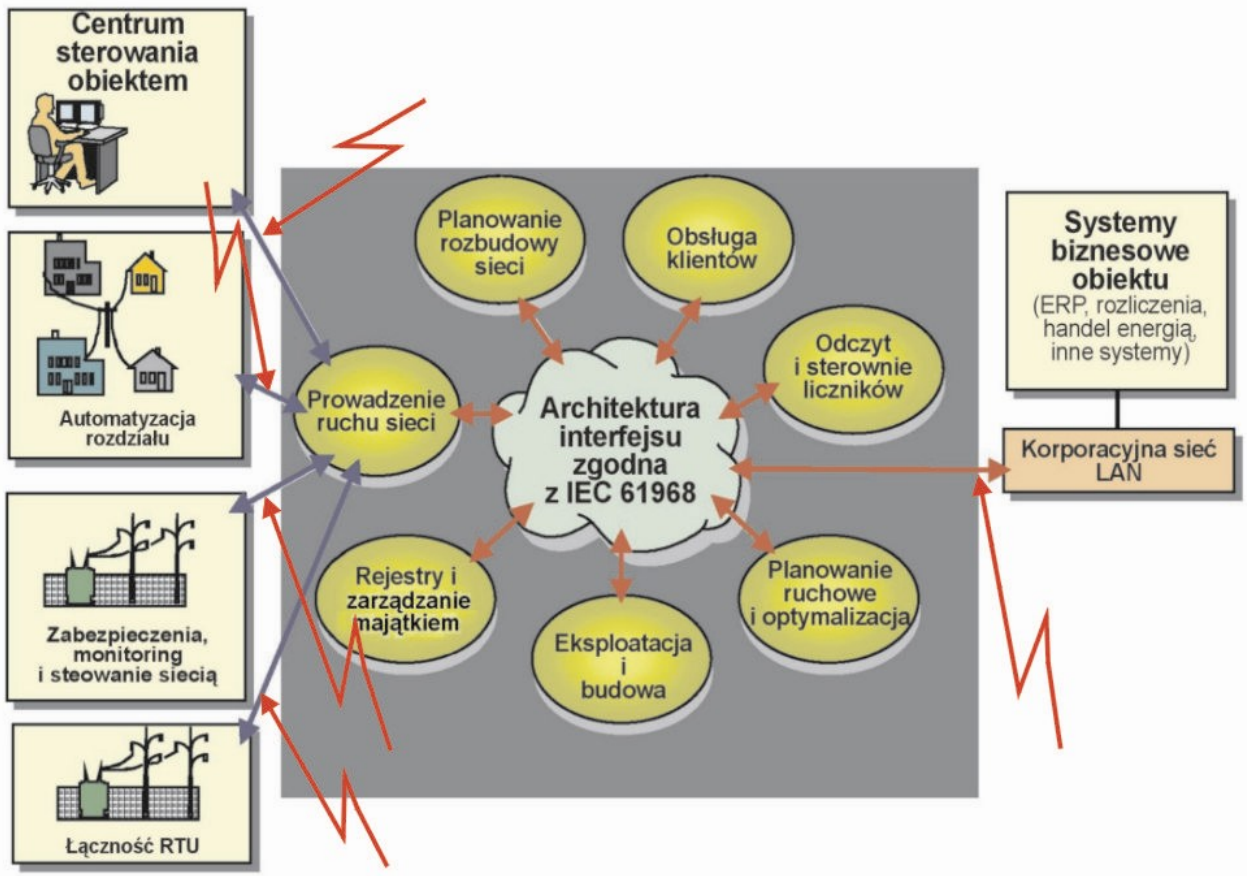
Bezpieczeństwo Infrastruktur Krytycznych

W systemie elektroenergetycznym, ingerencja na drodze elektronicznej w pracę np. systemów sterowania stacji w sieciach przesyłowych, mogłaby doprowadzić nie tylko do przerw w dostawie energii elektrycznej, ale również do fizycznego zniszczenia fragmentów stacji.

Raport USA zawiera stwierdzenie, że zagrożenia dla systemu energetycznego USA pochodzą ze źródeł, które obejmują: nieprzyjaźnie nastawione rządy, grupy terrorystów, inne zorganizowane grupy, niezadowolonych pracowników, złośliwych intruzów, sytuacje złożone oraz klęski żywiołowe i wypadki.

W czasie 15 lat poprzedzających opublikowanie raportu (w 2005 r.), udokumentowanych zostało przez Ministerstwo Energetyki USA ponad 1000 ataków skierowanych przeciwko systemowi energetycznemu. Pewna liczba tych incydentów związana była z przerwami w dostawie energii i znacznymi stratami.

W ostatnich latach zaczęły występować incydenty dokonywane z użyciem systemów komputerowych (ang. cyber incidents).



Źródło: PN-EN 61968 „Integracja aplikacji w przedsiębiorstwach elektroenergetycznych -Interfejsy systemowe do zarządzania dystrybucją"

System zarządzania dystrybucją z interfejsem o architekturze zgodnej z PN-EN 61968 – miejsca podatne na ataki

Bezpieczeństwo Infrastruktur Krytycznych – ochrona infrastruktur krytycznych

Ochrona infrastruktur krytycznych obejmuje:

- bezpieczeństwo fizyczne, uwzględniające wszystkie możliwe do przewidzenia zagrożenia z uwzględnieniem błędów ludzkich i klęsk żywiołowych;
- bezpieczeństwo elektroniczne (ang. cyber security);
- politykę bezpieczeństwa, która oprócz organizacyjnej koncepcji nadzoru nad bezpieczeństwem, uwzględnia uregulowania prawne, prace badawcze, szkolenia, itp.

Oprócz działań związanych z nieupoważnionym dostępem do poufnych danych firm sektora i do transakcji finansowych prowadzonych na wolnym rynku energii, co jest zagrożeniem nie różniącym się od tego typu zagrożeń w innych dziedzinach zastosowań sieci komputerowych, będą to przede wszystkim działania wykorzystujące funkcje systemów komputerowych związane z bezpieczeństwem, a więc takie, które związane są z zagrożeniem dla życia lub zdrowia, środowiska, urządzeń i układów systemu elektroenergetycznego lub dla bezpieczeństwa pracy systemu elektroenergetycznego.

Funkcje takie spełniają komputerowe systemy sterowania stosowane w elektrowniach, stacjach elektroenergetycznych oraz w centrach dyspozycji mocy oraz centrach nadzoru eksploatacyjnego.

Bezpieczeństwo Infrastruktur Krytycznych
Bezpieczeństwo systemów sterowania

Poprzez „system Sterowania” należy rozumieć systemy SCADA (Supervisory Control and Data Aquisition) – systemy Akwizycji Danych, Sterowania i Nadzoru i rozproszone systemy sterowań.

W aspekcie „Cybersecuirity’ (bezpieczeństwa elektronicznego) odnośnie systemów Sterowania identyfikacji wymagają:

- Znaczące ryzyka cybersecuirity związane ze zdalnymi sterowaniami
- Potencjalne i zidentyfikowane cyber-ataki na te systemy
- Kluczowe działania celem ochrony eksploatowanych systemów sterowania,
- Wysiłki zmierzające do budowy odpornych systemów sterowania

Bezpieczeństwo Infrastruktur Krytycznych
Bezpieczeństwo systemów sterowania

Przykładowe raportowane ataki na systemy sterowania:

- w 1994 r. w USA w stanie Arizona został zaatakowany i zablokowany system dyspozytorski głównego dystrybutora wody i elektryczności w Phoenix,
- w marcu 1997 r stanie Masssachusen w USA w miejscowości Worcester zdalnie zablokowano system łączności publicznej (ok. 600 odbiorców) dezorganizujac m.inn. Prace straży pożarnej i lotniska,
- jesienią 2000 r były pracownik firmy australijskiej w odwecie z zwolnienie z pracy, włamał się 46 razy do systemów sterowania przy użyciu nadajnika radiowego powodując wypływ niebezpiecznych ścieków chemicznych do rzeki i powodując groźne zniszczenie środowiska,
- wiosną 2001 roku hakerzy zaatakowali system sterowania kalifornijskiego ISO,
- we wrześniu 2003 r. NRC (Komisja Regulatora Energii Atomowej) poinformowała, że w styczniu 2003 r., że do sieci komputerowej w elektrowni David-Bess przedostał się robak „Slammer” unieruchamiając system bezpieczeństwa na 5 godzin, zaś odbudowa procesu produkcji trwała 6 godzin.

Bezpieczeństwo Infrastruktur Krytycznych – normy

Normy charakterystyczne dla sektora elektroenergetyki:

- IEC-EN 61508 „Functional safety of electrical/electronic/programable safety-related systems”
- IEC 62210 „Initial report from IEC TC 57 ad-hoc WG06 on data and communication security”
- IEC 62351 „Data and Communication Security”
- IEC 61443 „Security for industrial process Measurement and Control”
- ISO 15408 „Common Criteria for Information Technology Security Evaluation”
- ISO 17799 „Information Technology – Code of practice for information security management”

Poza typowymi niebezpieczeństwami wynikającymi z „cyber ataków” kilka czynników ma udział w eskalacji ryzyka specyficznego dla systemów sterowania:

- adaptacja standardowych technologii o określonej podatności,
- połączenia sieci transmitujących sygnały systemów sterowania z innymi sieciami,
- ogólnie dostępne informacje techniczne dotyczące systemów sterowania,
- niezabezpieczone zdalne sterowania.

Bezpieczeństwo Infrastruktur Krytycznych
Bezpieczeństwo systemów sterowania

Spodziewane rodzaje ataków na systemy sterowania:

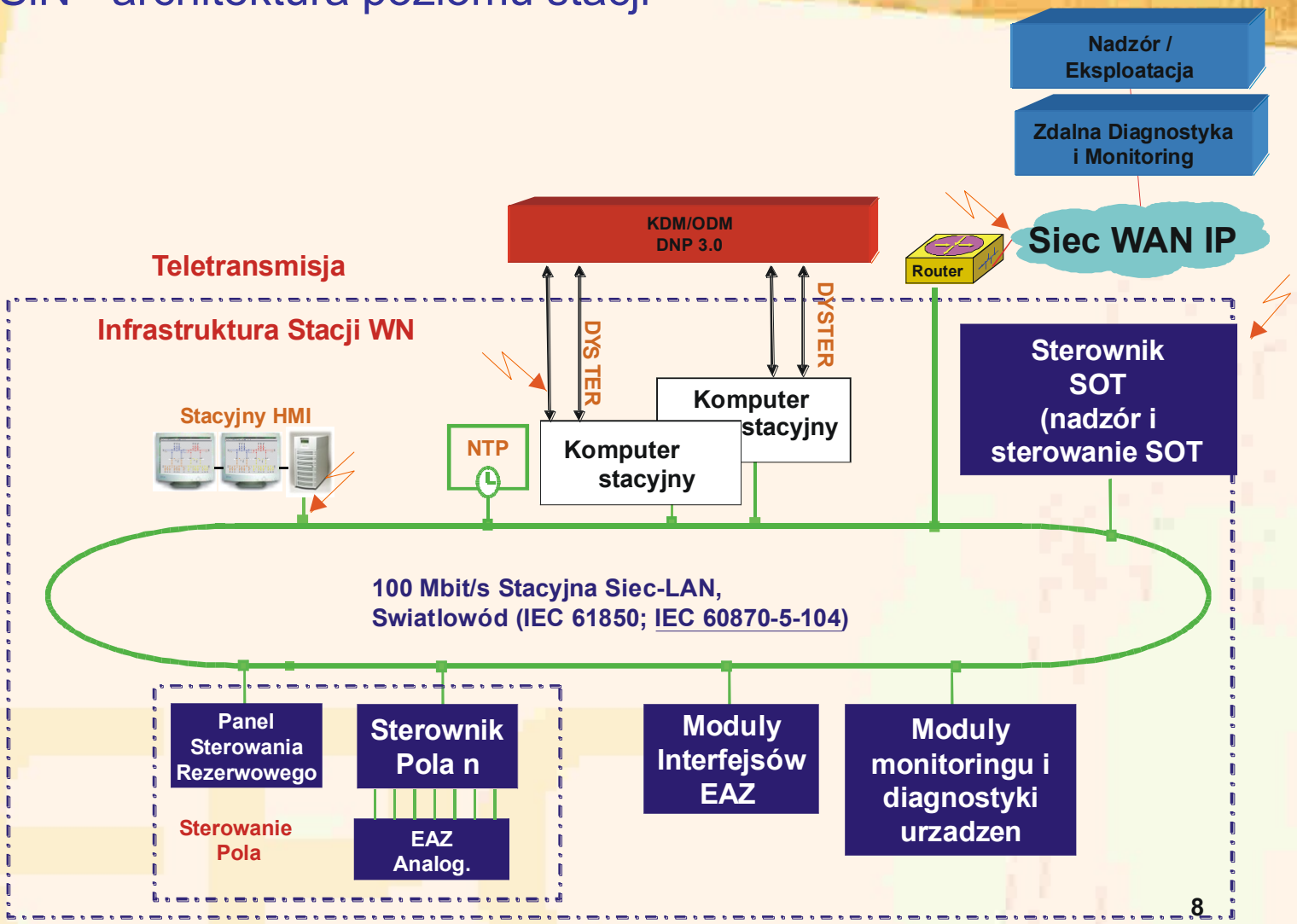
- przerwanie funkcjonowania systemów sterowania poprzez opóźnienie lub zablokowanie przepływu informacji przez sieć telekomunikacyjną, a tym samym odmowa dostępu do systemu dyspozytorom w centrach sterowania,
- wykonanie autoryzowanych zmian w sterownikach stacyjnych, polowych, stacyjnych komputerach łączności (RTU), zmiana progów pobudzenia, lub wysłać autoryzowane rozkazy do sterowanych urządzeń, które mogą skutkować w uszkodzeniu urządzeń, wyłączeniach a nawet black-oucie,
- wysłanie do dyspozytorów fałszywych informacji skutkujących podjęciem błędnych działań niewłaściwych łączeń i w efekcie awarii,
- dokonanie zmian w softwerze systemu sterowania prowadzących do awarii systemu elektroenergetycznego,
- Ingerencja w działanie systemu bezpieczeństwa.

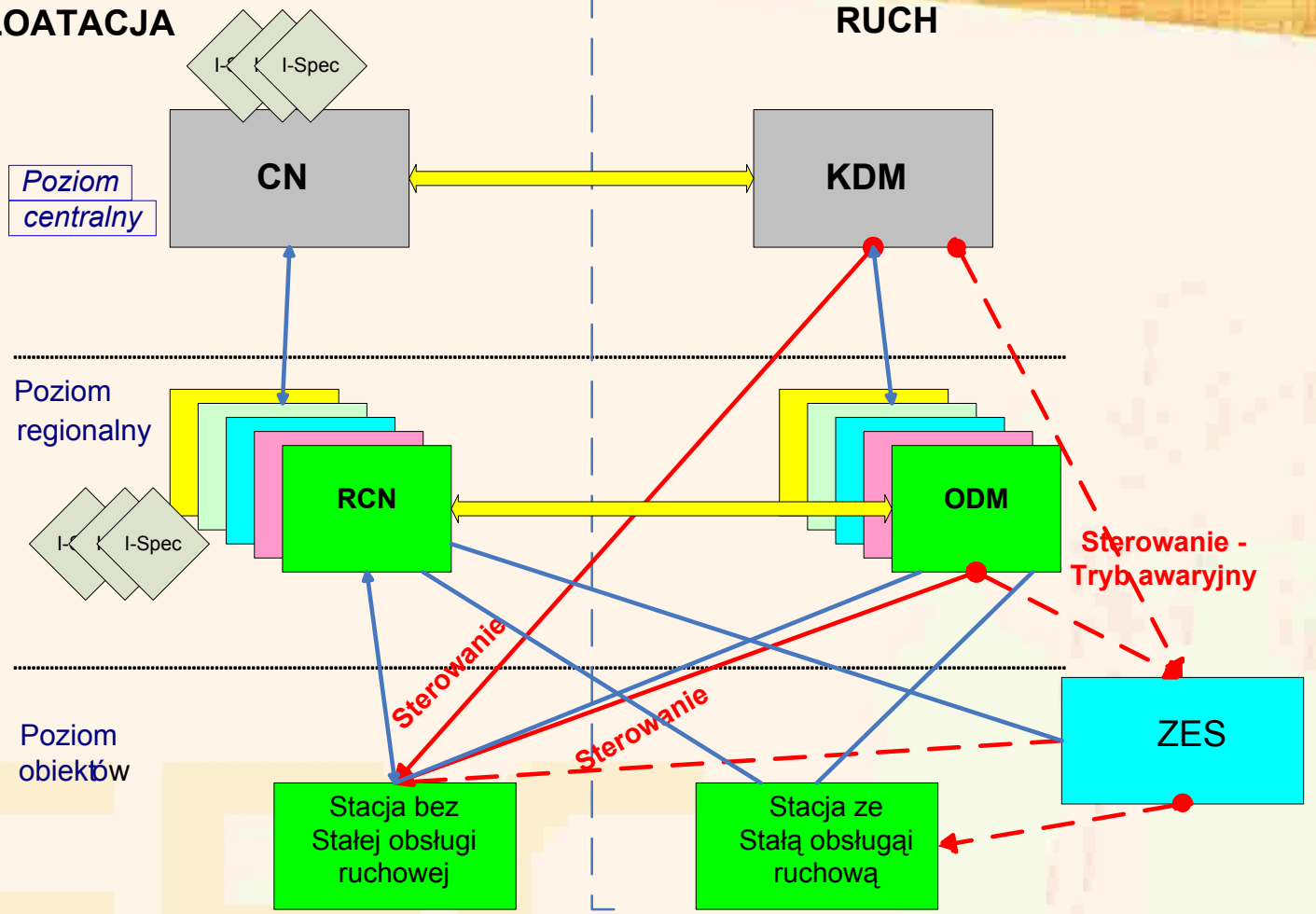
Departament energii USA wraz z labolatoriami opracował system demonstrujący podatność Systemu sterowania na w/w ataki.

Utrudnienia we wdrożeniu właściwego poziomu bezpieczeństwa w systemach sterowania:

- brak specjalistycznej Techniki bezpieczeństwa dla Systemów sterowania.
- obecne technologie bezpieczeństwa takie jak autoryzacja, uwierzytelnienie, kodowanie, wykrywanie wtargnięć, filtrowanie ruchu sieci i komunikacji, wymaga więcej szerokopasmowego przesyłu i pamięci niż posiadają to obecne systemy sterowania.
- rozpowszechnione wśród specjalistów przeświadczenie, że bezpieczeństwo systemów sterowania nie znajduje ekonomicznego uzasadnienia,
- dodatkowymi czynnikami utrudniającymi wdrożenie bezpieczeństwa jest fakt, że eksploatowane systemy sterowania były projektowane bez uwzględnienia wysokiego poziomu bezpieczeństwa, mają ograniczone zdolności przetwarzania i działają w czasie rzeczywistym.

SSiN - architektura poziomu stacji





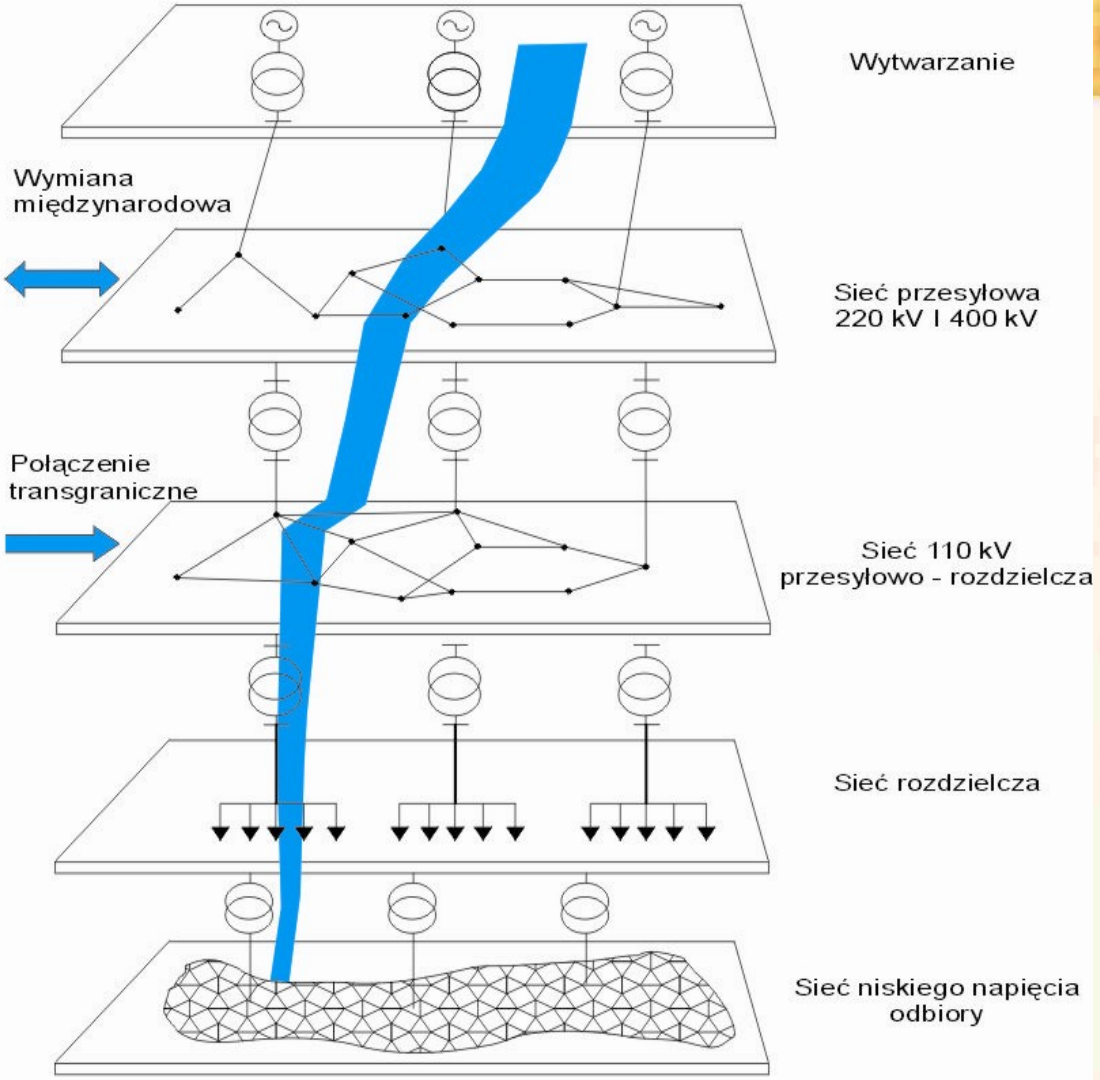
Sterowanie i nadzór stacji w systemie SSiN

Bezpieczeństwo Infrastruktur Krytycznych – Pierwsze laboratorium bezpieczeństwa SCADA w UE

Budowane przez Join Research Centre w Livoro (Włochy) laboratorium badania bezpieczeństwa systemów SCADA

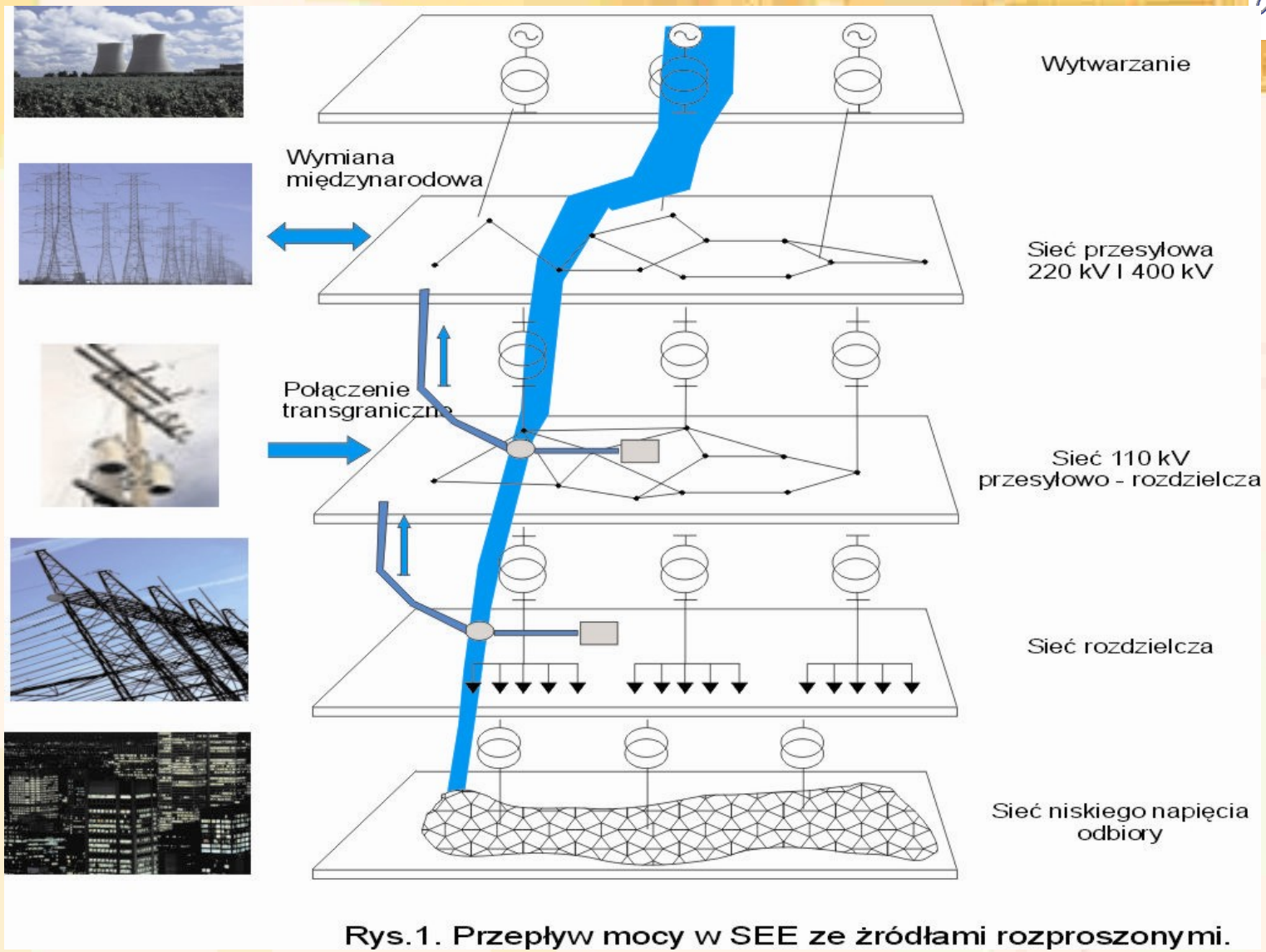
Stosuje:

- Test podatności (stopnia narażenia na ataki)
- Test eksploatacji (np. Patching)
- Badanie polityki ochrony (np. firewall)
- Symulowanie ataków i badanie środków zaradczych
- Porównanie architektur układów,
- Weryfikacja stosowanych norm i standardów



Rys.1. Przepływ mocy w tradycyjnym SEE.

Bezpieczeństwo Infrastruktur Krytycznych



Rys.1. Przepływ mocy w SEE ze źródłami rozproszonymi.

Bezpieczeństwo Infrastruktur Krytycznych

Prace związane z bezpieczeństwem Infrastruktury Krytycznej elektroenergetyki powinny dotyczyć lecz nie ograniczać się do:

- opracowania standardów bezpieczeństwa obowiązujących wszystkich uczestników procesu,
- opracowania zasad komunikacji i wymiany informacji między uczestnikami,
- doskonalenie planów ochrony i odbudowy KSE,
- opracowania i wdrażania procedur na wypadek wystąpienia zagrożeń,
- przeprowadzenia analiz podatności infrastruktury teleinformatycznej krajowej elektroenergetyki na „cyber ataki” i zaproponowanie środków zaradczych
- opracowania środków poprawy bezpieczeństwa elektroenergetyki.

Dziękujemy za uwagę