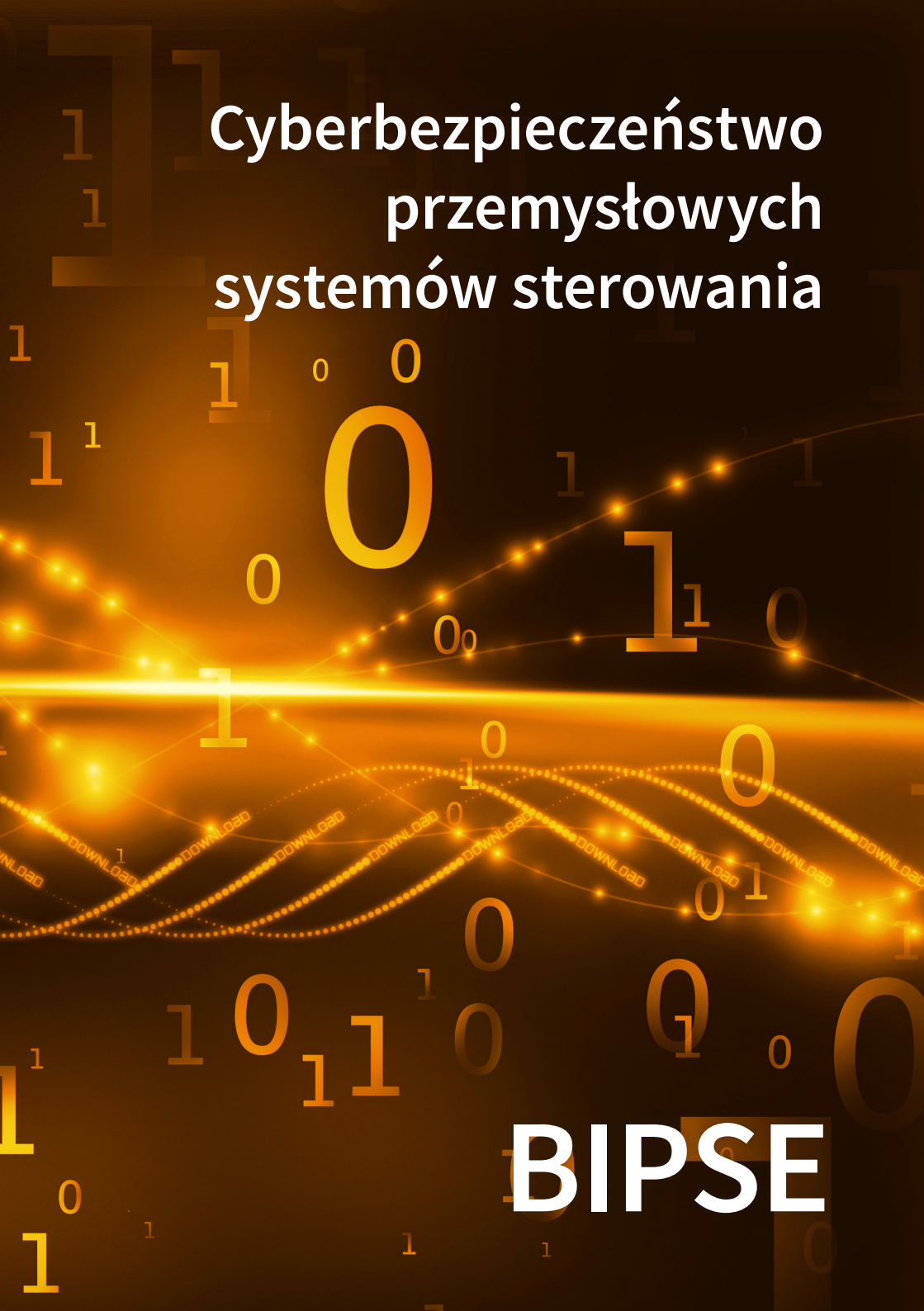
Cyberbezpieczeństwo przemysłowych systemów sterowania



BIPSE

System bezpieczeństwa komunikacji IP w sieciach sterowania

Systemy zarządzania procesami sterowania wykorzystywane w energetyce, gazownictwie, transporcie, wodociągach i kanalizacji, przemyśle, gospodarce komunalnej oraz w wielu innych sektorach gospodarki wymagają szczególnych zabezpieczeń i kompleksowej ochrony przed zagrożeniami komputerowymi. Systemy te są przedmiotem intensywnej inwigilacji prowadzonej nie tylko przez środowiska hakerów, ale także przez zespoły zajmujące się profesjonalnie walką cybernetyczną, a skutki przeprowadzonych ataków mogą mieć katastrofalne konsekwencje.

Bezpieczeństwo infrastruktury teleinformatycznej takich systemów nie może być zapewnione poprzez stosowanie wyłącznie proceduralnych i technicznych środków ochrony fizycznej, a także ich separację od innych sieci, w tym sieci publicznych. Ze względu na istotne różnice między typowymi sieciami teleinformatycznymi a infrastrukturą systemów sterowania procesami technologicznymi, wyrażające się zarówno ich architekturą, systemami operacyjnymi, wykorzystywanymi protokołami, jak i zadaniami systemów ochrony, konieczne jest tworzenie nowych, zaawansowanych zabezpieczeń, dostosowanych do specyficznych właściwości i uwarunkowań ich funkcjonowania.

W odpowiedzi na wzrastający poziom zagrożeń dla niezawodnego funkcjonowania takich systemów opracowany został System Bezpieczeństwa Komunikacji IP w Sieciach Sterowania, zwany dalej w skrócie Systemem BIPSE.

System BIPSE został opracowany w ramach projektu rozwojowego nr O ROB/0074/03/001 współfinansowanego przez Narodowe Centrum Badań i Rozwoju pt. „System zapewnienia bezpiecznej komunikacji IP w obszarze zarządzania siecią elektroenergetyczną" realizowanego w latach 2012 – 2015. Wykonawcą systemu BIPSE jest konsorcjum w składzie: Wojskowa Akademia Techniczna (lider

BIPSE

konsorcjum), Naukowa i Akademicka Sieć Komputerowa (NASK), Asseco Poland S.A oraz Wojskowy Instytut Łączności. W całym okresie tworzenia systemu wykonawcy ścisłe współpracowali z interesariuszami projektu, w szczególności z Polskimi Sieciami Elektroenergetycznymi S.A.

Prezentowane rozwiązanie jest jedynym na rynku tak zaawansowanym technicznie, kompleksowym i zintegrowanym systemem zapewnianiającym wszechstronną ochronę systemów zarządzania sieciami sterowania oraz pełne jego dostosowanie do specyfiki chronionego obiektu. W przeciwieństwie do typowych rozwiązań z rynku IT, system BIPSE integruje wiele zróżnicowanych mechanizmów monitorujących różne aspekty bezpieczeństwa infrastruktury teleinformatycznej, umożliwiając pozyskanie dokładnej i aktualnej informacji o potencjalnych zagrożeniach, oraz postrzeganie i rozumienie rzeczywistej sytuacji. Pozwala to na skuteczne, skoordynowane działania dla niezawodnej pracy chronionego obiektu.

Prototyp systemu BIPSE został w pełnym zakresie sprawdzony w docelowych warunkach operacyjnych na stacji elektroenergetycznej PSE S.A. oraz w mikrosystemie energetycznym, zasilającym fragment Politechniki Łódzkiej, uzyskując VIII poziom gotowości technologicznej.

1. Architektura systemu BIPSE

Architektura systemu BIPSE umożliwia jego pełne dostosowanie do ochrony sieci sterowania procesami technologicznymi wykorzystywanych w różnych sektorach gospodarki oraz jego integrację z już stosowanymi zabezpieczeniami.

Modułowa, elastyczna konstrukcja

System BIPSE składa się ze zbioru modułów programowych, które mogą być dowolnie rozmieszczane. W przypadku ochrony niewielkiej sieci, całość systemu może być zainstalowana na pojedynczym komputerze. W dużym, rozbudowanym obiekcie, możliwe jest wykorzystanie wielu komputerów rozmieszczonych zależnie od potrzeb. W każdym przypadku nadzór nad całością systemu BIPSE sprawuje pojedynczy koncentrator bezpiecznej komunikacji. Podział systemu na moduły różnych rodzajów, elastyczność ich rozmieszczania w elementach fizycznych oraz dokładne określenie interfejsów umożliwiają łatwe opracowywanie modułów adaptacyjnych pozwalających na dołączanie do systemu nowych typów i rodzajów zabezpieczeń.

Otwartość na zmiany

System BIPSE może zostać dostosowany do ochrony sieci sterowania dowolnego sektora gospodarki, rozszerzony o nowe funkcjonalności i skonfigurowany według indywidualnych potrzeb odbiorcy.

Brak szkodliwego wpływu na działanie chronionego systemu

Wszystkie analizy prowadzone są na kopii ruchu dostarczanej przez urządzenia sieciowe. Działanie systemu sterującego procesem technologicznym jest niezaburzone – przesyłane pakiety nie są modyfikowane, ani opóźniane.

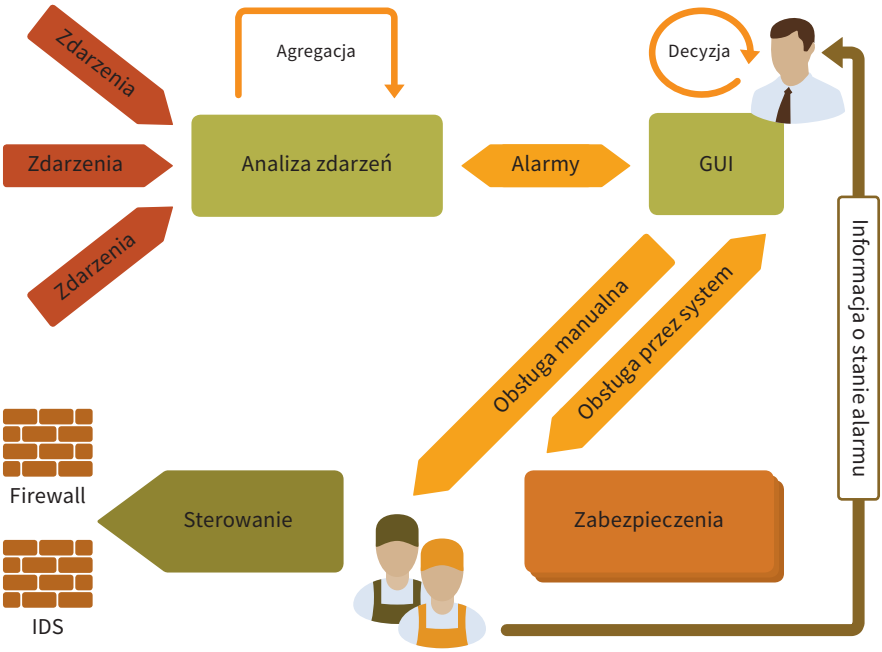
Funkcjonalny interfejs użytkownika w języku polskim

Wszystkie działania w systemie BIPSE podejmowane są poprzez wygodny graficzny interfejs użytkownika. Wykorzystanie przeglądarki umożliwia dostęp z dowolnego miejsca w chronionym obiekcie, jak również – o ile konfiguracja na to zezwala – zdalnie.

Współpraca systemów BIPSE

System BIPSE, zabezpieczający sieć sterowania procesem technologicznym w konkretnym obiekcie, może wymieniać informacje o zagrożeniach z systemami BIPSE innych obiektów zrzeszonych w domenie. Pozwala to wykorzystać efekt synergii – obserwacja zagrożenia dla jednego obiektu podnosi czujność wszystkich zainteresowanych.

O ile współpraca w domenie jest typowa dla wielu obiektów należących do jednego właściciela, to system BIPSE umożliwia także tworzenie federacji domen różnych właścicieli. W tym ostatnim przypadku, zakres wymienianych informacji pomiędzy systemami BIPSE oraz poziom ich agregacji są kontrolowane przez odpowiednie filtry, konfigurowane według wymagań podmiotów będących właścicielami systemów zarządzania procesami technologicznymi, zgodnie z przyjętą polityką bezpieczeństwa.



Obsługa alarmów

2. Wykrywanie działań rozpoznawczych – systemy pułapkowe

Pierwszą fazą większości złożonych cyberataków jest rozpoznanie atakowanej sieci, aby zidentyfikować cele ataków i wykryć obecne w systemie podatności. Zidentyfikowanie napastnika lub zainfekowanego komputera w tej fazie daje możliwość skutecznej reakcji jeszcze przed podjęciem właściwych szkodliwych działań.

Honeypoty SCADA

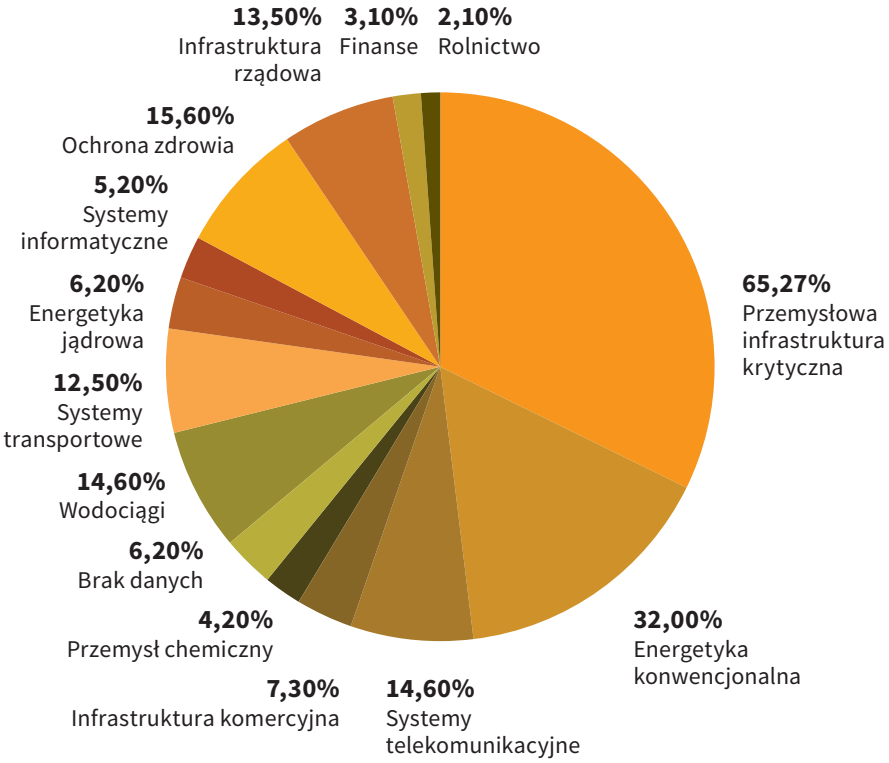
Wchodzący w skład systemu BIPSE moduł honeypota SCADA umożliwia umieszczenie w sieci sterowania procesem technologicznym dodatkowych, fikcyjnych urządzeń, nie uczestniczących w pracy systemu. System rejestruje całość kierowanego do niego ruchu, zapewniając nie tylko wykrycie atakującego, ale też identyfikację rodzaju działań, jakie próbuje podejmować. Obecnie zapewniona jest pełna obsługa typowego dla nowoczesnych sieci elektroenergetycznych protokołu IEC 61850 – MMS, istnieje możliwość adaptacji do innych protokołów przemysłowych.

Honeypoty Standard

Analogiczny do poprzedniego podsystem zapewnia możliwość umieszczenia w sieci urządzeń naśladujących zwykłe komputery. Stosowany w sąsiedztwie komputerów obsługi (HMI) czy w sieci korporacyjnej, zapewnia emulację typowych protokołów spotykanych w sieciach komputerowych. Wykorzystanie obu rodzajów sond umożliwia wykrycie różnych rodzajów ataków, niezależnie od ich działania.

Darknet

Dowolna liczba niewykorzystywanych przez rzeczywiste urządzenia (w tym sondy BIPSE) adresów IP może być monitorowana przez sondę Darknet. W przeciwieństwie do pozostałych, nie wchodzi ona w interakcję z atakującym – rejestruje jedynie próby połączeń w sposób niewidzialny dla atakującego. Jeśli obserwowane będą wszystkie niewykorzystane adresy, mechanizm gwarantuje wykrycie wszelkich nieprawidłowych połączeń, uniemożliwiając jakiekolwiek działania rozpoznawcze, w tym ataki prowadzone bez wcześniejszej znajomości topologii sieci. Jednocześnie ten rodzaj monitorowania adresów jest mało wymagający – jedna sonda może obsłużyć nawet wielką sieć.



3. Wykrywanie nieprawidłowego ruchu sterującego

Jeśli atakujący skutecznie połączy się z rzeczywistym urządzeniem, ma możliwość wykonywania wielu niebezpiecznych czynności. Zdarzenia takie są wykrywane przez moduł walidacji i analizy anomalii.

Walidacja protokołów

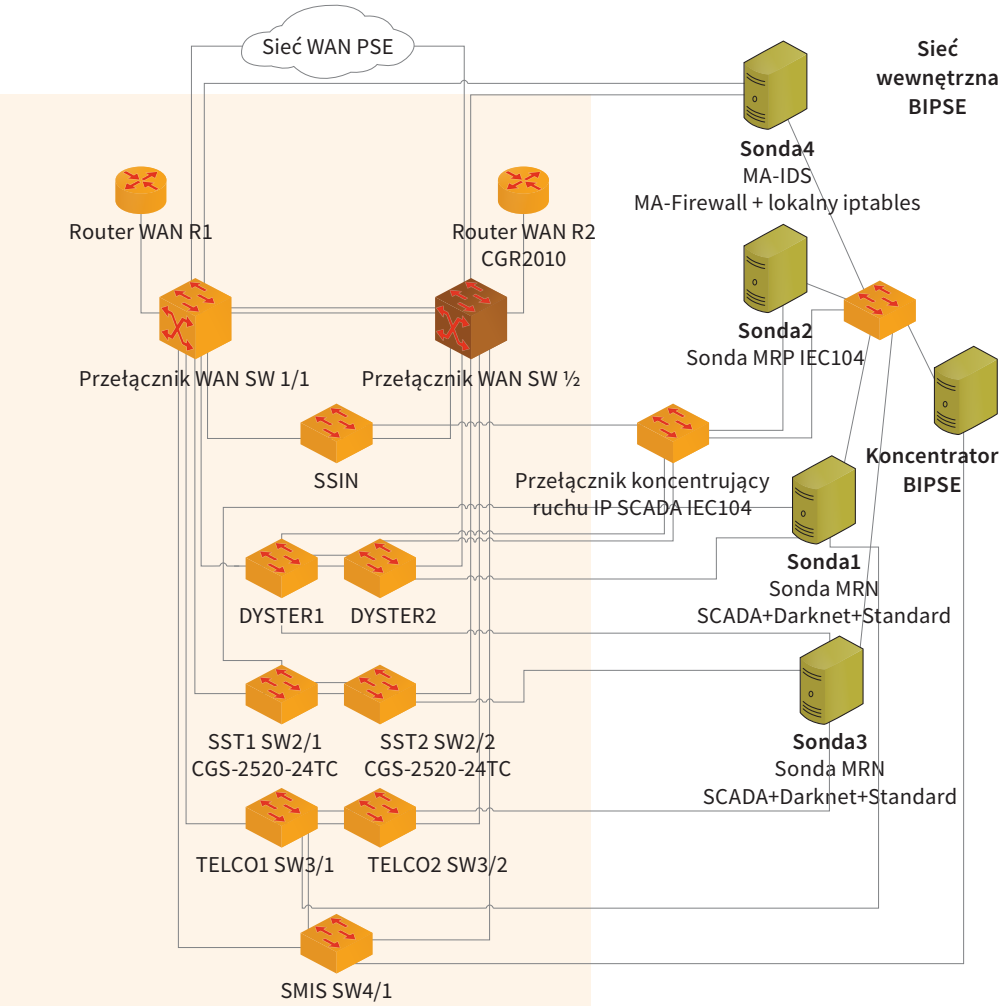
Sonda zapewnia możliwość wykrycia nieprawidłowych pakietów, niezgodnych ze specyfikacją danego protokołu. W zakresie sieci sterowania obecnie zapewniona jest analiza typowego dla sieci elektroenergetycznych protokołu IEC 60870-5-104, istnieje jednak możliwość dostosowania do dowolnego protokołu o znanej specyfikacji.

Analiza anomalii

Po instalacji moduł analityczny obserwuje obecny w sieci ruch przez pewien czas, ucząc się występujących w nim połączeń. Po zakończeniu procesu uczenia jest dzięki temu w stanie wykrywać zdarzenia nietypowe – np. połączenia w nietypowych relacjach, pakiety sterujące przesyłane z urządzeń, które wcześniej jedynie odczytywały rejestry z urządzeń, itp.

Wykrywanie regułowe – IDS

Dostępny w systemie BIPSE moduł adaptacyjny zapewnia integrację z klasycznymi systemami IDS. Znane rodzaje ataków mogą więc być skutecznie wykrywane przy użyciu dostępnych zbiorów reguł. Obecnie zapewniona jest integracja ze Snort – powszechnie znanym i wykorzystywanym otwartym systemem IDS. Dobrze zdefiniowane interfejsy systemu BIPSE pozwalają na łatwe opracowanie nowych modułów adaptacyjnych, umożliwiających wykorzystanie dowolnych systemów IDS, w tym zainstalowanych wcześniej w systemie.



Przykładowe wdrożenia

4. Inne mechanizmy detekcji

Poza wymienionymi wcześniej modułami ukierunkowanymi bezpośrednio na wykrywanie ataków, system zawiera wiele pomocniczych mechanizmów mogących zidentyfikować symptomy skutecznego ataku lub działania z nim związane.

Katalog systemu

Struktura chronionej sieci, jak i samego systemu BIPSE, odzwierciedlona jest w katalogu systemu. Dzięki temu identyfikacja zagrożeń jest o wiele łatwiejsza – już w samej treści alarmów zawarta jest informacja, które to urządzenie i do którego systemu należy.

Wykrywanie zmian topologii sieci

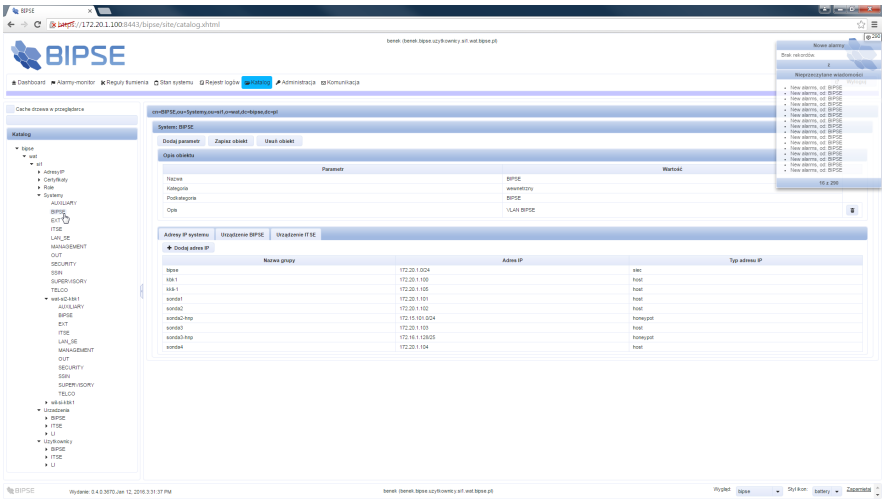
System BIPSE monitoruje stan portów urządzeń sieciowych chronionego systemu, pozwalając wykryć podłączenie nieautoryzowanego sprzętu, czy utratę łączności z poszczególnymi urządzeniami.

Wykrywanie zmian konfiguracji sprzętu sieciowego

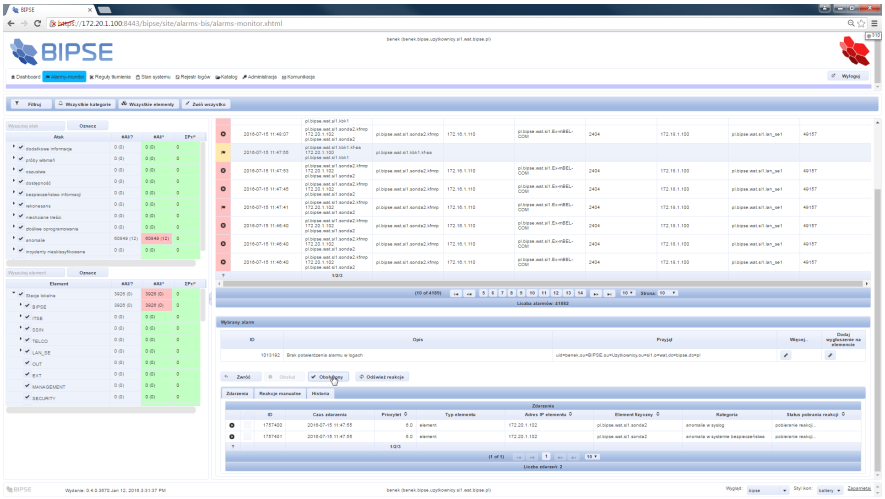
Osobny moduł wykrywa próby dostępu administracyjnego do urządzeń sieciowych, zapobiegając włamaniom i nieautoryzowanym próbom zmiany konfiguracji sieci. Monitorowana jest również konfiguracja poszczególnych urządzeń, dzięki czemu jej nieautoryzowana zmiana zostanie wykryta niezależnie od sposobu przeprowadzenia ataku.

Wykrywanie innych zdarzeń bezpieczeństwa

Elastyczne interfejsy systemu BIPSE pozwalają podłączać do systemu rozmaite mechanizmy zabezpieczeń. W obecnej konfiguracji system pozwala m. in. wykrywać rozbieżności między dostępnymi w systemie chronionym źródłami czasu, utratę łączności domenowej, czy zdarzenia bezpieczeństwa rejestrowane przez systemy HIDS na poszczególnych urządzeniach.



Obsługa alarmów



Stan systemu BIPSE

5. Monitorowanie łącza inżynierskiego

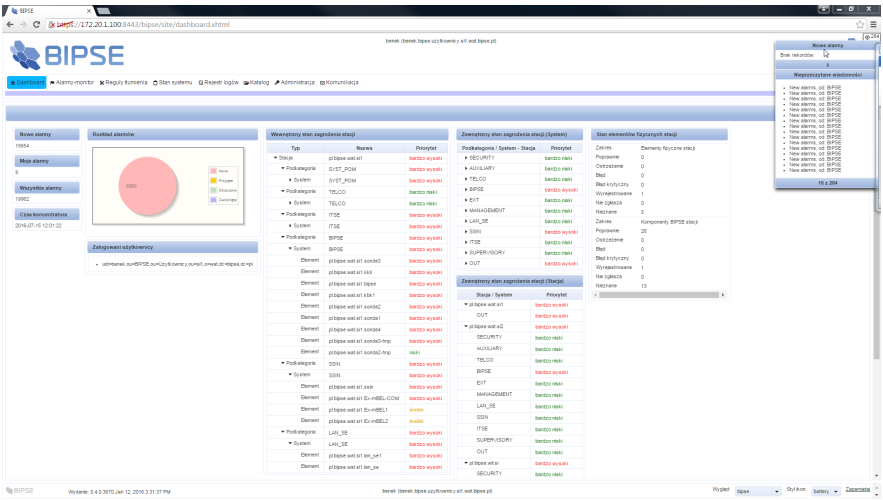
Zaawansowany moduł kontroli łącza inżynierskiego pozwala jednocześnie wygodnie i sprawnie serwisować urządzenia stacji, jak i zabezpiecza przed nadużyciami wykorzystującymi tę drogę ataku.

Uwierzytelnianie i kontrola dostępu

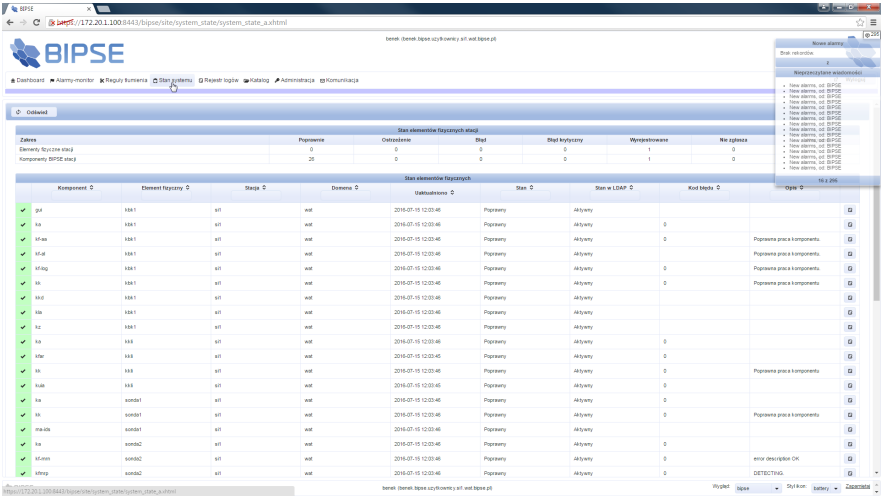
Dostęp do łącza inżynierskiego wymaga wcześniejszego zezwolenia z poziomu systemu BIPSE. Zezwolenie wydawane jest określonemu serwisantowi, do określonych urządzeń i na określony czas – a w przypadku, gdy wykorzystywane protokoły są znane, także tylko dla określonych rodzajów działań. W tym okresie ma on dostęp do maszyn wirtualnych zawierających odpowiednie aplikacje zarządcze. Nie jest możliwy dostęp bez odpowiednich uprawnień, a wszelkie próby przekroczenia zadeklarowanego zakresu prac (np. dostęp do innego urządzenia, niż serwisowane) zostaną zablokowane.

Pełna rejestracja sesji

Wszystkie czynności realizowane przez serwisanta są rejestrowane i mogą być weryfikowane w przypadku wątpliwości. Standardowo rejestrowane są dostępy do maszyn wirtualnych oraz połączenia z urządzeniami, ale w razie potrzeby możliwa jest też pełna rejestracja działań serwisanta (łącznie z wytworzeniem filmu obrazującego jego aktywność) z dokładnością do każdego kliknięcia.



Katalog systemu ITSE i BIPSE



Dashboard

6. Reakcja na zagrożenia

Zamknięta pętla reakcji

System BIPSE, w odróżnieniu do większości dostępnych na rynku rozwiązań, wspiera całość procesu reakcji na zagrożenia – od ich wykrycia, poprzez analizę, po wypracowanie i wdrożenie reakcji. Automatyczne moduły proponują sposób rozwiązania wykrytych problemów. Reakcje te mogą być wdrażane z poziomu systemu BIPSE, lub z jego pominięciem. Wprowadzenie reguły wymaga zawsze aktywności operatora systemu, co zapobiega zakłóceniu przez system pracy kluczowych mechanizmów sterowania procesem technologicznym.

Przetwarzanie dzienników zdarzeń

Analizę zarejestrowanych zdarzeń znacznie upraszcza dostępność w interfejsie użytkownika (GUI) systemu dzienników zdarzeń urządzeń stacyjnych – zarówno systemu BIPSE, jak i wszelkich innych, dla których ich zbieranie zostało włączone. Scentralizowane przetwarzanie dzienników umożliwia wygodne ich filtrowanie i korelację, a także analizę przez wbudowany moduł wykrywający istotne zdarzenia.

Wsparcie dla zapór sieciowych

Moduły adaptacyjne pozwalają na bezpośrednie wprowadzanie reguł blokujących zagrożenia, bez konieczności używania zewnętrznych narzędzi. Obecnie wspierane są urządzenia CISCO oraz moduł iptables systemu GNU/Linux, jednak dzięki dobrze zdefiniowanym interfejsom zapewnienie wsparcia dla dowolnych urządzeń tego typu jest prostym zadaniem.

Agregacja i tłumienie alarmów

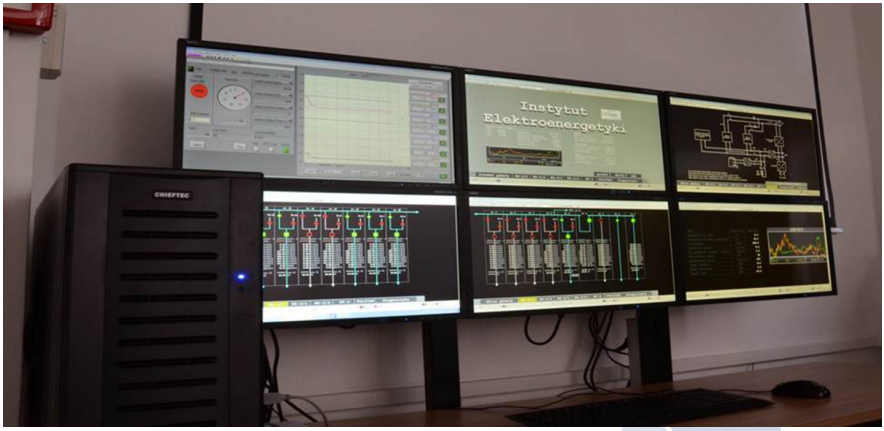
Wbudowane mechanizmy zapewniają agregację powtarzających się alarmów, a stwierdzone przez użytkownika fałszywe alarmy są tłumione – im dłuższa praca systemu, tym mniej błędów i pracy dla operatora.

7. Próbne wdrożenia

Prototyp systemu BIPSE został w pełnym zakresie sprawdzony w docelowych warunkach operacyjnych, uzyskując VIII poziom gotowości technologicznej. Wyczerpujące testy przeprowadzone w trzech środowiskach testowych stworzonych przez wykonawców systemu, umożliwiły dokonanie dwóch próbnych wdrożeń.

Laboratorium Generacji Rozproszonej Instytutu Elektroenergetyki Politechniki Łódzkiej

Laboratorium Generacji Rozproszonej Politechniki Łódzkiej było pierwszym poligonem doświadczalnym BIPSE. Działający stale mikrosystem energetyczny, obejmujący różne rodzaje urządzeń elektroenergetycznych, jest chroniony przez system BIPSE od roku.

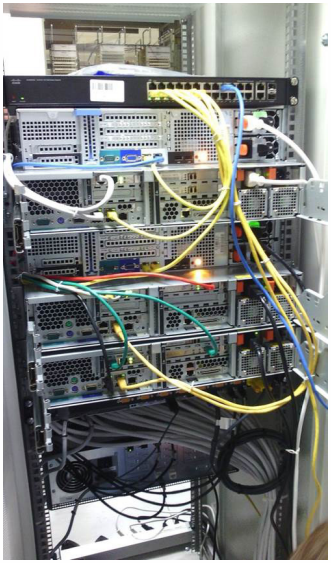


Laboratorium Generacji Rozproszonej Instytutu Elektroenergetyki Politechniki Łódzkiej

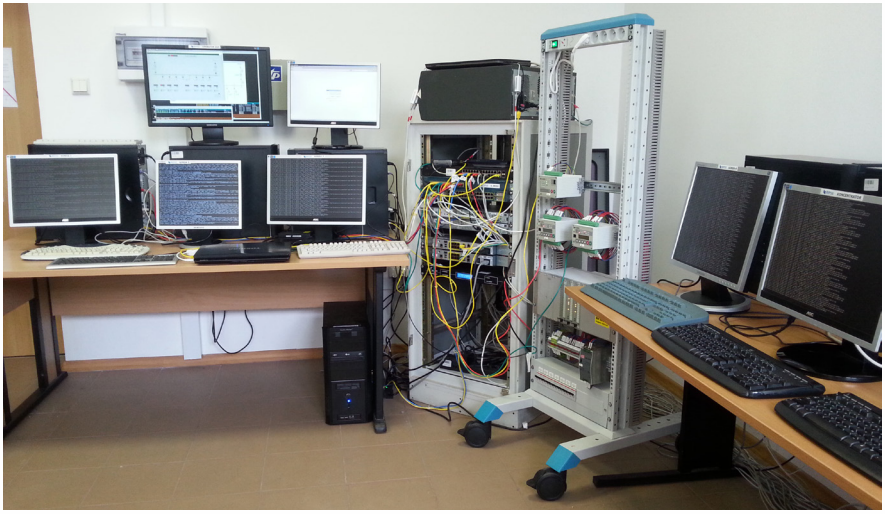
Stacja przesyłowa Polskich Sieci Elektroenergetycznych S.A.

W ramach testów VIII poziomu gotowości, system został zainstalowany na rzeczywistej stacji przesyłowej.

Stacja Stanisławów (PSE)



Laboratorium WAT (stacja 1)



BIPSE

8. Wykorzystanie i rozwój systemu

System BIPSE jest jedynym na rynku tak kompleksowym i zintegrowanym rozwiązaniem, zapewniającym wszechstronną ochronę sieci sterowania procesami technologicznymi. Cechy systemu BIPSE zapewniają jego dostosowanie do potrzeb małych i wielkich wdrożeń, a także na jego pełną adaptację do ochrony infrastruktury teleinformatycznej sieci sterowania w dowolnym sektorze gospodarki.

System BIPSE został w całości opracowany przez zespół polskich inżynierów, co zapewnia jego skuteczny rozwój i dalsze doskonalenie w miarę pojawiania się nowych form i technik ataków, a także jego adaptację do wymagań przyszłych użytkowników. Zapewnia to potencjalnym użytkownikom systemu pełną kontrolę nad instalacją, wykorzystaniem oraz rozwojem systemu chroniąc ich przed ryzykiem związanym z wdrażaniem do ochrony infrastruktury krytycznej państwa rozwiązań niezapewniających wystarczającego poziomu bezpieczeństwa ich stosowania.

Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
Wydział Elektroniki
ul. gen. S. Kaliskiego 2
00-908 Warszawa
http://www.wel.wat.edu.pl

kontakt:
Kierownik Projektu
prof. dr hab. inż. Marek Amanowicz
marek.amanowicz@wat.edu.pl

Naukowa i Akademicka Sieć
Komputerowa – instytut badawczy
ul. Kolska 12
01-045 Warszawa
http://www.nask.pl

kontakt:
Architekt Projektu
dr inż. Adam Kozakiewicz
adam.kozakiewicz@nask.pl

Wojskowy Instytut Łączności
im. prof. dr. hab. Janusza Groszkowskiego
ul. Warszawska 22A
05-130 Zegrze Południowe
http://www.wil.waw.pl

kontakt:
dr inż. Joanna Śliwa
Joanna.Sliwa@wil.waw.pl

Asseco Poland S.A.
ul. Branickiego 13
02-972 Warszawa
https://pl.asseco.com

kontakt:
Zdzisław Wiater
zdzislaw.wiater@asseco.pl


WAT
asseco
POLAND
NASK
WIŁ