

Defence in depth w systemie ECONTROL – skuteczny monitoring sieci OT

Adrian Machula, Marcin Starczewski, Michał Zając - Energotest

Streszczenie

W referacie opisano podejście specjalistów firmy Energotest do tematyki cyberbezpieczeństwa w systemie OT – ECONTROL, przy wykorzystaniu oprogramowania monitorującego sieć w czasie rzeczywistym oraz zastosowaniu funkcji głębokiej inspekcji pakietów.

1. Wstęp

W lipcu 2016 r. została wydana przez Parlament Europejski i Radę UE dyrektywa nr 2016/1148, dotycząca zabezpieczenia środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Dyrektywa podnosi między innymi kwestie ustanowienia procedur i obowiązku zgłaszania incydentów, dotyczących cyberbezpieczeństwa dla przedsiębiorców z sektorów kluczowych, nakłada na nich obowiązek ustanowienia szczególnych wymogów dotyczących zapewniania bezpieczeństwa i sugeruje przyjęcie na poziomie krajowym strategii w zakresie bezpieczeństwa sieci i systemów IT. Inne poruszane w dyrektywie kwestie to między innymi utworzenie CSIRT (ang. Computer Security Incident Response Teams) czyli sieci Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego, a także stworzenie międzynarodowej grupy zapewniającej współpracę oraz wymianę informacji.

W ślad za tym polski rząd przyjął uchwałę nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022. W uchwale oprócz kwestii dostosowania polskiego prawa do potrzeb i wyzwań jakie stawia przed nami tematyka cyberbezpieczeństwa, jest także mowa o opracowaniu i wdrożeniu odpowiednich standardów bezpieczeństwa sieci systemów informatycznych.

Ustawa dotyczy kilku kluczowych sektorów: energetyki, transportu, bankowości, służby zdrowia, gospodarki wodnej i infrastruktury sieciowej. Obowiązkiem operatorów usług kluczowych będzie wdrożenie systemu zarządzania bezpieczeństwem oraz jego okresowy audyt, począwszy od 2019 r. powtarzany z częstotliwością co dwa lata. Za niedopełnienie tego obowiązku ustawa przewiduje kary nawet do 200 tys. zł. System będzie musiał gromadzić odpowiednie dane i spełnić rygorystyczne wymagania. Jego główne zadania będą obejmowały zakres:

- analizy infrastruktury sieciowej pod kątem potencjalnych zagrożeń i podatności aktualnie zainstalowanych systemów na cyberataki,
- wykrywania incydentów i ich klasyfikację (np. w CSIRT), a następnie planowania działań naprawczych i zapobiegawczych,
- wsparcie zarządzania ryzykiem,
- ciągłego monitoringu sieci,
- zapewnienia bezpiecznej eksploatacji systemów OT/IT,
- zapewnienia bezpiecznej komunikacji.

2. Zagrożenia w 2018 r.

Według raportu Instytutu Kościuszki, celem ataków hackerskich w 2018 r. będzie infrastruktura krytyczna. W poprzednich latach zaobserwowaliśmy ataki na systemy ważne dla funkcjonowania państwa takie jak energetyka, logistyka, ochrona zdrowia. Dane, które udało się zebrać hackerom podczas tych ataków posłużyły do wykrycia podatności na ataki, które planowane są w najbliższym okresie (np. całkowite zaszyfrowanie danych na komputerach, shutdown). Uniwersytet Oksfordzki donosi o trwających przygotowaniach ataków także na sektory gospodarki wodnej i transport [3].

Istnieje wiele rodzajów ataków oraz wiele sposobów ich klasyfikacji. Podstawowy podział wyróżnia:

1. Ataki z wykorzystaniem fizycznego dostępu do komputera polegające na kradzieży poufnych i często strategicznych danych, których dzięki skutecznym zabezpieczeniom programowym nigdy nie udałoby się pozyskać w inny sposób. Należy mieć świadomość, że w praktyce nie da się przed nimi zabezpieczyć w 100 procentach. Dlatego kluczową sprawą jest zabezpieczenie fizyczne sieci jak również szkolenie pracowników w zakresie bezpieczeństwa [4].
2. Ataki zdalne wykonywane spoza sieci lokalnej lub z innego komputera pracującego w tej sieci:
 - ataki w warstwie dostępu do sieci,
 - ataki w warstwie Internetu,
 - ataki w warstwie aplikacji,
 - ataki działające w kilku warstwach jednocześnie.

3. ECONTROL a cyberbezpieczeństwo

W odpowiedzi na zapotrzebowanie rynku energetycznego na tego typu systemy opracowano w firmie Energotest rozwiązanie dla infrastruktury sieciowej popularnego systemu ECONTROL i nie tylko (może być z łatwością adaptowana w systemach innych integratorów). Założono ochronę zgodnie z modelem defence in depth (ochrona w głąb), który polega na projektowaniu zabezpieczeń dla systemów informatycznych w taki sposób aby doprowadzić do powstania wielu, niezależnych warstw. Idea ochrony w głębi jest zalecana dla systemów wymagających najwyższego poziomu zaufania i uzyskała rekomendację amerykańskiej agencji bezpieczeństwa (NSA). Zastosowanie nadmiarowości w postaci wielu warstw znacząco podnosi poziom ochrony systemu, zwiększa szanse na skuteczne wykrycie nadchodzącego ataku, co ma decydujący wpływ na jego uprzedzenie lub przygotowanie się i ograniczenie skutków jego oddziaływania.

Pakiet składa się z następujących programów i usług:

- systemu ciągłego monitoringu sieci, wykrywania i raportowania anomalii,
- odpowiednio dobranych i skonfigurowanych urządzeń Firewall, aby ograniczyć niepożądany w sieci OT ruch pochodzący z zewnątrz sieci,
- odpowiednia konfiguracja komputerów przemysłowych - hardening (antyvirus, aktualizacje zabezpieczeń, wyłączenie portów USB i autoodtwarzania),
- projekt i odpowiednia konfiguracja, segmentacja sieci szkieletowej (routery warstwy trzeciej, z wydzieloną strefą DMZ na poczet komunikacji z siecią zakładową), wyłączenie niektórych portów TCP/UDP itd.,
- opcji uwierzytelnienia - kontroli ról i uprawnień każdego użytkownika RBAC (ang. Role Based Access Control),
- mechanizmów tworzenia kopii zapasowej celem szybkiego odtworzenia uszkodzonych elementów systemu.

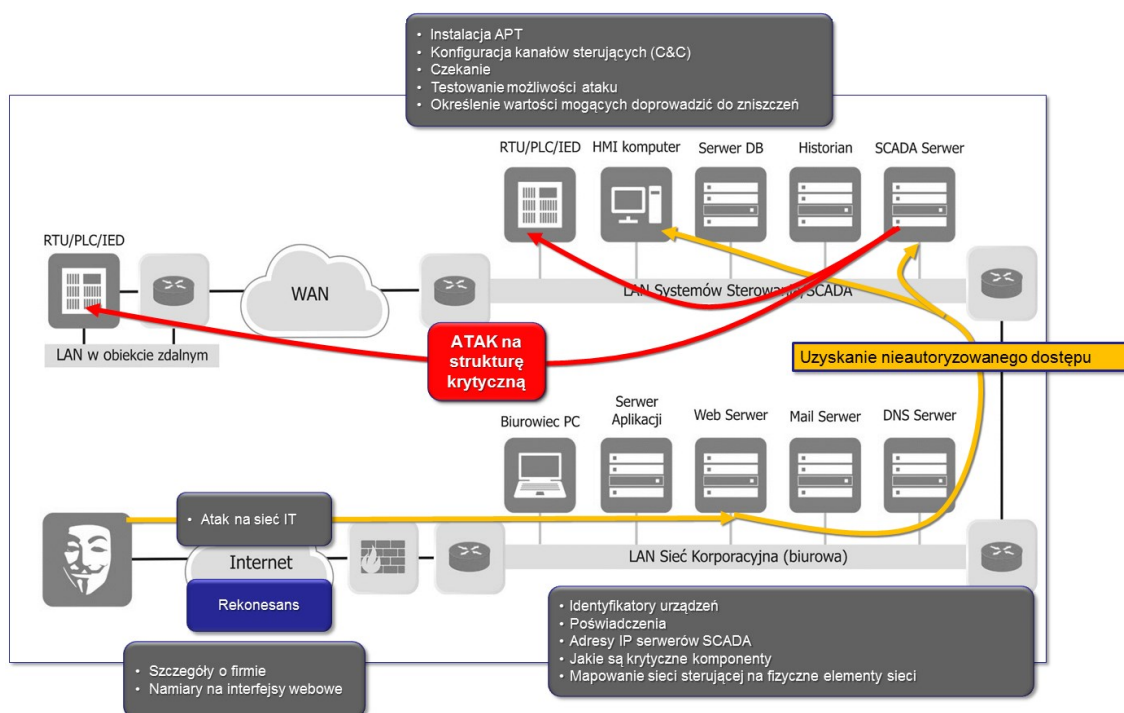
4. Jak działają cyberprzestępcy?

Ciągły monitoring sieci jest bardzo ważny. Zanim zostanie przypuszczony atak przestępcy muszą poświęcić dużo czasu na rozpoznanie infrastruktury sieciowej.

Istnieją dwie możliwości przeniknięcia do sieci:

- pierwsza: poprzez bezpośrednie wsparcie przestępców przez osoby pracujące w danym zakładzie pracy (świadome lub nieświadome) – np. włożenie zainfekowanego pendrive, otwarcie zarażonego załącznika, itp.,
- druga: poprzez złamanie dostępu do sieci z zewnątrz.

Na rys. 1 zobrazowano poszczególne etapy ataku na infrastrukturę krytyczną czyli urządzenia sklasyfikowane jako RTU/PLC/IED – elementy wykonawcze.



Rys. 1. Anatomia ataku na system SCADA

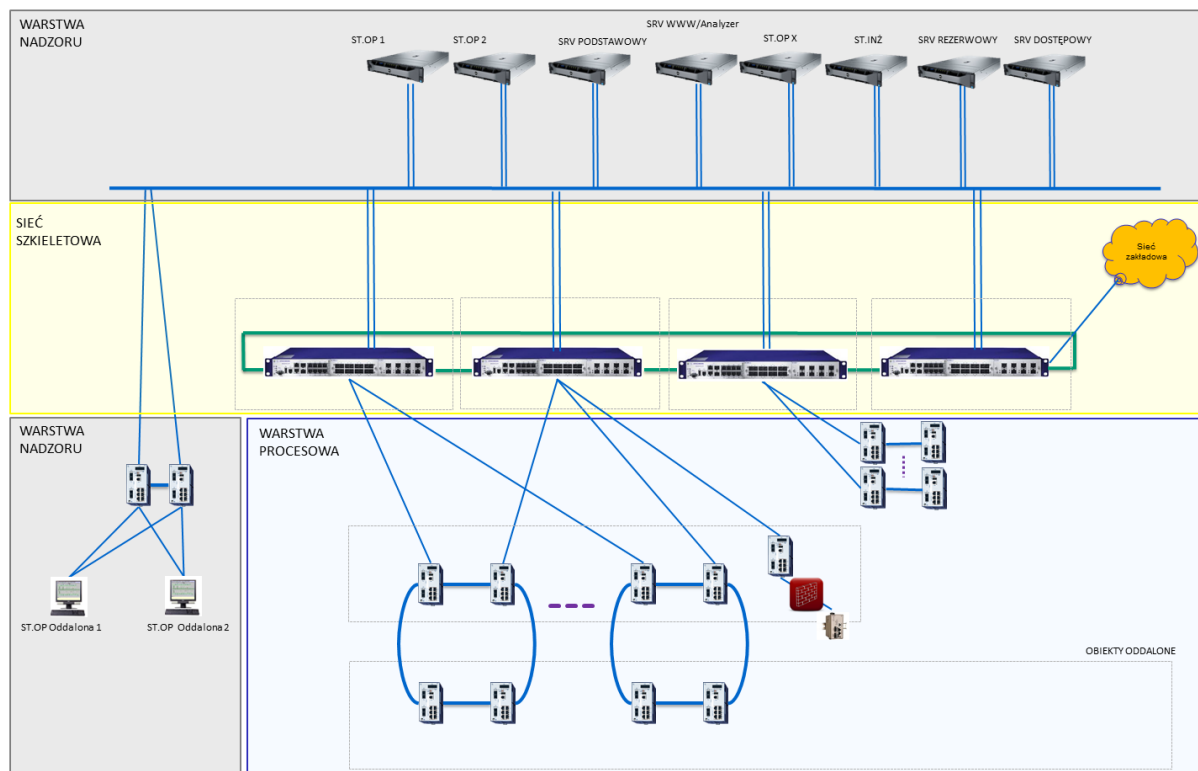
W pierwszej fazie cyberprzestępcy wnikają do sieci IT - rekonesans. Rozpoznają sieć biurową, zbierają informacje o komputerach i urządzeniach pracujących w tej sieci. W tej fazie w sieci pojawiają się anomalie w postaci niestandardowych zapytań pojawiających się raz po raz np. „czy pod danym adresem IP znajduje się jakieś urządzenie?”, „jaki typ urządzenia znajduje się pod danym adresem IP”, „wielokrotna próba uzyskania dostępu do konfiguracji urządzeń typu switch” i wiele innych. W niezainfekowanej sieci tego typu zdarzenia mają miejsce przeważnie tylko poprzez świadome działanie osób administrujących daną sieć. Jeżeli w sieci nie ma zainstalowanego systemu monitoringu pod kątem tego typu anomalii, przestępcy bezkarnie zbierają informacje na jej temat i tak długo jak tego chcą. Kwestią czasu jest uzyskanie dostępu do np. sieci LAN systemu SCADA – jest to drugi etap ataku na sieć OT.

W drugim etapie następują analogiczne działania jak w etapie pierwszym – ponowne zbieranie informacji o typach zainstalowanych urządzeń – komputer/sterownik PLC switch itd. Dodatkowo zbierane są informacje na temat budowy samego systemu SCADA, programów PLC sterowników, a także w jakich protokołach odbywa się wymiana sygnałów, jakie oprogramowanie zainstalowano na komputerach. Pod koniec tego etapu przestępcy mogą wykonać już atak, lub zdecydować o zainstalowaniu złośliwego oprogramowania w oczekiwaniu na sygnał aktywujący. Generalnie cyberprzestępcy nie mają interesu w wyłączeniu np. jednego urządzenia typu pompa czy silnik, bo to nie wyrządzi dużych szkód i cały zakład w krótkim czasie wróci do normalnej pracy. Dużo groźniejsze jest przygotowanie ataku tak, aby sparaliżować pracę zakładu na kilkadziesiąt godzin i wygenerować maksymalne straty finansowe, zaszyfrować lub usunąć wszelkie dane produkcyjne, sterujące – czyli trzeci etap skoordynowanego ataku na infrastrukturę RTU/PLC/IED.

5. Skuteczny monitoring jako uzupełnienie dla defence in depth

Aby skutecznie podjąć obronę przed typowym schematem ataku opisanym powyżej należy przede wszystkim zapewnić sobie dostęp do informacji. Możemy to porównać do funkcji kontrwywiadu podczas wojny. Za źródło informacji posłużyliśmy się w systemie ECONTROL oprogramowaniem SCADAfence. Oprogramowanie to gromadzi informacje na podstawie przekierowanego w jedną stronę całego ruchu sieci OT. Aby proces był przeprowadzony prawidłowo, należy odpowiednio skonstruować sieć OT. Najbardziej optymalnym technicznie i ekonomicznie rozwiązaniem będzie wydzielenie sieci szkieletowej (najczęściej 2 lub więcej routery warstwy trzeciej, do których wpięte są wszystkie komputery i urządzenia). Dzięki takiemu podejściu można wyeliminować wszelkie możliwe przypadki sterowań z pominięciem sieci szkieletowej, którą mamy zamiar monitorować. Przykład prawidłowo skonstruowanej sieci przedstawia rys. 2.

Dzięki zbieranim w czasie rzeczywistym informacjom, jesteśmy w stanie w szybki sposób odfiltrować zdarzenia potencjalnie niebezpieczne. Możemy skonfigurować, które zdarzenia są krytyczne i powinny wygenerować automatyczny e-mail i/lub sms do administratora sieci OT.

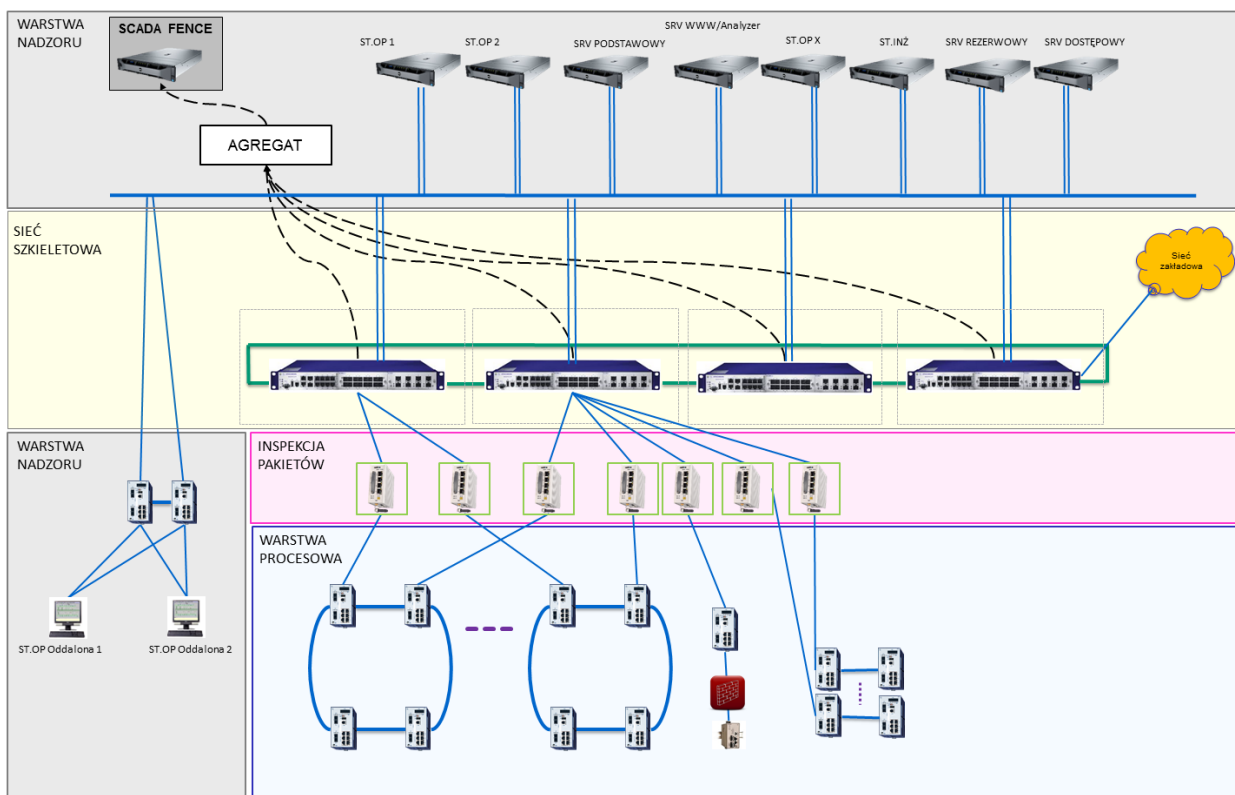


Rys. 2. Przykład sieci prawidłowo przygotowanej do skutecznego monitoringu – opracowanie własne

6. Inspekcja Pakietów (ang. deep packet inspection)

Aby wykonać kolejny krok w kierunku podniesienia bezpieczeństwa, należy się zastanowić nad możliwością blokowania niechcianych sterowań. Taką funkcjonalność możemy uzyskać poprzez dodanie pomiędzy siecią szkieletową, a warstwą procesową bram dostępowych RADiFlow 1031 z funkcją inspekcji pakietów. Blokada ta pozwoli administratorom sieci / operatorom SCADA spokojnie pracować nawet w przypadku bardziej wyrafinowanych prób ataku. Urządzenia te są zgodne z certyfikatem bezpieczeństwa NERC CIP V.5, co pozwala na jego stosowanie w aplikacjach zdalnego dostępu do podstacji energetycznych. Ponadto urządzenia obsługują certyfikaty X.509 dla IPsec VPN. Dzięki inspekcji pakietów jesteśmy w stanie zablokować wszystkie sterowania, które nie są autoryzowane przez system SCADA, ale np. mogłyby być „sztucznie wstrzyknięte” do sieci OT z zainfekowanego komputera (np. serwer www, komputer przenośny itp.). Przykładową architekturę sieci systemu ECONTROL z uwzględnieniem inspekcji pakietów przedstawiono na rys. 3. Tego typu rozwiązania wymagają dobrej znajomości sieci, którą zamierza się chronić.

Deep packet inspection polega na tym, że urządzenie (np. Radiflow 1031) na podstawie reguł w nim ustawionych przez firmę integrującą rozwiązanie, jest w stanie odczytać i zanalizować każdy przechodzący przez niego pakiet. Analiza polega na odczytaniu, źródła, celu oraz polecenia transportowanego przez pakiet. Urządzenie może to zrobić znając protokół komunikacyjny używany do komunikacji z RTU/PLC/IED oraz regułę zapisaną w urządzeniu. Na podstawie tych danych może podjąć decyzję o przepuszczeniu, odrzuceniu lub wysłaniu alarmu do systemu zbierającego dane. W sieciach, gdzie istnieje system ECONTROL, Energotest, na podstawie znajomości sieci i danych przesyłanych między poszczególnymi urządzeniami, jest w stanie sprawnie i skutecznie przeprowadzić modernizację sieci z uwzględnieniem potrzeb cyberbezpieczeństwa.



Rys. 3. Zwiększenie poziomu bezpieczeństwa poprzez dodanie inspekcji pakietów – opracowanie własne

7. Podsumowanie

Jeszcze kilkanaście lat temu tworząc w Polsce sieci OT dla infrastruktury krytycznej nikt nie zdawał sobie sprawy z tego z jakimi zagrożeniami przyjdzie nam się zmierzyć. Kilka-kilkanaście razy w ciągu roku słyszymy o tym, że używany przez nas sprzęt/oprogramowanie posiada „luki”, błędy umożliwiające hackerom dostęp do naszych danych. Liczba instalowanych „łatek”, aktualizacji krytycznych itp. rośnie rokrocznie. Praktycznie nie ma innej możliwości walki z cyberprzestępczością jak pełne stosowanie ochrony zgodnie z zasadami defence in depth czyli zespołu niezależnych zabezpieczeń – najnowsze, zaktualizowane oprogramowanie, podział sieci na warstwy, oprogramowanie antywirusowe i do tworzenia kopii zapasowych, monitoring sieci, inspekcja pakietów itp. Wydaje się, że nikt już nie zadaje sobie pytania CZY, ale KIEDY w Polsce nastąpią ataki na infrastrukturę krytyczną, w tym energetykę.

Pozostaje nam tylko przygotować się najlepiej jak to możliwe. Udaremnienie próby wyłączenia obiektu przez hackerów może być równoważne z zaoszczędzeniem milionów, a nawet dziesiątek milionów złotych. Energotest dostarcza kompletne rozwiązania, z uwzględnieniem potrzeb klienta, biorąc pod uwagę znajomość systemu i zachodzących w nim procesów, wydaje się że jest najlepszym wyborem dla sieci OT w energetyce. Jesteśmy przekonani, że tylko współpraca i wymiana doświadczeń wielu firm z branży pozwoli na osiągnięcie wspólnego celu jakim jest bezpieczeństwo.

Literatura

- [1] <https://www.gov.pl/cyfryzacja/projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa>
- [2] <http://legislacja.rcl.gov.pl/projekt/12304650/katalog/12466702>
- [3] [https://pl.wikipedia.org/wiki/Obrona_w_g%C5%82%C4%85b_\(informatyka\)](https://pl.wikipedia.org/wiki/Obrona_w_g%C5%82%C4%85b_(informatyka))
- [4] <https://www.pb.pl/najwieksze-zagrozenia-w-cyberprzestrzeni-prognoza-na-2018-902209>
- [5] www.kipr/Wyklady_PDF/Sieci_komputerowe_i_apl/SIECI_BEZP.pdf
- [6] <https://www.scadafence.com/>
- [7] <http://www.ik.org.pl/>
- [8] <https://automatykab2b.pl/katalog-produktow/produkt/10663-Radiflow1031>
- [9] https://pl.wikipedia.org/wiki/Deep_Packet_Inspection
- [10] http://isa99.isa.org/Public/Meetings/Committee/201205-Gaithersburg/ISA-99-Security_Levels_Proposal.pdf

