Profesor Zdzisław Trzaska
Politechnika Warszawska

Bezpieczeństwo systemu elektroenergetycznego i jego podatność na atak terrorystyczny

Wobec nasilającego się problemu zagrożenia światowym terroryzmem występuje pilna potrzeba identyfikowania potencjalnych działań paramilitarnych i zakresu zniszczeń, jakie może powodować użycie najnowszych broni, które są na wyposażeniu armii kilku państw oraz organizacji, czy bliżej nie rozpoznanych grup terrorystycznych aktywnych w różnych rejonach naszego globu. Dużego znaczenia nabiera również potrzeba rozpoznania taktyki i sposobów działań podejmowanych przez tego rodzaju jednostki zbrojne. Istotnym problemem w tym obszarze jest nie tylko świadomość możliwości wystąpienia zagrożeń, ale i posiadanie możliwie pełnej wiedzy o zagrożeniach oraz ich skutkach w odniesieniu do spodziewanych działań, jakie mogą być realizowane przez różne organizacje i grupy terrorystyczne lub nawet bliżej nieokreślone siły wrogie państwu, które mogą podjąć akcje zarówno z zewnętrz, jak i wewnątrz jego terytorium.

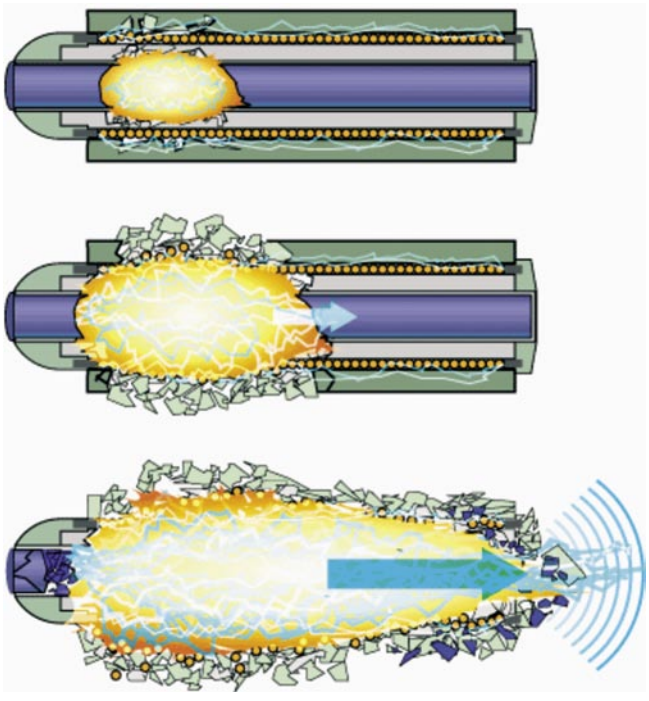
Od ataku na wieże World Trade Center w Nowym Jorku w dniu 11 września 2001 r. możliwość terrorystycznego ataku na infrastrukturę państwa jest poważna, a w tym szczególnie na ekonomiczne i socjalne funkcjonowanie społeczeństwa wskutek destrukcji zasilania energetycznego, obsługi telekomunikacyjnej, transportu itd. Atak choćby na jeden z tego rodzaju elementów infrastruktury jest w stanie zdewastować gospodarkę i zdegradować życie ludzi nie tylko w aglomeracji miejskiej, ale też na stosunkowo dużym terytorium kraju [1] – [4].

Szczególnej uwadze i trosce państwa powinien podlegać krajowy system elektroenergetyczny ze względu na jego bezcenne znaczenie dla współczesnej gospodarki i rozwoju kulturowego społeczeństwa. Bezsprzecznie stanowi on bardzo ważny element ogólnego bogactwa narodowego i powinien stale działać w niezawodny sposób przy zachowaniu znamionowych parametrów. Obecnie jest już niemal pewnikiem, że prawidłowe funkcjonowanie systemu elektroenergetycznego jest istotnym wyznacznikiem dla wskaźników ekonomicznych gospodarki i bezpieczeństwa państwa.

Zagrożenie w tym obszarze staje się jednak coraz bardziej prawdopodobne ze względu na rosnącą łatwość powszechnego dostępu do bardzo efektywnej broni najnowszej generacji. Tą najnowszą bronią są tak zwane bomby elektromagnetyczne zwane skrótowo *E-bombami*, które zyskały już miano broni humanitarnej, jako że swą siłą rażenia niszczą przede wszystkim urządzenia elektroniczne i informatyczne przeciwnika bez wyrządzania większych szkód w sferze biologicznej i środowisku naturalnym człowieka. Pojęcia równoważne *bomba elektromagnetyczna* oraz E-bomba odnoszą się do nienuklearnych bomb zarówno mikrofalowych, jak i niskiej częstotliwości. Ale to, czym zachwycają się wojskowi, budzi poważny niepokój ekspertów zajmujących się kwestiami bezpieczeństwa państwa. Bowiem największych zniszczeń bomby *E* mogłyby dokonać w wysoko uprzemysłowionych rejonach, gdzie nie można już sobie wyobrazić życia bez komputerów i elektroniki.

Niepokój budzi fakt, że tego rodzaju broń można wyprodukować bardzo tanio i przy użyciu niezbyt skomplikowanych technologii. Jej konstrukcja jest prosta i może mieć rozmiary mniejsze niż podróżny neseser, a jej ciężar może nie przekraczać 20 kg [3], [5].

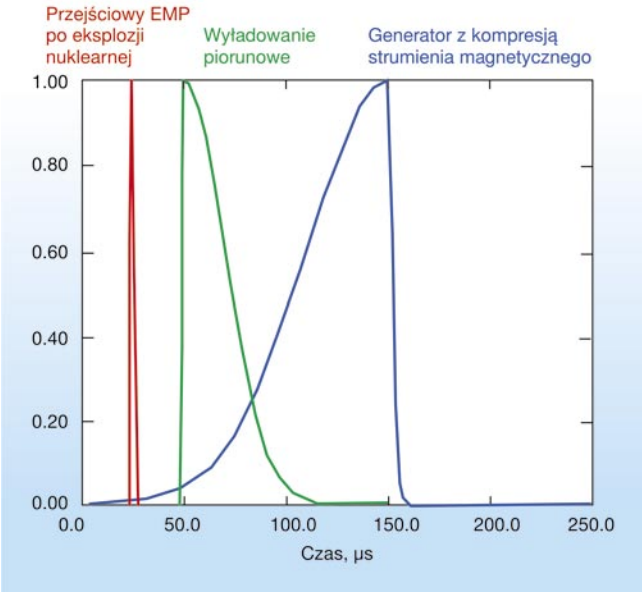
Bomba *E* w warsztatowym wykonaniu może mieć postać następującą: miedziana rura owinięta miedzianym drutem jest napełniona materiałem wybuchowym (rys.1). Całość jest pokryta twardym i mechanicznie wytrzymałym płaszczem polimerowym. Uzwojenie połączone za pośrednictwem odpowiednio skonstruowanego generatora Marxa z baterią naładowanych kondensatorów wytwarza silne pole magnetyczne w najbliższym jego otoczeniu. W chwili, gdy prąd w uzwojeniu osiąga wartość maksymalną, zostaje zdetonowany ładunek wybuchowy w środku i rura rozciągając się rozrywa kolejne zwoje powodując tym kompresję strumienia magnetycznego. Dochodzi wówczas do krótkiego spięcia zwojów cewki, które wędruje wzdłuż jej osi.



Rys. 1. Eksplozyjna generacja silnego impulsu elektromagnetycznego

Pole magnetyczne skoncentrowane wokół uzwojenia na ułamki sekund zostaje skompresowane, podczas gdy energia pozostaje skoncentrowana w małej stosunkowo przestrzeni wokół miedzianej rury. Efektem jest wyzwolenie olbrzymiego natężenia pola magnetycznego i impulsu elektrycznego rzędu milionów amperów i o ładunku znacznie przekraczającym ładunek pioruna.

Porównanie przebiegów trzech różnych unormowanych impulsów elektromagnetycznych przedstawiono na rysunku 2 [6], [7].



Rys. 2. Porównanie elektromagnetycznych impulsów różnej natury

Niszczące działanie *E-bomby*, zwanej też bronią w zakresie częstotliwości radiowych, (*MBDM* – mikrofalowa broń dużej mocy) wynika z tego, że przez ułamek mikrosekundy wysyła ona w określoną przestrzeń falę elektromagnetyczną w zakresie mikrofalowym o mocy chwilowej rzędu nawet kilku lub kilkudziesięciu GW. Rozprzestrzeniająca się w danym środowisku fala elektromagnetyczna wyemitowana przez *E-bombę* dociera w obszarze rażenia do znajdujących się tam urządzeń elektrycznych i indukuje w nich zmienne napięcia, które powodują znaczne uszkodzenia lub wywołują poważne zakłócenia w ich normalnym działaniu. Według opinii ekspertów, *E-bomby* zostały już użyte na polu walki przez armię Stanów Zjednoczonych w ramach operacji „Pustynny lis" w działaniach wojennych na terenie Kuwejtu, a następnie w operacjach wojskowych „Pustynna burza" na terenie Iraku.

Od wielu już lat są prowadzone na świecie badania zmierzające do konstrukcji mikrofalowych źródeł energii o bardzo dużej mocy (*MŹDM*) dla zastosowań nie tylko jako potencjalnie efektywna broń ofensywna na polu walki, ale także jako środki skutecznego sabotażu oraz działań terrorystycznych [2].

Ze względu na stosunkowo znaczną prostotę w budowie i łatwość przenoszenia, a także precyzyjnego skierowania na konkretny cel można oceniać, że różne odmiany broni elektromagnetycznej, a w tym również pistolety i małe rakiety mogą się wkrótce znaleźć w posiadaniu grup terrorystów najprzeróżniejszych autoramentów. Na listę przewidywanych ataków terrorystów wciągnięta została broń elektromagnetyczna wielorakiego kalibru i przeznaczenia. Ustalane są pilnie także najróżniejsze scenariusze ataków terrorystycznych z użyciem tych elektromagnetycznych broni. W scenariuszu takim znajduje się również atak na system elektroenergetyczny państwa jako ten, który spowoduje całkowity paraliż gospodarki i wszystkich jego służb społecznych.

Realizacja takiego scenariusza oznaczać może tysiące ofiar i miliardy dolarów strat, co może doprowadzić kraj do ekonomicznego i społecznego krachu. Stąd też ważnym problemem staje się ustalenie metod oceny odporności systemu elektroenergetycznego na różne postaci ataków terrorystycznych z użyciem broni elektromagnetycznych.

Niniejszy artykuł jest poświęcony prezentacji efektywnej procedury ogólnej umożliwiającej ustalenie skutków, jakie może wywołać określony typ ataku terrorystycznego nakierowanego na różne elementy tworzące rozległą sieć reprezentującą system elektroenergetyczny. Zasadnicza uwaga została skupiona na identyfikacji stopnia odporności określonej struktury sieci tworzącej system elektroenergetyczny na efekty ataków terrorystycznych różnej postaci.

Formy i efekty ataku terrorystycznego na system elektroenergetyczny

Ze względu na jawną strukturę i szczególną postać elementów systemu elektroenergetycznego jest on wyjątkowo podatny na różnorodne formy ataków terrorystycznych, a nawet zwykłych aktów sabotażu.

Znane są z niedawnej przeszłości liczne przypadki tego rodzaju działań w różnych rejonach na świecie [1], [3]. Koszty usuwania ich skutków dochodziły częstokroć do wielomilionowych sum. Ponadto stawały się one przyczyną poważnych awarii w działaniu systemów elektroenergetycznych w kilku krajach zarówno w Europie, jak i w Ameryce. Pociągnęły one za sobą również określone negatywne skutki w gospodarkach tych krajów, w których ataki terrorystyczne skierowane były na systemy elektroenergetyczne.

W odniesieniu do samego systemu elektroenergetycznego możliwe są trzy formy ataku terrorystycznego.

Bezpośredni atak na system

Celem ataku jest elektryczna infrastruktura systemu. Terroryści mogą na przykład zaatakować jednocześnie dwie podstacje lub kluczowe rozdzielnie w celu wywołania awarii na dużym obszarze sieci. Innym przykładem może być atak terrorystyczny na rynek energii elektrycznej.

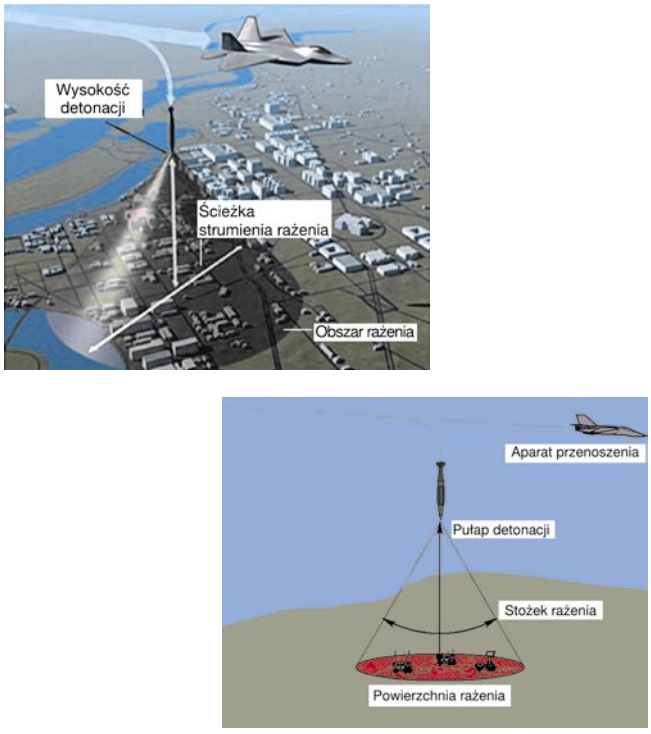
Atak za pomocą systemu elektroenergetycznego

Terroryści mogą użyć pewnych urządzeń będących elementami systemu do ataku na ludność, jak na przykład, wykorzystać słupy wysokiego napięcia do rozpylenia szkodliwych substancji chemicznych lub biologicznych.

Atak poprzez system elektroenergetyczny

Terroryści mogą użyć niektórych instalacji w systemie do zaatakowania cywilnej infrastruktury. Terroryści mogą na przykład wywołać silny impuls elektromagnetyczny w sieci w celu uszkodzenia komputerów i infrastruktury telekomunikacyjnej państwa lub jego znacznego obszaru.

W dalszej części artykułu przedstawiono informacje dotyczące bezpośredniego ataku na system elektroenergetyczny.



Rys. 3. Ilustracja obszaru rażenia w przypadku ataku z użyciem *E-bomby*

Doświadczeni specjaliści z zakresu złożonej dynamiki systemu elektroenergetycznego są zaniepokojeni możliwościami pojawienia się negatywnych skutków wywołanych nawet sporadycznym atakiem terrorystycznym z wykorzystaniem *MBDM*. W przypadku działania *E-bomby* pole rażenia objęte jest powierzchnią wyznaczoną przez typ bomby oraz pułap jej detonacji (rys. 3). Przestrzeń rażenia jest bardzo ściśle sprecyzowana, a selektywność osiągania celu jest wyznaczana na skalę nieosiągalną dotąd na polu walki. Z tego też powodu, w celu maksymalnego ograniczenia negatywnych efektów wywołanych atakiem terrorystycznym, niezbędna jest dokładna i właściwa analiza odporności na taki rodzaj działań w odniesieniu do poszczególnych elementów sieci. Jest to konieczne w celu określenia odporności na atak terrorystyczny nie tylko nowo projektowanych rozwiązań, ale również wpływu proponowanych modyfikacji na odporność systemów już istniejących lub też dla ustalenia niezbędnych modyfikacji dla osiągnięcia pożądanej jego właściwości w określonej sytuacji.

Ze względu na postępujące liberalizowanie przepisów i zasad korzystania z energii elektrycznej przez różnorodnych jej użytkowników wyłania się konieczność położenia wyraźnego akcentu na potrzebę opracowania dokładnych metod oceny niezawodności realizowanych rozpływów energii podczas wystąpienia określonego rodzaju ataku terrorystycznego. Wiąże się z tym konieczność ustalenia warunków ochrony i priorytetów dostępu do energii odbiorców zwiększonego ryzyka oraz uwzględnienia wpływu struktury sieciowej na działania zapewniające bezpieczeństwo sterowania, a także na potrzebę zawężania marginesu obszarów rażenia. Ponadto, jak wykazano w [8] – [10] tradycyjne modele sieciowe nie są w stanie dokładnie odzwierciedlić dynamiki systemu elektroenergetycznego w pewnych warunkach, a szczególnie w pobliżu granic obszarów rażenia skutkami zdetonowania *E-bomby*.

Należy jednak podkreślić, że obecnie funkcjonująca struktura systemu elektroenergetycznego nie może zostać zastąpiona całkowicie, przynajmniej w przewidywalnym horyzoncie czasowym, jakąś strukturą odporną na nieprzewidywalne miejsce ataku terrorystycznego, jego zasięg oraz siłę rażenia.

W związku z tym problemem wymagającym pilnego rozwiązania w najbliższej przyszłości staje się pokonanie trudności w szybkim sterowaniu napięciami węzłów, poprawą zbieżności procesów obliczeń rozpływów obciążenia i poszerzenie dotychczasowych wąskich obszarów stabilności stanów przejściowych. Pojawia się przy tym pytanie: w jaki sposób te wielkości powinny być sterowane w warunkach zaistnienia ataku terrorystycznego?

W odpowiedzi na tak postawione pytanie proponuje się wprowadzenie procedury umożliwiającej identyfikację krytycznej struktury systemu elektroenergetycznego z uwzględnieniem generatorów, linii przesyłowych, węzłów zasilających, stacji i transformatorów poprzez ocenę maksymalnej ich podatności na skoordynowane ataki na system. Poprzez badanie skutecznego sposobu ataku na system, ustalić można działania możliwe do podjęcia w celu zmniejszenia skutków określonego ataku terrorystycznego.

Głównie trzy czynniki określają znaczenie poszczególnych elementów w rozległej sieci, a mianowicie:

- podatność na uszkodzenia,
- wpływ uszkodzonego elementu na działanie systemu oraz
- trudności jego wymiany lub naprawy.

Czynniki te nabierają różnego znaczenia w poszczególnych sytuacjach działań terrorystycznych. Na przykład, elektrownie mogą zostać zniszczone przez terrorystów zamierzających wtargnąć do wnętrza budynku, lecz obecność tam obsługi wykonującej swe normalne zadania i obowiązki stanowi czynnik odstraszający. Jeśli jednak terrorystą staje się pracownik elektrowni, to realizacja ataku terrorystycznego staje się łatwiejsza. Rozległa i długotrwała awaria może być spowodowana jedynie jako wynik uszkodzenia równocześnie w wielu miejscach obwodów łączących elektrownie z odbiorcami. Pojedyncze uszkodzenie nie będzie mieć znaczącego wpływu na przepływ energii do odbiorców, ponieważ większość wytwórców energii utrzymuje poważne rezerwy zarówno w generacji, jak i transmisji energii w celu zabezpieczenia się na wypadek takiej awarii.

Natomiast w przypadku powstania większej liczby awarii, zarówno na poziomie elektrowni, jak i w układzie przesyłowym do odbiorców, rozległa sieć, jaką przedstawia sobą system elektroenergetyczny może się zdekomponować na strukturę wyspową. Po utworzeniu się takiej struktury, pewne z wysp będą miały nadmiary lub też niedobory zdolności wytwórczych i mogą utracić połączenie z innymi wyspami. Pozostałe wyspy działające w warunkach zbilansowania mogą podtrzymywać swe funkcje, nie będąc połączone z pozostałą częścią systemu. Kształt struktury wyspowej jest trudny do przewidzenia, gdyż zależy on od usytuowania odbiorów, rodzaju funkcjonujących elektrowni, konfiguracji systemu przesyłowego oraz od typu ataku.

W wyjątkowych sytuacjach może się zdarzyć poważna awaria całego systemu.

Współczesne układy zabezpieczeń powinny chronić system przed kaskadowym typem awarii, które wystąpiły w przeszłości zarówno w kilku systemach europejskich, jak i północnoamerykańskich. Jednakże pewność w tym zakresie jest kwestionowana, gdyż brak jest możliwości testowania takich sytuacji.

Większość poważnych odbiorców jest tak wyposażana w odpowiednie urządzenia, że po zaistnieniu miejscowej awarii może w ciągu dnia lub dwóch przywrócić swe zdolności do normalnego działania, podczas gdy poważne uszkodzenia linii przesyłowych i rozdzielczych mogą powodować przerwy trwające nawet kilka tygodni.

W przypadku uszkodzeń wszystkich transformatorów w wielu stacjach może wystąpić potrzeba sięgnięcia po pomoc towarzystw zagranicznych w celu wymiany urządzeń i odtworzenia właściwej obsługi. To, czy zagranica odpowie pozytywnie i szybko na taką sytuację nie jest pewne.

Ponadto należy brać pod uwagę również to, że system elektroenergetyczny traci margines rezerwy w miarę wzrostu obciążenia ponad warunki jego konstrukcji. Marginesy rezerwy są zazwyczaj bardzo duże i pozostają jak dotąd w pewnych obszarach, co stanowi znaczącą dogodność z punktu widzenia odbiorców. Stąd też w przypadku rozległego ataku terrorystycznego znaczne marginesy rezerw stają się wyjątkowo ważne, gdyż wydatnie ułatwiają odtworzenie zdolności zasilania dla określonych odbiorców. Operatorzy dysponują wówczas dodatkowymi możliwościami ustalenia sposobów zapewnienia na odpowiednim poziomie zarówno wytwarzania, jak i przesyłu do odbiorców niezbędnej dla nich energii.

Sposoby redukcji niesprawności systemu po ataku terrorystycznym mogą być zgrupowane według właściwości niepodatności na uszkodzenie, ograniczoności skutków uszkodzenia w dowolnym miejscu oraz czasu usunięcia uszkodzenia. Najpewniejszym zapobieganiem powstawania uszkodzeń jest udoskonalenie fizycznego bezpieczeństwa i odporności na atak oraz wyeliminowanie ułatwień. Wzmocnienie ścian rozdzielni, budowa odpowiednich ogrodzeń oraz systemy ochrony i ciągłego nadzoru wymagają niewielkich kosztów zwłaszcza w porównaniu z kosztem wymiany urządzeń.

Możliwe zabezpieczenia

Zabezpieczenie przed wyrafinowanym atakiem terrorystycznym okazuje się bardzo kosztowne, a prawdopodobieństwo jego skuteczności jest bardzo niskie, jeśli sposoby przeciwdziałania nie zostały podjęte na miejscu. Jednocześnie nawet w przypadku zastosowania odpowiedniej ochrony, odporność linii przesyłowych na atak terrorystyczny z powietrza jest bardzo kiepska. Bardzo łatwo mogą być uszkodzone izolatory na słupach, a nawet przerwane mogą być same przewody lub też łatwo można uziemić całą linię. Takie uszkodzenia można stosunkowo prosto i w miarę szybko usunąć, jeśli odpowiednie służby nadzoru i utrzymania ruchu dysponują zapasowymi elementami. Jednak terroryści mogą łatwo powtórzyć swój atak równie szybko na innym odcinku tej samej linii lub też na innych liniach. Kluczowe linie przesyłowe mogą być unieruchomione na dłuższy okres. Zabezpieczeniem przed taką sytuacją może być wcześniejsze zaplanowanie koordynacji działań z Agencją Bezpieczeństwa Wewnętrznego (ABW) w celu uzyskania ostrzeżeń, a także z policją i służbami wojskowymi.

W szkoleniu pracowników służb energetycznych należy uwzględnić istotny czynnik, jakim jest zwiększona czujność i reagowanie na podejrzane działania i rozpoznawanie zachowań terrorystów i powiadamianie o tym odpowiednich służb i instytucji. Przedsięwzięciami zapobiegającymi uszkodzeniom mogą być odpowiednie szkolenia operatorów systemu, tak aby potrafili oni rozpoznać i stosownie zareagować na poważne zakłócenia w pracy systemu, a w miarę potrzeby wprowadzić udoskonalenia w funkcjonowaniu ośrodków sterowania systemem oraz dokonać innych modyfikacji systemu, a także zwiększenia rezerwy łączeniowej. Intencją takich działań powinna być możliwość odizolowania uszkodzonej części i pozostawienie zasilania możliwie jak największej liczbie odbiorców. Szybkie działanie może zapobiec rozprzestrzenieniu się uszkodzenia na inne obszary.

Tabela 1

Możliwe środki polepszenia odporności systemu na atak terrorystyczny

Środki zaradcze	Łatwe do zastosowania	Niski koszt	Ukierunkowane na wzrost inwestycji
A. Zabopiegania uszkodzeniu			
Ochrona krytycznych urządzeń kluczowych podstacji ścianami, wzmocnionym wyposażeniem odpornym na uszkodzenia, itp.			x
Nadzór (zdalny monitoring) kluczowych urządzeń (sprzężony z siłami szybkiego reagowania).			x
Ustawienie agentów ochrony w kluczowych podstacjach			x
Udoskonalenie koordynacji z oficjalnymi agencjami bezpieczeństwa dla zapewnienia informacji uprzedzenia i koordynacji odpowiedzi	x		
	x		
B. Ograniczenie skutków			
Doskonalenie planowania bezpieczeństwa i szkolenie operacyjne	x		
Modyfikacja rzeczywistego systemu; doskonalenie centrów sterowania, zwiększenie marginesów rezerwy, itd.		X	X
Zwiększenie rezerw przełączeń		x	
C. Przyspieszenie napraw			x
Planowanie działań służb odpowiedzialnych za naprawę		x	
Porządkowanie prawno/instytucjonalnej odpowiedzialności za udostępnianie urządzeń zapasowych	x x		
Utrzymywanie zapasu krytycznych urządzeń (transformatorów) lub wszystkich innych specjalistycznych materiałów	x	x x	
Zapewnienie odpowiedniego transportu dla ciężkich urządzeń	x		
Monitorowanie krajowych możliwości produkcyjnych		x x	
D. Ogólna redukcja uszkodzeń			
Stosowanie technologii mniej podatnych na uszkodzenia			
Preferowanie zdecentralizowanych systemów wytwórczych			

Nabiera to szczególnego znaczenia w przypadku transformatorów dużej mocy. Czas usunięcia awarii może być znacznie skrócony jeśli dostępnych jest więcej elementów zapasowych. Potrzebna jest w tym zakresie odpowiednia legislacja, gdyż brak zapewnienia odpowiedniego sprzętu zapasowego we właściwej ilości może być przyczyną nadmiernych kosztów i długich przestojów w działaniu systemu lub jego części. Nie bez znaczenia jest tu maksymalnie możliwa standaryzacja urządzeń, a zwłaszcza transformatorów różnych poziomów napięć. Nasuwa się również potrzeba zwiększenia udziału podziemnych kabli odpornych na uszkodzenia w znacznie większym stopniu w porównaniu z powszechnie obecnie stosowanymi liniami napowietrznymi.

W tabeli 1 zestawiono działania zapobiegawcze:

- możliwe do wprowadzenia w obecnych warunkach bez ponoszenia większych nakładów finansowych
- takie, które mogą być wprowadzone przy umiarkowanych kosztach oraz
- te, które będą możliwe do wdrożenia, ale przy relatywnie wysokich nakładach finansowych.

Zapewne koszty wprowadzenia niektórych z tych działań będą musiały być przeniesione na odbiorców. Należy także podkreślić, że zakres niezbędnych działań oraz ich koszt nie mogą być ściśle ustalone, ponieważ zależą one w znacznym stopniu od skutków spowodowanych atakiem. W przypadku krańcowym koszt będzie zapewne wielokrotnie większy od kosztów działań uprzedzających.

Uznać jednak można, ze w przypadku dużego zagrożenia terroryzmem każdy wzrost kosztów inwestycji zapobiegających negatywnym skutkom tego rodzaju aktów destrukcyjnych jest całkowicie uzasadniony. Nie jest jednak możliwe dokładne sprecyzowanie, czy nawet kosztowne inwestycje będą w stanie zredukować skutki ataku. Wymaga to zastosowania odpowiednich modeli sieci rozległych na przypadek wystąpienia różnych form ataku terrorystycznego.

Modele matematyczne

Sformułowanie odpowiedzi na powyżej postawione pytanie oraz na inne z nim związane pojawia się dopiero po bardzo dokładnej analizie możliwie wszystkich czynników wpływających na odstępstwa w działaniu systemu od normy. Wynika to z tego, że nawet relatywnie biorąc małe zmiany parametrów sieci mogą prowadzić do powstania bardzo złożonej jej dynamiki. Jest to spowodowane kompleksowym charakterem rozległej sieci, w której bardzo duża liczba niezależnych od siebie czynników oddziaływa wzajemnie na bardzo wiele sposobów. W celu oceny tego zagadnienia możemy zidentyfikować krytyczne elementy sieci poprzez ustalenie matematycznego modelu zabronionego, który będzie reprezentował problem optymalnego ataku terrorystycznego, jaki grupa terrorystyczna może zrealizować w określonej strukturze. Jest on modelem *max-min* o postaci

$$\max_{\alpha\in\wp}\ \min_{\mathbf{p}}\ \mathbf{c}^{\mathrm{T}}\mathbf{p} \quad \text{przy} \quad \mathbf{f}(\mathbf{p},\alpha)\le\mathbf{b} \quad \text{oraz} \quad \mathbf{p}\ge\mathbf{0} \qquad (1)$$

gdzie: $\boldsymbol{p}$ jest wektorem, którego elementami są moce czynne generatorów, linii, odbiorników oraz „zrzut" mocy równy nie zaspokojonej potrzebie, a także kąty fazowe napięć w określonych węzłach systemu.

Element α_k dyskretnego zbioru P jest liczbą binarną i równa się 1 lub 0 gdy element systemu został lub nie został zaatakowany przez terrorystów. Zbiór P jest zbiorem dyskretnym i odzwierciedla atak, jaki grupa terrorystyczna podjęła w danym systemie.

W modelu (1) funkcja wektorowa $\boldsymbol{f}$ reprezentuje zbiór funkcji nieliniowych względem argumentu ($\mathbf{p}$, $\boldsymbol{\alpha}$). Wewnętrzny model zabroniony powstaje z modelu (1) przy przyjęciu funkcji $\boldsymbol{f}$ jako liniowo zależnej od $\boldsymbol{p}$ przy stałej wartości $\boldsymbol{\alpha} = \acute{\boldsymbol{\alpha}}$. Jeśli przyjąć, z punktu widzenia odbiorcy, że decydującą wielkością jest moc czynna P, a efekty związane z mocą bierną można zaniedbać, to otrzymujemy tzw. model zabroniony dla prądu stałego z optymalnym przepływem energii, a mianowicie

$$\begin{aligned}
&\min_{P^G,P^L,S,\Theta}\sum_k h_k P_k^G+\sum_n\sum_c g_{n,c}D_{n,c}, \quad \text{przy warunkach}\\
&P_k^L = B_k(\Theta_{o(k)}-\Theta_{d(k)})-\\
&-P'^L_k\le P_k^L\le P'^L_k,\ \ 0\le P_k^G\le P'^G_k,\forall k,\ \ 0\le S_{n,c}\le d_{n,c},\ \forall n,c \qquad (2)\\
&\sum_k P_k^G-\sum_{m|o(m)=i}P_m^L+\sum_{m\setminus d(m)=i}P_m^L=\sum_c(S_{i,c}-D_{i,c})\,\forall i
\end{aligned}$$

gdzie: $B_k = X_k/(R_k^2+X_k^2$ oznacza susceptancję linii o małych stratach a $D_{n,c}$ oznacza deficyt energii sektora c połączonego z węzłem n.
Obciążenie tego sektora w normalnych warunkach oznaczone jest przez $S_{n,c}$. Współczynniki h_k oraz $g_{n,c}$ wyrażają koszty jednostkowe energii, odpowiednio, wytwarzania oraz deficytu.

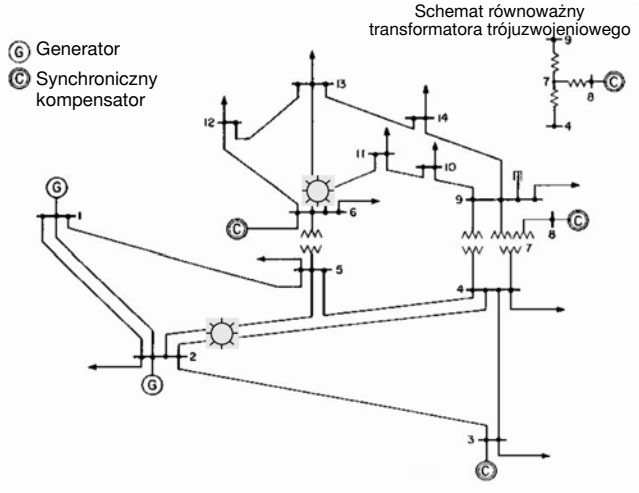
W ten sposób badane zagadnienie sprowadza się do minimalizacji kosztu wytwarzania i kosztu niedoboru energii w systemie zaatakowanym skutecznie przez terrorystów. Jeśli grupę terrorystów przyjmiemy jako „zakaz" działania określonego elementu w systemie, to w modelu (2) należy wprowadzić zbiór dodatkowych ograniczeń wynikających z określonego zakazu. Skutek tego „zakazu" uzależniony jest od zdolności destrukcyjnej, jaką dysponują atakujący terroryści. Każdy z elementów systemu wymaga zastosowania odpowiedniej siły destrukcyjnej w celu pozbawienia go swojej funkcji w systemie. Zależnie od siły destrukcji grupy terrorystycznej oraz punktów ataku, zdolność wytwórcza i przesyłowa systemu maleje nieliniowo, a odpowiedni wykres przedstawiający wzrost niedoboru w zaspokojeniu potrzeb odbiorców przypomina krzywą ładowania kondensatora od zerowego stanu początkowego.

Przykładowa sytuacja z dwoma punktami jednoczesnego ataku w systemie o 14 węzłach jest przedstawiona na rysunku 4 [10]. Punkty ataku zostały oznaczone symbolem ☼.

W przypadku siły destrukcji odpowiadającej 10 jednostkom niedobór w zasilaniu odbiorców zbliża się do 50%, a po przekroczeniu w sile destrukcji 25 jednostek dochodzi on do 90%. W ten sposób ujawnia się większe znaczenie grup terrorystów w porównaniu z indywidualnymi działaniami podejmowanymi przez pojedyncze osoby.

W grupie pełniej wykorzystywane są umiejętności poszczególnych jej członków, kontakty między nimi, a także lepiej realizowany jest przydział cząstkowych zadań.

Nie bez znaczenia jest także możliwość uprzedniego zdobycia szczegółowych informacji o przedmiocie ataku, jego zabezpieczeniu i formach alarmu. Z drugiej jednak strony grupa jest łatwiejsza do wykrycia i zidentyfikowania niż terroryści działający w pojedynkę.



Rys. 4. Standardowy IEEE model systemu o czternastu węzłach

Dalsze modyfikacje modelu (1) powinny podejmować takie zagadnienia, jak uwzględnienie liniowej zależności w nierówności przedstawiającej ograniczenia oraz rozszerzenie przyjętego modelu.

Wyniki symulacji

Wyniki symulacji komputerowych różnorodnych struktur rozległych sieci dla układów elektroenergetycznych z uwzględnieniem źródeł energii, systemu przesyłowego, podstacji oraz jej odbiorników wskazują na szereg możliwych sytuacji, które ujawniają bardzo niekorzystne wskaźniki eksploatacyjne spowodowane atakami terrorystycznymi o zróżnicowanej sile destrukcji i różnych miejscach ich wystąpienia.

Dla pewnych sił destrukcji i odpowiednich miejsc jednoczesnego ataku system może praktycznie biorąc utracić całkowicie swe zdolności do wytwarzania i przesyłu energii do odbiorców.

Możliwe są przy tym różne scenariusze zapobiegania skutkom ataków terrorystycznych, ale wymaga to odpowiednich inwestycji, stosownie do reguł przedstawionych w tabeli 1.

Tabela 2

Podatność na atak terrorystyczny
oraz restytycję sprawności działania

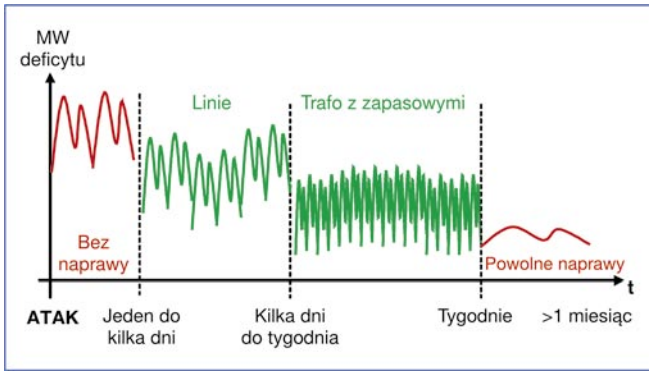
Element sieci	Zagrożenie	Siła ataku, liczba terrorystów	Czas trwania awarii, h
Linie (napowietrzne)	tak	1	72
Linie kablowe (podziemne)	nie	–	–
Transformatory	tak	2	768
Rozdzielnie	tak	3	360
Generatory	nie	–	–
Podstacje	tak	3	768

Wprowadzenie odpowiednich regulacji pozwala w dużym stopniu zmniejszyć podatność danego systemu na określony atak terrorystyczny, a także zniwelować znacznie jego skutki.

W tabeli 2 podano powszechnie stosowane miary określenia podatności poszczególnych elementów systemu na atak terrorystyczny oraz skutki nim wywołane.

Zmiany w deficycie mocy w różnych przedziałach czasu po ataku są przedstawione na rysunku 5.

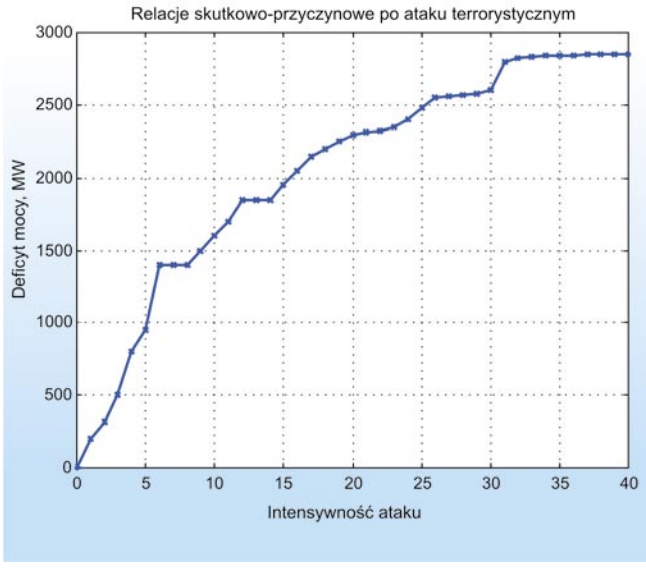
Przyjęte zostało, że siła ataku wyrażona jest liczbą terrorystów biorących w nim udział, a skutki wyrażone są powstałym niedoborem mocy w stosunku do normalnego działania tego systemu w określonym czasie po ataku .



Rys. 5. Przykładowe zmiany
w czasie niedoboru mocy w systemie

Zmiany te odzwierciedlone są krzywą niemalejącą przy wzroście liczby terrorystów. Granicznie, gdy liczba terrorystów przekroczy 30, system przestaje działać.

Na szczegółową postać tej zależności ma również wpływ liczba i odległości miejsc wystąpienia jednoczesnego ataku, a także rodzaj uszkodzonych elementów. Jednak ogólny charakter tej zależności pozostaje podobny do tego, który jest przedstawiony na rysunku 6.



Rys. 6. Zależność deficytu mocy w sieci od intensywności ataku terrorystycznego

Zauważyć można, że istotne znaczenie przy kształtowaniu tej zależności ma odporność poszczególnych elementów na atak terrorystyczny. Odporność ta jest wyrażana liczbą terrorystów niezbędnych do uszkodzenia danego elementu systemu. Odpowiada to sile ataku zgodnie z wyszczególnieniem podanym w tabeli 2. Dalsze badania powinny być jednak ukierunkowane na uwzględnieniu w modelu, a następnie w symulacji komputerowej zdolności usuwania skutków awarii spowodowanej atakiem.

Nie bez znaczenia jest stosowanie odpowiedniej ochrony zarówno materialnej, jak i logistycznej oraz właściwego współdziałania służb elektroenergetycznych z określonymi organami bezpieczeństwa państwa.

Podsumowanie

Analiza różnorodnych struktur układów elektroenergetycznych z uwzględnieniem źródeł energii, sieci przesyłowych, podstacji oraz odbiorów wskazuje na wiele możliwych sytuacji, które ujawniają bardzo niekorzystne wskaźniki eksploatacyjne spowodowane atakami terrorystycznymi o zróżnicowanej sile destrukcji i różnych miejscach ich wystąpienia. Dla pewnych sił destrukcji i odpowiednich miejsc ataku jednoczesnego system może, praktycznie biorąc, utracić całkowicie swe zdolności do wytwarzania i przesyłania energii do odbiorców. Możliwe są przy tym różne scenariusze zapobiegania skutkom ataków terrorystycznych, ale wymagają one odpowiednich inwestycji, stosownie do reguł przedstawionych w tabeli 1.

Niezbędne są także dalsze szczegółowe badania mające na celu uwzględnienia w modelu, a następnie w symulacji komputerowej zdolności prewencji materialnej i logistycznej, a także przyjęcie odpowiednich aktów prawnych pozwalających na efektywne usuwania skutków awarii spowodowanej atakiem oraz ich minimalizacji.

Nie bez znaczenia przy tym powinno być właściwe szkolenie służb energetycznych w zakresie identyfikacji zagrożeń wystąpienia ataku terrorystycznego w odniesieniu do systemu elektroenergetycznego oraz określonego ich współdziałania z właściwymi organami bezpieczeństwa państwa.

LITERATURA

[1] Salmeron J., Wood K., Baldick R.: Analysis of Electric Grid Security Under Terrorist Threat. *IEEE Trans. On Power Systems,* vol.19, No.2, 2004, ss. 905–912

[2] Szafranski R., Parallel War and Hyperwar. Rozdział 5 w Schneider B.R, Grinter L.E. (red.), Battlefield of the Future, 21st Century Warfare Issues, Air University Press, Maxwell AFB, 1995

[3] Kopp C., A Doctrine for the Use of Electromagnetic Pulse Bombs, Working Paper No.15, Air Power Studies Centre, Royal Australian Air Force, Canberra, July 1993

[4] Warden J.A. III, Air Theory for the Twenty-first Century, Chapter 4 in Schneider B.R, Grinter L.E., Battlefield of the Future, 21st Century Warfare Issues, Air University Press, Maxwell AFB, September 1995

[5] Trzaska Z.: Struktura i podstawowe właściwości elektromagnetycznej bomby: *e-bomby*. Mat. PES-5, Zakopane-Kościelisko, 20-24 czerwca 2005

[6] Trzaska Z.: Determining the Response of Power Transmission and Distribution Lines to a Nuclear Detonation at a High Altitude. Proc. Intern. Sympos. ELMECO'94, Lublin, Kazimierz Dolny, 1994, pp. 489-495

[7] Tesche F. M., Ianoz M. V., Karlsson T.: EMC Analysis methods and Computational Models. Wiley, New York, 1997

[8] Anderson P.M., Fouad A.A.: *Power System Control and Stability*. Ames, Iowa St. Univ. Press,1977

[9] Bergen A.R., Hill D.J.: A structure preserving model for power system stability analysis. *IEEE Transactions on Power Apparatus and Systems*, PAS-100, nr 1, 1981, ss.25-33

[10] Marszalek W., Trzaska Z.: Singularity Induced Bifurcations in Electrical Power Systems. *IEEE Trans. Power Systems*, 2005, Vol. 20, No. 1, pp. 312-320

[11] Kakudate Y., Usuba S., Yokoi H., Yoshida M., Fujiwara S., Kameyama R., and Miyamoto M.: Study on the Explosive-Driven Magnetic Flux Compression Generator for Large Current Production. *Journal of the Japan Explosive Society*, 1996, Vol. 57, pp. 123–128

[12] Kristiansen, M.; Gregor, J.: Explosive pulsed electric power generation. 28th IEEE International Conference on Plasma Science and 13th IEEE International Pulsed Power Conference, 2001, pp. 149–157

[13] Neuber A. A, Explosively Driven Pulsed Power. Helical Magnetic Flux Compression Generators. Springer, Berlin, Heidelberg, 2005

[14] Novac B.M., Smith I.R., Rankin D.F., Hubbard M.: A fast and compact θ-pinch electromagnetic flux compression generator. J. Phys. D: Appl. Phys. ,Vol. 37, 2004, pp. 3041–3055.

[15] Marshal S. V, DuBroff R.E., Skitek G.G.: Electromagnetic Concept and Aplications. 4th ed., Prentice Hall, Upper Saddle River, New Jersey, 1996

[16] Nalva H.S. (red.): Handbook of thin film materials. Academic Press, San Diego, 2001

[17] Trzaska M.: Electromagnetic properties of nanocrystalline copper conductors. Proc. XIII Int. Symp. Theoret. Electrical Engineering, ISTET'05, Lviv, July 4-7, 2005, pp.101-102

[18] Trzaska Z.: Shielding of Transient Electromagnetic Fields. Proc. Intern. Meeting PEDC 2001, Zielona Góra, 5-7 September 2001, pp.235-245

[19] Chatterjee R.: Advanced Microwave Engineering. Special Advanced Topics. Ellis Horwood, J. Wiley, New York, 1988

[20] Tsaliovich A: Electromagnetic Shielding Handbook for Wired and Wireless EMC Applications. Kluwer, Boston, Dordrecht, 1999