

O blackoutach w szerszym kontekście

Autor: Jacek Malko, Instytut Energoelektryki, Politechnika Wroclawska

(„Wokół Energetyki” – nr 6/2006)

Wprowadzenie

Najbardziej pesymistyczne przewidywania, będące efektem ataku na nowojorskie WTC 11 września 2001 r. i kolejnych katastrof energetycznych o zasięgu kontynentalnym (zwłaszcza efektownych w pechowym roku 2003) nie ziściły się (*na razie*, jak komentują pesymiści). Nie oznacza to, że dotychczas występujące zjawiska mają jedynie charakter niepowtarzalnych incydentów, a wręcz niezbędne staje się dokonanie analizy możliwych scenariuszy katastrofalnych. We wrześniowym numerze prestiżowego czasopisma amerykańskiego Instytutu Inżynierów Elektryków i Elektroników — *IEEE Spectrum* [1] zaprezentowano owoc analiz, przeprowadzonych pod kierownictwem Jeana Kumagai. Myślą przewodnią *dziewięciu opowieści ku przestrodze* było stwierdzenie: *Czy jesteśmy gotowi, jeżeli terroryści zdecydują się uderzyć raz jeszcze?* Ocena stanu gotowości do podjęcia wyzwań nie napawa otuchą. Spróbujmy zatem przyjrzeć się tym zagrożeniom, ocenić ich stopień trudności realizacyjnej, prawdopodobieństwo wystąpienia, skutki niematerialne i materialne oraz środki techniczne, którymi dysponujemy w działaniach prewencyjnych.

Szok elektryczny

Z wielu względów rolę szczególną w tej inwentaryzacji zagrożeń odgrywa atak na system elektroenergetyczny. Wynika to zarówno ze stosunkowej łatwości sabotażu, dość znacznego prawdopodobieństwa takiego zdarzenia, wysokich szkód (straty ludzkie i materialne) oraz braku skutecznych, technicznych środków zapobiegających atakowi na stacje elektroenergetyczne i infrastrukturę sieciową. Podstawowe wnioski, wynikające z analizy przypadku szoku elektrycznego są następujące:

- System elektroenergetyczny jest szczególnie ponętnym celem działań terrorystycznych. Przy długości linii przesyłowych USA równej w przybliżeniu 300 tys. km i olbrzymiej liczbie krytycznych węzłów systemu USA i Kanady, niemożliwe jest zapewnienie bezpieczeństwa całemu systemowi, a zatem zdeterminowana grupa terrorystów może z dużym prawdopodobieństwem dokonać dywersji w dowolnej części sieci przesyłowych.
- Szczególnie czułym punktem infrastruktury sieciowej są transformatory obniżające NN/SN. W USA liczność tej grupy sięga tysiąca sztuk, w większości ulokowanych w terenie i chronionych jedynie przez ogrodzenie siatkowe i kłódki. Atak przy wykorzystaniu przenośnych rakiet przeciwpancernych lub zaimprovizowanych ładunków wybuchowych jest łatwy i szybki w wykonaniu. Stworzenie stref bezpieczeństwa i obudowanie transformatorów ścianami betonowymi jest trudne i kosztowne w realizacji na skalę masową.
- Prowadzone są prace, zmierzające do wytypowania (przy współdziałaniu z przedsiębiorstwami energetycznymi) transformatorów największych mocy i zlokalizowanych w krytycznych punktach systemu w celu opracowania procedur ich zastępowania i wymiany w stanach awaryjnych. Prowadzone są również prace nad konstrukcją jednostek zastępczych,

Tab. 1. Zagrożenia, ich skutki i sposoby przeciwdziałania

Zagrożenie	Trudność realizacji*	Prawdopodobieństwo**	Szkody	Techniczne środki przeciwdziałania
1	2	3	4	5
bomba jądrowa w walizce	10	1	87 tys. natychmiastowych ofiar śmiertelnych plus nieznaną liczbą zgonów w rezultacie zachorowań nowotworowych. Niepoliczalne straty materialne (w mld USD) w wyniku zniszczonej infrastruktury i zahamowania handlu międzynarodowego	zintegrowany skaning gamma i radiacyjny może być pomocny, ale powoduje znaczne koszty i spowalnia globalną wymianę towarów
szok elektryczny	2	5	kilka tysięcy rannych lub zabitych, 6–7 mld strat tylko w USA	nie istnieją techniczne środki zapobieżenia atakowi terrorystycznemu na stacje energetyczne i słupy linii przesyłowych. Pomocne mogą być techniki szybkiej odbudowy sieci, lecz żadne z nich nie mają jeszcze gotowości operacyjnej ani też nie są planowane
katastrofa procesu technologicznego, uwalniająca substancje toksyczne	4	7	100 tys. ofiar śmiertelnych, potencjalnie znacznie większa liczba rannych lub poszkodowanych na zdrowiu	przekonstruowanie procesów przemysłowych, mogących uwalniać wysoce toksyczne gazy pod ciśnieniem
atak na urządzenia przetwórcze ropy naftowej	8	3	50 ofiar śmiertelnych wśród pracowników rafinerii, strażaków i ekip ratunkowych. Koszty ponad 2 mld USD zastąpienia zdolności przetwórczej 0,5 mln baryłek dziennie	zwielokrotnione rozproszone systemy sterowania łącznie z komputerami sterującymi spoza miejscami potencjalnego zagrożenia
sztuczne wywołanie zakaźnej choroby bydła (np. pryszczycy)	2	8	zrujnowani farmerzy, padnięcie setek milionów sztuk bydła, setki mln USD strat, możliwość recesji gospodarczej	najlepsza technika – szczepienia przeciwko chorobie – nie była przez lata stosowana z powodów organizacyjnych i finansowych, lecz obecnie jest coraz poważniejszą brana pod uwagę w skali światowej
ciemne Boże Narodzenie (terrorystyczny atak na duże centra handlowe i firmy kurierskie dla odstraszenia klientów w szczycie zakupów świątecznych)	5	8	setki mln USD strat w biznesie	brak
akcja skrajnych organizacji obrony zwierząt, skierowana przeciwko prestiżowej imprezie z udziałem gwiazd mass mediów (np. Oscary Akademii Filmowej) dla zniechęcenia do używania futer	8	2	90 mln USD strat wynikających z odstąpienia od transmisji TV	dentyfikatory z czipem mikroprocesorowym, i kamery nadzorujące i inne urządzenia kontroli dostępu – nie wykluczają jednak ataku od wewnątrz
masowe i burzliwe protesty rolników, sprzeciwiających się ograniczeniu subsydiowania produkcji rolnej w UE	1	1	pojedyncze ofiary śmiertelne, nieliczni ranni, setki milionów euro strat w zniszczonym majątku	brak środków uniemożliwiających wykorzystanie azotowych substancji nawozowych do produkcji materiałów wybuchowych, możliwe stosowanie <i>elektronicznych nosów</i> dla wykrywania substancji lotnych, wydzielających się groźnych dla otoczenia substancji, ale masowe stosowanie tych środków w miejscach publicznych jest procesem długotrwałym
przecenienie lub niedocenienie zagrożenia terrorystycznego (warianty A i B przyszłościowej polityki bezpieczeństwa)	1	10	miliardy utracone na nadmierne środki bezpieczeństwa i ograniczenie wolności obywatelskich lub stepiona czujność i zwiększone prawdopodobieństwo poważnego ataku	brak

* w skali 0–10 (10 – skrajnie wysoka trudność); ** w skali 0–10 (10 – prawdopodobieństwo bliskie pewności)

mogących szybko wejść w miejsce urządzenia niesprawnego.

- Kalifornijski Instytut EPRI we współpracy z europejskim ABB opracował zestaw kryteriów awaryjnej wymiany jednostek transformatorowych, oczekuje się większego zainteresowania tymi działaniami ze strony Ministerstwa Bezpieczeństwa Wewnętrznego USA (*US Dep. Of Homeland Security - DHS*). Niezbędne jest stworzenie procedur reagowania na stany awaryjne, zapewniające szybkie dostarczanie i montaż jednostek zastępczych.
- W najlepszym przypadku przy zaistniałej awarii system może być odbudowany szybko, a krytycznie ważni odbiorcy mogą odzyskać zasilanie niemal natychmiastowo. Aczkolwiek nie istnieje możliwość skutecznego zabezpieczenia przed atakiem terrorystycznym, to system powinien zostać skonfigurowany w taki sposób, by uszkodzenie (lub zniszczenie) dowolnych elementów mogło jedynie pogorszyć jakość dostarczonej energii, ale by cały system był nadal zdolny do spełnienia swej misji w każdym momencie.
- Przed 11 września 2001 r. Stany Zjednoczone — mimo swobody dostępu obywateli do broni - nie zaznały ataków bombowych skierowanych przeciwko ludności cywilnej i nie istniała taktyka zapobiegania takim incydentom. Dotychczasowe doświadczenia (np. policji nowojorskiej) wskazują, iż najbardziej skutecznym środkiem zapobiegawczym jest klasyczna (niemal staromodna) forma patroli, zwłaszcza w obszarach podwyższonego ryzyka.

O awariach katastrofalnych raz jeszcze

Bez względu na ich genezę temat wielkich awarii systemowych nadal daleki jest od rozwiązania. Świadectwem tego może być monotematyczny zeszyt *IEEE Power & Energy*, poświęcony w całości temu problemowi. Sześć ważnych artykułów [2-7] i editorial [8] prezentuje różnorodne aspekty 40-letniej historii amerykańskich blackoutów, opisane przez wybitnych elektroenergetyków - systemowców z USA i Kanady pod ogólnym hasłem: *Wielkie awarie sieci przesyłowych: doświadczenia, monitoring ograniczanie, prewencja, zabezpieczenia i odbudowa*. Poszczególne artykuły można scharakteryzować następująco:

Anatomia blackoutu [2], autorstwa liderów Grupy Zadaniowej IEEE-PES Dynamiki Systemu Elektroenergetycznego, poświęcona jest przeglądowi ostatnich wielkich awarii, ich podstawowych przyczyn oraz dynamiki obserwowanych przebiegów. Praca formułuje zasadnicze wnioski i zalecenia w celu polepszenia parametrów dynamiki systemów elektroenergetycznych oraz ograniczenia ryzyka takich zjawisk katastrofalnych.

Analiza retrospektywna blackoutów [3] **eksponuje rolę monitoringu** we wspieraniu badań zakłóceń wielkich skali i awarii katastrofalnych. Obserwacje wskazują, że dokładność i kompletność informacji o systemie, oparta na pomiarach, jest czynnikiem determinującym zarządzanie systemami elektroenergetycznymi. Zacytować tu można podsumowanie tych rozważań: *tanio pozyskane dane mogą stać się bardzo kosztownymi, jeżeli niezbędny stanie się długi czas na usunięcie ich niedostatków* [3].

Artykuł pod tytułem *Współczesne środki przeciwdziałania blackoutom* [4] opisuje wiele nowoczesnych technologii przesyłu energii elektrycznej, wykorzystujących elementy energo-elektroniczne. Należą do nich elastyczne układy przesyłu zmiennoprądowego (FACTS), czy też układy stałoprądowe najwyższych napięć (HVDC) mogące być pomocą w łagodzeniu wielu problemów, związanych z wielkimi awariami sieci. Artykuł dokonuje szczegółowej analizy dostępnych technologii wraz z potencjalnymi ich korzyściami dla systemu.

Problemy prewencji są rozważane w artykule [5]: *Wprowadzenie oceny bezpieczeństwa w trybie online*. Ta dynamiczność oceny, określana akronimem DSA jest rozwijana na całym świecie, a jej rozpowszechnienie daje nadzieje na poprawę bezpieczeństwa w czasie rzeczywistym, a stąd też i na poprawę niezawodności systemów elektroenergetycznych. W oparciu o doświadczenia wdrożeniowe można stwierdzić, że proces integracji DSA może wspomagać operatorów przedsiębiorstw energetycznych i sieci przesyłowych w formułowaniu kluczowych problemów podczas specyfikowania, rozwijania i instalowania nowych narzędzi. Ilustracją istniejących już możliwości i aplikatywności, nawet dla wielkich systemów elektroenergetycznych, są prezentacje licznych wdrożonych projektów DSA. Automatyka zabezpieczeniowa jest tematem artykułu *Blac-kouty i wnioski dla zabezpieczeń* [6]. Poruszono w nim kwestie filozofii zabezpieczania, działanie zabezpieczeń w warunkach pracy nienormalnej, kategorii nieprawidłowych zdarzeń oraz postęp, umożliwiany przez rozwój technologii: zabezpieczenia cyfrowe, zabezpieczenia adaptacyjne oraz wykorzystanie pomiarów wielkoobszarowych dla ulepszenia zabezpieczenia oraz zdolności do ograniczania zakłóceń na wielkich obszarach. Autorzy wyrażają pogląd, że rozpoczęta dyskusja doprowadzi do dialogu pomiędzy planistami systemów, specjalistami od zabezpieczeń oraz personelem eksploatacyjnym do szerszego uwzględnienia realiów funkcjonowania automatyki elektroenergetycznej w skrajnych warunkach systemowych oraz do wprowadzenia rozwiązań, możliwych dzięki innowacjom technologicznym. Przywrócenie funkcjonowania systemu po lawinie zdarzeń jest treścią artykułu *Odbudowa po awariach kaskadowych* [7]. Rozumowanie autorów sprowadza się do stwierdzenia, że o ile nie sposób uniknąć występowania awarii, to roztropnie jest przedsięwziąć niezbędne środki do ograniczenia ich rozległości, intensywności i czasu trwania. Wyzwaniem jest koordynacja mechanizmów sterowania i zabezpieczania z pracą jednostek wytwórczych i infrastruktury sieciowej.

Nauki płynące z doświadczeń

Ogólnym komentarzem do przedstawionych problemów może być w istocie retoryczne pytanie, zawarte w komentarzu od wydawcy P & E:

Co zdarzyło się w naszej elektroenergetyce w ciągu 3 lat, które upłynęły od 14 sierpnia 2003 roku — daty blackoutu północnoamerykańskiego i innych kolejnych blackoutów, które niemal jednocześnie wystąpiły we Włoszech, Szwecji, Danii, Chorwacji i Anglii? Odpowiedzią jest: zdarzyło się naprawdę wiele! [8].

W licznych dyskusjach, które zostały sprowokowane tymi wydarzeniami argumentowano, że nie jest ekonomicznie zasadne pełne wyeliminowanie awarii katastrofalnych. Wiele przedsiębiorstw energetycznych i operatorów planuje i buduje system wg klasycznej reguły niezawodności N-1, podczas gdy inne przyjmują nawet filozofię N-2. Niewielu stosuje kryterium bardziej skrajne niż N-2 (ale należy zauważyć, że większość blackoutów była skutkiem lawinowych zdarzeń dla przypadków ostrzejszych niż N-2). Padły również argumenty (równie zasadne), że pełna ochrona przed awariami jest nie tylko ekonomicznie nieuzasadniona, ale w istocie niemożliwa. Lepiej jest skoncentrować wysiłki na minimalizacji skutków blackoutów na drodze lepszego monitoringu, automatyki zabezpieczeniowej i sterowania, albo też ulepszyć techniki odbudowy poawaryjnej. W rzeczywistości wszystkie te obszary są krytycznie ważne dla niezawodnej eksploatacji współczesnych systemów elektroenergetycznych. Nie sposób także nie zauważyć, że inne niebezpieczeństwo kryje się za nasiloną ostatnio falą integracji przedsiębiorstw sektora elektroenergetycznego. *Rynki (w tym i rynki energii) są tak silnie ze sobą powiązane, że dowolny, ale znaczący incydent (zaburzenia społeczne, sabotaż, akt terroru...) nawet na peryferiach zglobalizowanej sieci*

powiązań ma efekt natychmiastowy; najdobitniej przejawia się to w gwałtownych skokach cenowych (...). Innym zjawiskiem jest szerokie otwarcie rynków i dostępność wiedzy o nich, co sprawia, że globalny system funkcjonuje bliżej fizycznych ograniczeń, co w sposób szczególny dotyczy rynków energii (...). Zawsze będą się rodzić sytuacje kryzysowe, wobec których rozsądnym przeciwdziałaniem jest maksymalna elastyczność i stałe dążenie do dywersyfikacji źródeł, metod i technologii [9]. Wnioski te są również aktualne dla elektroenergetyki polskiej, a obiecujące otwarcie krajowego operatora na współpracę z ważnymi ośrodkami naukowymi daje szansę pełniejszego wykorzystania ich potencjalnych możliwości. Kolejnym ostrzeżeniem mogą być ostatnie doniesienia o rozległym blackoucie w kilku systemach zachodniej Europy, spowodowanym jak zwykle niespodziewanym atakiem zimy (4/5 listopada 2006 r. [10]).

Piśmiennictwo

1. I. Kumagai (ed.). Terror — what's next: Nine Cautionary Tales. IEEE Spectrum, Sept. 2006.
2. P Pourbeik, PS. Kundur, C. W. Taylor: The Anatomy of Power Grid Blackout. IEEE Power & Energy, Vol. 4, Nr 5, Sept./Oct. 2006.
3. I.E. Dagle. Postmortem Analysis of Power Grid Blackouts. Ibidem.
4. P Pourbeik, M. Bahrman, E. John, W. Wong. Modern Counter measures to Blackouts. Ibidem.
5. L. Wang, K. Morison: Implementation of Online Security Assessment. Ibidem
6. S.H. Horowitz, A.G. Phadke. Blackouts and Relaying Considerations. Ibidem.
7. M.M. Adibi, L.H. Fink. Restoration from Cascading Failures. Ibidem.
8. I. Paserba, P Kundur. Power Grid Blackouts — Remembering and Sighting Grid Failures. Guest Editorial. IEEE Power Energy, Sept./Oct. 2006.
9. D. Howell of Guildford: The Global Energy Scene. Keynote speech at the 29th IAEE Conference. Potsdam. Newsletter of IAEE, Third Quarter 2006.
10. K. Niklewicz: Egipskie ciemności w Europie. GW, 6 listopada 2006.