

# KOMPUTEROWE WSPOMAGANIE ZARZĄDZANIA KRYZYSOWEGO PRZY ROZLEGŁYCH AWARIACH SYSTEMU PRZESYŁOWEGO ENERGII ELEKTRYCZNEJ

**Michał TOMASZEWSKI**

**Streszczenie:** W artykule zaproponowano program działań operatora sieci przesyłowej zmierzający do zmniejszenia zakresu skutków rozległych awarii systemu elektroenergetycznego (pozbawiających zasilania znaczną liczbę ludności na długi okres). Przedstawiono możliwości komputerowego wspomaganie zarządzania kryzysowego, które obejmuje: usuwanie skutków awarii, przywrócenie zasilania, zmiany rozwiązań technicznych i organizacyjnych (działania prewencyjne).

**Słowa kluczowe:** zarządzanie kryzysowe, komputerowe wspomaganie zarządzania, system elektroenergetyczny, rozległa awaria systemu przesyłowego.

## 1. Zjawiska atmosferyczne a awarie systemu elektroenergetycznego

Zwykle stany awaryjne systemu elektroenergetycznego powstają przy wyłączeniu z ruchu co najmniej dwóch elementów systemu. W sieciach przesyłowych i w sieciach dystrybucyjnych występują celowe redundancje, a wyłączenie jednego elementu nie może – w dobrze zaprojektowanej sieci – powodować długotrwałej przerwy w zasilaniu odbiorców.

Tab. 1. Podział zdarzeń powodujących awarie systemów elektroenergetycznych ze względu na przyczyny i zasięg skutków

Przyczyna zdarzenia	Zasięg skutków	Działanie podejmujące:
Błędy projektowe	<b>LOKALNY</b> uszkodzenie kilku elementów, pozbawienie zasilania do 10.000 mieszkańców	Służby eksploatacyjne operatora sieci dystrybucyjnych oraz dyspozytora sieci przesyłowych Instytucje publiczne lokalne
Błędy montażowe		
Wady materiałowe		
Procesy starzeniowe, zużycie		
Błędy eksploatacyjne		
Ekstremalne zjawiska atmosferyczne o zasięgu regionalnym	<b>REGIONALNY</b> Np. uszkodzenie kilkunastu elementów sieci, wypadnięcie węzła lokalnego, pozbawienie zasilania do 100.000 mieszkańców	Służby eksploatacyjne operatorów sieci dystrybucyjnych w ramach scenariuszy awaryjnych oraz dyspozytora systemu przesyłowego Instytucje publiczne i regionalne
Ekstremalne zjawiska atmosferyczne o zasięgu ponad regionalnym	<b>KRAJOWY</b> Np. uszkodzenie kilkudziesięciu do kilkuset elementów, pozbawienie zasilania dużej miejscowości lub obszaru z ponad 100.000 mieszkańców)	Działania kryzysowe w ramach planów i scenariuszy operatora systemu przesyłowego oraz operatorów sieci dystrybucyjnych Sztab kryzysowy Instytucje publiczne, regionalne i krajowe

Prawdopodobieństwo jednoczesnego wystąpienia kilku zwykłych awarii w różnych sieciach na tym samym obszarze, w tym samym miejscu, jest pomijalnie małe. A zatem zwykle awarie powodują ograniczone i przewidywalne skutki. Usuwanie skutków zwykłych awarii, zmniejszenie prawdopodobieństwa ich wystąpienia stanowi istotę każdego systemu eksploatacji i jest częścią zwykłego procesu zarządzania.

Każdy system elektroenergetyczny zawiera zbiór linii napowietrznych z natury rzeczy wrażliwych na oddziaływanie zjawisk atmosferycznych. Zmiany dynamiki zjawisk atmosferycznych, rejestrowane ostatnio również na obszarze Polski, zwiększają zagrożenie linii napowietrznych, głównie poprzez zwiększenie obciążeń mechanicznych przewodów i izolatorów, osprzętu i konstrukcji wsporczych, a w konsekwencji również zwisów przewodów. Oddziaływanie ekstremalnego zjawiska atmosferycznego obejmujące znaczny obszar może spowodować rozległą awarię systemu elektroenergetycznego. W Tab. 1 przedstawiono klasyfikację różnych rodzajów awarii prowadzących do pozbawienia odbiorców zasilania w energię elektryczną.

## 2. Przeciwdziałanie skutkom rozległych awarii systemu elektroenergetycznego

Polityka przeciwdziałania skutkom awarii systemu elektroenergetycznego winna określać zdarzenia uznawane za niedopuszczalne – powodujące stan kryzysu – których należy unikać nawet za wysoką cenę [BaT08a, BaT08b]. Należą do nich:

- a) rozpad systemu elektroenergetycznego wskutek utraty stabilności statycznej lub dynamicznej z różnych powodów. Odbudowa funkcjonowania systemu może wymagać okresu czasu kilkunastu lub więcej godzin, nawet wtedy gdy nie zachodzi potrzeba odbudowy zniszczonych elementów,
- b) pozbawienie zasilania w energię znacznego obszaru lub ograniczanie zasilania wskutek długotrwałej awarii dużego źródła,
- c) pozbawienie zasilania w energię elektryczną dużych aglomeracji na okres czasu liczony w dziesiątkach godzin, wskutek zniszczenia sieci na znacznym obszarze.

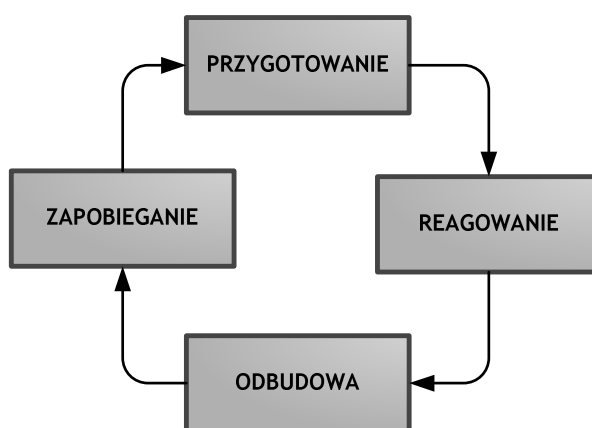
Zdarzenia typu a) i b) są dobrze poznane, można je symulować, przewidywać skutki i sposoby działania. W przypadku tych awarii zniszczenia dotyczą określonych, zwykle pojedynczych elementów. Sposób usuwania skutków jest znany i może być opisany w scenariuszach postępowania. W ostatnich kilkunastu latach nabierają wagi zdarzenia typu c) wywołane ekstremalnymi zjawiskami atmosferycznymi. Osadzanie mokrego śniegu na przewodach, a także oddziaływanie wiatru o charakterze huraganu, tornada może powodować obciążenia mechaniczne przekraczające wytrzymałość mechaniczną nawet nowych, dobrze zaprojektowanych linii. Zróżnicowanie współczynników bezpieczeństwa dla wytrzymałości mechanicznej linii 400 kV, 110 kV, SN i nn sprawia, że zasięg zniszczeń spowodowanych na określonym obszarze przez wystąpienie ekstremalnego obciążenia pochodzenia atmosferycznego jest zróżnicowany, najmniejszy dla napięcia 400 kV, największy w sieciach nn. Jednoczesne uszkodzenie setek elementów sprawia, że czas do przywrócenia zasilania osiąga wartości do 5 dni, nawet u dobrze zorganizowanych i wyposażonych operatorów systemu przesyłowego. Taka przerwa w zasilaniu powoduje skutki społeczne (stan kryzysu) i wymaga uruchomienia systemu zarządzania kryzysowego (zdefiniowanie struktur doraźnych dla opanowania awarii, opracowanie planów działań, opracowanie planów współdziałania z władzami, instytucjami publicznymi i mediami, powołanie zespołów odbudowy awaryjnej, stworzenie zaplecza logistycznego).

W opracowaniach CIGRE [Cig344] zajmujących się problemami występującymi wskutek ekstremalnych obciążeń linii napowietrznych, przyjęto określenie „*Big Storm*”

Events” (BSE), dla rozległych awarii, których przyczyną są zjawiska atmosferyczne. Poza Polską prowadzone są badania dotyczące awarii wywołanych ekstremalnymi zjawiskami atmosferycznymi oraz sposobami redukcji ich efektów wspierające pracę operatorów sieci przesyłowych [AdD06, HuH04, RiD04, Cig175, Cig353]. Jednak bezpośrednie zastosowanie w Polsce rozwiązań stworzonych dla operatorów nie jest możliwe. Każdy system elektroenergetyczny ma swoje struktury i właściwości, rozwiązania, ukształtowane w długim okresie. Ich głęboka zmiana może być niecelowa, a zwykle także niemożliwa. Wskazane jest zatem skorygowanie (uzupełnienie) dotychczasowych rozwiązań, w wyniku procesów, które można i należy przeprowadzić w okresie kilku lat, własnymi siłami, w oparciu o własne analizy i rozwiązania przy zastosowaniu komputerowych narzędzi wspomagających zarządzanie kryzysowe (*Information and Communications Technology for Disaster Management*).

### 3. Fazy zarządzania kryzysowego

Aby usuwać i zapobiegać skutkom kryzysu podejmowane są działania w czterech fazach [SaM06] przedstawionych na Rys. 1.



Rys. 1. Fazy zapobiegania lub usuwania skutków kryzysu

W fazie zapobiegania podejmowane są działania redukujące bądź eliminujące prawdopodobieństwo wystąpienia klęski żywiołowej albo w znacznym stopniu ograniczające jej skutki. Działania te powinny być podejmowane w ramach systemu zarządzania kryzysowego przez stałe grupy robocze.

W fazie przygotowania zespoły podejmują szereg działań planistycznych dotyczących sposobów reagowania w czasie wystąpienia kryzysu (plany działania, instrukcje, procedury). Celem podejmowanych działań jest też powiększenie zasobów sił i środków niezbędnych do efektywnego reagowania. Przygotowanie do wystąpienia kryzysu powinno być realizowane w ramach normalnych działań operatora sieci przesyłowej.

W fazie reagowania podejmowane są (zgodnie z przyjętymi planami) działania polegające na dostarczeniu pomocy poszkodowanym, zahamowaniu rozwoju występujących zagrożeń oraz ograniczeniu strat i zniszczeń. Działania obejmują:

- identyfikację stanu kryzysu i formalne uruchomienie procedur kryzysowych w obrębie przedsiębiorstwa,

- zawiadomienie:
  - władz publicznych o oczekiwanych skutkach zdarzeń i czasie ich trwania,
  - społeczeństwa poprzez media,
  - dużych odbiorców (bezpośrednie),
- etap działań technicznych zmierzających do przywrócenia stanu normalnej pracy sieci przesyłowej w możliwie krótkim czasie:
  - uruchomienie zespołów interwencyjnych (stałych i doraźnych),
  - uruchomienie działań instytucji i przedsiębiorstw zewnętrznych,
  - rejestracje wszelkiej komunikacji i działań.

W fazie odbudowy działania skierowane są na przywrócenie zdolności reagowania, odbudowę zapasów służb ratowniczych, odtworzenie i wzmocnienie infrastruktury elektroenergetycznej. Obejmują one:

- uporządkowanie dokumentacji zdarzeń,
- analizę przebiegu działań,
- analizę strat i kosztów,
- planowanie działań dla przywrócenia pełnej sprawności sieci przesyłowej lub jej rekonstrukcji,
- zmiany w systemie zarządzania kryzysowego wynikającego z analizowanych zdarzeń kryzysowych.

#### **4. Działania przy rozległych awariach systemu elektroenergetycznego**

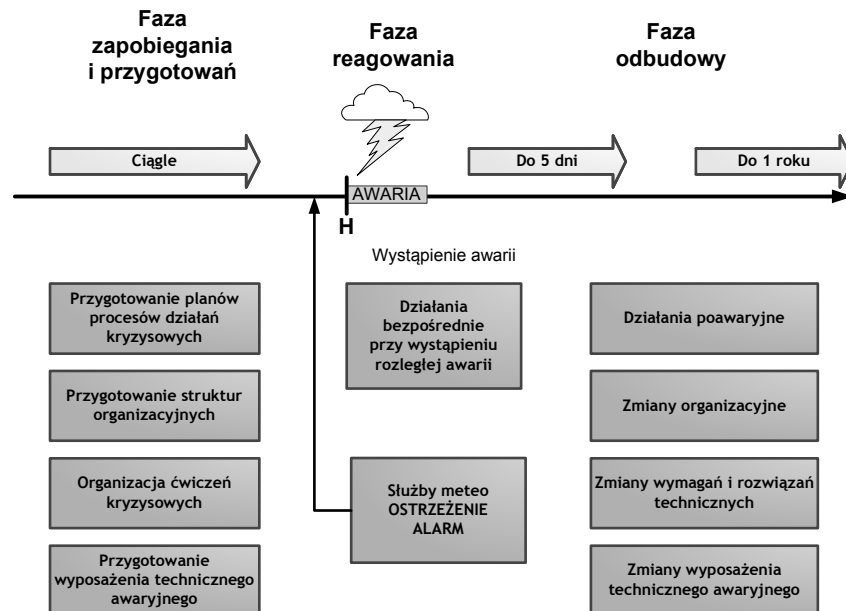
Z doświadczeń zachodnich operatorów [Rte04] wynika celowość powołania systemu zarządzania kryzysowego, obejmującego wszystkie wymienione wcześniej fazy, składającego się z dobrze zorganizowanych i odpowiednio wyposażonych struktur dla przeciwdziałania i szybkiego opanowania rozległych awarii:

- sztabu kryzysowego w przedsiębiorstwie,
- operacyjnego zespołu odbudowy (OZO) złożonego z pracowników operatora i pracowników przedsiębiorstw współpracujących z operatorem,
- magazynów sprzętu i części niezbędnych dla opanowania dużych awarii. Szczególne znaczenie przypisuje się posiadaniu przeróżnych, nadających się do szybkiego montażu odcinków linii napowietrznych, które mogą zastąpić uszkodzone przęsła. Długość linii i ich wykonanie są zróżnicowane w zależności od poziomu napięcia. Przy każdej dużej awarii ważne jest możliwe dokładne zidentyfikowanie i opisanie stanu sieci oraz podejmowanych działań.

System zarządzania kryzysowego powinien definiować:

- struktury organizacyjne (podmioty),
- zakres odpowiedzialności podmiotów,
- reguły współdziałania (procedury),
- sposoby finansowania,
- system komunikacji z mediami i społeczeństwem w przypadku wystąpienia sytuacji kryzysowej (działanie rzecznika, uzgodnione i skoordynowane wystąpienie członków zarządu spółki, przedstawicieli administracji publicznej).

Uwarunkowania czasowe działań podejmowanych w aspekcie rozległych awarii przedstawiono na Rys. 2.



Rys. 2. Elementy przygotowań i działań przedsiębiorstw sieciowych i instytucji publicznych w aspekcie rozległych awarii systemu elektroenergetycznego

Spółka przesyłowa (operator systemu przesyłowego) ponosi główny ciężar przygotowania systemu zarządzania kryzysowego:

- organizuje w obrębie systemu zarządzania odpowiednie struktury i wyposaża je w narzędzia (software),
- organizuje bazę materialną dla działań w przypadku kryzysu (katastrofy),
  - linie i części zapasowe,
  - sprzęt i narzędzia,
  - zapasowe źródła energii,
  - łączność awaryjną,
  - bazę logistyczną i środki transportu, ciężki sprzęt, zabezpieczenie mieszkalne, sanitarne itp.,
- organizuje zespół techniczny,
- prowadzi system szkoleń i treningów,
- zawiera odpowiednie umowy z pracownikami własnymi, administracją publiczną i przedsiębiorstwami remontowymi.

Zasięg uszkodzeń, zakres prac jakie należy wykonać dla przywrócenia zasilania po rozległej awarii znacznie przekraczają zdolności służb eksploatacyjnych każdego operatora. Operatorzy sieci elektroenergetycznych mogą podejmować działania bezpośrednie dla ograniczania czasu trwania przerwy w dopływie energii i zmniejszania obszaru pozbawionego zasilania. Skutki społeczne braku zasilania w okresach dłuższych od jednej doby wymagają podjęcia działań administracyjnych w zakresie zarządzania kryzysowego.

Dla skrócenia zwłoki między wystąpieniem stanu awarii (rozpoczęciem) a podjęciem

działań przez OZO istotne znaczenie ma działanie kierownictwa (sztabu kryzysowego w przedsiębiorstwie). Konieczne jest podjęcie jak najszybciej następujących czynności:

- ustalenie stanu sieci co najmniej według informacji dostępnych dla dyspozytorów i dokonanie wstępnej oceny przyczyn zdarzenia,
- oględziny uszkodzonych linii (helikopter, nagranie wideo) i podjęcie decyzji o zakresie niezbędnych działań,
- uruchomienie zespołu odpowiedzialnego za bezpieczeństwo publiczne,
- uruchomienie zespołu, który dokona analizy zakresu uszkodzeń i przygotuje program działań OZO,
- podjęcie działań przez OZO (personel operatora), ewentualne wezwanie pomocy ze strony innych podmiotów,
- stałe monitorowanie stanu sieci, rozwoju awarii, korygowanie decyzji.

Plan działań operatora w przypadku wystąpienia rozległej awarii winien uwzględniać:

- rezerwowanie źródeł zasilania dla określonych obiektów, w ramach umowy,
- budowę prowizorycznych linii zasilających (na wszystkich poziomach napięć), w przypadku rozległych awarii,
- szczególną troskę o przyszłe linie przebiegające nad miejscami publicznymi, w których może przebywać zbiór osób (rozwiązania techniczne, system inspekcji i diagnostyki, obsługa prewencyjna),
- organizację systemu powiadamiania władz publicznych o zagrożeniu ze strony linii elektroenergetycznych,
- wyznaczenie personelu odpowiedzialnego za zapewnienie bezpieczeństwa publicznego w przypadku awarii i współpracę z instytucjami i służbami publicznymi.

## **5. Komputerowe wspomaganie zarządzania kryzysowego**

Skuteczne działania przedsiębiorstwa przesyłowego w stanach kryzysu uzależnione są od:

- przygotowania w zakresie struktur organizacyjnych i personalnych,
- przygotowania wyposażenia technicznego i logistycznego,
- przeprowadzania szeregu analiz i prognoz,
- przeprowadzania okresowych ćwiczeń i symulacji.

Sprawny system zarządzania kryzysowego wymaga zastosowania wspomaganie komputerowego obejmującego okres przygotowania, okres trwania awarii oraz okres rekonstrukcji i odbudowy.

Warunkiem koniecznym przeciwdziałania zdarzeniom kryzysowym jest monitorowanie zagrożeń bezpieczeństwa. Powinno ono obejmować przewidywanie, wykrywanie i identyfikację (rozpoznanie) potencjalnych niebezpieczeństw. Dotyczy to zarówno rodzaju jak i wielkości zdarzenia. Od informacji o aktualnym stanie możliwych zagrożeń bezpieczeństwa podmiotu uzyskiwanej z systemów monitoringu [KoE08] zależy rodzaj i ilość środków użytych do przeciwdziałania ich skutkom, a także sposób prowadzenia działań ratowniczych. Sposób monitorowania rodzaju i stopnia zagrożeń oraz wykrywania i identyfikacji zdarzeń przez nie spowodowanych zależy od ich natury.

Skuteczny monitoring wymaga zastosowania nowoczesnych technologii telekomunikacyjnych, pozwalających na akwizycję dużej ilości danych oraz podsystemów

wspierających zarządzanie informacjami (bazami wiedzy). Występuje tutaj często problem przekazywania danych pomiędzy różnymi, niezależnymi podmiotami (niekompatybilności systemów telekomunikacyjnych) oraz problem z prawami dostępu do informacji.

Podstawą systemu monitoringu zagrożeń systemu przesyłowego są pomiary pochodzące z sieci sensorów monitorujących pracę systemu przesyłowego, stan elementów infrastruktury. Informacje te powinny być uzupełniane o dane napływające z baz danych innych służb (poza operatorem systemu przesyłowego):

- dane z systemów dystrybucji,
- dane meteorologiczne,
- dane przekazywane przez administrację rządową i samorządową (dane napływające z systemów wczesnego ostrzegania).

Na podstawie informacji z monitoringu zagrożeń podmiotu podsystem informacyjny, posługując się modelami matematycznymi i programowymi symulatorami, powinien opracowywać wielowariantowe prognozy i scenariusze możliwego rozwoju zdarzeń. [KoE08]. Celem jego działania jest ocena stanu aglomeracji i analiza stopnia zagrożenia:

- analiza danych określających aktualny stan bezpieczeństwa sieci przesyłowej,
- weryfikacja danych,
- prognozowanie możliwości wystąpienia zagrożenia,
- analiza ryzyka,
- rozpoznanie sytuacji kryzysowej.

W fazie reagowania system zarządzania kryzysowego powinien obejmować programy analityczno-doradcze zasilane danymi z monitoringu oraz dane operacyjne o siłach i środkach dysponowanych przez system zarządzania kryzysowego. Przykładowymi elementami mogą być dane o [KoE08]: stanach osobowych jednostek organizacyjnych systemu, ich wyposażeniu technicznym, parametrach sprzętu, infrastrukturze obiektów własnych, a ponadto dokumentacje jednostek, zakresy obowiązków osób funkcyjnych, procedury postępowania w określonych sytuacjach, plany ratownicze, itp. Programy analityczno-doradcze pozwalają na wskazanie możliwych wariantów działania dostosowanych do zaistniałej sytuacji oraz wspomaganie podejmowania decyzji, poprzedzane analizą i oceną sytuacji powstałej w wyniku zajścia zdarzenia oraz prognozą jej rozwoju. Czas i jakość wykonywania analiz (szczegółowość, liczba uwzględnianych czynników i wariantów, wiarygodność prognoz, itp.) zależy od stopnia zaawansowania zastosowanych narzędzi.

System zarządzania kryzysowego w przedsiębiorstwie winien komunikować się z instytucjami zewnętrznymi w sposób kontrolowany zarówno w zakresie treści informacji, ich formy oraz czasu przekazywania. Konieczne jest zastosowanie bezpiecznego i kodowanego systemu komunikacji (system łączności z co najmniej podwójną redundancją, z kontrolowanym, hierarchicznym dostępem). Wyklucza się używanie systemów otwartych, które mogą być dostępne dla osób niepowołanych. Dla ograniczenia skutków kryzysu bardzo ważne znaczenie ma także dobrze zorganizowany i ściśle kontrolowany przepływ informacji o zdarzeniach do mediów i społeczeństwa.

Elementem pozwalającym na wizualizację stanu zagrożeń jest odpowiedni System Informacji Przestrzennej (SIP), pozwalający na zobrazowanie zagrożeń w przestrzeni. Poprawnie skonstruowany SIP powinien zawierać dane o istotnym znaczeniu dla planowania i prowadzenia działań w sytuacji kryzysowej, a także prognozowania i likwidacji ich skutków.

Ważnym elementem systemu zarządzania są symulatory działania w sytuacjach

awaryjnych. Jak stwierdzono w [FiK07] technika badań symulacyjnych znajduje szerokie zastosowanie w badaniach złożonych procesów rzeczywistych, przebiegających w realnym czasie przy licznych ograniczeniach i interakcjach zewnętrznych. Zakres działania symulatorów w przypadku systemu zarządzania kryzysowego może obejmować:

- przewidywanie możliwych scenariuszy rozwoju zagrożeń z uwzględnieniem podejmowanych decyzji.
- symulację procesów podejmowania decyzji wraz z oceną ich skutków,
- przeprowadzenie szkoleń dla zespołów reagowania kryzysowego.

Symulatory wspierają proces przygotowania personelu do reagowania w sytuacjach kryzysowych poprzez przeprowadzanie okresowych ćwiczeń stanów awaryjnych według starannie przygotowanych scenariuszy. Analiza i ocena pracy personelu oraz przebiegu ćwiczeń stanowi podstawę do ulepszenia systemu zarządzania kryzysowego, a także podstawę bezpośredniej oceny osób.

## 6. Podsumowanie

- A. Stan kryzysu jest niemożliwy do opanowania jedynie poprzez współdziałania służb operatorów spółki przesyłowej. Rozległość uszkodzeń może spowodować konieczność planowego wykorzystania potencjału przedsiębiorstw montażowych współpracujących z operatorami dla skrócenia czasu przerw w zasilaniu oraz czasu odbudowy. Skutki społeczne długotrwałych przerw w zasilaniu znacznej liczby odbiorców powodują uruchomienie działań służb publicznych (zarządzanie kryzysowe).
- B. Osiągnięcie możliwości sprawnego i szybkiego działania przedsiębiorstwa przesyłowego w stanie kryzysu wymaga wieloletnich przygotowań obejmujących wszystkie obszary działań przedsiębiorstwa oraz zastosowania zaawansowanych narzędzi informatycznych.
- C. Opracowanie spójnego, racjonalnego systemu zarządzania kryzysowego dla operatora sieci przesyłowych wymagają współdziałania specjalistów z dziedziny zarządzania i ekonomii przedsiębiorstwa przesyłowego, eksploatacji sieci przesyłowych, projektantów oraz przedstawicieli firm wytwarzających elementy i montujących linie przesyłowe.
- D. Każda rozległa awaria winna podlegać szczególnej analizie i powodować doskonalenie systemu zarządzania kryzysowego (cykl Deminga). Stałe struktury w spółce przesyłowej powinny zajmować się analizą stanu technicznego linii i stacji (wytrzymałość na ekstremalne oddziaływanie), wyznaczać skalę (zagrożenia) i miejsce, planować środki przeciwdziałania na różnych poziomach (od ostrzeżenia operatora, poprzez prewencyjną odnowę do budowy zapasowych (równoległych) elementów. Wymienione procesy mogą być wspierane przez szereg narzędzi informatycznych przedstawionych w artykule.
- E. Działania przygotowujące zarządzanie kryzysowe i opanowanie kryzysów (katastrof) powinny być uwzględnione w planowaniu wydatków przedsiębiorstwa na eksploatację sieci przesyłowej. Wystąpienie dużych awarii jest prawdopodobne, ocena prawdopodobieństwa jest jednak trudna. Konieczne jest podjęcie badań wyznaczających ryzyko wystąpienia awarii systemu elektroenergetycznego spowodowanych ekstremalnymi zjawiskami atmosferycznymi w Polsce w celu uwzględnienia go w polityce przedsiębiorstwa. Analiza ekonomiczna skutków (kosztów) dużej awarii może być pomocna w wyznaczeniu poziomu nakładów na system zarządzania kryzysowego, jego wyposażenie i utrzymanie.



## Literatura

- [AdD06] Admirat P., Dalle B.: Lapeyre J-L. : Neige collante givre pluie verglacante sur les lignes electriques, EDF R&D, Paris, 2006.
- [BaT08a] Bartodziej G.: Tomaszewski M.: Polityka energetyczna i bezpieczeństwo energetyczne, Wydawnictwo Nowa Energia, Racibórz, 2009.
- [BaT08b] Bartodziej G., Tomaszewski M.: Dangers to domestic power system safety, XI Międzynarodowa Konferencja Naukowo-Techniczna Forum Energetyków GRE 2008, Zeszyty Naukowe Politechniki Opolskiej, seria Elektryka z. 60, Nr kol. 323/2008.
- [Cig175] CIGRE TB No 175 – WG 22.13, Management of Existing Transmission Lines.
- [Cig344] CIGRE TB No 344 – WG B2.06, 2008, Big Storm Events – What we have learned.
- [Cig353] CIGRE TB No 353 – WG B2.13, Guidelines for increased Utilization of existing Overhead Transmission Lines.
- [FiK07] Ficoń K.: Inżynieria zarządzania kryzysowego. Podejście systemowe, BEL Studio sp. z o.o., Warszawa, 2007.
- [HuH04] Huang J.A., Harrison S., Wehenkel L., Vanier G., Lévesque F., Valette A.,: Operation rules determined by risk analysis for special protection systems at Hydro-Québec, CIGRE Session 2004, Paryż.
- [KoE08] Kołodziński E.:Istota inżynierii systemów zarządzania bezpieczeństwem, [www.infocorp.com.pl/publikacje/Istota\\_inzynierii\\_systemow.pdf](http://www.infocorp.com.pl/publikacje/Istota_inzynierii_systemow.pdf), 2008.
- [RiD04] Rivard J., Delpet R., Lajoie-Mazenc C.:The application of RCM method to RTE overhead transmission lines, CIGRE Sesion 2004, Paryż.
- [Rte04] Réseau de Transport d'Electricité, 2004, Mémento de la sûreté du système électrique, Paris, 2004.
- [SaM06] Sanecki J., Maj K.:Zastosowania Systemów Informacji Przestrzennej w zarządzaniu kryzysowym, KNT, Warszawa, 2004.

Dr inż. Michał TOMASZEWSKI  
Instytut Elektroniki i Systemów Pomiarowych  
Wydział Elektrotechniki, Automatyki i Informatyki  
Politechnika Opolska  
45 - 273 Opole, ul. K. Sosnkowskiego 31  
tel./fax.: (0-77) 400 6215  
e-mail: m.tomaszewski@po.opole.pl



**KAPITAŁ LUDZKI**  
NARODOWA STRATEGIA SPÓJNOŚCI

Artykuł współfinansowany przez Unię Europejską  
w ramach Europejskiego Funduszu Społecznego

**UNIA EUROPEJSKA**  
EUROPEJSKI  
FUNDUSZ SPOŁECZNY

