Czego nas uczą wypadki i katastrofy

Tadeusz Missala

Przemysłowy Instytut Automatyki i Pomiarów PIAP w Warszawie

Streszczenie: Przedstawiono skrótowy opis dwóch katastrof lokalnych polskich (pożar w EC Żerań i katastrofa kolejowa na CEK) oraz dwóch katastrof nuklearnych w Fukushimie i Czarnobylu. Wskazano na naruszenie zasad bezpieczeństwa, które doprowadziły do tych katastrof.

Słowa kluczowe: bezpieczeństwo, wypadki, katastrofy, kolej, energetyka

1. Wprowadzenie

Duże wypadki i katastrofy przemysłowe i komunikacyjne wskazują na różne aspekty bezpieczeństwa technicznego, które nie są dostateczne uwzględniane w praktyce lub na niejednokrotnie elementarne błędy popełniane, z punktu widzenia bezpieczeństwa technicznego, w trakcie projektowania i eksploatacji obiektów.

Zadaniem niniejszego referatu jest przedstawienie, na przykładzie kilku zdarzeń, zaistniałych błędów i próba wyciągnięcia wniosków do prawidłowego postępowania. Analiza zostanie przeprowadzona z punktu widzenia zasad bezpieczeństwa funkcjonalnego sformułowanych m.in. w normach serii PN-EN 61508 [1, 2].

2. Pożar w EC Żerań

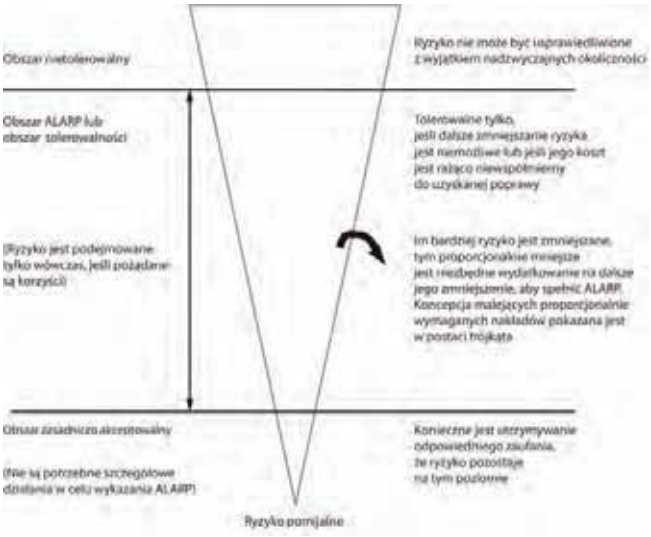
Rys. 1. Wozy strażackie na Żeraniu [1]
Fig. 1. Firetrucks in Żerań [1]

Na podstawie informacji prasowych [4–5] można wyrobić sobie następujący pogląd na przebieg zdarzeń: pożar wybuchł 6 września 2012 r. w galerii nawęglania. Rozmiar pożaru był tak duży, że ewakuowano pracowników z terenu zagrożonego. Jeden pracownik, który był zakleszczony w windzie, zmarł w szpitalu wskutek oparzeń.

Jak ustaliła Komisja Awaryjna, najbardziej prawdopodobną przyczyna pożaru była wysoka temperatura towarzysząca pracom remontowym, w tym spawaniu, cięciu i szlifowaniu, przy przenośniku taśmowym w dolnej części galerii nawęglania.

Przyjrzyjmy się sprawie przez pryzmat techniki bezpieczeństwa.

Jak wiadomo, za podstawę zarządzania bezpieczeństwem i zmniejszaniem ryzyka należy przyjmować zasadę ALARP (*As Low As Rationally Practicable* – tak niskie jak rozsądnie wykonalne), której zasadę przedstawiono na rysunku 2.



Rys. 2. Zasada ALARP [2]
Fig. 2. ALARP principle [2]

Rozróżnia się trzy strefy: strefa górna jest strefą ryzyka nietolerowalnego i gdy stwierdzi się, że obiekt lub sytuacja mieści się w jej obszarze, to należy przeprojektować obiekt lub zmienić sytuację, tak aby przesunąć je poza tę strefę. Strefa dolna jest strefą ryzyka zasadniczo akceptowalnego, niższego od normalnie spotykanego w życiu codziennym. Strefa środkowa jest strefą stosowania środków zmniejszania ryzyka, tak aby doprowadzić je do poziomu akceptowalnego.

W rozpatrywanym przypadku remontu w EC Żerań sytuację ciecia, spawania i szlifowania, to jest wykonywania operacji wydzielających znaczną energię cieplną i generujących iskry, wykonywaną w przenośniku taśmowym w strefie nawęglania, należy zakwalifikować do strefy

górnej wykresu ALARP, a więc zasadniczo niedopuszczalnej z punktu widzenia zarządzania ryzykiem.

W tej sytuacji jakakolwiek analiza zagrożeń i ryzyka byłaby nieadekwatną do istniejącego zagrożenia. Wnioskiem z powyższego jest, że na okres prac remontowych powinno zostać wstrzymane nawęglanie, a węgiel/miał usunięty ze strefy prac zagrażających. Na pewno byłoby to tańsze niż usuwanie skutków pożaru.

Jeśli jednak podjecie decyzji o przerwaniu ruchu wydawało się niemożliwe (**a po awarii stało się nie tylko możliwe, lecz konieczne)**, to należało przedsięwziąć szczególne środki zabezpieczające w postaci osłon termicznych i ewentualnie wentylacji, aby nie dopuścić do nadmiernego nagrzania dostarczanego węgla i/lub innych elementów łatwopalnych.

3. Katastrofa kolejowa na CMK

Centralna magistrala kolejowa (CMK) biegnie z Warszawy na Śląsk. Pociągi do Krakowa muszą zjechać z niej jednotorową łącznicą, aby potem wjechać na linię dwutorową do Krakowa. Tam stoi posterunek dyżurnego ruchu Starzyny [7]. Tu w dniu 5 marca 2012 r. nastąpiło zderzenie pociągów, wskutek nie przełączenia zwrotnicy przez dyżurnego ruchu.

Sytuację przedstawiono na rysunku 3.

Rys. 3. Układ torów kolejowych i nastawni [7]
Fig. 3. A layout of the railway tracks and control post [7]

Budowa pochodzi z lat 70. ubiegłego stulecia. Dyżurny ruchu przestawia zwrotnicę na wjazd z Warszawy na kontrtor – tor ruchu z Krakowa, bez zablokowania wjazdu od strony Krakowa.

Pociąg może wjechać na tor niezabezpieczony od ruchu z przeciwka – stworzone warunki do zderzenia czołowego.

Dyżurny ruchu przestawia zwrotnicę do zjazdu na właściwy tor i, w przypadku gdy zapas czasu jest dostateczny, likwiduje narażenie na zderzenie czołowe.

Wykonanie sekwencji bezpieczeństwa jest oparte na dobrym i niezawodnym działaniu człowieka – wiadomo dzisiaj, że człowiek jest najbardziej zawodnym ogniwem w łańcuchu bezpieczeństwa.

Nie jest spełnione wymaganie konstrukcji „bezpiecznej samej w sobie" (*inherent safety*) – układ torów generuje sytuację zagrożenia przy każdym przejeździe pociągu.

Taka sytuacja mieści się w obszarze ryzyka nietolerowalnego – patrz rysunek 2 – i takie rozwiązanie nie powinno być dopuszczone do eksploatacji.

W rozpatrywanym przypadku, bardzo szczęśliwie, dobra praca ludzi umożliwiła aż osiemnastoletni odstęp między wypadkami.

Jeżeli przyjąć czas 18 lat, jaki upłynął miedzy katastrofami, jako średni czas do uszkodzenia (MTTF), to mamy:

$$MTTF = 18 \times 8760h = 157680h$$

$$\lambda = \frac{1}{MTTF} = \frac{1}{157680} = 6{,}34E-06$$

Z tabeli 1 wynika, że otrzymuje się poziom nienaruszalności bezpieczeństwa SIL 1.

Tab. 1. Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na częste przywołanie lub ciągłym [1]
Tab. 1. Safety integrity: target measures for safety function operating in high demand mode of operation or continuous mode of operation [1]

Poziom nienaruszalności bezpieczeństwa (SIL)	Rodzaj pracy na częste przywołanie lub ciągły (Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę)
4	od $\geq 10^{-9}$ do $< 10^{-8}$
3	od $\geq 10^{-8}$ do $< 10^{-7}$
2	od $\geq 10^{-7}$ do $< 10^{-6}$
1	od $\geq 10^{-6}$ do $< 10^{-5}$

Zmiana zasady blokady i sterowania umożliwia, tanim kosztem, przejście do strefy środkowej, tj. zarządzania ryzykiem i umożliwienie wprowadzenia stosownych funkcji bezpieczeństwa o odpowiednim poziomie jego nienaruszalności.

Funkcją bezpieczeństwa będzie odpowiednia sekwencja przestawiania zwrotnic za pomocą urządzeń o odpowiednim poziomie nienaruszalności bezpieczeństwa.

A tak powinno przebiegać (lub przebiega, bo może poprawiono):

1. Otwarta zwrotnica na wjazd z Krakowa blokuje otwarcie zwrotnicy na wjazd z Warszawy na kontrtor oraz zamknięta zwrotnica na wyjazd do Krakowa blokuje otwarcie zwrotnicy na wjazd z Warszawy. Pociąg nie może wjechać na kontrtor;
2. Dyżurny ruchu jednym elementem sterowniczym uruchamia sekwencję:
   – zamyka i blokuje zwrotnicę na wjazd z Krakowa;
   – otwiera zwrotnicę na wyjazd do Krakowa,
   – następuje odblokowanie i przestawienie zwrotnicy na wjazd z Warszawy na kontrtor;
3. Pociąg może wjechać na tor zabezpieczony od ruchu z przeciwka i może opuścić ten tor – istnieje zabezpieczenie przed zderzeniem czołowym.

Aby ustalić poziom nienaruszalności bezpieczeństwa toru wymienionej wyżej funkcji bezpieczeństwa, należy prze-

prowadzić analizę zagrożeń i ryzyka. Wybrano metodę podana w PN-EN 61062 [7].
Polega ona na zestawieniu tablicowym i kwantyfikowaniu:

- poziomu ostrości szkody (Se);
- częstotliwości i czasu trwania ekspozycji (Fr);
- prawdopodobieństwa wystąpienia narażenia (Pr);
- prawdopodobieństwa uniknięcia lub ograniczenia szkody (Av)

i następnie obliczeniu klasy prawdopodobieństwa szkody (Cl) jako sumy:

$$Cl = Fr + Pr + Av$$

Kombinacja wartości przypisanych parametrom Se i Cl wskazuje wymagany poziom nienaruszalności bezpieczeństwa SIL. Kwantyfikację podaną w [7] przedstawiono w tablicach od 2 do 6.

Tab. 2. Kwantyfikacja poziomu ostrości (Se)
Tab. 2. Severity (Se) classification

Konsekwencje	**Przypisana wartość *Se***
Nieodwracalne, np. śmierć, utrata oka lub ręki	4
Nieodwracalne, np. złamania kończyn(-y), utrata palca(-ów)	3
Odwracalne – wymagana interwencja personelu medycznego	2
Odwracalne – wymagana pierwsza pomoc	1

Tab. 3. Kwantyfikacja częstości i czasu trwania ekspozycji (Fr)
Tab, 3. Fequency and duration of exposure (Fr) classification

Częstość ekspozycji	**Przypisana wartość *Fr***
> 10 min do ≤ 1 h	5
>1 h do ≤ 1 dzień	5
> 1 dzień do ≤ 2 tygodnie	4
> 2 tygodnie do ≤ 1 rok	3
> 1 rok	2

Tab. 4 Kwantyfikacja prawdopodobieństwa narażenia (Pr)
Tab. 4. Probability (Pr) classification

Prawdopodobieństwo wystąpienia	**Przypisana wartość *Pr***
Bardo wysokie	5
Dogodne	4
Możliwe	3
Rzadkie	2
Pomijalne	1

Tab. 5. Kwantyfikacja prawdopodobieństwa uniknięcia lub ograniczenia szkody (Av)
Tab. 5. Probability of avoiding or limiting harm (Av) classification

Prawdopodobieństwo uniknięcia lub ograniczenia	**Przypisana wartość *Av***
Niemożliwe	5
Rzadkie	3
Prawdopodobne	1

Tab. 6. Macierz przypisywania SIL
Tab. 6. SIL assignment matrix

Ostrość (*Se*)	**Klasa (*Cl*)**				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

UWAGA Pola zaczernione wskazują właściwy SIL. Obszar zacieniony na szaro (OM) może być wykorzystany przy zastosowaniu innych środków bezpieczeństwa.

W rozpatrywanym przypadku otrzymuje się kwantyfikacje:
Konsekwencje nieodwracalne: Se = 4
Częstotliwość i czas trwania: Fr = 5
Prawdopodobieństwo wystąpienia narażenia: Pr = 5
Prawdopodobieństwo uniknięcia: Av = 1
Cl = Fr + Pr + Av = 11
Przy Se = 4
Otrzymuje się: SIL 3.

Należy zastosować urządzenia certyfikowane na poziom nienaruszalności bezpieczeństwa SIL 3 i przez odpowiednią konfigurację uzyskać poziom SIL 3 na całą funkcję bezpieczeństwa.

4. Katastrofa w elektrowni Fukushima

4.1. Przebieg

W marcu 2011 r., w następstwie podmorskiego trzęsienia ziemi i wywołanego przezeń tsunami, wystąpiła awaria i wybuch w elektrowni atomowej Fukushima Daiichi Nuclear Plant. To zdarzenie ma wprawdzie podłoże w zjawiskach niezależnych od obsługi, jednakże bliższa analiza wskazuje, że jego rozmiary w dużej mierze wynikają z niewłaściwego zachowania ludzi na różnych etapach projektowania, eksploatacji i postępowania w obliczu awarii. Takie stwierdzenie Przewodniczącego Japońskiej Komisji badającej katastrofę jest zacytowane przez prof. Gudelę Grote [11].

Na podstawie publikacji Wikipedii [8] opartej na 82 opracowaniach źródłowych, w tym komunikatach Międzynarodowej Agencji Energii Atomowej i Państwowej Agencji Atomistyki w Polsce, można przedstawić poniższy schemat następstwa zdarzeń.

1. U wybrzeży wyspy Honsiu, z epicentrum w odległości około 130 km na wschód od wybrzeża Tohoku, na którym znajduje się elektrownia, na głębokości 24 km lub 32 km następuje trzęsienie ziemi o sile 9 stopni w skali Richtera;
2. Zjawiskiem wtórnym związanym trzęsieniem ziemi jest fala tsunami o wysokości przekraczającej wysokość ochronnego muru oporowego;
3. Po zarejestrowaniu trzęsienia ziemi obsługa wyłącza z pracy trzy czynne reaktory BWR (pozostałe trzy były wyłączone z powodu przeglądów okresowych);
4. Wyłączenie reaktorów powoduje utratę zasilania własnego podstawowego i potrzebę przejścia na zasilanie z sieci zewnętrznej;
5. Sieć zewnętrzna jest uszkodzona w wyniku trzęsienia ziemi i nie można z niej zasilić elektrowni;
6. Zostają włączone generatory zasilania awaryjnego napędzane silnikami diesla, które po ok. godzinie pracy zostają zalane falą tsunami, która przelała się górą przez mur ochronny;

Rys. 4. Pożar Elektrowni Jądrowej Fukushima [9]
Fig. 4. A fire of Fukushima Nuclear Power Plant [9]

7. Elektrownia zostaje bez jakiegokolwiek zasilania, co powoduje wyłączenie chłodzenia reaktorów, przegrzania rdzeni, wybuch wodoru, pożar i ogromne skażenie środowiska oraz ofiary w ludziach i ewakuację mieszkańców pobliskich miejscowości;
8. Podejmowane działania zaradcze są już spóźnione.

4.2. Analiza – zagrożenia i przyjęte funkcje bezpieczeństwa

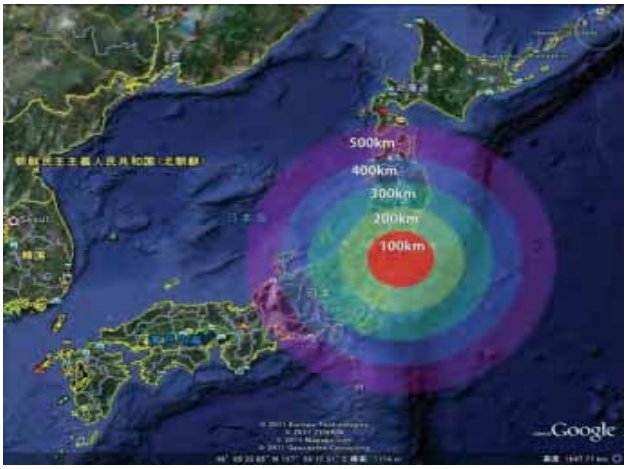
Zagrożenia, które można zidentyfikować na podstawie dostępnych opisów i które niewątpliwie były znane budowniczym elektrowni można podzielić na wewnętrzne i zewnętrzne.

Zagrożeniem wewnętrznym o potencjale katastroficznym jest utrata chłodzenia rdzeni reaktora prowadząca do ich przegrzania i destrukcji reaktora połączonej z możliwym wybuchem wodoru i pożarem. Przyjętymi funkcjami bezpieczeństwa były:

a. zasilanie awaryjne z sieci rozdzielczej,
b. zasilanie awaryjne z agregatów prądotwórczych napędzanych silnikami diesla zlokalizowanych na terenie elektrowni, w piwnicy lub na poziomie parteru (co wynika z opisu katastrofy, że woda zalała „Nisko umieszczone" agregaty).

Zagrożeniami zewnętrznymi, wynikającymi z lokalizacji elektrowni, są wstrząsy sejsmiczne i wysokie fale oceaniczne. Przyjętymi funkcjami bezpieczeństwa były:

a. procedury odstawiania reaktorów z pracy w przypadku pojawienia się wstrząsów sejsmicznych,
b. przypuszczalnie budowa o charakterze antysejsmicznym.
c. Mur ochronny przed wlaniem się fali oceanicznej o wysokości wynikającej z wiedzy o pojawiających się falach pochodzącej z okresu budowy elektrowni, tj. sprzed 40 lat.



Rys. 5. Obszar skażenia po awarii [10]
Fig. 5. A contaminated area [10]

4.3. Analiza – błędy projektu i postępowania

Pierwszy błąd – projekt. Jeżeli zagrożeniem jest możliwość zalania wodami niesionymi przez falę oceaniczną, to zabezpieczenie systemu krytycznego z punktu widzenia wielkiej awarii – tu agregatów prądotwórczych zasilających pompy układu chłodzenia – powinno być co najmniej podwójną warstwą zabezpieczeń. Poza ochroną przez mur oporowy stanowiący pierwszą warstwę zabezpieczeń, urządzenia powinny być tak umieszczone, aby nie mogły być zalane w przypadku przedarcia się wody przez tę pierwszą warstwę zabezpieczeń. Drugą warstwą zabezpieczeń powinno być umieszczenie na bezpiecznej wysokości ponad poziomem gruntu.

Przy takim rozwiązaniu zabezpieczenia nie nastąpiłoby zalanie agregatów i ich wyłączenie, a zatem nie byłoby utraty chłodzenia rdzeni reaktorów.

Drugi błąd – eksploatacja. Ocean Indyjski jest obszarem wysoce sejsmicznym, w którym w ciągu ostatnich lat dochodziło do wstrząsów poddennych i wysokich fal tsunami spowodowanych tymi wstrząsami. Np. w 2004 roku trzęsienie ziemi o amplitudzie 9,1 w skali Richtera i o epicentrum w pobliżu zachodniej Sumatry wywołało falę tsunami o wysokości 15 m. Notowane są fale tsunami w wąskich przesmykach dochodzące do 500 m.

Zachodzi podejrzenie, że personel odpowiedzialny za bezpieczeństwo nie analizował zjawisk zachodzących w pobliżu na Oceanie Indyjskim i nie zostało podjęte zwiększenie wysokości muru oporowego chroniącego elektrownię.

Trzeci błąd – postępowanie podczas zagrożenia awarią. Obsługa, postępując ściśle i bezkrytycznie według procedur nakazujących konkretny sposób postępowania, po odczytaniu informacji o wstrząsach sejsmicznych wyłączyła czynne reaktory, pozbawiając elektrownię zasilania własnego. Nie sprawdzono stanu zasilania zewnętrznego, gdyż tego nie przewidywała procedura. Przy uszkodzeniu tego zasilania i unieruchomieniu agregatów prądotwórczych zasilania awaryjnego doszło do opisanej katastrofy.
Tu należy przytoczyć wypowiedź Przewodniczącego japońskiej komisji do badania katastrofy [11]:
„Podstawowe przyczyny są do znalezienia w konwencjach zakorzenionych w kulturze japońskiej: naszym posłuszeństwie, naszej niechęci do kwestionowania zwierzchników, naszemu oddaniu do 'tkwienia w programie', naszej stadności i naszej zaściankowości"

Ta opinia stanowi motto do rozważań G. Grote [11] nad zwiększaniem bezpieczeństwa przez dopuszczenie pewnych niepewności i zarządzania nimi. Wprowadziłoby to do systemu zabezpieczeń pewien element podatności sprężystej (*resilience*) nadający cechy układu sprężystego, który nieco poddaje się, by tym energiczniej przeciwstawić się niebezpieczeństwu.

Istotnie nasuwa się pytanie, czy gdyby zostawić czynny jeden reaktor zapewniający zasilanie własne wszystkich układów chłodzenia, nie uniknęłoby się katastrofy o takich rozmiarach. To przypuszczenie należy do sfery zarządzania niepewnością; to, że reaktory nie uległy uszkodzeniu wskutek wstrząsów sejsmicznych, a tylko na drodze termicznej, wskazuje na konieczność brania pod uwagę takiego wariantu postępowania.

5. Katastrofa w elektrowni Czarnobyl

5.1. Przebieg

26 kwietnia 1986 r. w elektrowni jądrowej w Czarnobylu (ZSRR, obecnie Ukraina), w której były czynne reaktory typu RBMK-1000, nastąpiła katastrofa w wyniku wybuchu wodoru z reaktora bloku energetycznego nr 4. Katastrofa miała jedno uwarunkowanie zewnętrzne – w trakcie przygotowania, po zmniejszeniu mocy reaktora do 50 %, jedna z okolicznych elektrowni została wyłączona i dyspozytornia mocy zażądała opóźnienia eksperymentu, co poskutkowało przeprowadzaniem go przez niedostatecznie przeszkoloną załogę z nocnej zmiany oraz przemęczeniem ekspertów oczekujących wiele godzin na próbę. Całe zdarzenie było wynikiem łańcucha niewłaściwych działań człowieka, w tym wymienionego wyżej opóźnienia przeprowadzenia eksperymentu.

Na podstawie publikacji Wikipedii [12] opartej na 32 opracowaniach źródłowych, w tym komunikatach oficjalnych i prasowych oraz artykule A. Strupczewskiego [14], można przedstawić poniższy schemat następstwa zdarzeń.

W dniu poprzedzającym katastrofę personel obsługujący czwarty reaktor elektrowni prowadził przygotowania do eksperymentu zaplanowanego na kolejny dzień. Ten eksperyment miał odpowiedzieć na pytanie, czy zmiany w projekcie zmierzające do zapewnienia właściwego zasilania systemów własnych (dopływu wody chłodzącej, sterowania, zabezpieczenia itp.) w przypadku konieczności wyłączenia reaktora działają poprawnie. Te zmiany były wprowadzone przed oddaniem reaktora do eksploatacji i eksperyment powinien zostać przeprowadzony wówczas, lecz nie został ze względu na polityczny termin oddania do ruchu.

W celu przeprowadzenia eksperymentu potrzebne było symulowanie sytuacji awaryjnej. W ramach przygotowań zostały wyłączone niektóre z systemów kontroli pracy reaktora, w tym system automatycznego wyłączenia reaktora w razie awarii. **Wyłączenie tego systemu nie było konieczne, został on wyłączony ze względu na wygodę przeprowadzenia eksperymentu.**

Kolejno następowały błędy obsługi. W ich wyniku doszło do nadmiernego obniżenia mocy reaktora, co doprowadziło do zatrucia ksenonem 135, czego załoga nie była świadoma (brak odpowiedniego czujnika). W tej sytuacji zaczęto usuwać pręty reaktora. Spowodowało to zaburzenia w wytwarzanej energii, zaburzenia w procesie chłodzenia i reaktor osiągnął stan krytyczny. Nie mogły zadziałać systemy automatycznego wyłączenia reaktor, bo były wyłączone.

W tej sytuacji krytycznej rozpoczęto eksperyment, w którym ujawniły się tak wszystkie wady konstrukcyjne reaktora, jak i niewyszkolenie załogi. W wyniku niewłaściwych działań doprowadzono do eksplozji pary wodnej, która zniszczyła osłonę antyradiacyjną reaktora, a następnie doszło do wybuchu tlenu i wodoru, co spowodowało zniszczenie budynku i uwolnienie pyłu radioaktywnego.

Akcja gaśnicza też była prowadzona nieprofesjonalnie, przez strażaków nieprzeszkolonych do tego rodzaju akcji.

Straty w ludziach były ogromne, skażenie środowiska katastrofalne na terenie ok. 10 tys. km^2.

5.2. Analiza – konstrukcja reaktora

Reaktory typu RBMK miały konstrukcję niestosowaną gdzie indziej niż w ZSRR. Jeden reaktor tego typu, RBMK-1500 był zainstalowany w elektrowni Ignalina na Litwie i po rozpadzie ZSRR i uzyskani przez Litwę niepodległości stał się dostępny dla ekspertów z poza ZSRR i został poddany analizie i przeróbkom zwiększającym jego bezpieczeństwo [13].

Pierwsze ustalenia wykazały, że wprawdzie reaktor RBMK jest wystarczająco zabezpieczony przed wypadkami inicjowanymi przez uszkodzenie wyposażenia, przez

reaktywność i utratę chłodzenia, o ile nie jest ona spowodowana degradacją przepływów lokalnych. Wykryto także, że w przypadku degradacji przepływów lokalnych może dojść do katastrofy wskutek niedostateczne szybkiej reakcji układów sterowania i zabezpieczenia. Analiza ATWS (Anticipated Transients Withsout Scram) wykazała, że niektóre jej scenariusze mogą prowadzić do konsekwencji nieakceptowanych.

Analizę przeprowadzono na modelu komputerowym opracowanym w Idaho National Engineering Laboratory i dostosowanym do reaktora RBMK tak, aby symulował dokładnie jego warunki pracy. Uzyskane wyniki wskazywały, że w niektórych sytuacjach reaktor zachowywał się jak obiekt o dodatnim sprzężeniu zwrotnym i następowało przekroczenie wartości krytycznych parametrów.
Zastosowano dodatkowy układ zabezpieczający, który usunął to zjawisko.

5.3. Analiza – wnioski

Można zidentyfikować cały zbiór postępowań niewłaściwych z punktu widzenia zasad bezpieczeństwa i stwarzających potencjalne zagrożenie katastrofami:

- konstrukcja reaktora nie była „bezpieczna sama w sobie"; z punktu widzenia zasady ALARP w ogóle nie powinna być dopuszczona do eksploatacji w przemyśle cywilnym,
- o tej sytuacji nie wiedzieli ludzie obsługujący reaktor i przeprowadzający eksperyment,
- ze względów politycznych nie przeprowadzono sprawdzenia prawidłowości działania przeprojektowanych systemów wewnętrznych przed oddaniem reaktora do eksploatacji,
- zgodzono się na opóźnienie eksperymentu – na okres prac badawczych przy reaktorze blok energetyczny powinien zostać wyjęty z pod jurysdykcji dyspozytora sieci,
- wskutek opóźnienia eksperyment przeprowadzono na zmianie na której personel był w ogóle nieprzygotowany na jego przeprowadzenie,
- do przeprowadzenia eksperymentu, ze względu na ułatwienie ewentualnego powtórzenia, wyłączono system wyłączenia reaktora w stanie awarii,
- personel postępował nieprofesjonalnie, bo był nieprzeszkolony i nieświadomy zagrożeń,
- jak wykazały późniejsze badania było możliwe właściwe zabezpieczenie reaktora, tak by przeciwdziałać skutecznie jego wadzie konstrukcyjnej.

Wyniki są znane.

6. Podsumowanie

Z przykładów przedstawionych w niniejszym opracowaniu wyłania się nieodparty wniosek, że naruszanie zasad bezpieczeństwa, w dowolnej fazie cyklu życia systemu i/lub instalacji prowadzi, prędzej czy później, do zdarzeń katastrofalnych. Szczególnie groźne jest niedostatecznie staranne przeprowadzenie analizy zagrożeń i ryzyka, co skutkuje nie rozpatrzeniem możliwych zagrożeń i powzięcie właściwych działań:

- zmian projektowych i/lub,
- wprowadzenie odpowiednich funkcji bezpieczeństwa.

Dodatkowym groźnym czynnikiem jest niestaranne lub nieświadomie błędne działania człowieka wynikające najczęściej z nieuświadomienia sobie możliwych zagrożeń. Czasem nakłada się na to zwykły błąd ludzki – jak wiadomo człowiek jest najsłabszym ogniwem w dobrze zaprojektowanym systemie bezpieczeństwa technicznego.

Bibliografia

1. PN-EN 61508-1:2010 (IEC 61508-1:2010), Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne. (oryg.)
2. PN-EN 61508-5:2010 (IEC 61508-5:2010), Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa. (oryg.)
3. PN-EN 62061:2005 (IEC 62061:2005), Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów związanych z bezpieczeństwem
4. *Pożar w Elektrociepłowni Żerań w Warszawie.* www.Wiadomości.wp.pl/drukuj.html?id=14905333
5. *Pożar w EC Żerań; dwie osoby poszkodowane.* http://wyborcza.pl/2029020,1238583.html
6. Znane są już przyczyny pożaru w EC Żerań. www.reo.pl/podano-przyczyny-pozaru-w-ec-zeran
7. *Fatalny lewy tor*, Wyborcza.pl, 6 marca 2012 r.
8. Katastrofa elektrowni jądrowej Fukushima 1 – Wikipedia wolna encyklopedia. www.pl.wikipedia.org/wiki/katastrofa_elektrowni_jadrowej_Fukushima_I#Przebieg_awarii_i_dalsze_dzia.C5.82ania
9. www.google-Fokushima-explosion-2.jpg
10. www.google-Fokushima_radiations.jpg
11. Grote G., *Promoting safety by increasing uncertainty.* Prezentacja na konferencji WOS2012 "Towards safety through advanced solutions. Sopot, wrzesień 2012.
12. www.pl.wikipedia.org/w/index.php?title=Katastrofa_elektrowni_jadrowej_w_Czarnobylu&oldid=33026400
13. Uspuras E., Vilemas J., *Development of new control and protection systems at the Ignalina Nuclear Power Plant.* Preprints of 7th IFAC Symposium on Automated Systems Based on Human Skill. Aachen, 2007.

Incidents and Catastrophes – what they teach us

Abstract: The synthetic description of two local polish catastrophes: fire in EC Żerań and railway incident on CMK are presented, as well as two nuclear catastrophes: Fukushima and Czarnobyl. The contravening of safety rules that leaded to the catastrophes is indicated.

Keywords: safety, incidents, catastrophes, railway, power industry

prof. dr inż. Tadeusz Missala

Absolwent Wydziału Elektrycznego PŁ, doktoryzował się w 1963 r. na Wydziale Elektrycznym PW. Po 10-letniej pracy w przemyśle i 7-letniej na WAT od 1967 r. jest pracownikiem PIAP. W latach 1967–1988 kierował Ośrodkiem Automatyki Elektrycznej, obecnie piastuje stanowisko Pełnomocnika Dyrektora ds. certyfikacji. Specjalności: automatyka i robotyka przemysłowa, bezpieczeństwo przemysłowe, elektromechaniczne elementy automatyki. Autor i współautor 5 książek oraz ponad 150 publikacji naukowych. Przewodniczący Komitetu Technicznego PKN nr 50 ds. Automatyki i robotyki przemysłowej.

e-mail: tmissala@piap.pl