PL-BY-UA 2007-2013

Współfinansowane ze środków Unii Europejskiej

DOI: 10.5604/20830157.1148053

ANALIZA NIEZAWODNOŚCI SYSTEMU ZABEZPIECZENIA REAKTORA TYPU PWR

Karol Kowal, Mieczysław Borysiewicz
Narodowe Centrum Badań Jądrowych (NCBJ), Zakład Energetyki Jądrowej

Streszczenie. *Celem niniejszej pracy było określenie prawdopodobieństwa niedostępności systemu zabezpieczenia reaktora typu PWR firmy Westinghouse. Obiektem referencyjnym, dla którego wykonano analizę była Elektrownia Jądrowa Surry zlokalizowana w Stanach Zjednoczonych. Praca ta obejmuje utworzenie drzewa uszkodzeń i wykonanie analizy ilościowej w programie SAPHIRE oraz oszacowanie niepewności za pomocą metod Monte Carlo.*

Słowa kluczowe: System Zabezpieczenia Reaktora, Probabilistyczne Analizy Bezpieczeństwa, Analiza Drzewa Uszkodzeń, SAPHIRE, Symulacje Monte Carlo

АНАЛІЗ НАДІЙНОСТІ СИСТЕМИ ЗАХИСТУ РЕАКТОРА ТИПУ PWR

Анотація. *Метою даного дослідження було визначити ймовірність відмови системи захисту реактора типу PWR фірми Westinghouse. Посилаючись на об'єкт, для якого був проведений аналіз AEC Surry (США). Ця робота включає в себе створення дерева відмов і виконання кількісного аналізу в програмі SAPHIRE та оцінки невизначеності за допомогою методу Монте-Карло.*

Ключові слова: система захисту реактора, пробабілістичний аналіз безпеки, аналіз дерева відмов, SAPHIRE, симуляція Монте-Карло

RELIABILITY ANALYSIS OF PWR REACTOR PROTECTION SYSTEM

Abstract. *The aim of this work was to assess the probability of the Westinghouse PWR reactor protection system (RPS) unavailability. The reference facility for which the analysis has been made was Surry Nuclear Power Plant located in the United States. This work includes RPS fault tree development and qualitative analysis using the SAPHIRE code, as well as the uncertainty assessment by applying the Monte Carlo techniques.*

Keywords: Reactor Protection System (RPS), Probabilistic Safety Assessment (PSA), Fault Tree Analysis (FTA), SAPHIRE, Monte Carlo Simulation

Wprowadzenie

Z każdym rodzajem działalności ludzkiej jest związane pewne ryzyko wystąpienia niepożądanych zdarzeń zagrażających życiu lub zdrowiu człowieka oraz jego otoczeniu. Ryzyko to nigdy nie zostanie zredukowane do zera, chyba że dana działalność zostanie wyeliminowana. Nawet wówczas istnieje jednak możliwość, że zaprzestanie danej działalności spowoduje jedynie zmianę źródła zagrożenia. Jest to podstawowa koncepcja w dziedzinie oceny ryzyka i zarządzania nim. Każda działalność powinna więc uwzględniać ryzyko jakie się z nią wiąże oraz dążyć do jego zredukowania do pewnego określonego poziomu akceptacji. W praktyce, definiuje się tzw. funkcje bezpieczeństwa, których realizacja pozwala uniknąć zagrożenia lub ograniczyć jego skutki. Za realizację poszczególnych funkcji bezpieczeństwa odpowiadają systemy bezpieczeństwa, których niezawodność, rozumiana jako prawdopodobieństwo poprawnej pracy przez wymagany czas, powinna być przedmiotem oceny ilościowej [1].

Ocena niezawodności systemów bezpieczeństwa reaktorów jądrowych stanowi szczególny przypadek ze względu na rodzaj oraz zakres zagrożenia, jakie niesie ze sobą uwolnienie do środowiska substancji promieniotwórczych. Jest ona istotnym elementem probabilistycznych analiz bezpieczeństwa – PSA (ang. Probabilistic Safety Assessment), które stanowią podstawę oceny ryzyka związanego z funkcjonowaniem elektrowni jądrowych. Analizy PSA dzielą się na trzy poziomy. Celem poziomu 1 PSA jest identyfikacja ciągów zdarzeń prowadzących do stopienia rdzenia, oszacowanie częstości uszkodzeń rdzenia związanych z tymi ciągami, oraz ocena silnych i słabych punktów systemów bezpieczeństwa, a także procedur opracowanych dla zapobiegania uszkodzeniom rdzenia [3]. Analizy PSA Poziomu 2 identyfikują sposoby uwolnień radioaktywnych z instalacji oraz pozwalają na oszacowanie ich wielkości i częstości. Umożliwiają również ocenę przydatności zastosowanych środków zapobiegania awariom oraz minimalizowania ich skutków. Poziom 3 PSA stanowią obliczenia transportu uwolnień radiacyjnych w środowisku (powietrzu, wodzie i glebie) oraz szacowanie ich skutków dla zdrowia ludzi, skażenia środowiska i żywności [1].

W przypadku wystąpienia zdarzeń inicjujących, które mogą prowadzić do uszkodzenia rdzenia reaktora, wymagana jest więc

Введення

Кожен вид людської діяльності пов'язаний з певним ризиком виникнення небезпечних ситуацій для життя або здоров'я людини та навколишнього середовища. Цей ризик не може бути зведеним до нуля, хіба що діяльність перестане існувати. Навіть тоді коли діяльність припиниться, то зміниться тільки джерело небезпеки. Це основна концепція галузі оцінки та управління ризиками. Таким чином, кожна діяльність повинна враховувати ризик, пов'язаний з ним і спробувати скоротити його до рівня прийнятності. На практиці це визначає так звана функція безпеки реалізації котра дозволяє уникнути небезпеки або зменшити її наслідки. За реалізацію різних функцій безпеки відповідають системи безпеки, надійність яких, розуміємо як ймовірність правильної роботи протягом необхідного часу, який є предметом кількісної оцінки [1].

Оцінка надійності систем ядерної безпеки реактора є особливим випадком, з погляду на рід і ступінь ризику, який пов'язаний з викидом радіоактивних речовин у навколишнє середовище. Це є важливим елементом імовірнісного аналізу безпеки – PSA (англ. Probabilistic Safety Assessment), який є основою для оцінки ризиків, пов'язаних з експлуатацією атомних електростанцій. Аналіз PSA ділиться на три рівні. Ціллю рівня 1 PSA є виявлення послідовності подій, що ведуть до розтоплення ядра, оцінити частоту таких відмов і послідовностей, а також оцінити сильні і слабкі сторони системи безпеки і процедур, призначених для запобігання пошкодження ядра [3]. Аналіз 2 рівня PSA, допомагає визначити шляхи радіоактивних викидів і дозволяє оцінити їх розмір і частоту. Допомагає провести оцінку придатності заходів щодо запобігання аварій і звести до мінімуму їх наслідки. Рівень 3 PSA складається з розрахунків транспортованих викидів радіації в навколишнє середовище (повітря, вода і грунт) та оцінки їх впливу на здоров'я людини, забруднення навколишнього середовища і продуктів харчування [1].

У разі виникнення небезпеки, яка може призвести до пошкодження ядра реактора потрібна негайна перевірка програми, щоб виключити ризик або, принаймні, мінімізувати

natychmiastowa odpowiedź instalacji w celu wyeliminowania zagrożenia lub przynajmniej zminimalizowania jego skutków. Oznacza to uruchomienie odpowiednich systemów, z których każdy pełni określoną funkcję bezpieczeństwa, np. zapewniając chłodzenie rdzenia reaktora, redukcję ciśnienia w obudowie bezpieczeństwa lub usuwanie substancji promieniotwórczych z jej atmosfery. Przede wszystkim jednak zwykle wymagane jest szybkie wyłączenie reaktora. Rolę tę pełni system zabezpieczenia reaktora – RPS (ang. Reactor Protection System). Budowa i zasada działania RPS różni się w zależności od danej technologii i typu reaktora. Jednakże podstawową funkcją tego systemu jest zawsze wprowadzenie do rdzenia reaktora substancji silnie absorbującej neutrony, aby przerwać reakcję rozszczepienia oraz zredukować moc cieplną rdzenia.

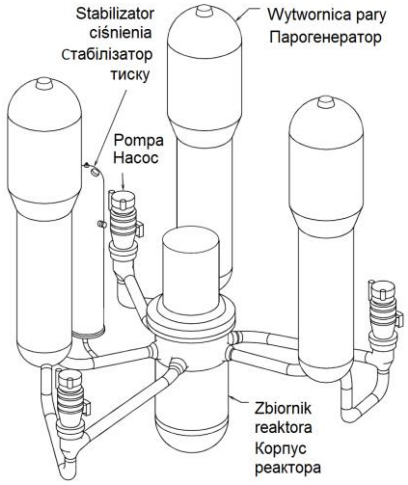
Celem niniejszej pracy było określenie prawdopodobieństwa niedostępności systemu RPS w reaktorze wodnym ciśnieniowym – PWR (ang. Pressurised Water Reactor). Obiektem, dla którego wykonano analizę, był reaktor Westinghouse o mocy 800 MWe z Elektrowni Jądrowej Surry (USA). Reaktor ten posiada trzy pętle obiegu pierwotnego ze wspólnym stabilizatorem ciśnienia (rys. 1). Wszelkie informacje dotyczące specyfikacji technicznej, parametrów pracy, a także niezbędne dane niezawodnościowe dla poszczególnych komponentów systemu RPS zaczerpnięto z raportów amerykańskiej komisji dozoru jądrowego (U.S. NRC) [4, 5, 6]. Analiza ta była częścią szerszej ekspertyzy wykonanej na zlecenie Państwowej Agencji Atomistyki (PAA) [2].

Obliczenia zostały wykonane przy użyciu kodu U.S. NRC SAPHIRE, przeznaczonego do oceny bezpieczeństwa obiektów jądrowych na terenie USA. Opracowano uproszczone drzewo uszkodzeń dla systemu RPS opisujące możliwe sekwencje jego awarii. Następnie przeprowadzono 10 000 prób Monte Carlo, losując wartości prawdopodobieństwa awarii poszczególnych komponentów systemu RPS na podstawie znanych rozkładów eksperymentalnych. Otrzymano rozkład prawdopodobieństwa niedostępności systemu RPS (P_{RPS}) oraz udział procentowy poszczególnych sekwencji zdarzeń w wartości P_{RPS}.

наслідки. Це означає мобілізацію відповідних систем, кожна з яких має функцію безпеки, наприклад забезпечення охолодження активної зони реактора, знизити тиск в корпусі безпеки або видалення радіоактивних речовин з її атмосфери. Як правило, такі ситуації вимагають швидкого відключення реактора. Цю функцію виконує система захисту реактора – RPS (англ. Reactor Protection System). Конструкція і робота RPS буде змінюватись в залежності від конкретної технології і типу реактора. Тим не менш, основною функцією цієї системи завжди залишиться введення в реактор матеріалу субстанції серцевини швидко поглинаючої нейтрони, щоб зупинити поділ і зменшити теплову потужність активної зони.

Метою даного дослідження було визначити ймовірність недоступності системи RPS в водяному енергетичному реакторі – PWR (англ. Pressurised Water Reactor). Об'єкт, для якого був виконаний аналіз – реактор Westinghouse потужністю 800 МВт з Атомної Електоростанція Surry (США). Цей реактор має три петлі первинного ланцюга із загальним стабілізатором тиску (мал. 1) Будь-яка інформація, що стосується технічних характеристик, експлуатаційних параметрів, а також необхідної достовірності даних для окремих компонентів системи RPS взяті з доповіді американської комісії ядерного регулювання (U.S. NRC) [4, 5, 6]. Цей аналіз був частиною більш широкої експертизи, зробленої на замовлення Національного Агентства з Атомної Енергії (PAA) [2].

Розрахунки були зроблені з використанням коду U.S. NRC SAPHIRE, призначеного для оцінки безпеки ядерних установок в США. Було розроблене спрощене дерево відмов для системи RPS, що описує можливі наслідки аварії. Далі проведено 10 000 проб в системі Монте-Карло, спираючись на ймовірність виходу з ладу окремих компонентів системи RPS на основі відомих експериментальних розподілів. Отримано розподіл ймовірностей відсутності системи (P_{RPS}) і відсоток кожної послідовності подій в значенні P_{RPS}.



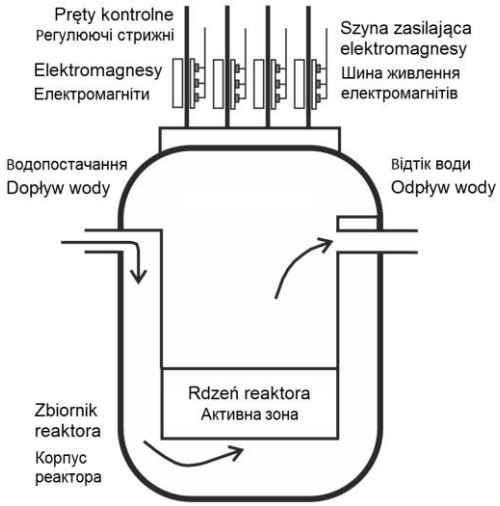
Rys. 1. Trzy pętle obiegu pierwotnego reaktora PWR firmy Westinghouse [6]
Мал. 1. Три петлі первинного контуру реактора PWR фірми Westinghouse [6]

1. Zasada działania systemu RPS

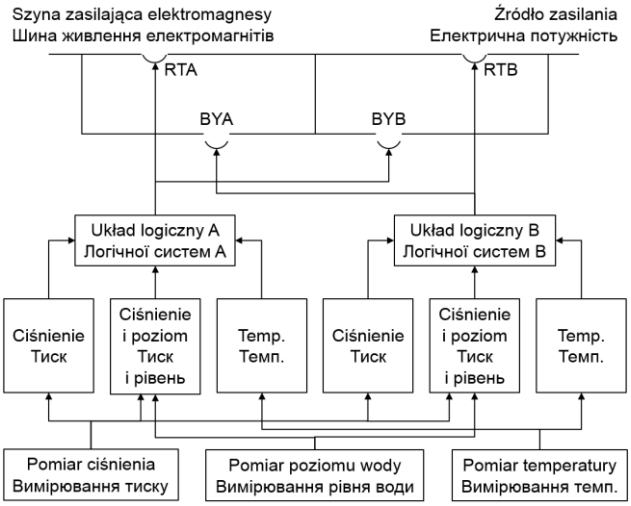
Podstawowym elementem konstrukcyjnym systemu RPS w reaktorze typu PWR jest zestaw prętów kontrolnych silnie absorbujących neutrony. Podczas normalnej eksploatacji reaktora pręty te są utrzymywane nad rdzeniem poprzez elektromagnesy, do których doprowadzane jest zasilanie (rys. 2). Ich położeniem można jednak sterować w celu czasowego zmniejszenia mocy reaktora jeśli jest to konieczne. Wówczas pojedyncze pręty są opuszczane do określonego poziomu, tak aby uzyskać pożądane parametry pracy reaktora. Za sterowanie położeniem prętów kontrolnych odpowiedzialny jest jednak oddzielny system.

1. Принципи роботи системи RPS

Основним структурним елементом системи RPS в реакторі типу PWR є комплект контрольних стержнів сильнопоглинаючих нейтрони. Під час нормальної роботи реактора стержні проходять над ядром через електромагніти, до яких подається електроенергія (мал.2). При необхідності їхнє положення можна контролювати, щоб тимчасово зменшити потужність реактора. Потім окремі стержні опускаються до певного рівня, таким чином, щоб отримати бажані робочі параметри реактора. За розміщення регулюючих стержнів відповідає, окрема система.



Rys. 2. Zasada działania systemu RPS w reaktorze typu PWR [por. 4]
Мал. 2. Принцип роботи системи RPS в реакторі типу PWR [пор. 4]



Rys. 3. Uproszczony schemat funkcyjny systemu RPS w reaktorze typu PWR [por. 4]
Мал. 3. Спрощена схема функціонування системи RPS в реакторі PWR [пор. 4]

Po wystąpieniu zdarzenia inicjującego, które wymaga natychmiastowego wyłączenia reaktora, następuje grawitacyjny zrzut wszystkich prętów kontrolnych poprzez odłączenie zasilania od elektromagnesów, co w krótkim czasie prowadzi do stanu podkrytycznego reaktora. Oznacza to, że liczba neutronów generowanych w wyniku reakcji rozszczepienia jest mniejsza od liczby neutronów absorbowanych i rozpraszanych. W takich warunkach reakcja łańcuchowa nie może być dłużej utrzymywana, a moc cieplna rdzenia szybko maleje w czasie.

Istnieje wiele nieustannie monitorowanych parametrów, których wartości określają stan instalacji w danej chwili czasu. Przekroczenie pewnych określonych wartości progowych tych parametrów może świadczyć o zaistniałej awarii i konieczności wyłączenia reaktora. Wyłączenie reaktora podczas awarii może być np. zainicjowane poprzez sygnał niskiego ciśnienia, niskiego poziomu wody w stabilizatorze ciśnienia lub po odnotowaniu zbyt wysokiej temperatury wody w obiegu pierwotnym (rys. 3). Każdy z tych parametrów monitorowany jest za pomocą trzech niezależnych kanałów analogowych. Kanały te obejmują zestaw odpowiednich sensorów oraz komparatorów pozwalających na porównanie mierzonych wielkości fizycznych z wartościami referencyjnymi. W przypadku przekroczenia wartości progowych sygnał sterowania przesyłany jest do dwóch identycznych podukładów logicznych A i B, które sterują przełącznikami głównymi, odpowiednio RTA i RTB (rys. 3).

Otwarcie przynajmniej jednego z tych przełączników pozwala na odcięcie zasilania od elektromagnesów, co w konsekwencji powoduje grawitacyjny spadek prętów kontrolnych do rdzenia reaktora. Szyna zasilająca elektromagnesy wyposażana jest także w dwa dodatkowe przełączniki BYA i BYB, które zamykane są tylko na czas konserwacji, testów lub naprawy przełączników głównych. Sterowanie przełącznikiem BYA odbywa się wówczas za pomocą układu logicznego B, natomiast przełącznikiem BYB za pomocą układu logicznego A. System RPS wymaga więc zasilania elektrycznego tylko w czasie normalnej pracy reaktora. W stanach awaryjnych natomiast zasilanie to jest celowo odcinane. Tak więc awaria systemu elektrycznego nie prowadzi do awarii RPS, lecz wymusza automatyczne wyłączenie reaktora.

Operatorzy elektrowni mają również możliwość awaryjnego wyłączenia reaktora niezależnie od sygnałów sterowania wychodzących z kanałów pomiarowych systemu RPS. Manualne wyłączenie reaktora może być konieczne np. w przypadku pożaru. Nawet jeśli dany pożar nie zagraża bezpośrednio systemom bezpieczeństwa reaktora i żadne anomalia nie zostały odnotowane przez kanały pomiarowe RPS, to wyłączenie reaktora może być wymagane np. przez wewnętrzne procedury przeciwpożarowe. Wówczas operator odcina zasilanie od elektromagnesów RPS bezpośrednio z poziomu sterowni.

Коли виникає ситуація, яка вимагає негайної зупинки реактора, з подальшим гравітаційним розвантаженням всіх керуючих стержнів, відключення живлення електромагнітів, швидко призводить до критичного стану реактора. Це означає, що число нейтронів, утворених реакцією розщеплення менше, ніж число нейтронів, поглинених і розсіяних. В таких умовах, ланцюгова реакція вже не може бути забезпечена, і субстанція серцевини теплової енергії швидко зменшується. Є багато постійно контрольованих параметрів, значення яких визначає стан системи в даний момент часу. Перевищення певних встановлених порогових значень цих параметрів може свідчити про знайдення несправності і необхідності в зупинці реактора. Зупинка реактора в разі відмови може бути, спричинена сигналом низького тиску, низьким рівнем води в стабілізаторі тиску або занадто високою температурою води в первинному контурі (мал. 3). Кожен з цих параметрів буде контролюватися за допомогою трьох незалежних аналогових каналів. Ці канали включають в свій набір відповідні датчикі і компаратори, які дозволяють порівняти вимірювані фізичні величин з еталонними значеннями. Якщо перевищено граничне значення сигнал керування передається на двох однакових логічних підсистем А та В, які контролюють основні перемикачі відповідно RTA і RTB (мал. 3).

Відкривання щонайменше одного з цих перемикачів дозволяє вимкнути живлення електромагнітів, які в свою чергу призводить до гравітаційного спадання контрольного стержня в серцевину реактора. Шина живлення електромагнітів оснащена двома додатковими перемикачами BYA і BYB, які вимикаються тільки під час обслуговування, перевірки або ремонту основних перемикачів. Управління перемикачем BYA виконується за допомогою логічної системи В, а перемикачем BYB за допомогою логічної системи А. Система RPS в реакторі вимагає живлення тільки під час нормальної експлуатації реактора. У аварійних ситуаціях, живлення навмисно відключається. Таким чином, вихід з ладу електричної системи не призводить до виходу з ладу RPS але змушує автоматично відключити реактор.

Оператори АЕС також мають можливість аварійного відключення реактора, незалежно від сигналів, що надходять з вимірювальних каналів RPS. Ручне закриття реактора може бути необхідним, наприклад в разі виникнення пожежі. Навіть, якщо вогонь не безпосередньо загрожує системі безпеки реактора і ніякі збої не записані в системі RPS, зупинка реактора може знадобитися, під час пожежогасіння. Тоді оператор відключає живлення електромагнітів RPS в реакторі безпосередньо з диспетчерської.

2. Drzewo uszkodzeń systemu RPS

Istnieje wiele metod stosowanych w analizach niezawodności systemów. Aktualnie jednak najczęściej wykorzystywana jest analiza drzew uszkodzeń – FTA (ang. Fault Tree Analysis). Drzewo uszkodzeń opracowane dla danego systemu jest modelem określającym zależności logiczne pomiędzy potencjalnymi uszkodzeniami elementarnych komponentów systemu, błędami obsługi a wystąpieniem określonego zdarzenia, jednoznacznego z niewypełnieniem odpowiedniej funkcji bezpieczeństwa przez analizowany system. Zależności te są rezultatem oddziaływań pomiędzy systemami lub ich elementami, wynikających z zasad konstrukcyjnych obiektu lub też pochodzą z uwarunkowań zewnętrznych dla urządzeń takich jak obsługa operatorska, środowisko pracy, powodzie, zalania, pożary, itp. [1].

Proces konstrukcji drzewa uszkodzeń polega na identyfikacji potencjalnych przyczyn zdarzenia szczytowego, tzn. takich warunków, w których analizowany system nie może spełnić przypisanej mu funkcji bezpieczeństwa. Warunki te, czyli tzw. kryteria uszkodzeń systemu muszą więc być ściśle zdefiniowane przed rozpoczęciem modelowania. Następnie wprowadza się do modelu zdarzenia pośrednie, opisujące główne ścieżki awarii, które zwykle identyfikują przyczyny na poziomie podsystemów, a nie elementarnych komponentów. Uwzględnienie relacji funkcyjnych między nimi dokonywane jest przez wprowadzenie odpowiednich bramek logicznych łączących poszczególne zdarzenia. Zdarzenia pośrednie są analizowane w analogiczny sposób, tzn. ich potencjalne przyczyny stanowią kolejny, niższy poziom drzewa uszkodzeń. Proces ten jest kontynuowany aż do momentu, gdy zostanie osiągnięty taki poziom rozdzielczości drzewa, w którym analiza zostanie sprowadzona do zdarzeń podstawowych, tj. awarii elementarnych komponentów systemu oraz błędów ludzkich, których prawdopodobieństwo może zostać oszacowane i wprowadzone do modelu.

Dane dotyczące częstości występowania awarii danego typu komponentów są gromadzone podczas wieloletniej eksploatacji elektrowni jądrowej. Każdorazowa wymiana lub naprawa danego typu komponentu jest odnotowywana i wprowadzana do bazy danych niezawodnościowych.

Najlepsze oszacowanie niezawodności dla poszczególnych systemów bezpieczeństwa można uzyskać wykorzystując dane zebrane podczas eksploatacji danej instalacji. W przypadku gdy nie ma dostępu do takich danych, lub gdy dane te nie mogły być zebrane, np. w przypadku nowych elektrowni, stosowane są dane uśrednione z innych obiektów. Warto jednak podkreślić, iż analiza drzewa uszkodzeń dostarcza ważnych wyników jakościowych w postaci sekwencji zdarzeń prowadzących do niedostępności lub awarii konkretnych systemów bezpieczeństwa. Nawet wówczas gdy brak jest odpowiednich danych niezawodnościowych, aby dokonać analizy ilościowej, można przeprowadzać analizy porównawcze, np. w celu określenia słabych i mocnych punktów alternatywnych opcji modernizacji instalacji.

W ramach niniejszej pracy utworzono drzewo uszkodzeń dla systemu RPS reaktora PWR firmy Westinghouse. Na podstawie specyfikacji technicznej tego reaktora przyjęto założenie, że aby system RPS mógł spełnić swoją funkcję niemal wszystkie pręty kontrolne (min. 46 z 48) muszą zostać wprowadzone do rdzenia. Niedostępność systemu RPS (zdarzenie szczytowe) zdefiniowano więc jako sytuację, podczas której więcej niż 2 pręty kontrolne nie mogą być umieszczone w rdzeniu, gdy jest to konieczne.

Przyczyną takiego stanu może być jednoczesna awaria obu podukładów A i B odcinających zasilanie od elektromagnesów lub odkształcenia mechaniczne rdzenia lub prętów, które blokują swobodny spadek pomimo odcięcia zasilania. Oba podukłady, A i B mogą tez zostać utracone w wyniku błędów podczas kalibracji aparatury pomiarowej (rys. 4). Niewłaściwe ustawienia sensorów i komparatorów uniemożliwiają bowiem wykrycie anomalnych wartości parametrów pracy reaktora.

Główne drzewo uszkodzeń systemu RPS obejmuje więc 3 zdarzenia podstawowe: CED0000X – odkształcenie mechaniczne rdzenia reaktora, CED0001X – odkształcenia co najmniej dwóch

2. Дерево відмов RPS

Є багато методів, використовуваних в аналізах надійності системи. В даний час найбільш часто використовується аналіз дерева відмов – FTA (англ. Fault Tree Analysis). Дерево відмов розроблене для даної системи є моделью, яка визначає логічну залежність між потенційним пошкодженням елементарних компонентів системи, помилками при обслуговуванні, які можуть спровокувати аварію, недотримання відповідних засобів безпеки аналізованою системою. Ці взаємозалежності є результатом взаємодії між системами або їх елементами, відповідно до правил будівництва об'єкта, або походять з зовні це обслуга оператора, робоче середовище, повені, затоплення, пожежі і т.д. [1].

Процес будівництва дерева відмов, полягає на визначенні можливих причин головної події, тобто таких умов, в яких аналізована система не зможе виконати своєї функції безпеки. Ці умови, тобто критерії пошкоджень системи, повинні бути більш чітко визначені перед початком моделювання. Потім до моделі вводять проміжну подію, що описує головні шляхи аварії, яка, як правило, визначає причину на рівні підсистем, а не елементарних компонентів.

Функціональні відносини між ними досягаються введенням відповідних логічних елементів, що поєднують кожну подію. Проміжні події аналізовані тим же чином, тобто їх можливі причини, знаходяться на нижчому рівні дерева відмов. Цей процес продовжується до тих пір, поки він не досягне рівню дерева, на якому аналіз зводиться до основних подій, тобто, аварії елементарних компонентів даної системи і людських помилок, які можна оцінити і включити в модель.

Дані про поширеність того чи іншого виду аварії компонентів зібрані під час тривалої експлуатації атомних електростанцій. Всякий раз, коли замінюється або ремонтується даний тип компонента, дані записуються і вносяться до бази даних про надійність.

Найкращу оцінку надійності окремих систем безпеки можна знайти за допомогою даних, зібраних в ході роботи станції. У випадку, якщо ви не маєте доступу до таких даних, або дані не можуть бути зібрані, наприклад, у разі нових електростанцій використовуються середнені дані з інших об'єктів. Слід зазначити, що аналіз дерева відмов дає важливі якісні результати у вигляді послідовності подій, що призвели до недоступності або відмови конкретних систем безпеки. Навіть, якщо бракує відповідних даних про надійність, щоб зробити кількісний аналіз, то можна провести порівняльний аналіз, наприклад для того щоб визначити сильні і слабкі сторони альтернативних варіантів модернізації установки.

В рамках цієї роботи було створено дерева відмов для системи RPS реактора PWR фірми Westinghouse. На підставі технічних характеристик даного реактора передбачається, що система RPS, щоб мати можливість виконувати свої функції, то практично всі регулюючі стержні (мін. 46 з 48) повинні бути введені в ядро. Недоступність даної системи RPS (кульмінаційна подія), визначається як ситуація, в якій більше двох стержнів управління не можуть бути розміщені в ядрі, якщо це необхідно.

Причиною цього може бути одночасна відмова двох підсистем A та B, які відключають живлення електромагнітів або механічна деформація ядра, або стержнів, які блокують вільне падіння, незважаючи на відключення електроенергії. Обидві підсистеми, A і B також можуть бути втрачені через помилки під час калібрування вимірювальної апаратури (мал.4). Неправильне налаштування датчиків і компараторів перешкоджають виявленню аномальних значень параметрів реактора.

Головне дерево відмов системи RPS включає в себе 3 основні події: CED0000X – механічна деформація активної зони реактора, CED0001X – деформація, принаймні двох стержнів безпеки і COO0000X – систематична людська помилка під час калібрування вимірювальної апаратури. Крім

prętów bezpieczeństwa i COO0000X – systematyczny błąd ludzki podczas kalibracji aparatury pomiarowej. Ponadto, rozwinięto poddrzewa opisujące możliwe sekwencje zdarzeń prowadzące do niedostępności podukładu A (rys. 5) oraz podukładu B (rys. 6) systemu RPS. Drzewa te uwzględniają zarówno błędy układów logicznych jak i awarie przełączników, w tym także utratę sterowania nad przełącznikiem BYA (BYB) podczas gdy jest on zamknięty ze względu na konserwację lub testy RTA (RTB).

Nie przeprowadzono natomiast szczegółowej analizy awarii aparatury kontrolno-pomiarowej ani układów logicznych A i B. Elementy te zostały potraktowane jako oddzielne podsystemy, których prawdopodobieństwo awarii jest znane. Nie uwzględniono również możliwości manualnego wyłączenia reaktora przez operatora i ewentualnych błędów ludzkich z tym związanych. Przyjęto założenie, że zaistniała awaria wymaga automatycznego, natychmiastowego wyłączenia reaktora, a czas niezbędny aby operator rozpoznał zagrożenie i wyłączył reaktor jest zbyt długi. Takie założenie jest równoznaczne z potraktowaniem możliwego błędu operatora jako zdarzenie pewne.

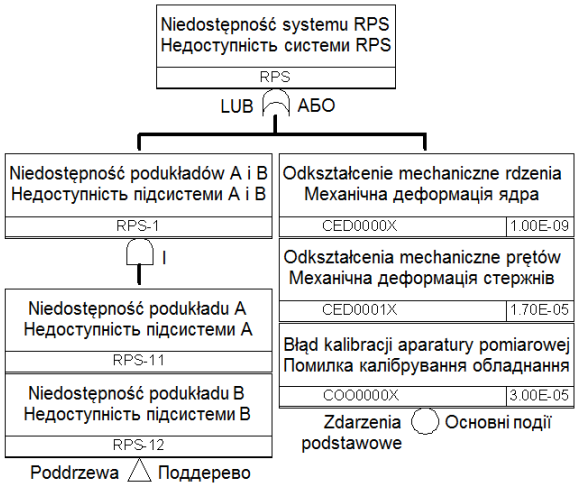
Prawdopodobieństwo P wystąpienia poszczególnych zdarzeń uwzględnionych w drzewie uszkodzeń systemu RPS wynosi:

$$P = \lambda \cdot t \tag{1}$$

gdzie: λ – obserwowalna częstość występowania danego zdarzenia [1/h], a t – czas narażenia [h]. W niniejszej pracy wartości λ pobrano z raportu bezpieczeństwa U.S. NRC opracowanego dla elektrowni jądrowej Surry [4]. Za t przyjęto natomiast średni czas pomiędzy testami systemu RPS, który wg. tego raportu wynosi 15 dni (360h). Ponadto, przyjęto założenie, iż wartości λ i P dla wszystkich zdarzeń podstawowych mają rozkład logarytmiczny normalny, dla którego współczynnik błędu EF wynosi:

$$EF = \frac{P_{95}}{P_{ME}} \tag{2}$$

gdzie: P_{ME} – mediana rozkładu prawdopodobieństwa P (tab. 1), natomiast P_{95} – kwantyl 95% rozkładu prawdopodobieństwa P. Takie podejście pozwala na szacowanie niepewności wyników na podstawie wielokrotnych (w tym przypadku 10 000) symulacji Monte Carlo, podczas których wartości P poszczególnych zdarzeń podstawowych są losowane z uwzględnieniem charakterystyki odpowiadających im rozkładów.



Rys. 4. Główne drzewo uszkodzeń systemu RPS
Мал. 4. Основне дерево відмов системи RPS

того, розроблено піддерева, які описують можливі послідовності подій, що призвели до недоступності підсистеми A (мал. 5) і підсистеми B (мал. 6) системи RPS. Ці дерева висвітлюють, як логічні помилки так і аварії вимикачів, в тому числі втрату контролю над перемикачем BYA (BYB), під час коли він закритий на технічне обслуговування або тестування RTA (RTB).

Не проводився детальний аналіз аварії контрольно-вимірювальниих приладів, а ні логічних A і B. Ці елементи розглядаються, як окремі підсистеми, якіх ймовірність аварії відома. Не аналізувалися зупинки реактора вручну оператором і потенціальні людські помилки. Передбачалося, що аварійна ситуація, потрібує автоматичного, негайного відключення реактора, а час який потрбує оператор щоб визначити загрозу і зупинити реактор занадто довгий. Це припущення еквівалентно обробці можливих помилок оператора, як однозначної події.

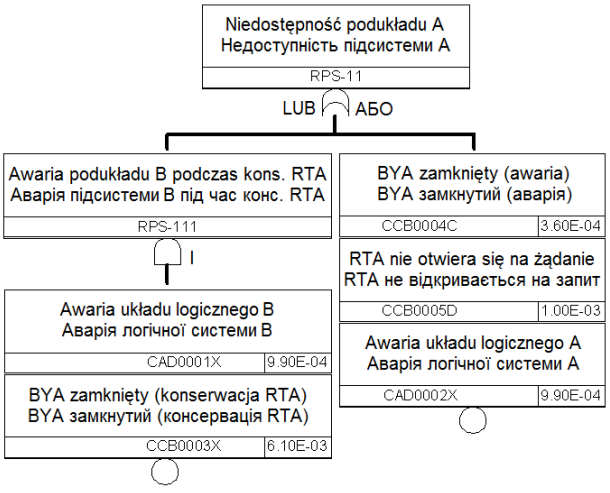
Імовірність P подій, які передбачені в дереві відмов системи RPS складає:

$$P = \lambda \cdot t \tag{1}$$

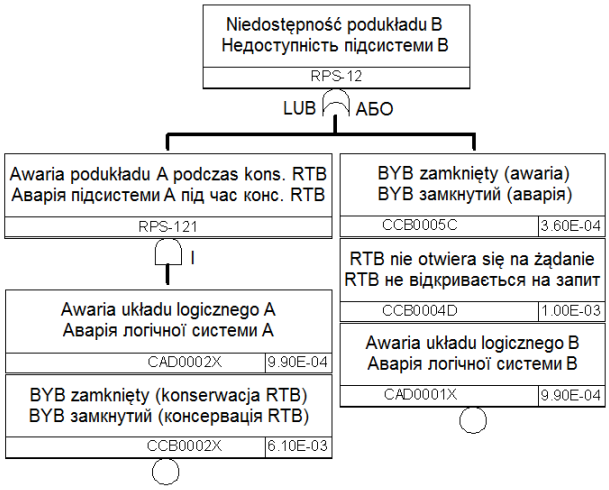
де: λ – зафіксована частота конкретної події [1/h], а t – час впливу [h]. В даній статті значення λ взято зі звіту безпеки U.S. NRC підготовленого для AEC Surry [4]. За t прийнятий середній час між тестуванням системи RPS , який згідно з рапортом складає 15 днів (360 годин). Крім того, передбачається, що значення λ і P для всіх основних подій мають нормальний логарифмічний розподіл, для якого частота помилок EF складає:

$$EF = \frac{P_{95}}{P_{ME}} \tag{2}$$

де: P_{ME} – середній розподіл ймовірностей P (таб. 1), натомість P_{95} – 95% квантиль розподілу ймовірностей P. Такий підхід дозволяє оцінити невизначеність результатів на основі декількох (в даному випадку 10 000) симуляцій Монте-Карло, в якому P значення кожної події, яка відібрана з врахуванням характеристики відповідних для неї розподілів.



Rys. 5. Drzewo uszkodzeń dla podukładu A systemu RPS
Мал. 5. Дерево відмов для підсистеми A системи RPS



Rys. 6. Drzewo uszkodzeń dla podukładu B systemu RPS
Rys. 6. Дерево відмов для підсистеми B системи RPS

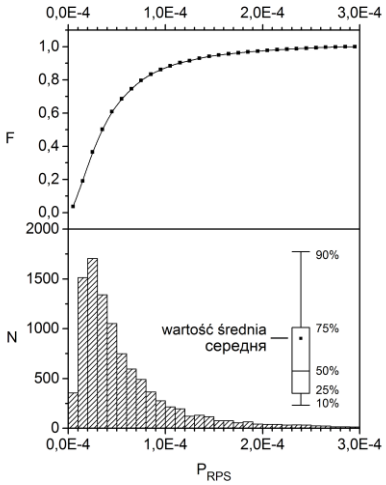
Tab. 1. Lista zdarzeń podstawowych uwzględnionych w drzewie uszkodzeń RPS [4]
Таб. 1. Перелік основних подій які враховані в дереві відмов RPS [4]

Nr №	Oznaczenie Позначення	Opis zdarzenia Опис події	P_{ME}	EF
1	CAD0001X	Awaria układu logicznego B Аварія логічної системи B	9,9E-04	10
2	CAD0002X	Awaria układu logicznego A Аварія логічної системи A	9,9E-04	10
3	CCB0002X	BYB zamknięty (konserwacja RTB) BYB замкнутий (консервація RTB)	6,1E-03	4
4	CCB0003X	BYA zamknięty (konserwacja RTA) BYA замкнутий (консервація RTA)	6,1E-03	4
5	CCB0004C	Przełącznik BYA zamknięty (awaria) Вимикач BYA замкнутий (аварія)	3,6E-04	3
6	CCB0004D	Przełącznik RTB nie otwiera się na żądanie Вимикач RTB не відкривається на запит	1,0E-03	3
7	CCB0005C	Przełącznik BYB zamknięty (awaria) Вимикач BYB замкнутий (аварія)	3,6E-04	3
8	CCB0005D	Przełącznik RTA nie otwiera się na żądanie Вимикач RTA не відкривається на запит	1,0E-03	3
9	CED0000X	Odkształcenie mechaniczne rdzenia Механічна деформація ядра	1,0E-09	---
10	CED0001X	Odkształcenia mechaniczne prętów Механічна деформація стержнів	1,7E-05	---
11	COO0000X	Błąd kalibracji aparatury pomiarowej Помилка калібрування обладнання	3,0E-05	10

3. Wyniki obliczeń i wnioski

Ze względu na stosunkowo prostą zasadę działania oraz brak konieczności zasilania elektrycznego, system RPS charakteryzuje się wysoką niezawodnością. Prawdopodobieństwo niedostępności tego systemu na żądanie (P_{RPS}) wynosi zaledwie ok. 6,5E-5, co stanowi wartość średnią rozkładu otrzymanego na podstawie symulacji Monte Carlo wykonanych dla 10 000 prób (rys. 7).

Rozkład ten jest jednomodalny o wyraźnym maksimum przypadającym na wartości z przedziału od 2,0E-5 do 3,0E-5. Widoczna jest jednak silna asymetria prawostronna co sprawia, iż lepszą miarą tendencji centralnej jest w tym przypadku mediana, która wynosi ok. 4,0E-5. Asymetrię tę można zauważyć także w typowym przedziale zmienności, tj. pomiędzy pierwszym (25%) a trzecim kwartylem (75%). Dominują więc wartości niskie (mniejsze niż średnia), natomiast wartości wysokie (powyżej trzeciego kwartyla) charakteryzuje duże zróżnicowanie. Stąd stosunkowo wysoka wartość odchylenia standardowego (9,5E-05), która wskazuje na duży rozrzut otrzymanych wyników.



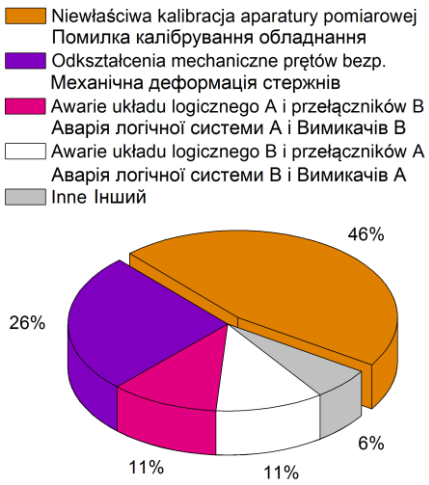
Rys. 7. Rozkład (N) i dystrybuanta (F) prawdopodobieństwa P_{RPS}
Мал. 7. Розподіл (N) функція розподілу (F)імовірність P_{RPS}

Dominujący wkład w prawdopodobieństwo niedostępności systemu RPS mają błędy ludzkie, popełnione podczas kalibracji aparatury kontrolno-pomiarowej (ponad 46%). Ok. 26% wkładu w P_{RPS} mają uszkodzenia prętów kontrolnych, uniemożliwiające ich wprowadzenie do rdzenia nawet po odcięciu zasilania. Istotny wpływ (ok. 22%) mają też zdarzenia, w których następuje utrata jednego z układów logicznych podczas gdy przełącznik główny odpowiadający drugiemu z układów jest w naprawie, w trakcie konserwacji, lub też nie otwiera się na żądanie. Wszystkie pozostałe awarie stanowią zaledwie ok. 6% P_{RPS} (rys. 8, tab. 2).

3. Результати розрахунків висновків

Через відносно простий принцип роботи і відсутність потреби електропостачання, система RPS характеризується високою надійністю. Імовірність недоступності даної системи на вимогу (P_{RPS}) тільки прибл. 6,5E-5, що складає середній показник, отриманий на основі розподілу методом Монте-Карло для 10 000 разів (мал. 7).

Цей розподіл з виразним максимумом значення в діапазоні від 2,0E-5 до 3,0E-5. Тим не менш, є сильна асиметрія правостороння , що робить кращу міру центральної тенденції в даному випадку є медіана, яка становить бл. 4,0E-5. Асиметрію можна спостерігати також в типовому діапазоні змін, між першим (25%) і третім квартилем (75%). Переважають низькі значення (менші ніж середня), натомість високі значення (вище третього квартиля) характеризуються великою різницею. Таким чином, відносно високе стандартне відхилення (9,5E-05), яке показує великий діапазон результатів.



Rys. 8. Udział procentowy poszczególnych sekwencji awaryjnych w P_{RPS}
Мал. 8. Відсоткова сектограма послідовностей аварійних ситуацій в P_{RPS}

Основний внесок у ймовірність недоступності системи RPS мають людські помилки, здійснені під час калібрування контрольно-вимірювальних приладів (більше 46%). Прибл. 26% в P_{RPS} мають ушкодження контрольних стержнів, які не можуть ввійти в ядро, навіть після відключення живлення. Значний вплив (прибл. 22%) мають також ситуації, де є втрата однієї логічної системи, в той час як головний перемикач, відповідний другому з підсистеми є в ремонті під час технічного обслуговування, або не відкривається на вимогу. Всі інші аварії складають лише прибл. 6% P_{RPS} (мал. 8, табл. 2).

Raporty dotyczące analiz niezawodności dla reaktorów PWR firmy Westinghouse z elektrowni jądrowej Surry podają wartości mediany P_{RPS} w zakresie od 1,0E-5 [5] do 3,6E-5 [4]. Wyniki obliczeń wykonanych w ramach niniejszej pracy przekraczają nieznacznie te wartości. Różnice te mogą być spowodowane innym podejściem do modelowania oraz szczegółowością analizy. Niniejsza praca nie uwzględniała np. awarii poszczególnych komponentów aparatury pomiarowej, takich jak przetworniki, sensory czy komparatory. Przyjęto założenie, iż ze względu na wysoki poziom redundancji (kilka równoległych kanałów mierzących tę samą wielkość fizyczną) awaria uniemożliwiająca wykrycie anomalii w wyniki niezależnych uszkodzeń aparatury jest bardzo mała w porównaniu z błędami systematycznymi, jakie mogą zostać popełnione przez człowieka podczas konserwacji, testów oraz kalibracji sprzętu. Pomimo jednak pewnych różnic i ograniczeń w dostępie do danych otrzymane wartości P_{RPS} są zbliżone to tych, które zostały opublikowane przez NRC [4, 5].

Рапорт аналізу надійності для реакторів PWR фірми Westinghouse AEC в Surry подають значення медіани P_{RPS} в діапазоні від 1,0E-5 [5] до 3,6E-5 [4]. Результати розрахунків, проведених в даній роботі трохи перевищують ці значення. Ці відмінності можуть бути через різницю підходу до моделювання і детального аналізу. В ці дослідження не включали відмови окремих компонентів вимірювальної апаратури, таких як перетворювачі, датчикі чи порівнювачі. У зв'язку з високим рівнем надмірності (кілька паралельних каналів для вимірювання тієї ж фізичної величини) аварія перешкоджає виявити аномалії в результатах незалежних пошкоджень обладнання є дуже мала в порівнянні з систематичними помилками, які можуть бути вчинені людиною під час технічного обслуговування, тестування і калібрування обладнання. Незважаючи на деякі відмінності і обмеження доступу до даних, отриманих P_{RPS} значення близькі до тих, які були опубліковані NRC [4, 5].

Tab. 2. Lista możliwych sekwencji zdarzeń prowadzących do awarii systemu RPS [2]
Таб. 2. Перелік можливих послідовностей подій, що призводять до відмови системи RPS [2]

Nr	Sekwencja zdarzeń Хід подій	Prawdopodobieństwo Вірогідність	Udział procentowy Відсотки	№	Sekwencja zdarzeń Хід подій	Prawdopodobieństwo Вірогідність	Udział procentowy Відсотки
1	COO0000X	3,00E-05	46,45%	8	CAD0001X, CAD0002X	9,79E-07	1,52%
2	CED0001X	1,70E-05	26,32%	9	CCB0004C, CCB0004D	3,60E-07	0,56%
3	CAD0001X, CCB0003X	6,04E-06	9,34%	10	CCB0005C, CCB0005D	3,60E-07	0,56%
4	CAD0002X, CCB0002X	6,04E-06	9,34%	11	CAD0001X, CCB0004C	3,56E-07	0,55%
5	CCB0004D, CCB0005D	1,00E-06	1,55%	12	CAD0002X, CCB0005C	3,56E-07	0,55%
6	CAD0001X, CCB0005D	9,90E-07	1,53%	13	CCB0004C, CCB0005C	1,30E-07	0,20%
7	CAD0002X, CCB0004D	9,90E-07	1,53%	14	CED0000X	1,00E-09	< 0.01%

Podziękowania

Praca powstała w ramach projektu *PL-NTU Transgraniczna wymiana doświadczeń* PBU.03.01.00-06-386/11-00 współfinansowanego w ramach Programu Współpracy Transgranicznej Polska-Białoruś-Ukraina 2007-2013 finansowanego ze środków Unii Europejskiej w ramach Europejskiego Instrumentu Sąsiedztwa i Partnerstwa.

Niniejsza publikacja została stworzona przy pomocy Unii Europejskiej. Wyłączną odpowiedzialność za zawartość niniejszej publikacji ponoszą Karol Kowal i Mieczysław Józef Borysiewicz oraz w żaden sposób nie może być ona postrzegana jako odzwierciedlenie poglądów Unii Europejskiej.

Завдяки

Робота створена в рамках проекту PL-NTU Прикордонного обміну досвідом PBU.03.01.00-06-386/11-00, фінансованих в рамках Програми Транскордонного Співробітництва Польща-Білорусь-Україна 2007-2013 фінансується Європейським Союзом в рамках Європейського Інструменту Сусідства та Партнерства.

Ця публікація була створена за допомогою Європейського Союзу. Відповідальність за зміст цієї публікації лежить на Каролі Ковалі і Мечиславові Юзефові Борисевичу, і жодним чином не може розглядатися як відображення поглядів Європейського Союзу.

Literatura || Література

[1] Borysiewicz M.: Wykorzystanie probabilistycznych analiz bezpieczeństwa (PSA) w tworzeniu wymogów bezpieczeństwa dla elektrowni jądrowych. Raport NCBJ, Warszawa 2010.
[2] Borysiewicz M., Kowal K., Łuszczek K., Potempski S.: Analiza niezawodności wybranych systemów bezpieczeństwa reaktora PWR przy użyciu programu SAPHIRE. Raport wewn. PAA, Warszawa 2013.
[3] IAEA: Development and Application of Level-1 PSA. IAEA, Vienna 2010.
[4] U.S. Nuclear Regulatory Commission: Reactor Safety Study – An assessment of accident risks in U.S. nuclear power plants. U.S. NRC, Washington 1975.
[5] U.S. Nuclear Regulatory Commission: Reliability Study: Westinghouse Reactor Protection System, 1984-1995. U.S. NRC, Washington 1999.
[6] U.S. Nuclear Regulatory Commission: Nuclear Power for Electrical Generation. U.S. NRC, Washington 2012.

Mgr inż. Karol Kowal
e-mail: k.kowal@ncbj.gov.pl

Absolwent Wydziału Fizyki i Informatyki Stosowanej krakowskiej AGH, gdzie w roku 2008 ukończył studia magisterskie o specjalności Fizyka Jądrowa. W latach 2008-2009 odbył studia podyplomowe z Informatyki w Politechnice Rzeszowskiej. Od roku 2010 doktorant Wydziału Elektrotechniki i Informatyki Politechniki Lubelskiej. Od marca 2011 roku zajmuje stanowisko starszego specjalisty w Zakładzie Energetyki Jądrowej Narodowego Centrum Badań Jądrowych w Świerku. Staż zawodowy odbył w General Electric w USA.

Магістр інж. Кароль Коваль
e-mail: k.kowal@ncbj.gov.pl

Закінчив факультет фізики та прикладної інформатики AGH в Кракові, де в 2008 році закінчив магістратуру в галузі ядерної фізики. У 2008-2009 відбув післядипломне навчання з Іконформатики в Жешувському університеті. З 2010 року аспірант факультету електротехніки та інформатики в Люблінській Політехніці. З березня 2011 року працює старшим спеціалістом у Департаменті атомної енергетики Національного науково-дослідного центру ядерних досліджень в Свєрку. Стажувався в General Electric в США.

Dr Mieczysław Józef Borysiewicz
e-mail: manhaz@cyf.gov.pl

Z-ca kier. Zakładu Energetyki Jądrowej Narodowego Centrum Badań Jądrowych w Świerku. Do 2012 roku dyr. Centrum Doskonałości MANHAZ - Zarządzanie Zagrożeniami dla Zdrowia i Środowiska. Profesor wizytujący w Uniwersytecie w Bolonii w latach 1977, 1978, 1980 oraz 1983, a także w Uniwersytecie Libre w Brukseli w latach 1972-1973. Autor licznych publikacji i monografii dotyczących oceny ryzyka poważnych awarii i systemów wspomagania decyzji w stanach kryzysowych.

Д-р Мєчислав Юзеф Борисевич
e-mail: manhaz@cyf.gov.pl

Заступник керівника Департаменту атомної енергетики Національного науково-дослідного центру ядерних досліджень в Свєрку. До 2012 року директор Центру підвищення кваліфікації MANHAZ – Управління охорони здоров'я та навколишнього середовища. Викладав в Болонському університеті в 1977, 1978, 1980 і 1983, а також в університеті Лібре в Брюсселі в 1972-1973. Автор численних публікацій і монографій які оцінюють ризик серйозних аварій і систем підтримки прийняття рішень в надзвичайних ситуаціях.

otrzymano/ отримано/received: 04.03.2015 *przyjęto do druku/ прийнято до друку/accepted: 15.03.2015*