**Státní úřad
pro jadernou bezpečnost**

**jaderná
bezpečnost**

VÝBĚR A HODNOCENÍ PROJEKTOVÝCH A NADPROJEKTOVÝCH UDÁLOSTÍ A RIZIK PRO JADERNÉ ELEKTRÁRNY

bezpečnostní návod JB-1.7

SÚJB
Prosinec 2010

Jaderná bezpečnost

VÝBĚR A HODNOCENÍ PROJEKTOVÝCH A NADPROJEKTOVÝCH UDÁLOSTÍ A RIZIK PRO JADERNÉ ELEKTRÁRNY

Vydal: Státní úřad pro jadernou bezpečnost, prosinec 2010

Účelová publikace bez jazykové úpravy

OBSAH

1. ÚVOD

DŮVOD VYDÁNÍ

(1.1) Státní úřad pro jadernou bezpečnost (SÚJB) je ústředním orgánem státní správy, který vykonává státní správu a dozor při využívání jaderné energie a ionizujícího záření, v oblasti radiační ochrany a v oblasti jaderné, chemické a biologické ochrany.

(1.2) V rámci své pravomoci a působnosti, v souladu se zásadami činnosti správních orgánů a mezinárodní praxí, vydává bezpečností návody, ve kterých dále rozpracovává požadavky jaderné bezpečnosti.

CÍL

(1.3) Tento bezpečnostní návod VÝBĚR A HODNOCENÍ PROJEKTOVÝCH A NADPROJEKTOVÝCH UDÁLOSTÍ A RIZIK PRO JADERNÉ ELEKTRÁRNY je součástí série bezpečnostních návodů, které rozpracovávají požadavky, které definovala asociace WENRA vydáním Referenčních úrovní – „WENRA Reactor Safety Reference Levels, 2008“ [8] (dále jen jako „Referenční úrovně“) a dále rozpracováním požadavků Mezinárodní agentury pro atomovou energii [9], [12] .

(1.4) Je určen zejména pro držitele povolení k provozu jaderného zařízení, kterému nabízí možný postup, jehož dodržení mu zajistí, že jeho aktivity v dané oblasti budou v souladu s požadavky Atomového zákona, jeho prováděcími předpisy a naplní příslušné Referenční úrovně WENRA.

PŮSOBNOST

(1.5) Tento návod se primárně soustředí na jaderné elektrárny ve smyslu Společné úmluvy o jaderné bezpečnosti - „civilní“ jaderné elektrárny, jeho principy a postupy lze vztáhnout také na další jaderná zařízení.

PLATNOST

(1.6) Toto vydání se ověřuje po dobu 12 měsíců, po vydání návodu SÚJB. V tomto období se návrhy na změnu a doplnění příslušných částí realizují postupem, který určí SÚJB. Před uplynutím doby platnosti na základě vydaných změn a doplnění, v souladu s novými poznatky vědy a techniky a získaných zkušeností s praktickým používáním připraví SÚJB vydání nové, které na toto bezprostředně naváže.

2. ZKRATKY, DEFINICE, POJMY

ZKRATKY

ČR – Česká republika

MAAE – Mezinárodní agentura pro atomovou energii (též IAEA)

SÚJB – Státní úřad pro jadernou bezpečnost

PSA – Probabilistic Safety Assessment (Pravděpodobnostní hodnocení bezpečnosti)

WENRA - Western European Regulator's Association

DEFINICE A POJMY

Projektová východiska jaderné elektrárny: Souhrn podmínek, stavů a událostí, které jsou uvažovány při projektování jaderné elektrárny a pro které je prokázáno, že nedojde k překročení projektových kritérií. (*Tím je zaručeno, že vlastnosti jaderné elektrárny jsou schopny zabránit vzniku abnormálního provozu a havarijních podmínek nebo omezit jejich nežádoucí účinky a v případě jejich výskytu zajistit, že potenciální dávky ozáření, jimž může být vystaveno obyvatelstvo a pracovníci jaderné elektrárny, nepřesáhnou nejnižší reálně dosažitelné hodnoty dávek ionizujícího záření.)*

Normální provoz: Všechny stavy a podmínky provozu jaderného zařízení při dodržení limitů a podmínek bezpečného provozu; pro jaderná zařízení podle § 2 písm. h) bod 1. zákona (dále jen „reaktor") jsou to zejména uvádění reaktoru do kritického stavu, ustálený provoz na výkonu, ~~a~~ odstavování reaktoru, zvyšování a snižování jeho výkonu, odstavený stav, údržba, opravy, testování a výměna paliva.

Abnormální provoz: stavy, podmínky a události, odkloňující se od normálního provozu, jejichž výskyt lze při provozu jaderného zařízení očekávat; a které nevedou vzhledem k projektovým opatřením k závažnému poškození zařízení důležitých z hlediska jaderné bezpečnosti a po jejich ukončení, resp. odstranění příčin a následků je jaderné zařízení schopné normálního provozu.

Očekávaná provozní událost: viz abnormální provoz.

Nejnižší reálně dosažitelné hodnoty dávek ionizujícího záření: Hodnoty optimalizované z hlediska radiační ochrany podle zvláštního právního předpisu (v současnosti Vyhláška č. 307/2002 Sb. O radiační ochraně).

Havarijní podmínky: Všechny stavy, podmínky a události nad rámec abnormálního provozu, zahrnující projektové a nadprojektové nehody.

Stávající jaderná elektrárna: jaderná elektrárna, která je v daném čase v provozu anebo má k tomuto datu platné stavební povolení.

Projektová nehoda: havarijní podmínky uvažované v projektových východiscích, při kterých nedojde k porušení nebo překročení projektových kritérií projektových nehod.

Projektová kritéria: hodnoty parametrů, jejichž splněním je prokázáno, že nebudou překročeny nejnižší reálně dosažitelné dávky ionizujícího záření.

Projektová kritéria projektových nehod: hodnoty parametrů, jejichž splněním je prokázáno splnění základních bezpečnostních funkcí projektu a zachování fyzických bariér.

Nadprojektová nehoda: Havarijní podmínky, při kterých dojde k porušení nebo překročení projektových kritérií projektových nehod. Nadprojektové nehody mohou, ale nemusí být spojeny s významným poškozením aktivní zóny.

Těžká havárie: Nadprojektová nehoda, při které došlo k vážnému poškození a ztrátě struktury aktivní zóny reaktoru nebo palivových souborů, a která může vést k radiační nehodě. (Pro lehkovodní reaktory je těžká havárie ztotožňována s havárii spojenou s významným tavením aktivní zóny.)

Postulovaná iniciační událost: Odchylka od podmínek normálního provozu, zahrnutá do projektových východisek, jejíž rozvoj může vést k abnormálnímu provozu nebo havarijním podmínkám. *Primární příčinou události může být selhání zařízení elektrárny anebo souvisejících zařízení mimo elektrárnu, anebo chyba provozní obsluhy a také vnější události buď vyvolané přírodou anebo člověkem*.

Projektové události: soubor událostí abnormálního provozu a projektových nehod.

Bezpečnostní funkce: Účel, který musí být dosažen, aby byla zajištěna jaderná bezpečnost.

Bezpečnostní systémy: Zařízení důležitá z hlediska jaderné bezpečnosti v jaderných zařízeních, vybraná do bezpečnostní tříd způsobem, stanoveným zvláštním právním předpisem (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd), která zajišťují plnění základních bezpečnostních funkcí při událostech abnormálního provozu a projektových nehodách; bezpečnostní systémy jsou tvořeny soubory ochranných, akčních a podpůrných bezpečnostních systémů.

Velký časný únik: Uvolnění radionuklidů, která vyžaduje zavedení ochranných opatření k omezení ozáření osob a životního prostředí. K těmto následkům dochází z důvodu rychlosti rozvoje události dříve, než je možno tato ochranná opatření použít.

Jednoduchá porucha: Událost, vedoucí ke ztrátě schopnosti některého prvku vykonávat stanovenou funkci, přičemž všechny ostatní prvky pracují správně. Následné poruchy vyvolané počáteční jednoduchou poruchou jsou považovány za součást této jednoduché poruchy.

Prakticky vyloučené podmínky: Takové podmínky, jejichž výskyt je prokazatelně fyzikálně nemožný, nebo které mohou nastat s extrémně nízkou pravděpodobností. Kriteria pro praktické vyloučení některých podmínek jsou dány zvláštními právními předpisy.

Kanál: Řetězec komponent a zařízení, potřebných k vytvoření samostatného ochranného, řídícího nebo monitorovacího signálu. Kanál končí v místě, kde dochází ke kombinaci jím vytvářeného signálu se signály z jiných zálohujících ochranných, řídících nebo monitorovacích kanálů.

Deterministická metoda: Metoda analýzy, která má za cíl určit odezvu jaderného zařízení a jeho systémů na jednotlivé postulované iniciační události a která prokazuje splnění projektových kritérií.

Deterministická bezpečnostní analýza: Předikuje průběh odezvy jaderné elektrárny na stanovené iniciační události vznikající za předem definovaných provozních stavů, s použitím definovaného souborů předpokladů (pravidel) analýzy a kritérií přijatelnosti. Analýzou se prokazuje splnění kritérií přijatelnosti anebo (obecněji) stanovených bezpečnostních cílů.

Pravděpodobnostní metoda: Metoda, která oceňuje pravděpodobnost vzniku iniciačních událostí a poruchových scénářů a jejich průběhu , rozvoje a následků.

Pravděpodobnostní bezpečnostní analýza: Komplexně oceňuje pravděpodobnost vzniku poruchových scénářů a jejich následku. Obvyklým výsledkem analýzy je určení pravděpodobnosti poškození aktivní zóny (obecněji palivového systému), pravděpodobnosti velkých úniků radioaktivních materiálů do okolí elektrárny, anebo celkového rizika plynoucího z provozu jaderné elektrárny.

Palivový element: Jaderný materiál hermeticky uzavřený pokrytím. *Může to být konstrukční jednotka, jejíž základní složkou je jaderné palivo; zahrnuje pokrytí, palivové tabletky, plnicí plyn, pružiny, uzávěry apod.*

Palivový soubor: Seskupení palivových elementů, které jsou do reaktoru zaváženy a vyjímány z něj jako jeden celek.

Palivový systém: Projektem určená sestava palivových souborů a dalších komponent aktivní zóny, nezbytných k řízení reaktivity a udržení projektové struktury palivových souborů v aktivní zóně reaktoru. *Palivový systém je obvykle tvořen konstrukčními komponentami aktivní zóny, jako jsou např.: palivové soubory a jejich komponenty, vnitřní řídicí komponenty aktivní zóny jako regulační proutky, proutky s vyhořívajícími absorbéry, jsou-li použity, proutky s neutronovými zdroji, opěrné desky, apod*

Aktivní zóna: Strukturovaná část reaktoru, vymezená palivovým systémem, ve které probíhá řízená štěpná řetězová reakce.

Porušení palivových elementů: Narušení hermetičnosti pokrytí palivového elementu s následnou možností úniku štěpných produktů.

Poškození aktivní zóny: Překročení projektových kritérií pro porušení palivových elementů a pro poškození palivového systému. *Obvykle se tím rozumí významná ztráta geometrie zóny spojená s významným únikem radioaktivity, jenž má za následek překročení kritérií pro projektovou havárii, pro lehkovodní reaktory je typickou příčinou přehřátí aktivní zóny.*

Verifikace (výpočetních prostředků): Ověření, jestli výpočetní prostředek v každé fázi svého životního cyklu vyhovuje stanoveným požadavkům a je připraven k použití

Validace (výpočetních prostředků): Prokázání a vyhodnocení schopnosti výpočetního prostředku dostatečně věrně stanovit odezvu modelované komponenty, systému, nebo celé jaderné elektrárny. Validace musí zahrnovat porovnání s experimentálními výsledky sledování modelovaného procesu.

3. VÝCHODISKA

(3.1) Požadavky na projekty jaderných elektráren, vedoucí k dosažení vysoké provozní spolehlivosti a odolnosti proti vnitřním a vnějším vlivům jsou podmínkou pro dosažení bezpečnosti provozu jaderných zařízení. Základní požadavky na projekt jsou stanoveny zákonem č. 18/1997 Sb. a jeho prováděcí vyhláškou 195/1999 Sb. Obecné principy bezpečnosti jsou dále obsaženy v Fundamental Safety Principles SF-1 [8] a v Bezpečnostních požadavcích MAAE NS-R-1, případně v doporučeních návodů NS-G-1.1 až NS-G-1.12.

(3.2) V harmonizační studii pracovní skupiny pro harmonizaci bezpečnosti energetických reaktorů asociace WENRA vydané v roce 2006 a aktualizované v roce 2008 jsou stanoveny pro tematické oblasti E a F tzv. referenční úrovně, které vyjadřují požadavky na tuto oblast pro země EU [8]. Ty uvádějí výběr požadavků a doporučení MAAE na návrh a provoz jaderných elektráren, a jejich systémů, konstrukcí a komponent, majících vztah k bezpečnosti, s cílem určit společné minimální požadavky na zajištění bezpečnosti provozovaných jaderných elektráren.

(3.3) SÚJB zpracoval výše uvedené podklady do návrhu vyhlášky, nahrazující současnou vyhlášku 195/1999 Sb. „o požadavcích na jaderná zařízení k zajištění jaderné bezpečnosti, radiační ochrany a havarijní připravenosti“, jejíž vydání je vázáno na nový připravovaný Atomový zákon. S ohledem na současnou potřebu aktualizovaného textu požadavků dozoru, související s přípravou výstavby nových jaderných bloků SÚJB paralelně připravuje vydání textu návrhu nové vyhlášky o požadavcích na jaderná zařízení jako referenční text formou návodu SÚJB a dále vydává tento návod, kompatibilní s návrhem textu uvedené vyhlášky, jako výklad některých požadavků stávající vyhlášky 195/1999 Sb. s rozšířeními, zaměřenými na oblast bezpečnostních analýz.

ROZSAH

(3.4) Tento návod se zabývá projektovými východisky jaderných elektráren, kterými se rozumí rozsah podmínek, provozních stavů a událostí, které jsou uvažovány při projektování jaderné elektrárny a pro které je prokázáno, že vlastnosti jaderné elektrárny jsou schopny zabránit vzniku abnormálního provozu a havarijních podmínek nebo omezit jejich nežádoucí účinky a v případě jejich výskytu zajistit, že potenciální dávky ozáření, jimž může být vystaveno obyvatelstvo a pracovníci jaderné elektrárny, nepřesáhnou nejnižší reálně dosažitelné hodnoty dávek ionizujícího záření.

(3.5) Specificky tento návod definuje a konkretizuje požadavky pro následující oblasti:

- Základní bezpečnostní cíle,
- Ochrana do hloubky,
- Bariéry proti úniku radioaktivních látek,
- Bezpečnostní funkce,
- Projektová východiska a specifikace postulovaných iniciačních událostí,
- Soubor projektových událostí,
- Nadprojektové nehody a těžké havárie,
- Vnitřní a vnější rizika,

- Odolnost pro případ sabotáže,
- Kombinace událostí,
- Kategorizace událostí podle frekvence výskytu,
- Deterministické bezpečnostní cíle a kritéria přijatelnosti,
- Pravděpodobnostní bezpečnostní cíle,
- Deterministické průkazy bezpečnosti projektu a bezpečnostních rezerv,
- Analýzy projektových událostí (provozních stavů a projektových nehod),
- Analýzy nadprojektových nehod (včetně těžkých havárií),
- Analýzy vnitřních a vnějších rizik,
- Obecné požadavky na plnění bezpečnostních funkcí,
- Funkce odstavení reaktoru,
- Funkce odvodu tepla,
- Funkce ochranné obálky,
- Měřící a řídící systémy,
- Bloková dozorna,
- Ochranné systémy,
- Havarijní elektrické napájení,
- Posuzování projektu.

V příloze 2 k tomuto návodu je uvedený typický seznam postulovaných iniciačních událostí, charakteristických pro jaderné elektrárny s tlakovodním reaktorem.

STRUKTURA

(3.6) Struktura tohoto návodu v značné míře odpovídá struktuře referenčních úrovní WENRA. Při přípravě tohoto návodu bylo důsledně prověřeno, zda všechny požadavky referenčních úrovní WENRA jsou v plném rozsahu pokryty. Jelikož však existující úrovně WENRA byly vypracovány pro stávající elektrárny, byly do tohoto návodu s využitím stejných výchozích dokumentů a podkladů doplněny ty požadavky, které se týkají nově budovaných jaderných elektráren, konkrétně elektráren s reaktory III. generace. V textu návodu byla v maximálním možném rozsahu použita terminologie podle stávajících anebo připravovaných vyhlášek SÚJB.

(3.7) Jak již bylo uvedeno, tento návod je zaměřen na jeden typ jaderných elektráren (jaderných zařízení s tlakovodním reaktorem o tepelném výkonu vyšším než 50 MW). Je vypracován s předpokladem, že i nové jaderné elektrárny v ČR budou realizovány s využitím technologie tlakovodního reaktoru. V případě výstavby jiného typu reaktoru bude vydán relevantní specifický dokument.

(3.8) Návod byl vypracován především pro potřeby hodnocení bezpečnosti v případě výstavby nových jaderných zdrojů. Pro stávající jaderné elektrárny se požadavky tohoto návodu uplatní jako požadavky současného standardu v rámci jejich periodického hodnocení bezpečnosti a to v přiměřeném rozsahu a s cíli, které jsou rozumně dosažitelné s uvážením míry rizika, nákladů na realizaci požadavku a s ohledem na očekávaný příspěvek ke zvýšení

bezpečnosti. V odůvodněných případech (především v souvislosti s opatřeními pro zvládání těžkých havárií) je v tomto návodu rozdílnost přístupů k stávajícím a novým elektrárnám specificky uvedena.

4. ZÁKLADNÍ BEZPEČNOSTNÍ CÍL

(4.1) V souladu se základními bezpečnostními principy MAAE (Fundamental Safety Principles [8]) je základním cílem jaderné bezpečnosti chránit osoby, společnost a životní prostředí před nežádoucími účinky ionizujícího záření. Pro dosažení co nejvyšší rozumně dosažitelné úrovně bezpečnosti je potřebné:

- Zabránit nekontrolovanému ozáření osob a uvolnění radionuklidů do životního prostředí.
- Minimalizovat pravděpodobnost vzniku takých událostí, které by mohly vést ke ztrátě kontroly nad aktivní zónou reaktoru, nad štěpnou řetězovou reakcí, radioaktivním zdrojem nebo jakýmkoli jiným zdrojem záření.
- V případe vzniku takovýchto událostí zvládnout je tak, aby byly minimalizovány jejich následky.

(4.2) Dodržení základního bezpečnostního cíle musí být zajištěno ve všech fázích existence jaderné elektrárny, včetně jeho plánování, umisťování, projektování, výroby, výstavby, uvádění do provozu, provozu až po vyřazení elektrárny z provozu a to i se zahrnutím transportu radioaktivních materiálů a nakládaní s radioaktivními odpady.

(4.3) Projekt elektrárny musí mít za cíl prevenci vzniku podmínek abnormálního provozu a havarijních podmínek a omezení jejich nežádoucích účinků a musí v případě jejich výskytu zajistit, že potenciální dávky ozáření, jimž může být vystaveno obyvatelstvo a pracovníci jaderné elektrárny, nepřesáhnou nejnižší reálně dosažitelné hodnoty dávek ionizujícího záření.

(4.4) Projekt musí zabezpečit, že požadované bezpečnostní a provozní cíle jsou prokazatelně dosažitelné s přiměřenými rezervami i při respektování neurčitostí metod bezpečnostního hodnocení.

5. BEZPEČNOSTNÍ STRATEGIE

Ochrana do hloubky

(5.1) V souladu s bezpečnostními požadavky MAAE, NS-R-1 [11] musí být dodržení bezpečnostního cíle zabezpečeno v projektu elektrárny uplatněním principu ochrany do hloubky, který se opírá o použití vícenásobných fyzických bariér proti úniku radionuklidů a o zabezpečení integrity těchto bariér systémem vzájemně se doplňujících technických a organizačních opatření. K nejdůležitějším technickým opatřením patří vnitřní (inherentní) bezpečnostní charakteristiky reaktoru s prokázanými bezpečnostními rezervami, spolehlivý systém řízení provozu elektrárny, soustava aktivních a pasivních bezpečnostních systémů elektrárny a další opatření a systémy pro zajištění ochrany osob a životního prostředí před účinky ionizujícího záření. Tato opatření musí být hierarchicky uspořádána do několika (běžně pěti) úrovní ochrany tak, že v případě selhání opatření na nižší úrovni se v dalším kroku uplatňují opatření vyšší úrovně. Uplatněním principu ochrany do hloubky se zabezpečí, že dokonce ani při vícenásobném selhání zařízení nebo obsluhy i na více úrovních ochrany nedojde k ohrožení osob ani životního prostředí.

(5.2) Cíle ochrany do hloubky na jednotlivých úrovních jsou následující:

1 . Předcházení odchylkám od normálního provozu;
2. Identifikace a náprava událostí abnormálního provozu;
3. Kompenzační zásahy a odpovídající nápravná opatření, vedoucí k odvrácení rozvoje, nebo ke zvládání havarijních podmínek projektovými prostředky, k zachycení úniků radiace a radionuklidů a omezení důsledků jejich úniků, pokud k nim dojde;
4. Zvládání nadprojektových nehod včetně těžkých havárií;
5. Opatření na ochranu pracovníků jaderné elektrárny a opatření na ochranu osob a životního prostředí při radiační nehodě.

Specifikace základních prostředků pro dosažení uvedených cílů je v přiložené tabulce:

Charakteristika pěti úrovní ochrany [MAAE, INSAG-10, NS-R-1]

Úroveň ochrany	Cíl	Základní prostředky pro dosažení cíle
Úroveň 1	Předcházení odchylkám od normálního provozu, předcházení poruchám	Inherentní vlastnosti systémů, vedoucí k zajištění jaderné bezpečnosti, konzervativní rysy projektu a vysoká kvalita konstrukce a provozu zařízení, systémy kontroly a řízení provozu
Úroveň 2	Identifikace poruch a zvládání očekávaných provozních událostí	Systémy kontroly a řízení a příslušné provozní předpisy (organizační opatření)

	(náprava abnormálního provozu), přechod do bezpečného, stabilizovaného a kontrolovaného stavu (V106)	
Úroveň 3	Zvládaní projektových nehod a přechod do bezpečného, stabilizovaného a kontrolovaného stavu	Bezpečnostní systémy a havarijní předpisy (organizační opatření)
Úroveň 4	Předcházení a zmírňování následků těžkých havárií	Doplňková opatření, včetně specifických systémů (technické prostředky) a programů pro zvládaní těžkých havárií (organizační opatření)
Úroveň 5	Zmírňování radiačních následků významných úniků radioaktivních látek	Opatření na ochranu obyvatelstva a životního prostředí při radiační nehodě

(5.3) Vysoká úroveň ochrany do hloubky musí být zajištěna především tím, že

- Spolehlivost a účinnost systémů na různých úrovních ochrany bude zajištěna tak, aby byla dosažena co nejnižší pravděpodobnost odchylek od normálního provozu, co nejvyšší spolehlivost řídících a bezpečnostních systémů elektrárny jakož i systémů a postupů pro zvládání nadprojektových nehod a těžkých havárií, aby byla co nejnižší pravděpodobnost vzniku těžkých havárií s velkým poškozením aktivní zóny a v důsledku toho nejnižší pravděpodobnost velkých úniků radioaktivních látek do okolí elektrárny.
- Nově budované jaderné zdroje musí mít vyřešenu odpovídajícím způsobem nezávislou funkci všech linií ochrany do hloubky a zejména musí být vybaveny odpovídajícími systémy pro vyloučení nebo zvládání těžkých havárií, spojených s roztavením aktivní zóny reaktoru, které se implementují s ohledem na stále nízkou znalost fenomenologie takových havárií a vysokou neurčitost stanovení pravděpodobné četnosti jejich výskytu; tyto systémy mají za cíl především zachování funkčnosti ochranné obálky i při těžkých haváriích.
- Systémy určené pro zabezpečení ochrany bariér na různých úrovních musí být v maximálně možném rozsahu nezávislé. Systémy, speciálně určené pro zvládání těžkých havárií musí být v maximální možné míře nezávislé na zařízení, které zajišťuje zvládání projektových událostí.
- Zvláštní pozornost musí být věnována těm vnitřním a vnějším událostem, které mohou současně ohrozit více než jednu bariéru anebo mohou způsobit současnou poruchu všech zálohujících se (redundantních) divizí bezpečnostních systémů.

Bariéry proti úniku radioaktivních látek

(5.4) Pro tlakovodní reaktor jsou bariérami proti úniku radionuklidů materiál (struktura) jaderného paliva a hermetické pokrytí palivových elementů, hermetická tlaková hranice chladícího systému reaktoru a hermetická hranice systému ochranné obálky (kontejnment). Projekt musí v maximální prakticky možné míře zabránit nadměrnému zatížení fyzických bariér a tím zajistit eliminaci rizik vedoucích k ohrožení integrity bariér, zabránit poškození, selhání anebo obtoku bariéry v případě jejího ohrožení nadměrnou zátěží, zabránit poškození

bariéry v důsledku poškození jiné bariéry a minimalizovat významné úniky radionuklidů do okolí v případě poškození bariéry.

(5.5) Bariéry a systémy ochrany do hloubky se musí konstruovat tak, aby se

- při normálním a abnormálním provozu zachovala integrita všech bariér a v havarijních podmínkách projektových nehod byla při postulovaném porušení jedné bariéry zachována integrita všech zbývajících bariér,
- v podmínkách těžkých havárií zachovala vždy integrita poslední fyzické bariéry, t.j. ochranné obálky. Pro stávající elektrárny se podmínka zachování integrity ochranné obálky v podmínkách těžkých havárií uplatňuje v takovém rozsahu, jak je to rozumně dosažitelné.

6. BEZPEČNOSTNÍ FUNKCE

(6.1) Pro udržení funkčnosti všech bariér proti úniku radionuklidů během normálního a abnormálního provozu a v požadovaném rozsahu i v havarijních podmínkách (minimálně v havarijních podmínkách projektových nehod) je třeba zajistit základní bezpečnostní funkce [11], kterými jsou:

1. řízení reaktivity tak, aby bylo možné za všech podmínek bezpečně odstavil reaktor a udržet ho v podkritickém stavu,
2. odvod tepla z jaderného paliva (z aktivní zóny nebo systému pro skladování jaderného paliva) po dostatečně dlouhou dobu,
3. zadržení radioaktivních materiálů uvnitř fyzických bariér, zachycení ionizujícího záření a zabránění nekontrolovanému úniku radionuklidů do životního prostředí, t.j. omezení úniků tak, aby nebyly překročeny stanovené limity při všech projektem uvažovaných stavech.

(6.2) Tyto základní bezpečnostní funkce musí být plně zajištěny za normálního a abnormálního provozu, i za podmínek projektových nehod. V případě nadprojektových nehod musí být základní bezpečnostní funkce zajištěny v rozumně dosažitelném rozsahu jinými prostředky. Realizace základních bezpečnostních funkcí musí být zajištěna implementací vzájemně se doplňujících technických a organizačních bezpečnostních opatření na jednotlivých úrovních ochrany do hloubky. Efektivnost a spolehlivost bezpečnostních opatření musí být prokázána kombinací deterministických a pravděpodobnostních metod hodnocení.

7. PROJEKTOVÁ VÝCHODISKA A SPECIFIKACE POSTULOVANÝCH INICIAČNÍCH UDÁLOSTÍ

Projektová východiska

(7.1) Projektová východiska musí obsahovat předem definovaný rozsah provozních stavů, odchylek od normálního provozu a iniciačních událostí, které mohou vést k abnormálnímu provozu a k havarijním podmínkám. Jaderná bezpečnost musí být prokázána s dostatečnou spolehlivostí pro všechny podmínky a události normálního i abnormálního provozu a i pro události, vedoucí k havarijním podmínkám, které jsou zahrnuté do projektových východisek dané jaderné elektrárny v dané lokalitě a to i po událostech, vyvolaných přírodními podmínkami a jevy, které nelze prakticky vyloučit. Systémy, konstrukce a komponenty důležité z hlediska bezpečnosti musí zvládnout všechny předpokládané stavy a podmínky s dostatečnými bezpečnostními rezervami.

(7.2) Odchylky od normálního provozu zahrnuté do projektových východisek, jejichž rozvoj může vést k abnormálnímu provozu nebo havarijním podmínkám, se označují společným názvem postulované iniciační události. Předpokládá se vznik postulovaných iniciačních událostí jak během provozu elektrárny na výkonu, tak i v režimech s odstaveným reaktorem, s uvážením poruch v chladicích systémech elektrárny, předpokládá se vznik poruch v bazénech skladování čerstvého i vyhořelého paliva, v systémech pro zpracování nebo skladování radioaktivních odpadů, jakož i při zacházení s jaderným palivem. Musí být vyhodnoceny iniciační události vyvolané poruchami zařízení, chybami provozních pracovníků nebo v důsledku vnějších jevů a událostí.

(7.3) Projektová východiska musí specifikovat ty vlastnosti jaderné elektrárny, se kterými bude schopno zvládat projektem stanovený rozsah provozních stavů (tj. normální a abnormální provoz), a havarijních podmínek, při dodržení požadavků radiační ochrany podle zvláštního předpisu (Vyhláška č. 307/2002 Sb. ve znění vyhlášky č. 499/2005 Sb. o radiační ochraně).

(7.4) Projektová východiska musí obsahovat specifikaci podmínek normálního provozu, abnormálního provozu a havarijních podmínek, které mohou nastat po postulovaných iniciačních událostech, a s tím související zařazení zařízení, důležitých z hlediska bezpečnosti, do bezpečnostních tříd v souladu s požadavky zvláštního právního předpisu (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd), a specifikaci důležitých předpokladů a souvisejících metod analýz bezpečnosti.

(7.5) Projektová východiska musí zahrnout všechny postulované iniciační události s vlivem na jadernou bezpečnost, které tam přísluší s ohledem na pravděpodobnou četnost výskytu a možné radiologické důsledky. Reprezentativní spektrum iniciačních událostí musí být určeno s využitím deterministických a pravděpodobnostních metod, s uplatněním provozních zkušeností a inženýrských odhadů, relevantních pro daný typ zařízení.

(7.6) Je vhodné provádět zařazení postulovaných iniciačních událostí do skupin, pro které platí obdobná kriteria přijatelnosti a obdobné předpoklady analýz. Běžně se iniciační události zařazují podle :

(a) základního mechanizmu, vedoucího k potenciálnímu ohrožení bezpečnostních funkcí,

(b) základní příčiny vzniku postulované iniciační události,

(c) četnosti výskytu a potenciálních důsledků iniciační události a jejích možných rozvojů,

(d) možností následného poškození systémů, zajišťujících bezpečnostní funkce, po iniciační události,

(e) vztahu rozvoje postulované iniciační události k projektem předpokládaným událostem a jejich vyřešeným rozvojům.

(7.7) Výsledky analýz podle seznamu projektových a nadprojektových událostí musí být použity pro stanovení mezních podmínek, na něž budou projektovány systémy, konstrukce a komponenty významné pro jadernou bezpečnost tak, aby bylo prokázáno, že budou řádně zajištěny potřebné bezpečnostní funkce a budou dosaženy bezpečnostní cíle. Pro stávající elektrárny se tento postup použije při analýzách bezpečnosti elektrárny a realizaci potřebných modifikací zařízení v rozumně proveditelném rozsahu.

(7.7a) Schopnost zařízení zvládnout provozní události a havarijní podmínky s dodržením stanovených bezpečnostních cílů se musí ověřit deterministickými metodami. Pravděpodobnostní metody se musí použít k ocenění rizika, vztahujícího se k projektovému řešení i k provozu jaderné elektrárny.

(7.8) Projektová východiska Projektová východiska musí být ve všech fázích existence jaderné elektrárny systematicky ověřována, doplňována a dokumentována tak, aby odrážela jeho aktuální stav.

Postulované iniciační události, vedoucí k abnormálního provozu a projektovým nehodám

(7.9) Projektová východiska musí zahrnout stavy a postulované iniciační události a jejich rozvoje, které jsou vyvolané poruchami zařízení elektrárny nebo chybami obsluhy. Podle vlivu na degradaci základních bezpečnostních funkcí a podle příčin vzniku iniciační události je možno stanovit skupiny událostí s příklady konkrétních iniciačních událostí uvedených v příloze 2 A.

(7.10) Seznam postulovaných iniciačních událostí uvedený v příloze 2 A má charakter doporučení, slouží pro kontrolu úplnosti seznamu, specifického pro daný projekt reaktoru. Ten může být změněn (rozšířen nebo zúžen) tak, aby odpovídal přijatým projektovým řešením a administrativním opatřením. Je na projektantovi, aby rozhodl a náležitě zdůvodnil, které iniciační události budou použity v bezpečnostních analýzách. Obzvláště v případě nových reaktorů III. generace, používajících koncepčně nové systémy, je potřebné do seznamu iniciačních událostí (případně scénářů rozvoje těchto událostí) zařadit možné poruchy v těchto systémech.

Nadprojektové nehody a těžké havárie

(7.11) Jaderná bezpečnost musí být vyhodnocena i pro nadprojektové nehody, aby se zavedla odpovídající preventivní a zmírňující opatření a omezily radioaktivní úniky, ohrožující obyvatelstvo a životní prostředí i v případech událostí s velmi nízkou četností výskytu.

(7.12) Tyto nehody mohou být důsledkem vícenásobných selhání zařízení nebo chyb obsluhy a mohly by potenciálně vést k velkým únikům radioaktivních látek. I pro tyto nehody musí být stanovené specifické požadavky na projekt, metody analýzy a kritéria přijatelnosti. Je potřebné uvažovat dvě skupiny podmínek:

- Nadprojektové nehody při kterých nedochází k tavení aktivní zóny reaktoru
- Těžké havárie spojené s tavením aktivní zóny.

(7.13) Doporučený výběr typů nadprojektových nehod by měl zahrnovat především události uvedené v příloze 2 B, nejsou-li tyto součástí projektových událostí.

(7.14) Těžké havárie mohou být vyvolány libovolnou iniciační událostí, uvedenou v předchozích oddílech, v kombinaci s vícenásobným selháním zařízení nebo chybami obsluhy, nad rámec specifikace projektových nehod JE. Těžké havárie a jejich scénáře jsou zpravidla identifikovány ve studiích pravděpodobnostního hodnocení bezpečnosti druhé úrovně a pokrývají všechny provozní režimy dané JE (výkonové, nevýkonové provozní režimy i otevřený reaktor).

(7.15) Konkrétní výběr scénářů těžkých havárií by měl být proveden na základě pravděpodobnostního hodnocení bezpečnosti a s respektováním existující mezinárodní praxe. I v případě, že bude pravděpodobnost poškození aktivní zóny velmi nízká, musí být uvažovaná minimálně jedna těžká havárie spojená s roztavením aktivní zóny při nízkém tlaku. Měla by být zvolena taková havárie s nezanedbatelnou pravděpodobností, která vede k největšímu zatížení ochranné obálky jak z hlediska jeho mechanického namáhání, tak i z hlediska zdrojového členu radioaktivity. Pro tuto reprezentativní (referenční) havárii musí být v projektu nové JE navržena opatření, která zabezpečí s vysokou pravděpodobností dodržení bezpečnostních cílů. U stávajících JE by měl být tento požadavek uplatněn tak, aby bylo riziko poškození ochranné obálky a úniku radionuklidů v rozumně dosažitelné míře sníženo.

Vnitřní a vnější rizika

(7.16) Projekt musí kromě poruch technologického zařízení nebo chyb obsluhy taktéž uvážit specifická zatížení a parametry prostředí, které souvisí s poruchami ostatních zařízení uvnitř elektrárny , nebo s lokalitou umístění elektrárny a působí na systémy, konstrukce a komponenty jako vnitřní a vnějších vlivy nebo rizika.

(7.17) Mezi vnitřní vlivy patří dynamické účinky úniku chladiva z vysokoenergetických potrubí, švihy potrubí, vnitřní projektily, vznikající např. z roztržení rotujících strojních částí, jakým je utržení lopatky turbíny, vnitřní záplavy, vnitřní požáry a výbuchy, pády a nárazy těžkých břemen, selhání tlakových častí, opor a jiných konstrukčních částí, elektromagnetické interference mezi zařízeními elektrárny, úniky vody, plynu, páry nebo škodlivých látek. Ve skupině vnějších vlivů musí být uvažovány dvě podskupiny událostí s vyhodnocením reálné možnosti výskytu specificky pro danou lokalitu:

- přírodní události, jako zemětřesení, vichřice, blesky, vnější záplavy, extrémní vnější teploty, extrémní dešťové a sněhové srážky, tvorba ledu, zvýšení hladiny spodní vody,

extrémní sucho, extrémní teploty chladicí vody a zamrzání, jiná rizika v dodávce chladící vody a vzduchu, apod.,

- události způsobené lidskou činností jako vnější požáry a výbuchy (včetně velkého požáru plynového potrubí), náhodné pády letadel, elektromagnetické interference se zařízením mimo elektrárnu, ohrožení z dopravy a průmyslových činností v okolí elektrárny i na území elektrárny (letící předměty, plynový oblak, výbuchy), rizika ze sousedních objektů a zařízení včetně sousedních jaderných zařízení, šíření toxických, korozívních nebo hořlavých plynů, apod.

(7.18) I v případě nízké pravděpodobnosti náhodného pádu letadla jakékoliv velikosti, musí být v projektu nové elektrárny a při dimenzování jejích konstrukcí a systémů deterministicky uváženy pády letadel, od malého sportovního letadla až po vojenské a velké dopravní letadlo v důsledku sabotáže. Pro stávající elektrárny se pád letadla (pokud nebyl uvažován v původním projektu) považuje za nadprojektovou událost, pro kterou se přijímají rozumně realizovatelná opatření pro zmírnění následků takové události.

Obecný bezpečnostní cíl je takový, že pád letadla nezpůsobí závažné důsledky pro obyvatelstvo a životní prostředí. Bezpečnostní systémy a další potřebné prostředky musí být schopny aktivace a musí vykonávat své funkce s dostatečnou spolehlivostí tak, aby jaderné zařízení dosáhlo stabilizovaného bezpečného stavu.
Zvláště musí být zajištěno:

- řízení reaktivity včetně rychlého odstavení reaktoru,
- chlazení aktivní zóny a vyhořelého paliva v bazénu (i dlouhodobě), takovým způsobem, aby se zabránilo tavení paliva,
- udržení integrity ochranné obálky (kterou se rozumí zachování bezpečnostních funkcí ochranné obálky).

Při hodnocení následků pádu letadla musí být zváženy okamžité i následné vlivy a následky pádu letadla. Mezi tyto vlivy patří:

- vliv rázu na mechanickou odolnost konstrukcí (přímý ráz a odpadlé části)
- vliv vibrací na konstrukce a bezpečnostní systémy a zařízení
- vliv hoření a nebo exploze paliva z letadla na integritu konstrukcí a na ventilační systémy (tlaky a teploty).

Požáry, způsobené palivem z letadla musí být hodnoceny jako různé typy ohnivých koulí v kombinaci s hořením v rozlivu. K hodnocení nadprojektových událostí může být použit realistický přístup, který nepředpokládá další postulované poruchy. Analýzy mohou vyhodnocovat odolnost zařízení vůči jednotlivým typům zatížení podle obecných zátěžových křivek formou citlivostní analýzy, zaměřené na hledání zlomových bodů charakteristik odolnosti. Vliv události na činnosti obsluhy a dalších pracovníků elektrárny musí být uvažován.

(7.19) Elektrárna by měla být projektována tak, aby bylo možné její spolehlivé a bezpečné odstavení a dochlazení i při maximálním výpočtovém zemětřesení s pravděpodobností vzniku pro danou lokalitu menší než $1x10^{-4}$ za rok, minimálně však v souladu s bezpečnostním návodem MAAE NS-G-3.3, s horizontální složkou zrychlení 0,1 g. Pro lokalitu s vyšší hodnotou intenzity maximálního výpočtového zemětřesení musí být vhodnou metodou prokázáno, že takovéto zemětřesení nebude mít významné následky.

(7.20) Dodržení bezpečnostních cílů musí být v případě vnitřních a vnějších vlivů zabezpečeno při splnění následujících podmínek:

- Výskyt události se předpokládá při nejnepříznivějších provozních podmínkách.

- Projekt musí uvážit primární (např. porušení bariéry) i sekundární (např. vibrace, vyvolané požáry nebo exploze) účinky události.
- Je-li pravděpodobnost vzniku náhodné události nižší než 1.10^{-7} za rok, nevyžaduje se kromě organizačních opatření realizace specifických technických opatření.
- Uvedené pravděpodobnostní vylučovací kritérium není možné použít v případě úmyslného zásahu, způsobeného lidskou činností.
- Realizace specifických technických opatření není též potřebná v případě, když jsou účinky události obálkově překryté některou z vnitřních iniciačních událostí.
- Když je míra rizika velkého úniku radionuklidů větší než 1.10^{-7} za rok, je potřebné v projektu elektrárny realizovat technická opatření pro zvýšení spolehlivosti bezpečnostních systémů, které mají za cíl odvrátit významné úniky radioaktivních látek do okolí elektrárny; těmito opatřeními jsou obvykle účinné bariéry proti poškození zařízení nebo fyzické oddělení zálohujících se (redundantních) větví bezpečnostních systémů.
- Pro projektové nehody se požaduje dosažení bezpečného odstaveného stavu za předpokladu jednoduché poruchy v bezpečnostních systémech (podle okolností též společně s předpokladem údržby jedné větve bezpečnostních systémů) podobně, jako je to předpokládáno pro vnitřní iniciační události.
- Uvedené požadavky a předpoklady mohou být zmírněny v případě vysoce nepravděpodobných událostí, tj. událostí, jejichž frekvence výskytu odpovídá frekvenci výskytu nadprojektových nehod (viz odst. 8.1) .

Sabotáž

(7.21) Pro nové jaderné elektrárny musí být projektem zabezpečena zvýšená odolnost pro případ sabotáže, stanovené projektovou hrozbou (týká se diverzních akcií s využitím výbušnin, pozemních i leteckých transportních prostředků, vnitřních i vnějších narušitelů) vyváženým použitím technických řešení i fyzické ochrany. Použitelná technická řešení jsou např. fyzické oddělení, zálohování, zodolnění, ochranné překrytí, použití nouzové dozorny, apod.

(7.22) V případě stávajících elektráren je potřebné přijmout taková režimová opatření, která minimalizují pravděpodobnost úspěšnosti diverzních akcií anebo zajistí zmírnění jejich následků.

(7.23) Postupy pro projektování zvýšené odolnosti pro případ sabotáže by měly vycházet z následujících zásad:

- Projekt by měl vycházet ze souboru obálkových parametrů reprezentujících nejtěžší zátěžové podmínky způsobené sabotáží, jak jsou náraz, výbuch, teplo/oheň, vibrace.
- Měla by být identifikována všechna zařízení důležitá pro bezpečnost, která mohou v případě napadení přímo anebo nepřímo vest k nepřijatelným radiologickým následkům. Jako ochranná opatření by měly být uvažovány fyzické oddělení a zálohování.
- Projekt by měl zabezpečit, aby v případě sabotáže zůstal vždy provozuschopný minimálně jeden kanál bezpečnostních systémů.
- Jako speciální případ by se měla uvažovat opatření pro zabránění důsledkům napadení počítačových systémů elektrárny, včetně detekce napadení, protiopatření v

případě napadení a zmírnění následků.

- Nouzová dozorna by měla být umístěna s dostatečným oddělením od hlavní blokové dozorny tak, aby žádný jednotlivý akt sabotáže nemohl způsobit jejich současné vyřazení. K nouzové dozorně by měly ze stejných důvodů existovat dvě nezávislé přístupové cesty.
- Vstup do nouzové dozorny by měl být střežen a přísně řízen. Systém fyzické ochrany by měl být vyprojektován tak, aby žádný jednotlivec neměl neřízený a nekontrolovaný přístup ke všem odděleným bezpečnostním zálohujícím se systémům.

Kombinace událostí

(7.24) V projektu elektrárny musí být uváženy kombinace zátěží od vnitřních iniciačních událostí i vnějších vlivů, pokud nebudou souběhy těchto události vysoce nepravděpodobné. Tyto kombinace událostí mohou být vybrány na základě inženýrského posouzení a pravděpodobnostními metodami.

Posuzování základů projektu

(7.25) Projektová východiska musí být pravidelně prověřována a aktualizována během celého života elektrárny tak, aby odrážely provozní zkušenosti a byla v souladu s nejnovějším stavem poznání v příslušných oblastech souvisejících s bezpečností. Toto prověřování by mělo zahrnovat kombinaci deterministických a pravděpodobnostních bezpečnostních analýz z cílem identifikovat možnosti dalšího zdokonalení projektu. Vhodnou příležitostí je např. periodické hodnocení bezpečnosti anebo příprava dokumentace žádosti o povolení provozu při prodloužení doby provozu elektrárny. Pokud ze závěrů hodnocení vyplyne potřeba modifikací elektrárny, realizace těchto modifikací se může uskutečnit i pouze v míře rozumně dosažitelné s uvážením ekonomické náročnosti a společenské přijatelnosti, po předchozím projednání a odsouhlasení programu realizace opatření Státním úřadem pro jadernou bezpečnost.

8. KATEGORIZACE UDÁLOSTÍ A KRITÉRIA PŘIJATELNOSTI

Kategorizace událostí podle frekvence výskytu

(8.1) Stavy elektrárny jsou obvykle rozděleny do omezeného počtu kategorií podle četnosti jejich výskytu. V souladu s bezpečnostními standardy MAAE je typické rozdělení iniciačních událostí do následujících čtyř kategorií:

a) abnormální provoz (očekávané provozní události s frekvencí výskytu větší než 10^{-2}/rok) je definován jako očekávané odchylky od normálního provozu JE, vyvolané nesprávnou činností systémů nebo chybami obsluhy. Tyto události by neměly mít vážné bezpečnostní následky, které by po odstranění příčin události znemožňovaly pokračování v provozu;

b) projektové nehody, které jsou definovány jako výjimečné odchylky od normálního provozu způsobené samostatnou poruchou, jejichž výskyt je možný, ale málo pravděpodobný a které jsou uvažovány v projektu JE. Projektové nehody mají mít četnost výskytu menší než 10^{-2} /rok, a existují skupiny iniciačních událostí, které jsou tradičně uvažovány jako projektové nehody přesto, že jejich četnost výskytu může být menší než 10^{-5}/rok. Při projektových nehodách může být poškození JE takového rozsahu, že rychlé uvedení do provozu po odstranění prvotní příčiny události není možné. Poškození aktivní zóny a jaderné elektrárny a uvolnění radioaktivních látek do okolí nesmí překročit stanovená projektová kritéria pro projektové nehody;

c) nadprojektové nehody, které jsou způsobeny vícenásobným selháním (zařízení, obsluhy, bezpečnostních systémů) nad rámec projektových nehod. Výskyt nadprojektových nehod je nepravděpodobný (četnost výskytu je menší než 10^{-4}/rok) a jejich radiologické následky mají být udrženy v rámci odpovídajících projektových kritérií a pod stanovenými limity;

d) těžké havárie jako podskupina nadprojektových nehod, které by měly mít extrémně nízkou četnost výskytu. Mohly by být způsobeny vícenásobným selháním zařízení, obsluhy, bezpečnostních systémů v takovém rozsahu, že vedou k rozsáhlému poškození aktivní zóny s tavením paliva. Poškození paliva a radiologické následky jsou takové, že si mohou vyžádat uplatnění ochranných opatření na ochranu obyvatelstva.

(8.2) Pro každou z uvedených kategorií musí být projektem definovány specifické deterministické bezpečnostní cíle nebo kritéria přijatelnosti a metody průkazu splnění těchto cílů, často specificky pro různé iniciační události a průběhy scénářů. Časté iniciační události smí mít pouze minimální nebo žádné radiologické důsledky, události s pravděpodobně vážnými následky musí být prakticky vyloučeny. Např. v případě abnormálního provozu (po očekávaných provozních událostech) se pro zabezpečení integrity pokrytí palivových elementů se požaduje vyloučení vzniku krize varu na povrchu kteréhokoliv elementu v aktivní zóně, v případě projektových nehod se méně přísně připouští porušení omezeného počtu palivových elementů.

Deterministické bezpečnostní cíle a kritéria přijatelnosti

(8.3) V souladu s deterministickým přístupem k projektu musí být pro všechny stavy elektrárny (normální a abnormální provoz, jakož i pro havarijní podmínky) stanoveny kvantitativní radiologické a další technické bezpečnostní cíle, odstupňované tak, že čím je vyšší četnost výskytu dané situace, tím jsou požadavky na její bezpečné zvládnutí přísnější. Události s vyšší frekvencí výskytu musí mít zanedbatelné nebo velmi malé radiační účinky.

(8.4) Pro normální a abnormální provoz musí tyto cíle zajistit shodu se závaznými dávkovými limity pro pracovníky a obyvatelstvo, stanovenými v příslušných předpisech. Pro havarijní podmínky včetně těžkých havárií musí být tyto cíle stanoveny tak, aby nebylo potřebné ani v blízkém okolí elektrárny přijímat rozsáhlejší neodkladná ani dlouhodobá opatření na ochranu obyvatelstva v rámci havarijního plánu a také aby byl omezen ekonomický dopad havárie v okolí elektrárny. Radiologické důsledky událostí souboru nadprojektových nehod včetně těžkých havárií musí splňovat obecné limity nebo alespoň limity pro ochranná opatření v souladu s požadavky zvláštních právních předpisů.

(8.5) Pro konkrétní typy reaktorů musí být v návaznosti na stanovené radiologické bezpečnostní cíle určeny odvozené technické bezpečnostní cíle tak, aby se při jejich dodržení zajistilo splnění základních bezpečnostních funkcí a zachovala integrita bariér proti únikům radioaktivních látek. Takovéto technické bezpečnostní cíle (projektová kritéria) jsou zaměřeny na zachování integrity jaderného paliva, pokrytí palivových elementů, tlakové hranice primárního a bezpečnostně důležité části sekundárního okruhu a ochranné obálky (kontejnmentu).

(8.6) Nejdůležitější bezpečnostní cíle jsou určeny jako kritéria přijatelnosti pro bezpečnostní analýzy, specificky stanovená pro jednotlivé kategorie iniciačních událostí. Kritéria jsou zpravidla různá v závislosti na frekvenci výskytu dané iniciační události, přísnější kritéria jsou stanovena pro události s vyšší četností výskytu. Kritéria přijatelnosti jsou stanovena projektantem jaderné elektrárny a musí být potvrzena SÚJB v rámci schvalování bezpečnostní dokumentace. Kritéria musí být stanovena tak, aby byla zajištěna dostatečná bezpečnostní rezerva mezi kritériem přijatelnosti a bezpečnostním limitem pro porušení bariéry proti úniku radioaktivního materiálu. Při stanovení kritérií přijatelnosti v závislosti na konkrétním projektovém řešení jsou používány následující skupiny a příklady projektových kritérií:

- Kritéria pro zajištění celistvosti (integrity) jaderného paliva: maximální teplota paliva, maximální radiálně středovaná entalpie paliva (obě hodnoty v závislosti na vyhoření a na konkrétním izotopickém složení palivové matrice - obsahu příměsí),
- Kritéria pro zajištění celistvosti (integrity) pokrytí palivových elementů: minimální rezerva do krize varu, maximální teplota povlaku, maximální lokální oxidace povlaku,
- Kritéria pro zajištění celistvosti (integrity) aktivní zóny jako celku: dostatečná podkritičnost, maximální celková tvorba vodíku z oxidace materiálů v aktivní zóně, maximální počet porušených palivových elementů v zóně, maximální deformace palivových souborů (geometrie umožňující chlazení, zavedení regulačních orgánů a demontáž),
- Kritéria pro zajištění celistvosti (integrity) primárního okruhu: maximální tlak a maximální-minimální teplota chladiva, tlakové a teplotní změny a vyvolaná napětí v tlakové hranici primárního okruhu,
- Kritéria pro zajištění celistvosti (integrity) bezpečnostně významné části sekundárního okruhu: maximální tlaky, maximální teploty medií, tlakové a teplotní změny v zařízeních sekundárního okruhu,

- Kritéria pro zajištění celistvosti (integrity) ochranné obálky (kontejnmentu) a limitování úniků do okolí: maximální a minimální tlak, maximální teplota, velikost úniků, koncentrace hořlavých/výbušných plynů, vyhovující prostředí pro požadovanou činnost systémů; obzvláště v případě ochranné obálky je potřebné odlišit kriteria pro projektové a pro nadprojektové události.

(8.7) Pro iniciační události vznikající v průběhu provozních stavu s odstaveným reaktorem případně pro události v bazénu vyhořeného paliva, při kterých je některá z bariér proti úniku radioaktivity nefunkční, je účelné projektová kritéria dále zpřísnit, např. požadavkem na vyloučení varu chladiva v reaktorové nádobě anebo v bazénu skladování paliva, případně požadavkem na zabránění odhalení palivových souborů.

Pravděpodobnostní bezpečnostní cíle

(8.8) Pro každý projekt jaderné elektrárny musí být zpracovány analýzy pravděpodobnosti vzniku těžké havárie, vyjádřené četností vzniku poškození palivového systému (PSA úrovně 1) a analýzy pravděpodobnosti vzniku radiační havárie, vyjádřené četností časného velkého úniku radioaktivních látek z ochranné obálky jaderné elektrárny (PSA úrovně 2), které musí být využívány při kontrole vyváženosti a slabých míst projektu jaderné elektrárny a jeho změn. Cílem pravděpodobnostního hodnocení bezpečnosti je prokázat, že projekt elektrárny splňuje vyváženým způsobem současné národní a mezinárodní požadavky na bezpečnost jaderných elektráren. Pro tento účel jsou definovány následující pravděpodobnostní bezpečnostní cíle:

a) střední hodnota roční četnosti výskytu (sumární frekvence) závažného (nadprojektového) poškození aktivní zóny (CDF) nesmí být pro jednotlivý blok větší než $1x10^{-5}$/rok (pro stávající bloky $1x10^{-4}$/rok) při uvážení výkonových provozních stavů jakož i režimů při odstaveném reaktoru, vnitřních iniciačních událostí, vnitřních rizik a rizik, vyplývajících z odpojení od vnější sítě. V přiměřeném rozsahu by měl být hodnoce i příspěvek vnějších vlivů (rizik) k celkovému riziku;

b) sumární frekvence časného velkého úniku radionuklidů (LERF) nesmí být větší než $1x10^{-6}$/rok (pro stávající bloky $1x10^{-5}$/rok); sumární frekvence událostí, které by mohly vést buď k časnému poškození ochranné obálky a anebo k velkému časnému úniku radionuklidů s závažnými a neodvratitelnými radiologickými důsledky, musí být prakticky vyloučeny.

Pokud stávající JE bezpečnostní cíle nesplňují, musí být vypracován a SÚJB odsouhlasen program pro jejich dosažení.

(8.9) Uvedené pravděpodobnostní bezpečnostní cíle jsou ve shodě se současnými mezinárodními doporučeními, publikovanými v příslušných dokumentech Mezinárodní agentury pro atomovou energii (MAAE, NS-G-1.2; INSAG 12). Metodika, která bude použita pro pravděpodobnostní hodnocení musí být v souladu s mezinárodně akceptovatelnými postupy. Na porovnání s pravděpodobnostními bezpečnostními cíli se použijí střední hodnoty výsledků pravděpodobnostního hodnocení bezpečnosti. Pravděpodobnostní hodnocení bezpečnosti se musí v průběhu projektování i během provozu jaderné elektrárny aktualizovat.

Metodika pravděpodobnostního hodnocení rizika je podrobněji popsána v návodu SÚJB - Pravděpodobnostní hodnocení bezpečnosti.

9. DETERMINISTICKÉ PRŮKAZY BEZPEČNOSTI PROJEKTU A BEZPEČNOSTNÍCH REZERV

Obecné požadavky na deterministické analýzy bezpečnosti

(9.1) Bezpečnost jaderné elektrárny (dodržení kritérií přijatelnosti anebo bezpečnostních cílů) musí být prokázána provedením deterministických bezpečnostních analýz pro celé spektrum postulovaných iniciačních událostí, včetně analýz komplexních událostí, vedoucích k nadprojektovým a těžkým havárií. Cílem analýz je použitím předepsaných postupů prokázat s dostatečnou rezervou, že v průběhu procesu po postulované iniciační událostí nedojde k narušení deterministických bezpečnostních cílů (kritérií přijatelnosti) ani při uplatnění obvyklé míry konzervativnosti výpočtu.

(9.2) Při deterministických bezpečnostních analýzách musí být přednostně použity realistické (best estimate) výpočetní prostředky (kódy - včetně kódů pro těžké havárie), které musí být dokumentovaným způsobem verifikovány a validovány s cílem prokázat jejich vhodnost a vyhovující přesnost pro danou oblast použití. Používané kódy musí odpovídat dosažené úrovni poznání v příslušné oblasti. Postupy SÚJB pro hodnocení výpočtových kódů jsou popsány v interní směrnici SÚJB VDS 030.

(9.3) Pokud rozdílně od předchozího doporučení bude pro analýzy použit konzervativní kód, potom taková analýza musí být doplněna vhodnými citlivostními výpočty anebo podpůrnou analýzou pomocí realistického výpočtového kódu, s cílem prokázat, že nejsou zanedbány, nebo silně zkresleny některé důležité bezpečnostní aspekty analyzovaného procesu.

(9.4) Pro zabezpečení dostatečných bezpečnostních rezerv mohou být realistické výpočtové kódy použity buď v kombinaci s vhodnou volbou konzervativních vstupních údajů nebo v kombinaci s realistickými vstupními údaji, avšak s kvantitativním vyhodnocením neurčitostí výpočtu. Možnost použití realistických vstupních údajů se však nevztahuje na předpoklady o provozuschopnosti systémů elektrárny, pro které musí být v každém případě použity konzervativní předpoklady (viz 9.12). Kvantifikace neurčitostí je důležitá především v případech, když neurčitosti mají významný dopad na přijetí závěrů z výpočtových analýz.

(9.5) Bezpečnostní analýzy použité v bezpečnostní dokumentaci musí podléhat programu zajištění jakosti a musí být v přiměřeném rozsahu nezávisle ověřeny. To je důležité především pro nové JE s inovativními projektovými řešeními.

Analýzy projektových událostí (událostí abnormálního provozu a projektových nehod)

(9.6) Dodržení bezpečnostních cílů musí být v případě projektových událostí prokázáno při splnění následujících pravidel:

(9.7) Konzervativizmus výpočtových analýz při použití realistických kódů může být zabezpečen volbou vstupních údajů, okrajových a počátečních podmínek (včetně respektování

možných nepřesností v nastavení parametrů) a přijímáním dodatečných omezujících předpokladů (např. aplikací kritéria jednoduché poruchy). Vstupní údaje jsou v tomto případě voleny takovým způsobem, aby průběh procesu byl co nejnepříznivější s ohledem na dosahované hodnoty limitujících parametrů.

(9.8) Pro každou analyzovanou iniciační událost musí být stanoveno, která kritéria přijatelnosti jsou relevantní a které fyzikální parametry jsou limitující. Výběr konzervativních počátečních a okrajových podmínek musí být samostatně proveden pro každé relevantní kritérium přijatelnosti. Pokud je pro uvažovaný typ události při ověřování různých kritérií přijatelnosti možná nejednoznačná volba počátečních a okrajových podmínek (přičemž není zřejmý jejich dopad), musí být provedeny citlivostní výpočty s cílem ocenit vliv dané volby. Z provedených citlivostních výpočtů musí být zřejmé, že použitá konzervativní volba počátečních a okrajových podmínek je postačující k tomu, aby zaručila konzervativnost výsledků analýz i s uvážením neurčitosti výpočtových modelů i kódu jako celku. Vzhledem k obtížnosti tohoto úkolu se doporučuje, aby přinejmenším v případech s malými bezpečnostními rezervami byla použita analýza nejlepšího odhadu spojená s kvantitativním vyhodnocením neurčitosti.

(9.9) Počáteční a okrajové podmínky musí být stanoveny konzervativním způsobem s výjimkou případu, když je analýza nejlepšího odhadu spojena s vyhodnocením neurčitostí. Konzervativní volba počátečních a okrajových podmínek se uplatňuje nejen v analýzách neutronových a tepelně-hydraulických procesů, ale i v strukturálních a radiologických analýzách (ve stanovení zdrojového členu, transportu radionuklidů i jejich zdravotních účinků) aspektů.

(9.10) Při bezpečnostních analýzách událostí abnormálního provozu a projektových nehod se musí vycházet z toho, že ke zvládnutí analyzované projektové události, tj. k převedení reaktoru do stabilizovaného stavu, mohou být použity pouze bezpečnostní systémy, zařazené do bezpečnostních tříd 1. a 2. a jejich podpůrné systémy v souladu s požadavky zvláštního předpisu (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd), tedy se zaručenou spolehlivostí. Parametry charakterizující výkonnost bezpečnostních systémů musí být zvoleny konzervativně z hlediska daného kritéria přijatelnosti. Funkce nekvalifikovaných aktivních systémů se při zvládání události abnormálního provozu a projektových nehod mohou a musí uvážit pouze tehdy, jestliže zhorší průběh projektové události. To znamená, že v průběhu zvládání události abnormálního provozu a projektové nehody se funkce aktivních systémů, neklasifikovaných jako vybraná zařízení bezpečnostní třídy 1 a 2 neuvažují, nebo se uvažuje jejich působení před vznikem a v průběhu události způsobem, který je pro zvládnutí události nejméně příznivý.

(9.11) Ve všech bezpečnostních analýzách iniciačních událostí abnormálního provozu a projektových nehod musí být uplatněno kritérium jednoduché poruchy. Výskyt nejzávažnější jednoduché poruchy a všech dalších jí způsobených poruch resp. v důsledku postulovanou iniciační událostí vzniklých poruch se musí uvažovat pro kteroukoliv z komponent zajišťujících potřebné bezpečnostní funkce, a to buď v okamžiku vzniku iniciační události, nebo později, v nejméně příhodném okamžiku a při nejméně příhodné konfiguraci zařízení, realizujícího bezpečnostní funkce. Není však nutné uvažovat poruchy pasivních komponent, pokud lze důvodně považovat jejich výskyt za velmi nepravděpodobný a lze předpokládat jejich neovlivnění analyzovanou iniciační událostí.

(9.12) Pro každý systém používaný pro zajištění bezpečnostních funkcí musí být uvažována nejzávažnější jednoduchá porucha; vznik poruchy současně v několika systémech se neuvažuje. V analýze musí být uváženy všechny následné poruchy, vznikající v důsledku iniciační události anebo v důsledku nejzávažnější jednoduché poruchy.

(9.13) Pro průběh událostí abnormálního provozu jakož i pro projektové nehody musí být tam, kde to má významný vliv na plnění kritérií přijatelnosti, jako další zhoršující porucha uvažováno zaseknutí jedné řídící komponenty aktivní zóny (jako přídavné zhoršující poruchy) s nejvyšší efektivností v horkém bezvýkonovém stavu, za účelem zjištění dostatečnosti rezervy na odstavení reaktoru. Konzervativnost analýzy zavádění (záporné) reaktivity při rychlém odstavení reaktoru je třeba dále zvýšit užitím konzervativního časového zpoždění pádu řídících komponent a konzervativní závislosti zaváděné reaktivity na polohách tyčí. Zaseknutí řídící komponenty může být v analýzách projektových nehod bráno jako jednoduchá porucha, představuje-li samo o sobě nejzávažnější jednoduchou poruchu.

(9.14) Pro projektové nehody musí být jako další konzervativní porucha uvažována ztráta pracovních a záložních zdrojů elektrického napájení v časovém okamžiku s nejnepříznivějším vlivem na průběh a následky nehody, pokud ztráta napájení není uvažována jako následná porucha (např. v důsledku rozpadu vnější sítě).

(9.14a) Události abnormálního provozu by (s výjimkou zásahu systému rychlého odstavení reaktoru v některých případech) neměly vést k zapracování bezpečnostních systémů určených pro ochranu v případě projektových nehod. Proto se doporučuje nad rámec výše popsaných konzervativních analýz prokázat, že správná funkce systémů kontroly a řízení je schopna zabránit inicializaci bezpečnostních systémů.

Analýzy nadprojektových nehod (včetně těžkých havárií)

(9.15) V analýzách přijatelnosti projektových řešení pro zvládání nadprojektových nehod se pomocí výpočtových analýz prokazuje splnění stanovených kritérií přijatelnosti, které mají obvykle formu mezí kvantitativních anebo kvalitativních teplotechnických parametrů, mechanických zatížení anebo radiologických následků. Výsledky výpočtu by zejména měly umožnit vyhodnocení indukovaného poškození chladícího okruhu reaktoru (reaktorové nádoby anebo parogenerátoru), zatížení ochranné obálky, systémů ochranné obálky a možné ztráty integrity ochranné obálky, zdrojového členu v ochranné obálce a zdrojového členu do okolí, pracovních podmínek pro přístrojové vybavení a pro zařízení důležitá pro odvod tepla a pracovních podmínek pro činnost obsluhy.

(9.16) Požadavek na použití validovaných kódů se v maximálně možném rozsahu uplatňuje i pro bezpečnostní analýzy nadprojektových nehod a těžkých havárií. Je však potřebné vzít v úvahu, že stupeň validace u kódů pro těžké havárie je obvykle menší, než v případě kódu pro projektové nehody a rigorózní statistické hodnocení neurčitosti výsledků výpočtu je zatím ve fázi výzkumu a vývoje. Obvykle je taktéž pro komplexní analýzy nutno použít několik specifických navzájem navazujících kódů. Požaduje se, aby jako součást analýz byly též vykonány analýzy strukturální odezvy zařízení s cílem určit schopnost konstrukčních materiálů zvládnout mechanická zatížení.

(9.17) Analýzy nadprojektových nehod se provádí realistickými výpočty vzhledem k tomu, že je důležité získat co nejlepší přiblížení skutečné odezvě elektrárny. Mohou být použity realistické předpoklady o konfiguraci a chování zařízení a zmírněná kritéria přijatelnosti oproti analýzám projektových nehod. V analýzách však musí být použity nejméně příznivé možné počáteční podmínky.

(9.18) Potenciálně větší neurčitost výsledků analýz z důvodu neurčitostí v modelech, počátečních a okrajových podmínkách je nutno respektovat použitím dostatečných rezerv při využití výsledků pro stanovení časového vývoje havárie a velikosti jejích následků. Vzhledem k obtížnosti kvantifikace neurčitostí se doporučuje získat doplňující informace pomocí citlivostních analýz.

(9.19) Z hlediska předpokladů o provozuschopnosti zařízení a systémů elektrárny je možné v analýzách předpokládat činnost všech systémů kromě těch, jejichž selhání vedlo k analyzované nadprojektové nehodě anebo těžké havárii a těch, které podle realistického odhadu mohou být poškozeny v důsledku analyzované události. Pro nové JE by v souladu s principy nezávislosti jednotlivých úrovní hloubkové ochrany měla být prokázána možnost zvládnutí těžkých havárií jen použitím specifických systémů určených pro zvládání těchto havárií. Při analýzách není nutné aplikovat kritérium jednoduché poruchy pro bezpečnostní systémy.

10. ZAJIŠTĚNÍ BEZPEČNOSTNÍCH FUNKCÍ

Obecné požadavky na zajištění bezpečnostních funkcí

(10.1) Základní bezpečnostní funkce jsou zpravidla rozděleny do určitého počtu odvozených bezpečnostních funkcí. Zařízení důležitá z hlediska jaderné bezpečnosti (potřebná pro splnění každé bezpečnostní funkce) musí být identifikována a systematicky zařazena do bezpečnostních tříd podle jejich významu pro plnění bezpečnostních funkcí způsobem stanoveným zvláštním právním předpisem (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd). Musí být stanoveny specifikace, podle kterých budou tato vybraná zařízení navržena, vyrobena, smontována a provozována tak, aby jejich jakost a spolehlivost stále odpovídala této klasifikaci. Klasifikace zařízení podle zvláštního právního předpisu musí být prováděna a ověřována deterministickými metodami, doplněnými kde je třeba, technickým posouzením a pravděpodobnostními metodami. Pro každou bezpečnostní třídu se musí stanovit:

a) odpovídající pravidla a specifikace pro návrh, výrobu, montáž a kontroly,

b) požadavky na záložní elektrické napájení a kvalifikaci na podmínky prostředí; pro zařízení určená ke zvládání těžkých havárií musí být prokázána jejich schopnost splnit požadované funkce i při podmínkách těžkých havárií,

c) stavy pohotovosti a nepohotovosti systémů při postulovaných iniciačních událostech, uplatněné v deterministických bezpečnostních analýzách,

d) požadavky na spolehlivost,

e) další opatření pro zajištění jakosti v souladu s požadavky zvláštního právního předpisu (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd).

f) Specificky mohou být definovány požadavky na zařízení a systémy, určené pro zvládání těžkých havárií.

(10.2) V projektu systémů a komponent důležitých pro jadernou bezpečnost musí být uplatněn princip bezpečné poruchy, zajišťující, aby při poruše, nebo při vzniku podmínek, znemožňujících řádné provádění bezpečnostní funkce systému přešel do bezpečného stavu, nebo do jiného stavu, jehož přijatelnost je zdůvodněna a prokázána analýzou..

(10.3) V souladu s principy ochrany do hloubky musí být opatření a systémy použité na různých úrovních ochrany do hloubky v maximální možné míře nezávislé. Především musí být zabezpečeno, aby porucha systému, určeného pro normální provoz, neovlivnila plnění bezpečnostních funkcí.

(10.4) Pro zabezpečení bezpečnostních funkcí mohou být použity automaticky řízená aktivní nebo pasivní zařízení nebo systémy s tím, že v obou případech musí být spolehlivost systémů kvantifikovatelná. Při použití pasivních systémů musí být věnována pozornost otázkám jejich bezpečnostní klasifikace, uplatnění kritéria jednoduché poruchy, spolehlivosti a testovatelnosti systémů.

(10.5) Projekt musí zohlednit problematiku lidského faktoru a rozhraní člověk - stroj v souladu s ergonomickými principy. Projekt musí podporovat úspěšnou činnost operátora z hlediska dostupného času, očekávaného pracovního prostředí a psychologického tlaku. Projekt musí zohlednit skutečnost, že spolehlivost zásahu operátora je možné zajistit jen tehdy, pokud má operátor dostatek času na zjištění změny stavu zařízení, na rozhodnutí a na provedení zásahu, pokud má potřebné informace, tyto informace jsou jednoznačné a pokud pracovní prostředí po události je přijatelné.

(10.6) S výjimkou případů, kdy je nesprávný zásah operátora příčinou iniciační události se musí předpokládat, že operátor v průběhu prvních 30 minut (resp. 60 minut, když se jedná o zásah mimo blokovou dozornu) nevykoná žádné zásahy. V případě jasné a spolehlivé indikace v analýze bezpečnosti je možné předpokládat, že reakční doba na indikaci pro zásah operátora může být kratší, ale musí být alespoň 15 minut. Při zvládání těžkých havárií je možné činnost operátora hodnotit realistickým způsobem; přesto se však doporučuje předpokládat správnou činnost operátora v čase ne kratším než 30 minut po zjištění symptomu (indikace) pro stanovení zásahu, pokud se činnost uskutečňuje na hlavní blokové dozorně a v čase ne kratším jako 1 hodina pro činnost mimo dozorny. Kromě toho se předpokládá, že operátor má k dispozici adekvátní provozní předpisy a návody a že je pro použití těchto předpisů náležitě vyškolen.

(10.7) Systémy, konstrukce a komponenty (dále jen „zařízení“) důležité pro jadernou bezpečnost a radiační ochranu musí zajišťovat jejich spolehlivou funkci při normálním a abnormálním provozu a v havarijních podmínkách a schopnost omezovat důsledky poruch a nehod v souladu s projektem. Mezní podmínky, pro něž bude zařízení projektováno, musí odpovídat nehodám, zahrnutým do projektových východisek.

(10.8) Zařízení důležitá pro jadernou bezpečnost musí být navrhována tak, aby umožňovala provádět za provozu kontrolu stavu a zkoušky jejich funkčních schopností a spolehlivosti metodami, odpovídajícími současnému stavu vědy a techniky. Technické řešení těchto zařízení musí obsahovat opatření, kompenzující výskyt nezjištěných poškození za provozu jaderné elektrárny a po postulovaných iniciačních událostech (např. zvýšení bezpečnostních rezerv, výpočtové zdůvodnění, nepřímé metody kontroly).

(10.9) Musí se předpokládat možnost výskytu jednoduchých poruch i vícenásobných poruch ze společné příčiny. Pro dosažení požadované spolehlivosti provedení bezpečnostních funkcí musí být použito dostatečné zálohování relevantních zařízení s použitím buď identických nebo různých komponent. Potenciální příčiny poruch se společnou příčinou, které mohou vést k současnému selhání většího počtu komponent, musí být důkladně analyzovány a jejich vznik minimalizován použitím principů diverzity, nezávislosti a funkčního a fyzického oddělení.

(10.10) Použité řešení musí zabezpečit odolnost vůči jednoduché poruše i při splnění požadavků na údržbu elektrárny při provozu na výkonu v souladu s limitami a podmínkami bezpečného provozu. Jedním z přijatelných technických řešení je použití tzv. kritéria N+2 (uvažování jednoduché poruchy současně s údržbou na jedné větvi bezpečnostního systému). Jinak může být ošetřen požadavek zálohování pro pasivní systémy, na které mohou být nižší

nároky na zálohování než na aktivní systémy. Výše uvedené požadavky na odolnost vůči jednoduché poruše se netýkají zařízení pro zvládání nadprojektových nehod.

(10.11) Systémy, konstrukce a komponenty, které vykonávají bezpečnostní funkce musí být na očekávané pracovní podmínky kvalifikovány. Požadavky na kvalifikaci komponent a systémů na souběh různých zatížení, obvyklé pro projektové události, nemusí být u systémů určených výhradně pro zvládání těžkých havárií vzhledem k jejich extrémně nízké pravděpodobnosti splněny ve stejném rozsahu. Ze stejného důvodu také mohou být zmírněny požadavky na zálohování systémů (včetně systémů pro zásobování energiemi) a jejich seizmickou odolnost. Musí však být prokázána schopnost zařízení vykonávat vyžadované činnosti a schopnost zařízení vykonávat bezpečnostní funkci i za podmínek těžké havárie.

(10.12) Musí být respektována zásada, že pokud plnění bezpečnostních funkcí vyžaduje funkčnost nějakého systému, je zároveň vyžadována funkčnost jeho příslušných podpůrných systémů (zabezpečujících např. energie, média, mazání, apod.). Funkčnost takovýchto systémů musí být zachována při všech projektem uvažovaných iniciačních událostech.

(10.13) Konstrukce zařízení, včetně volby použitých materiálů musí být provedena tak, aby byly požadované bezpečnostní charakteristiky zachovány po celou dobu životnosti elektrárny s respektováním všech efektů stárnutí zařízení.

Funkce odstavení reaktoru

(10.14) Reaktor musí být vybaven systémy pro řízení reaktivity a odstavení reaktoru, které jsou schopny jej odstavit za normálního a abnormálního provozu a za havarijních podmínek projektových nehod. Musí jej udržet odstavený i za situace, způsobující nejvyšší reaktivitu aktivní zóny. Účinnost, rychlost a rezerva na odstavení musí zaručovat, že stanovené projektové limity nebudou překročeny.

(10.15) Prostředky pro odstavení reaktoru musí tvořit nejméně dva diverzní systémy. Mimořádná pozornost musí být věnována vyloučení možnosti selhání v důsledku poruchy se společnou příčinou v případě, že oba diverzní systémy používají číslicovou technologii.

(10.16) Nejméně jeden ze těchto dvou systémů musí být sám o sobě schopen rychle uvést reaktor z provozních stavů i v průběhu projektových nehod do podkritického stavu s dostatečnou rezervou podkritičnosti, i za předpokladu jednoduché poruchy. Výjimečně je možné akceptovat krátkodobou opětovnou kritičnost reaktoru za podmínky, že nebudou narušeny projektové limity pro palivo a jiné komponenty.

Funkce odvodu tepla

(10.17) Reaktor musí být vybaven technologickými soubory a zařízeními pro odvod tepla uvolněného štěpením a zbytkového a provozního tepla v podmínkách normálního a abnormálního provozu a v havarijních podmínkách.

(10.18) Tyto technologické soubory a zařízení musí za normálního a abnormálního provozu a havarijních podmínek, zahrnutých do projektových východisek, spolehlivě zajišťovat odpovídající chlazení reaktoru, skladů vyhořelého jaderného paliva a ostatních zařízení tak, aby systémy, zajišťující ochranu do hloubky byly funkční, a aby projektové limity zařízení nebyly překročeny. Dále musí být schopny dlouhodobě rozptylovat uvolňované teplo do okolního prostředí, aniž by došlo k nežádoucímu šíření radioaktivity.

(10.19) Systémy odvodu tepla, která jsou vybranými zařízeními podle zvláštního právního předpisu (Vyhláška č. 132/2008 Sb. o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd), se musí v potřebné míře zálohovat, fyzicky oddělovat a současně i vzájemně propojit tak, aby plnily svoji funkci i při jednoduché poruše. Odvod tepla, zprostředkovaný těmito systémy, musí být zajištěn i při ztrátě některého ze zdrojů elektrického napájení minimálně po dobu, nutnou pro zvládnutí projektových nehod. Systém odvodu tepla musí být dimenzován i na úplné prasknutí největšího potrubí v chladicím systému reaktoru.

(10.20) Jaderná elektrárna musí mít zajištěny dostatečně funkčně nezávislé systémy odvodu tepla, umožňující zvládání nejpravděpodobnějších nadprojektových nehod včetně těžkých havárií i v případě ztráty bezpečnostních systémů v důsledku poruch o společné příčině..

Funkce ochranné obálky

(10.21) Jaderná elektrárna musí mít systém ochranné obálky, který zahrnuje:

- hermetické konstrukce obklopující všechny komponenty primárního okruhu,
- přidružené systémy řízení tlaku a teplot v systému ochranné obálky,
- prostředky pro izolaci ochranné obálky,
- prostředky pro kontrolu a řízení složení směsi vzduchu, vodní páry , štěpných produktů, a ostatních plynných a aerosolových složek, které by mohly být uvolněny do atmosféry v ochranné obálce.
- prostředky pro průběžné monitorování a řízenou filtraci úniků z hermetické obálky.

(10.22) Systém ochranné obálky musí být schopen zachycovat a filtrovat úniky z ochranné obálky při projektových nehodách, a prakticky vyloučit nepřijatelné důsledky nadprojektových nehod, spojené s poškozením a tavením paliva, úniky radionuklidů a jimi uvolňovaného ionizujícího záření.

(10.23) Systémy ochranné obálky nově budovaných jaderných elektráren by měly být tvořeny primární a sekundární ochrannou obálkou (kontejnmentem) takovým způsobem, aby sekundární obálka překrývala úplně nebo částečně primární obálku, aby se zabezpečilo zadržení, filtrování a řízené vypouštění podstatné části radioaktivních látek, které by mohly potenciálně unikat z primární obálky. Za sekundární obálku mohou být považovány též všechny konstrukce, které umožňují zachycení úniků z primární obálky, jejich řízené filtrování do okolí a výsledné snížení množství radioaktivních látek uvolněných do životního prostředí.

(10.24) Primární obálka musí být s dostatečnou rezervou dimenzována na všechny projektové nehody včetně úplného prasknutí největšího potrubí v chladicím systému reaktoru. Sekundární obálka musí být schopna zvládnout výše specifikované vnější vlivy a ohrožení.

(10.25) Důležitá zařízení systému ochranné obálky musí být zálohována a napájena tak, aby mohla pracovat při napájení z elektrizační soustavy nebo při nouzovém napájení z vlastních zdrojů jaderné elektrárny spolehlivě i při jednoduché poruše na zařízení. Požadavek na zálohování při uplatnění kritéria jednoduché poruchy se netýká zařízení speciálně určených pro zvládání nadprojektových nehod, především těžkých havárií.

(10.26) Systém ochranné obálky musí zabezpečit, že únik radioaktivních látek do okolí bude nižší než stanovené limity, zajišťující nejnižší dosažitelné hodnoty dávek ionizujícího záření.

(10.27) Projektová technická a administrativní opatření musí prakticky vyloučit možnost přímého uvolnění radioaktivních látek do okolí elektrárny obtokem ochranné obálky. Tato opatření musí mimo jiné uvážit možnost přímého uvolnění radioaktivních látek prostřednictvím úniku z primární do sekundární strany parogenerátorů, včetně poškození trubkovnice parogenerátorů při vysoké teplotě, vznikající v průběhu těžkých havárií.

(10.28) Každé potrubí, které prochází stěnou ochranné obálky a je součástí tlakové hranice primárního okruhu, nebo je přímo propojeno do atmosféry ochranné obálky, musí být automaticky a spolehlivě uzavíratelné při projektových nehodách. Tato potrubí musí být vybavena nejméně dvěma uzávěry (oddělovacími armaturami) zapojenými v sérii, které se umísťují vně a uvnitř hermetické obálky a jsou nezávisle a spolehlivě ovladatelné. Vnější oddělovací armatury musí být umístěny tak blízko ke hranici ochranné obálky, jak je to jen prakticky možné.

(10.29) Každé potrubí, které prochází stěnou ochranné obálky a není součástí tlakové hranice primárního okruhu, a ani není přímo propojeno do atmosféry ochranné obálky, musí být opatřeno nejméně jedním odpovídajícím oddělovacím uzávěrem. Tento uzávěr musí být umístěn vně ochranné obálky a tak blízko jeho stěně, jak je to jen prakticky možné.

(10.30) Funkci oddělovací uzávěrů podle odst. 10.29 a 10.30 musí zajišťovat buď automaticky řízený uzavírací prvek, nebo manuálně uzavíratelný, případně zajistitelný uzavírací prvek, nebo uzavírací prvek dálkově ručně ovládaný. Za přijatelný uzavírací prvek se nepovažuje zpětná klapka.

(10.31) Integrita a v potřebném rozsahu i těsnost ochranné obálky musí být zaručena po dobu trvání havarijních podmínek (včetně těžkých havárií) a dostatečně dlouhou dobu po jejich ukončení, po vzniku těžké havárie minimálně po dobu potřebnou k realizaci opatření na ochranu obyvatelstva. Pro nové elektrárny musí být respektování všech těchto požadavků součástí projektu a jejich splnění musí být prokázáno v bezpečnostní dokumentaci. Pro existující JE je potřebné stanovit potřebnou míru implementace v rozumně dosažitelné míře a stanovit individuální časový harmonogram implementace pro konkrétní blok, ale zásadně tak, aby výsledkem implementace bylo faktické zvýšení odolnosti elektrárny i proti nadprojektovým nehodám včetně těžkých havárií.

(10.32) Jmenovitě musí být použita následující opatření:

- Musí být zajištěno zachování funkčnosti izolačních zařízení, průchodek a průlezů pro obsluhu v průběhu havarijních podmínek včetně těžkých havárií. Musí být zabezpečené monitorování a podstatné omezení úniků z primárního ochranné obálky netěsnostmi.
- Systém odvodu tepla z ochranné obálky musí být navržen tak, aby fungoval v průběhu havarijních podmínek včetně těžkých havárií.
- Musí být použita opatření a technické prostředky pro omezení koncentrace výbušných plynů, produktů štěpení a jiných radionuklidů, uvolněných v průběhu těžkých havárií do atmosféry ochranné obálky.
- Integrita ochranné obálky musí být zabezpečena v průběhu těžkých havárií i za předpokladu možného vznícení hořlavých plynů. Musí být zajištěná prevence

prostorového výbuchu vodíku, avšak integrita ochranné obálky musí být zajištěna i s uvážením potenciální místní exploze hořlavých plynů. V projektu musí být respektovány účinky hoření vodíku v realistické kombinaci se všemi ostatními zátěžemi.

- Musí být k dispozici technická a organizační opatření pro zabránění přetlakování ochranné obálky nebo proti nepřijatelně nízkému tlaku v ochranné obálky. Jako ochrana proti přetlakování ochranné obálky je přípustné použití filtrované ventilace, která však nesmí být použita v časné fázi havárie.
- Musí být použity technické prostředky a organizační opatření pro zabránění tavení aktivní zóny při vysokém tlaku v primárním okruhu tak, aby mohla být s vysokou pravděpodobností vyloučena možnost protavení reaktorové nádoby s vypuzením taveniny do ochranné obálky při vysokém tlaku.
- Musí být použity technické prostředky a organizační opatření pro zabránění protavení tlakové hranice ochranné obálky. Za tímto účelem musí být vyhodnocena možnost a v souladu s tímto vyhodnocením přijata opatření pro uchlazení trosek roztavené zóny buď uvnitř nádoby reaktoru nebo mimo ní uvnitř ochranné obálky.

11. MĚŘÍCÍ, INFORMAČNÍ, ŘÍDÍCÍ A OCHRANNÉ SYSTÉMY

Měřící systémy

(11.1) Jaderná elektrárna musí mít nainstalovány měřící systémy pro měření všech hlavních parametrů, které mohou ovlivňovat štěpný proces, integritu aktivní zóny reaktoru, systému chlazení reaktoru a ochranné obálky, a pro získání všech informací o elektrárně, potřebných pro její spolehlivý a bezpečný provoz. Musí být zavedena opatření pro automatický záznam měření všech odvozených parametrů důležitých pro jadernou bezpečnost. Měřící systémy musí být schopny zabezpečit rychlou, jednoduchou a dostatečně přesnou detekci poruch a identifikaci jejich příčin.

(11.2) Měřící systémy musí být postačující pro měření parametrů elektrárny a musí být kvalifikovány na prostředí odpovídající příslušným provozním stavům a havarijním podmínkám elektrárny. Pokud odpovídající přístrojové vybavení není kvalifikováno na pracovní podmínky nadprojektových a těžkých havárií, musí se vzít v úvahu, že informace z přístrojů mohou být nepřesné anebo nespolehlivé. Pro tyto případy musí být k dispozici alternativní metody pro získání potřebné informace a rovněž návody pro další postup i bez těchto informací.

Bloková dozorna

(11.3) Elektrárna musí být vybavena blokovou dozornou pro bezpečné řízení bloku ve všech stavech normálního a abnormálního provozu a pro realizaci opatření k udržení elektrárny v bezpečném stabilizovaném stavu nebo její navrácení do tohoto stavu po vzniku předpokládaných provozních událostí, projektových i nadprojektových nehod. Bloková dozorna musí umožňovat ruční ovládání elektrárny ve všech režimech provozu elektrárny na výkonu.

(11.4) Všechny potřebné informace, obzvlášť symptomy používané pro zvládání abnormálních stavů a havarijních podmínek (včetně těžkých havárií) musí být zabezpečeny přístrojovým vybavením elektrárny a musí být v přiměřeném rozsahu k dispozici na všech místech, kde jsou dělána příslušná rozhodnutí ohledně dalšího postupu při zvládání havarijních podmínek (např. hlavní bloková dozorna, nouzová dozorna, technické podpůrné středisko).

(11.5) Tyto informace z přístrojů musí být zobrazeny a musí s nimi být spojeny výstrahy takovým způsobem, aby bylo umožněno včasné vyhodnocení stavu všech kritických bezpečnostních funkcí, a to i v podmínkách těžkých havárií.

(11.6) Bloková dozorna musí být vybavena zařízením, které efektivním způsobem generujuje vizuální a případně i zvukové výstrahy, informující o existenci odchylek od normálního provozu, ovlivňujících bezpečnost. V projektu dozorny musí být uplatněny ergonomické faktory. Operátorovi musí být k dispozici odpovídající informace pro sledování výsledků automatických zásahů.

(11.7) Zvláštní pozornost musí být věnována stanovení těch událostí vnitřních a vnějších z hlediska blokové dozorny, které by mohly ohrozit její běžný provoz, a projektem musí být zajištěna opatření pro minimalizaci vlivu takovýchto událostí na provoz dozorny.

(11.8) U všech zásahů obsluhy, vyžadovaných pro zvládání havarijních podmínek, musí být prokázána jejich proveditelnost při předpokládaných radiačních dávkách a negativních vlivech, vyvolaných havarijními podmínkami včetně těžkých havárií, případně musí být pro obsluhu zabezpečena potřebná ochranná opatření.

(11.9) Projekt ventilačního systému musí vzít v úvahu možné vnitřní i vnější zdroje radioaktivních látek a toxických plynů, které by mohly ohrozit činnosti obsluhy; dozorna musí mít k dispozici zařízení pro detekci a filtraci, případně musí být pro obsluhu zabezpečena potřebná ochranná opatření.

(11.10) Pro dobu, kdy hlavní bloková dozorna není k dispozici, musí být na jiném místě (pomocné dozorně), fyzicky a elektricky odděleném od blokové dozorny, zajištěn přístup k sestavě měřících a řídících zařízení, dostatečné pro odstavení reaktoru a jeho udržování v odstaveném stavu, k odvádění zbytkového tepla a k monitorování důležitých parametrů elektrárny.

Ochranné systémy

(11.11) **Jaderné elektrárny** musí být vybaveny ochrannými systémy, které musí být:

- schopny rozeznávat podmínky abnormálního provozu a automaticky uvést do chodu a vypnout a odpojit nebo připojit podle potřeby příslušné systémy, včetně výkonného bezpečnostního systému pro odstavení reaktoru tak, aby bylo zajištěno, že projektová kritéria pro abnormální provoz nebudou překročena,
- schopny rozeznávat havarijní podmínky a uvést do chodu příslušné výkonné bezpečnostní systémy, určené ke zmírnění následků těchto podmínek,

Míra zálohování a nezávislosti uplatněná v projektu ochranných systémů musí postačovat přinejmenším pro zajištění takové spolehlivosti, že:

- žádná jednoduchá porucha nepovede ke ztrátě bezpečnostní funkce,
- vyřazení jakékoliv komponenty nebo kanálu bezpečnostního systému z provozu nepovede ke ztrátě minimálního nezbytného stupně zálohování (redundance),
- je minimalizováno možné ohrožení spuštění funkcí bezpečnostních systémů i pro případ předem neidentifikovatelných poruch ze společné příčiny v ochranných systémech , jako jsou chyby v programech, poruchy čidel aj.

(11.12) Projekt musí umožnit, aby všechny prvky zajišťující funkci ochranných systémů, od senzoru po vstupní signály ovládaných výkonných komponent, byly testovatelné za provozu. Každá případná výjimka z plnění tohoto ustanovení musí být náležitě zdůvodněna.

(11.13) Projekt ochranných systémů reaktoru musí minimalizovat pravděpodobnost, že by zásahy obsluhy mohly znehodnotit účinnost ochranných systémů; přitom musí být ochranným systémem zajištěny prostředky pro záložní ruční spuštění automaticky iniciovaných ochranných zásahů z provozní dozorny i záložního zařízení (nouzové dozorny). Ochranný

systém reaktoru ovšem nesmí bránit správným zásahům obsluhy, pokud jsou tyto v havarijních podmínkách nezbytné.

(11.14) Digitální systémy, užívané v ochranných systémech, musí splňovat požadavky odpovídajících současných standardů v rámci systému jakosti podle Atomového zákona a vyhlášky 132/2008 Sb. s tím, že :

- je použit hardware a software s prokázanou kvalitou, vyvinutý ověřenými postupy,
- celý proces vývoje hardware a software, včetně řízení změn projektu, jim příslušných zkoušek a uvádění upravených systémů do provozu (verifikace, validace a testování) , je systematicky dokumentován a kontrolován,
- pro potvrzení důvěry ve spolehlivost digitálních systémů musí být provedeno hodnocení všech fází vývojového a výrobního cyklu digitálních systémů odborníky, nezávislými na projektantovi a dodavatelích,
- kde nelze při projektování s ohledem na koncepci projektu jaderné elektrárny demonstrovat nezbytnou integritu systému, a zvláště odolnost proti poruchám o společné příčině a proti šíření poruch, na vysoké úrovni důvěryhodnosti, musí být již ve fázi návrhu implementovány principiálně odlišné (diverzní) prostředky pro iniciaci bezpečnostních funkcí.

Nouzové elektrické napájení

(11.15) Nouzové napájecí zdroje a příslušná rozvodná zařízení musí zabezpečit napájení systémů a komponent důležitých z hlediska bezpečnosti potřebným výkonem ve všech provozních stavech, jakož i při projektových nehodách i za předpokladu jednoduché poruchy a současné ztráty vnějšího elektrického napájení. V případě nových jaderných elektráren musí mít systémy určené pro zvládání těžkých havárií zabezpečeno napájení z nezávislého nouzového zdroje, u kterého se však uplatnění předpokladu jednoduché poruchy nevyžaduje.

12. ZÁVĚR

(12.1) Návod uvedený v tomto dokumentu rozšiřuje požadavky návodu BN –JB 1.0 , zaměřeného na požadavky na jaderná zařízení a doplňuje výklad některých ustanovení vyhlášky 195/1999 Sb. především v oblasti doporučení k provádění deterministických bezpečnostních analýz o podrobnější výklad aplikace těchto dokumentů na připravovanou výstavbu nových jaderných zdrojů.

13. REFERENCE

[1] SMĚRNICE RADY 2009/71/EURATOM ze dne 25. června 2009, kterou se stanoví Rámec Společenství pro jadernou bezpečnost jaderných zařízení.

[2] Úmluva o jaderné bezpečnosti (INCIFIR/449, 5.7.1994, sdělení MZV č. 67/1998 Sb.).

[3] Zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů.

[4] Vyhláška SÚJB č. 106/1998 Sb., o zajištění jaderné bezpečnosti a radiační ochrany jaderných zařízení při jejich uvádění do provozu a provozu.

[5] Vyhláška SÚJB č. 195/1999 Sb., o požadavcích na jaderná zařízení k zajištění jaderné bezpečnosti, radiační ochrany a havarijní připravenosti.

[6] Vyhláška SÚJB č. 132/2008 Sb., o systému jakosti při provádění a zajišťování činností souvisejících s využíváním jaderné energie a radiačních činností a o zabezpečování jakosti vybraných zařízení s ohledem na jejich zařazení do bezpečnostních tříd.

[7] Reactor Safety Reference Levels, WENRA, 2008.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles: Safety Fundamentals, IAEA Safety Standards Series No. SF-1, IAEA, Vienna, 2006.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standard Series, Periodic Safety Review of Nuclear Power Plants, Safety Guide No. NS-G-2.10, IAEA, Vienna, 2003.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY IAEA, Ageing Management for Nuclear Power Plants, Safety Guide No. NS-G-2.12, IAEA, Vienna 2009.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants**:** Design Safety Requirements, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna, 2000.

[12] Návod SÚJB BN-JB-1.6 /2010 - Pravděpodobnostní hodnocení bezpečnosti

14. PŘÍLOHA 1 – SROVNÁNÍ S REFERENČNÍMI ÚROVNĚMI

WENRA Reactor Safety Reference Levels – oblast E

WENRA Reactor Safety Reference Levels Oblast E Design basis Envelope for Existing Reactors	**PROVÁDĚCÍ ODSTAVCE TOHOTO NÁVODU**
1. Objective	
1.1 The design basis shall have as an objective the prevention or, if this fails, the mitigation of consequences resulting from anticipated operational occurrences and design basis accident conditions. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed prescribed limits and are as low as reasonably achievable.	2. - definice 4.3
2. Safety strategy	
2.1 Defence-in-depth shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases. The design shall therefore provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment, and an adequate protection of the barriers.	5.1
2.2 The design shall prevent as far as practicable: - challenges to the integrity of the barriers; - failure of a barrier when challenged; - failure of a barrier as consequence of failure of another barrier.	5.1 5.4
3. Safety functions	
3.1 The plant shall be able to fulfil the following fundamental safety functions: - control of reactivity, - removal of heat from the core and - confinement of radioactive material,	6.1
4. Establishment of the design basis	
4.1 The design basis shall specify the capabilities of the plant to cope with a specified range of plant states within the defined radiation protection requirements. Therefore, the design basis shall include the specification for normal operation and transients/accident conditions from Postulated Initiating Events (PIEs), the safety classification, important assumptions and, in some cases, the particular methods of analysis.	7.1 7.3
4.2 A list of PIEs shall be established to cover all events that could affect the safety of the plant. From this list, a set of design basis events shall be selected with deterministic or probabilistic methods or a combination of both, and used to set the boundary conditions according to which the structures, systems and components important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished and the safety objectives met.	7.4
4.3 The design basis shall be systematically defined and documented to reflect the actual plant.	7.4
5. Set of design basis events	
5.1 Internal events such as loss of coolant accidents, equipment failures, maloperation and hazards, and their consequential events, shall be taken into account in the design of the plant. The list of events shall be plant specific. (see Appendix for assessment of implementation)	7.3 7.8

	App. 2A
5.2 The following types of natural and man made external events shall as a minimum be taken into account in the design of the plant according to site specific conditions: - extreme wind loading - extreme outside temperatures - extreme rainfall, snow conditions and site flooding - extreme cooling water temperatures and icing - earthquake - airplane crash - other nearby transportation, industrial activities and site area conditions which reasonably can cause fires, explosions or other threats to the safety of the nuclear power plant	7.17
6. Combination of events	
6.1 Credible combinations of individual events, including internal and external hazards, that could lead to anticipated operational occurrences or design basis accident conditions, shall be considered in the design. Engineering judgement and probabilistic methods can be used for the selection of the event combinations.	7.23
7. Definition and application of technical acceptance criteria	
7.1 Initiating events shall be grouped into a limited number of categories that correspond to plant states, according to their probability of occurrence. Radiological and technical acceptance criteria shall be assigned to each plant state such that frequent initiating events shall have only minor or no radiological consequences and that events that may result in severe consequences shall be of very low probability.	8.1 8.3
7.2 Criteria for protection of the fuel rod integrity, including fuel temperature, DNB, and cladding temperature, shall be specified. In addition, criteria shall be specified for the maximum allowable fuel damage during any design basis event.	8.6
7.3 Criteria for the protection of the (primary) coolant pressure boundary shall be specified, including maximum pressure, maximum temperature, thermal- and pressure transients and stresses.	8.6
7.4 If applicable, criteria in 7.3 shall be specified as well for protection of the secondary coolant system.	8.6
8. Demonstration o reasonable conservatism and safety margins	
8.1 The initial and boundary conditions shall be specified with conservatism	9.1
8.2 The worst single failure shall be assumed in the analyses of design basis events. However, it is not necessary to assume the failure of a passive component, provided it is justified that a failure of that component is very unlikely and it remains unaffected by the PIE.	9.10
8.3 Only safety systems shall be credited to carry out a safety function. Non-safety systems shall be assumed to operate only if they aggravate the effect of the initiating event	9.12
8.4 A stuck control rod shall be considered as an additional aggravating failure in the analysis of design basis events.	9.13
8.5 The safety systems shall be assumed to operate at their performance level that is most penalising for the initiator.	9.12
8.6 Any failure, occurring as a consequence of a postulated initiating event, shall be regarded to be part of the original PIE.	9.10
8.7 The impact of uncertainties, which in specific cases are of importance for the results, shall be addressed in the analysis of design basis events.	9.8 , 9.9
9. Design of safety functions	
General	

9.1 The fail-safe principle shall be considered in the design of systems and components important to safety.	10.3
9.2 A failure in a system intended for normal operation shall not affect a safety function.	10.4
9.3 Activations and manoeuvring of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes after the initiating event. Any operator actions required by the design within 30 minutes after the initiating event shall be justified.	10.7
9.4 The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, physical and functional separation and isolation.	10.10
Reactor shutdown functions	
9.5 The means for shutting down the reactor shall consist of at least two diverse systems.	10.16
9.6 At least one of the two systems shall, on its own, be capable of quickly rendering the nuclear reactor sub critical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure.	10.17
Heat removal functions	
9.7 Means for removing residual heat from the core after shutdown, and during and after anticipated operational occurrences and accident conditions, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.	10.18 , 10.20
Confinement functions	
9.8 A containment system shall be provided in order to ensure that any release of radioactive material to the environment in a design basis accident would be below prescribed limits. This system shall include: - leaktight structures covering all essential parts of the primary system; - associated systems for control of pressures and temperatures; - features for isolation; - features for the management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.	10.22
9.9 Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident. These lines shall be fitted with at least two containment isolation valves arranged in series. Isolation valves shall be located as close to the containment as is practicable.	10.29
9.10 Each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve. This valve shall be outside the containment and located as close to the containment as practicable.	10.30
10. Instrumentation and control systems	
10.1 Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information on the plant necessary for its reliable and safe operation. Provision shall be made for automatic recording[26] of measurements of any derived parameters that are important to safety.	11.1
10.2 Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.	11.2
Control room	
10.3 A control room shall be provided from which the plant can be safely operated in all its operational states, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences and design basis accidents.	11.3

10.4 Devices shall be provided to give in an efficient way visual and, if appropriate also audible indications of operational states and processes that have deviated from normal and could affect safety. Ergonomic factors shall be taken into account in the design of the control room. Appropriate information shall be available to the operator to monitor the effects of the automatic actions.	11.6
10.5 Special attention shall be given to identifying those events, both internal and external to the control room, which may pose a direct threat to its continued operation, and the design shall provide for reasonably practicable measures to minimize the effects of such events.	11.7
10.6 For times when the main control room is not available, there shall be sufficient instrumentation and control equipment available, at a single location that is physically and electrically separated from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant parameters can be monitored.	11.10
Protection system	
10.7 Redundancy and independence designed into the protection system shall be sufficient at least to ensure that: - no single failure results in loss of protection function; and - the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.	11.11
10.8 The design shall permit all aspects of functionality of the protection system, from the sensor to the input signal to the final actuator, to be tested in operation. Exceptions shall be justified.	11.12
10.9 The design of the reactor protection system shall minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operation and anticipated operational occurrences. Furthermore, the reactor protection system shall not prevent operators from taking correct actions if necessary in design basis accidents.	11.13
10.10 Computer based systems used in a protection system, shall fulfil the following requirements: - the highest quality of and best practices for hardware and software shall be used; - the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewed; - in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and - where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.	11.14
Emergency power	
10.11 It shall be ensured that the emergency power supply is able to supply the necessary power to systems and components important to safety, in any operational state or in a design basis accident, on the assumption of a single failure and the coincidental loss of off-site power.	11.15
11. Review of the design basis	
11.1 The actual design basis shall regularly[27], and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach to identify needs and opportunities for improvement. Reasonably practicable measures shall be taken with respect to backfitting or other measures justified from a safety point of view.	7.25
Appendix	7.17

WENRA Reactor Safety Reference Levels – oblast F

WENRA Reactor Safety Reference Levels Oblast F Design Extension of Existing Reactors	**PROVÁDĚCÍ ODSTAVCE TOHOTO NÁVODU**
1. Objective	
1.1 The design extension analysis shall examine the performance of the plant in specified accidents beyond the design basis, including selected severe accidents, in order to minimise as far as reasonably practicable radioactive releases harmful to the public and the environment in cases of events with very low probability of occurrence.	7.10
2. Selection and analysis of Beyond Design Basis Events	
2.1 Beyond design basis events shall be selected and considered in the safety analysis to determine those sequences for which reasonable practicable preventive or mitigative measures can be identified and implemented (see Appendix for assessment of implementation).	7.10
2.2 Realistic assumptions and modified acceptance criteria may be used for the analysis of the beyond design basis events.	9.17
3. **Instrumentation for the management of beyond design basis accident conditions**	
3.1 Adequate instrumentation shall exist which can be used in severe accident environmental conditions in order to manage such accidents according to guidelines/procedures for severe accidents.	11.2
3.2 Necessary information from instruments shall be relayed to the control room as well as to a separately located supplementary control room/post and be presented in such a way to enable a timely assessment of the plant status and critical safety functions in severe accident conditions.	11.4 , 11.5
4. Protection of the containment against selected beyond design basis accidents	
4.1 Isolation of the containment shall be possible in a beyond design basis accident. However, if an event leads to bypass of the containment, consequences shall be mitigated.	10.33
4.2 The leaktightness of the containment shall not degrade significantly for a reasonable time after a severe accident.	10.32
4.3 Pressure and temperature in the containment shall be managed in a severe accident.	10.33
4.4 Combustible gases shall be managed in a severe accident.	10.33
4.5 The containment shall be protected from overpressure in a severe accident.	10.33
4.6 High pressure core melt scenarios shall be prevented.	10.33
4.7 Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.	10.33
Appendix	

15. PŘÍLOHA 2 - Typický seznam postulovaných iniciačních událostí, charakteristických pro jaderné elektrárny s tlakovodním reaktorem

A Jednoduché postulované iniciační události

Iniciační události pro provoz reaktoru na výkonu

1 Zvýšení odvodu tepla sekundárním okruhem

1.1 Porucha v systému napájecí vody, která snižuje teplotu napájecí vody

1.2 Porucha v systému napájecí vody, která zvyšuje průtok napájecí vody

1.3 Porucha regulace tlaku v sekundárním okruhu, která vede k zvýšení průtoku páry z parogenerátorů

1.4 Chybné otevření pojišťovacích ventilů parogenerátoru anebo hlavního parovodu, přepouštěcí stanice do atmosféry, anebo přepouštěcí stanice do kondenzátoru

1.5 Spektrum prasknutí parních potrubí uvnitř nebo vně ochranné obálky

2 Snížení odvodu tepla sekundárním okruhem

2.1 Porucha nebo zásah, vedoucí ke snížení průtoku páry z parogenerátorů

2.2 Poruchy vedoucí ke snížení průtoku nebo zvýšení teploty napájecí vody

2.3 Ztráta vnějšího elektrického zatížení

2.4 Zavření rychlozávěrných ventilů turbíny

2.5 Uzavření armatur na parovodech

2.6 Ztráta vakua v kondenzátoru

2.7 Výpadek hlavních napájecích čerpadel

2.8 Ztráta vnitřních a vnějších zdrojů elektrického napájení

2.9 Prasknutí potrubí napájecí vody

3 Snížení průtoku primárního chladiva

3.1 Chybné uzavření jedné hlavní uzavírací armatury v cirkulační smyčce

3.2 Zablokování rotoru jednoho hlavního cirkulačního čerpadla

3.3 Zlomení hřídele na jednom hlavním cirkulačním čerpadle

3.4 Různé kombinace výpadků hlavních cirkulačních čerpadel

4 Poruchy reaktivity a změny rozložení výkonu

4.1 Nekontrolované vytažení skupiny řídících komponent při spouštění

4.2 Nekontrolované vytažení skupiny řídících komponent na výkonu

4.3 Neřízený pohyb řídících komponent

- pád jedné řídící komponenty do aktivní zóny

- vytažení jedné řídící komponenty

- odlišná poloha jedné řídící komponenty

4.4 Chybné připojení odstavené cirkulační smyčky

4.5 Vystřelení řídící komponenty z aktivní zóny

4.6 Snižování koncentrace bóru v primárním chladivu v důsledku chybné funkce systému doplňování a borové regulace

4.7 Chybné zavezení a provoz palivového souboru v nesprávné poloze

5 Zvýšení množství chladiva v primárním okruhu

5.1 Chybné uvedení do činnosti havarijního chlazení aktivní zóny při provozu na výkonu

5.2 Chybná činnost normálního systému doplňování, která zvyšuje množství chladiva v primárním okruhu

6 Ztráta primárního chladiva

6.1 Spektrum postulovaných prasknutí potrubí tvořících tlakový celek s primárním okruhem

6.2 Prasknutí parního potrubí mezi kompenzátorem objemu a pojistnými ventily

6.3 Chybné otevření pojistného ventilu kompenzátora objemu

6.4 Úniky z primární na sekundární stranu parogenerátoru - prasknutí trubky parogenerátoru - netěsnost primárního kolektoru až do odtržení víka kolektoru

6.5 Prasknutí impulsní trubky systému kontroly a řízení nebo jiného potrubí připojeného k primárnímu okruhu a procházejícího stěnou ochranné obálky

6.6 Chybné otevření jedné zpětné nebo uzavírací armatury oddělující primární okruh od nízkotlaké části systému

7 Úniky radioaktivity ze systémů nebo komponent

7.1 Únik nebo porucha v systému radioaktivních plynných odpadů

7.2 Únik nebo porucha v systému radioaktivních kapalných odpadů

7.3 Pád palivového souboru během výměny paliva

7.4 Pád kontejneru s čerstvým nebo vyhořelým palivem

8 Události vedoucí k zatížení ochranné obálky

8.1 Spektrum havárií s únikem primárního nebo sekundárního chladiva do ochranné obálky

9 Události způsobující tlakově-teplotní šoky

9.1 Spektrum havárií s únikem chladiva z primárního okruhu

9.2 Chybné otevření pojistného (odlehčovacího) ventilu kompenzátoru objemu

9.3 Úniky chladiva z primární do sekundární strany parogenerátoru

9.4 Nesprávné uvedení do činnosti systému havarijního doplňování chladiva do primárního okruhu

9.5 Chybná činnost normálního systému doplňování, která zvyšuje množství chladiva v primárním okruhu

9.6 Nesprávné uvedení do činnosti elektroohříváků kompenzátoru objemu

9.7 Chybné otevření pojistného ventilu parogenerátoru, přepouštěcí stanice páry do atmosféry, nebo přepouštěcí stanice do kondensátoru

9.8 Spektrum prasknutí parních potrubí uvnitř nebo vně ochranné obálky reaktoru

9.9 Prasknutí potrubí napájecí vody

9.10 Chlazení tlakové nádoby reaktoru (TNR) zvně v případě zaplavení šachty reaktoru

10 Zatížení primárního a sekundárního okruhu a jejich vnitřních částí

10.1 Namáhání vnitroreaktorových částí

Iniciační události pro nevýkonové provozní režimy

1 Události spojené se změnou reaktivity

1.1 Snižování koncentrace boru v důsledku chybné funkce systému doplňování a borové regulace

1.2 Chybné připojení odstavené cirkulační smyčky

1.3 Snižování koncentrace boru v důsledku průniku nebórované vody při promývání filtrů systému normálního doplňování a borové regulace

1.4 Snižování koncentrace boru v důsledku nebórované vody pronikající přes netěsné tepelné výměníky

2 Ztráta chladiva (nečekaná ztráta chladiva z primárního okruhu)

2.1 Únik chladiva do pomocných systémů (obtok ochranné obálky)

2.2 Únik chladiva vyvolaný operátorem (údržba, zkoušení, lidská chyba)

2.3 Únik chladiva následkem porušení těsnosti systému odvodu zbytkového tepla

3 Ztráta odvodu zbytkového tepla následkem degradace cirkulace primárního chladiva

3.1 Poddrenážování primárního okruhu

3.2 Průnik nezkondenzovatelných plynů do primárního okruhu (včetně průniku nezkondenzovatelných plynů z izolované smyčky)

3.3 Odtlakování a náhlé vychlazení s vytvořením bubliny v primárním okruhu

4 Ztráta odvodu zbytkového tepla v důsledku selhání podpůrných systémů

4.1 Ztráta elektrického napájení

4.2 Ztráta chladicí vody

5 Ztráta odvodu zbytkového tepla následkem poruch zařízení

5.1 Ztráta jednoho čerpadla nebo chybné uzavření armatury systému nízkotlakého doplňování chladiva do primárního okruhu používaného pro odvod zbytkového tepla

5.2 Neočekávané přerušení průtoku smyčkou primárního okruhu (např. uzavření hlavní uzavírací armatury)

5.3 Ztráta průtoku technologickým kondensátorem (například selhání čerpadla, uzavření armatury a pod.)

5.4 Ztráta technické vody důležité

6 Zvýšení množství chladiva v primárním okruhu

6.1 Neočekávané uvedení do činnosti havarijního chlazení zóny

6.2 Uzavření trasy odpouštění chladiva z primárního okruhu

6.3 Neočekávané připojení hydroakumulátorů k primárnímu okruhu

6.4 Zapnutí elektroohřívačů kompenzátoru objemu

6.5 Dodání energie do "tvrdého" primárního okruhu v důsledku neočekávaného spuštění hlavního cirkulačního čerpadla

7 Události v systému chlazení bazénu skladování vyhořelého jaderného paliva

7.1 Otevření drenážní linie z bazénu skladování vyhořelého paliva

7.2 Únik chladiva z bazénu skladování vyhořelého paliva

7.3 Ztráta chlazení bazénu skladování vyhořelého paliva

8 Poškození bazénu skladování vyhořelého paliva během výměny paliva

8.1 Poškození palivové kazety zavážecím strojem

8.2 Pád kazety s vyhořelým palivem do reaktoru nebo bazénu skladování vyhořelého paliva

B Nadprojektové události

Doporučený výběr typů událostí, které je minimálně třeba analyzovat pro ověření bezpečnosti projektu, nejsou-li součástí souboru událostí abnormálního provozu a projektových nehod, by měl zahrnout přinejmenším:

I. Rozvoje jednoduchých postulovaných iniciačních událostí abnormálního provozu při postulovaném selhání bezpečnostního systému rychlého odstavení reaktoru:

1. Nekontrolované vytažení skupiny regulačních orgánů
2. Úplná ztráta vnitřních a vnějších zdrojů elektrického napájení
3. Ztráta elektrického zatížení turbogenerátoru
4. Úplná ztráta napájení parogenerátorů vodou
5. Ztráta vakua v kondenzátoru
6. Neřízené otevření přepouštěcí stanice do kondenzátoru
7. Uzavření armatur hlavních parovodů

II. Další postulované nadprojektové události, které mohou vést v případě vícenásobných selhání zařízení nebo provozních pracovníků k těžké havárii:

1. Úplná dlouhodobá ztráta vnitřních a vnějších zdrojů elektrického napájení
2. Úplná dlouhodobá ztráta dodávky napájecí vody
3. Havárie se ztrátou primárního chladiva při současné ztrátě havarijního chlazení aktivní zóny reaktoru
4. Neřízený pokles hladiny nebo ztráta cirkulace v reaktoru při chlazení otevřeného reaktoru nebo při výměně paliva
5. Úplná ztráta systému chlazení komponent (vložených uzavřených chladících okruhů)
6. Ztráta systému odvodu zbytkového tepla reaktoru
7. Ztráta chlazení bazénu skladování
8. Ztráta koncového systému odvodu tepla (ze sekundárního okruhu)
9. Neřízené ředění koncentrace kyseliny borité v reaktoru (tlakovodní reaktory)
10. Vícenásobné porušení trubek parogenerátoru (tlakovodní reaktory)
11. Prasknutí parovodu spojené s prasknutím trubek parogenerátoru
12. Ztráta potřebných bezpečnostních systémů při jejich dlouhodobém využití po iniciační události.