ČESKÁ SPOLEČNOST PRO JAKOST
Novotného lávka 5, 116 68 Praha 1

SPOLEHLIVOST A ANALÝZA RIZIK

MATERIÁLY Z X. SETKÁNÍ
ODBORNÉ SKUPINY PRO SPOLEHLIVOST

Praha, březen 2003

OBSAH

PRAVDĚPODOBNOSTNÍ HODNOCENÍ RIZIKA **3**
Ing. Pavel Fuchs, CSc.

STÁTNÍ DOZOR V JADERNÉ ENERGETICE A PRAVDĚPODOBNOSTNÍ HODNOCENÍ BEZPEČNOSTI **16**
Ing. Josef Dušek, CSc.

POSTUPY PSA VYUŽÍVANÉ V ÚJV ŘEŽ **45**
RNDr. Jaroslav Holý

PRAVDĚPODOBNOSTNÍ HODNOCENÍ RIZIKA

Ing. Pavel Fuchs, CSc., Technická univerzita v Liberci

1 ÚVOD

V moderním řízení velkých průmyslových podniků se řízení rizika stává běžnou součástí managementu. Řízení rizika vychází z akceptování skutečnosti, že veškeré procesy, které probíhají v průmyslovém podniku (a nejen v průmyslovém podniku), jsou náhodného charakteru. Přes veškerou péči, kterou podnikatelský subjekt řízení průmyslového provozu věnuje, není schopen vyloučit řadu nežádoucích situací, které jeho podnikání ohrožují. Jako příklad některých situací lze uvést:

- poruchy dodavatelsko-odběratelských vztahů
- nejistota v oblasti pracovních sil (nevhodná kvalifikace, nedostatek pracovníků, nespolehlivost pracovníků - fluktuace, stávkové hnutí apod.)
- neurčitost finančních zdrojů (nesolventnost obchodních partnerů, nejistota úvěru, problémy s pojištěním apod.)
- havárie a velké poruchy na provozovaném zařízení
- průmyslové havárie u jiných subjektů
- živelné události
- politická nebo hospodářská nestabilita v regionu, kde je průmyslový provoz lokalizován

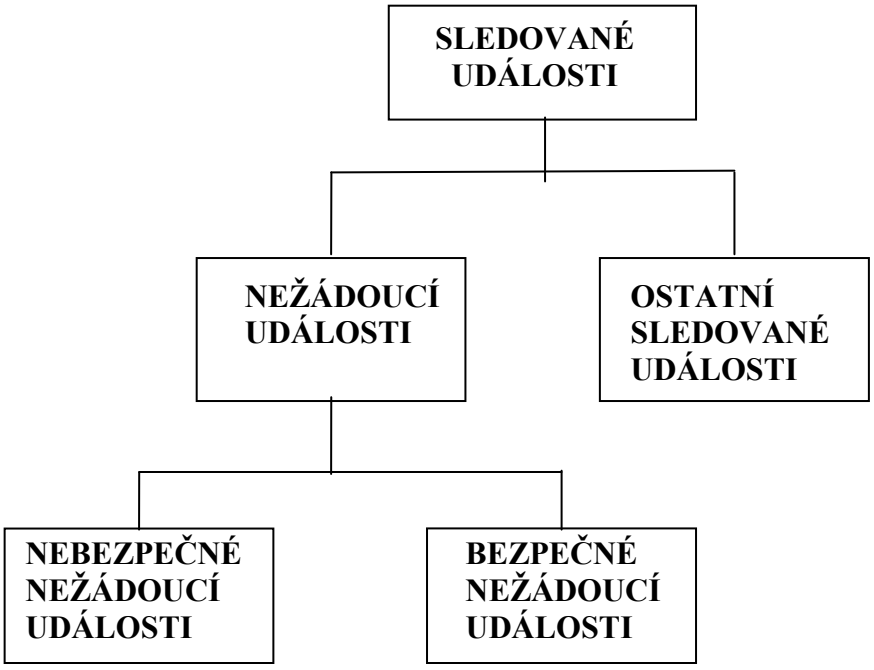
Pro uvedené situace je charakteristická náhodnost jejich vzniku a nepříznivé následky pro podnikatelský subjekt. Proto je věnována značná pozornost studiu zákonitostí těchto náhodných událostí, jejich příčinám a následkům. Cílené snižování rizika je možné jen při respektování jeho ekonomických souvislostí, je tedy třeba provádět optimalizaci nákladů na řízení rizika.

Pro průmyslové provozy připadá z celkového rizika zpravidla největší podíl na riziko spojené s vlastní výrobou. To platí zejména pro provozy hornictví a energetiky, petrochemického průmyslu a dopravy, které svým provozem zásadním způsobem ovlivňují své okolí (ekonomicky, ekologicky, bezpečnostně).

2 RIZIKO, ZÁKLADNÍ POJMY

V průmyslovém provozu se obvykle sleduje nějaká množina jevů (událostí). Pouze některé prvky množiny událostí mají charakter nežádoucích událostí. S každou nežádoucí událostí (z této množiny událostí) je spojen nějaký nepříznivý následek. K účinnému

ovlivňování spolehlivosti a bezpečnosti je třeba nejprve definovat hierarchii jevů (událostí), které lze v průmyslovém provozu očekávat. Při návrhu hierarchie struktury událostí je zásadní definice nebezpečné události. Pojem bezpečí a nebezpečí se v původním významu vztahuje pouze k životu a zdraví člověka. Z toho vychází hierarchie událostí na obr. 1 a s ní spojené definice pojmů. Hierarchie událostí je sestavena na základě členění událostí podle jejich následků.



Obr. 1: Struktura událostí průmyslového provozu - podle následků

Sledované události - z teoreticky nekonečného počtu jevů, které se u průmyslového provozu vyskytují, se sleduje omezená množina jevů (událostí). Sledují se ekonomické parametry výroby, spotřeba hmot a energií, teplofyzikální parametry výrobního procesu, havárie, poruchy, opravy apod.

Nežádoucí události - takové události, které mají nepříznivé důsledky pro průmyslový provoz a jeho okolí.

Ostatní sledované události - ostatní provozní situace, tj. zbytek množiny sledovaných událostí po vyloučení nežádoucích událostí.

Nebezpečné nežádoucí události - podmnožina nežádoucích událostí, která zahrnuje ty události, jejichž následkem je ohrožení zdraví a života člověka. Zahrnuje rovněž události s následky na životní prostředí (ekologické škody), lze-li prokázat jejich vazbu na ohrožení zdraví a života člověka.

Bezpečné nežádoucí události - zbytek množiny nežádoucích událostí po vyloučení nebezpečných nežádoucích událostí. Události, které způsobí jen hmotnou (finanční) ztrátu.

Průmyslový provoz není od svého okolí izolován, nýbrž prostřednictvím řady existujících vazeb své okolí ovlivňuje a naopak je svým okolím ovlivňován. Proto se při analýze nežádoucích událostí a jejich následků přistupuje k rozdělení příčin vzniku nežádoucích událostí na:

- nežádoucí události z vnitřních příčin průmyslového provozu
- nežádoucí události z vnějších příčin

Nežádoucí události z vnitřních příčin

Příčina těchto událostí je obsažena v průmyslovém provozu. Příkladem takovýchto příčin je:

- porucha technologického zařízení
- porucha řídicího zařízení
- porucha elektrických subsystémů průmyslového provozu
- chyba člověka
- transportní nehoda v areálu průmyslového provozu apod.

Nežádoucí události z vnějších příčin

Nežádoucí událost vzniká v průmyslovém provozu z příčin, které jsou způsobeny okolím. Jako příklad lze uvést:

- živelná událost (zemětřesení, vichr, povodeň, úder blesku, ...)
- pád letícího předmětu do areálu průmyslového provozu
- ztráta elektrického napájení z veřejné sítě
- exploze produktovodu umístěného poblíž průmyslového provozu
- extremistický čin apod.

Riziko

Terminologie spojená s řízením rizika se postupně ustálila. Počáteční problémy při používání termínu "riziko" vznikaly z toho, že slovo riziko, použité v běžné řeči, není emocionálně neutrální. Nese s sebou zápornou emoci strachu, obav a je v různých významových odstínech užíváno a překládáno. Pro potřeby analýzy rizika a řízení rizika je však nezbytné používat definovaný pojem, který lze exaktně vyjádřit.

Riziko se intuitivně chápe jako očekávání něčeho nepříznivého. Již v tomto intuitivním pojímání jsou zahrnuty dva oddělené aspekty:

- Očekávání, že dojde k výskytu nějaké nepříznivé situace, události. Událost vzniká náhodně v čase a prostoru.
- Výše újmy spojené s nepříznivou událostí. Výše újmy může být známa předem nebo je náhodného charakteru.

Z uvedeného vyplývá definice rizika formulovaná v souladu s přístupem převažujícím v současné praxi:

riziko = pravděpodobnost nežádoucí události x následek nežádoucí události

Předností této definice rizika je, že dovoluje riziko měřit a porovnávat, což je nezbytným předpokladem úspěšného řízení rizika.

3 DRUHY RIZIKA, ČÍSELNÉ HODNOTY RIZIKA

Přestože je pravděpodobnost bezrozměrnou veličinou, bývá v praxi často vztažena k některému parametru a získává tak míru. Rovněž následky lze vyčíslit různými jednotkami, viz tab. 1. Z výše uvedené definice proto vyplývá, že riziko lze udávat v různých jednotkách.

Tab. 1: Míry vztažené pravděpodobnosti a následků

Vztažená pravděpodobnost	**Následek**
rok^{-1}	hmotná škoda [Kč]
km^{-1}	okamžité úmrtí [počet]
$km^{-2}.\ rok^{-1}$	úmrtí z pozdních následků [počet]

Teoreticky lze používat značný počet různých měr rizika. Běžně se jich používá jen několik. Například riziko úmrtí z dopravních nehod na 1 km cestování dopravním prostředkem, riziko úmrtí či poškození zdraví při havárii průmyslového zařízení. Riziko, ať se uvádí v jakékoli míře, si **vždy** zachovává pravděpodobnostní charakter.

Při posuzování rizikovosti lidských aktivit vzniká otázka porovnatelnosti různých měr rizika. Pro praktické použití se riziko zpravidla hodnotí prostřednictvím ekonomické ztráty nebo poškození lidského zdraví, užívají se tedy dvě základní míry rizika - finanční a zdravotní. Blíže lze tyto dvě míry rizika ilustrovat na příkladu chemického provozu, kde s průměrnou četností jednou za 100 let (vztažená pravděpodobnost 1.10^{-2} rok^{-1}) může dojít k nadlimitnímu úniku nebezpečných látek. Následkem úniku jsou materiální škody a poškození zdraví obyvatel, které mohou být různě velké např. v závislosti na meteorologické situaci - pro kvantifikaci rizika se průměrují. Finanční míra rizika [$Kč.rok^{-1}$] udává průměrnou výši finančních prostředků, které musí podnik kumulovat, aby byl schopen pokrýt následky havárie (včetně zdravotních). Zdravotní míra rizika (zvýšení úmrtnosti a poškození zdraví nad hodnotu z přirozených příčin) pak určuje výši rizika osob ohrožených únikem nebezpečných látek z chemického provozu nebo radioaktivních látek z jaderného zařízení. Finanční míra rizika (která v sobě obsahuje i finanční náhradu za poškození zdraví či úmrtí) představuje náklady, které je nutno zahrnout do ceny produkce (prostřednictvím nákladů na pojistné). Naproti tomu zdravotní míra rizika by měla být rozhodujícím ukazatelem pro orgány státního dozoru, které rozhodují o povolení provozu průmyslového podniku. S přihlédnutím k náhodnému charakteru vzniku havarijní situace a k reálné době existence výroby či průmyslového podniku, je pro podnik obvykle výhodné řešit kumulaci finančních prostředků prostřednictvím přiměřeného pojistného.

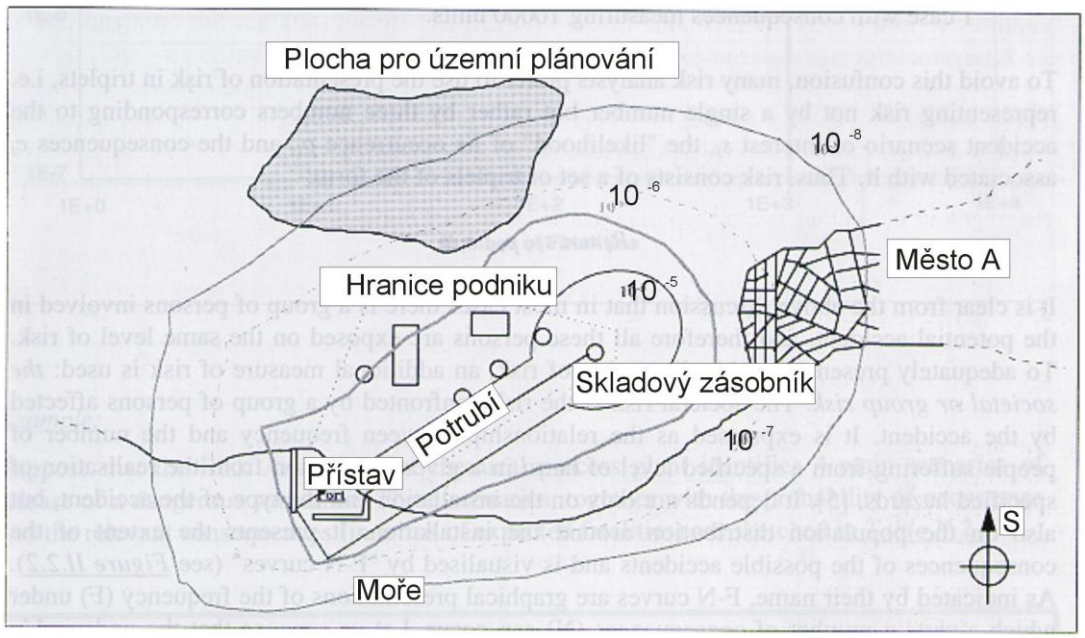
Z uvedeného příkladu je patrné, že finanční míra rizika průmyslového provozu má komplexní charakter. Pokud nelze při posuzování rizikovosti lidských aktivit v případě různých měr rizika rozhodnout, která aktivita je rizikovější, je vhodné převést hodnoty rizika na finanční vyjádření a tyto porovnat (viz pojišťovnictví).

Při používání zdravotní míry rizika je nutné rozhodnout, na koho je vztažena. Například při velké průmyslové havárii jsou jiné dopady a následky pro osoby v těsné blízkosti havárie než pro obyvatele přilehlého města nebo regionu. Riziko konkrétního jednotlivce se bude lišit podle toho, v jakém postavení (nejen topologickém) se při havárii

nachází. Riziko vztahované k jednotlivci se nazývá **individuální riziko**. Riziko vztahované ke skupině osob je **společenské riziko.**

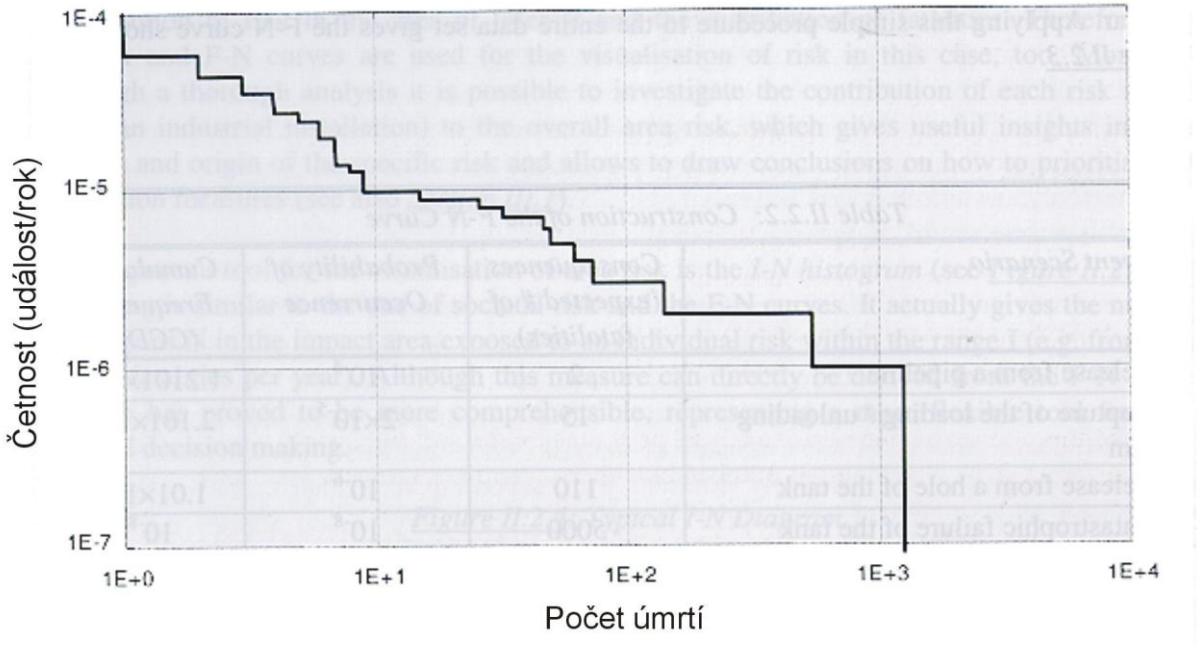
Individuální riziko poukazuje na riziko, kterému je vystavena osoba v blízkosti zdroje rizika. Tato míra zahrnuje povahu poškození osoby, pravděpodobnost, že toto poškození nastane a časové období, během kterého toto poškození může nastat. Existuje riziko individuální fatality, vztahuje-li se poškození k usmrcení osoby, individuální riziko zranění (např. popálením), jestliže jde o zranění příjemce právě takovým poškozením nebo individuální riziko ozáření nebo obdržení nebezpečné toxické dávky, jestliže se poškození vztahuje k určité expozici toxickou látkou (koncentrace toxické látky x čas).

Individuální riziko je pravděpodobnost výskytu nežádoucích následků způsobených událostí osobě nacházející se v bodě (x, y) v okolí nebezpečného zařízení. Hodnoty individuálního rizika v různých bodech dávají geografické rozdělení rizika a jsou charakteristikou oblasti okolo nebezpečného zařízení. Křivka rizika je definována jako množina bodů (x, y) okolo zařízení, kde individuální riziko má stejnou hodnotu. Na obr. 2 jsou zobrazeny typické izorizikové křivky. Tyto křivky zvané též kontury (obrysy, vrstevnice) individuálního rizika většinou závisí na samotném zařízení, jsou nezávislé na hustotě populace v okolí a poskytují představu o riziku okolo zařízení.



Obr. 2: Křivky stejných hodnot (vrstevnice) individuálního rizika

Z uvedeného vyplývá, že na dané úrovni individuálního rizika se může vyskytovat více osob zasažených případnou událostí (všechny tyto osoby jsou vystaveny téže hladině rizika). Pro přiměřenou představu tohoto rozměru rizika se používá další míra rizika - skupinové nebo společenské riziko. Společenské riziko je riziko, jemuž je vystavena skupina osob ovlivněných událostí. Je vyjádřeno jako vztah mezi frekvencí a počtem lidí, kteří v dané populaci při realizaci určitého rizika budou určitým způsobem poškozeni. Toto riziko závisí nejen na typu zařízení s nebezpečnou látkou a typu události, ale také na rozdělení populace okolo zařízení. Představuje rozsah následků možných událostí a je vizualizováno křivkami F - N (viz obr. 3).



Obr. 3: Křivka F - N

Křivky F - N představují grafický vztah frekvence události (F), při které může nastat určitý počet nežádoucích následků (N). Předpokládejme, že může nastat určitý počet následků (N) a že jako nežádoucí následky nás budou zajímat úmrtí lidí. Distribuce úmrtí (fatalit), tj. graf vyjadřující pravděpodobnost určitého počtu úmrtí, vede nejen k individuálnímu riziku, ale také ukazuje, jak mnoho lidí je vystaveno této hladině rizika. Bod na křivce F - N udává frekvenci (F) výskytu události s úmrtností vyšší než počet (N) lidí.

Významným faktorem při řízení rizika je skutečnost, zda riziko je jednotlivcem přijímáno dobrovolně nebo mu je nějakým způsobem vnuceno (nedobrovolné riziko). S tím úzce souvisí i otázka přijatelnosti a vnímání rizika.

V případě dobrovolného rizika příjemce dobrovolně vybírá svůj stupeň spoluzodpovědnosti a ohrožení vlastním rizikem. Týká se to například rizika při určitých sportovních aktivitách, rizika požívání určitých léků a podrobení se lékařským procedurám, rizika na pracovišti a rizika určitých návyků, jako je např. kouření. Spoluodpovědnost za všechny tyto činnosti byla příjemcem dobrovolně vybrána.

Rozlišení mezi dobrovolným a nedobrovolným rizikem má souvislost s přijatelností rizika. V mnoha studiích bylo popsáno, že „typický“ člověk dokáže přijmout mnohem vyšší hladiny rizika, pokud si riziko vybere sám, než když mu bylo riziko vnuceno někým jiným. Podle jedné takové studie je riziko kouření 50 000 x vyšší než riziko výroby elektrické energie v jaderné elektrárně. Přesto riziko kouření je mnohem přijatelnější, než riziko výroby elektřiny zmíněným způsobem. Toto „typické“ chování není příliš překvapivé, jelikož příjemce dobrovolného rizika se obvykle domnívá, že se mu dostávají jakoby protiúčtem některé přímé požitky z „rizikové činnosti“ a věří, že celou činnost, a tudíž případné riziko, má pod svou kontrolou.

Jak již bylo uvedeno, je riziko měřitelná veličina. I když odhad rizika poskytuje objektivní hodnoty rizika, jeho vnímání velmi závisí na subjektivních charakteristikách hodnotitele rizika. Každá osoba vnímá hladinu rizika absolutně rozdílným způsobem podle své kultury, charakteru, víry a začlenění v životě. Jinými slovy, každá osoba používá svoji „hodnotovou funkci“ k „objektivním“ mírám rizika popsaným výše a činí rozhodnutí podle této hodnotové funkce a podle vnímané hladiny rizika.

Veřejnost ochotněji akceptuje relativně vysoké riziko z aktivit, kterých se zúčastňuje dobrovolně (sport, kouření, cestování apod.), než nízké riziko spojené např. s chemickým provozem nebo provozem jaderné elektrárny. Riziko z dobrovolných aktivit bývá přitom až o tři řády vyšší (tab. 2).

Tab. 2: Roční riziko úmrtí

PŘÍČINY ÚMRTÍ	**RIZIKO** **[osoba^{-1} . rok^{-1}]**
Úmrtí ze všech příčin:	
- střední hodnota pro celou populaci	$1{,}15 \cdot 10^{-2}$
- muži ve věku 55 - 64 let	$1{,}53 \cdot 10^{-2}$
- ženy ve věku 55 - 64 let	$9{,}1 \cdot 10^{-3}$
- muži ve věku 35 - 44 let	$1{,}7 \cdot 10^{-3}$
- ženy ve věku 35 - 44 let	$1{,}2 \cdot 10^{-3}$
- chlapci 5 - 14 let	$2{,}3 \cdot 10^{-4}$
- dívky 5 - 14 let	$1{,}6 \cdot 10^{-4}$
Kouření (20 cigaret denně)	$5 \cdot 10^{-3}$
Těžba plynu a ropy (úmrtí zaměstnance)	$1 \cdot 10^{-3}$
Silniční dopravní nehoda	$1 \cdot 10^{-4}$
Těhotenství	$8 \cdot 10^{-5}$
Kopaná	$4 \cdot 10^{-5}$
Užívání plynu v domácnosti	$1 \cdot 10^{-6}$
Užívání elektřiny v domácnosti	$1 \cdot 10^{-6}$
Protržení hráze vodního díla	$1 \cdot 10^{-7}$
Havárie JE (úmrtí osoby v okruhu do 1 km od JE)	$1 \cdot 10^{-7}$
Úder blesku	$1 \cdot 10^{-7}$
Pád meteoritu	$1 \cdot 10^{-11}$

Veřejnosti rovněž méně vadí relativně častá úmrtí a poškození zdraví malého počtu osob (pracovní úrazy, automobilové nehody) než řídké případy havárií s jednorázovým větším počtem obětí. Proto se při stanovení zdravotních limitů rizika bere v úvahu kromě ryze racionálních hledisek i postoj laické veřejnosti.

4 METODY A POSTUPY HODNOCENÍ RIZIKA

Jak je zřejmé z definice rizika, je při hodnocení rizika nutné uvažovat jak pravděpodobnost vzniku nežádoucí události, tak její následek. Následky nežádoucích událostí jsou rozmanité. Jejich spektrum sahá od jednoduchých ekonomických analýz ztrát způsobených výpadkem výrobního zařízení až po složité modely úniků nebezpečných látek a radioaktivity do jednotlivých složek životního prostředí. Popis metod a postupů hodnocení následků značně překračuje rozsah a zaměření tohoto materiálu. Proto je pozornost věnována stručnému popisu metod používaných k hodnocení vzniku nežádoucích událostí.

Metody používané k hodnocení rizika lze dělit zhruba do tří kategorií podle stupně podrobnosti analýzy rizika a schopnosti kvantifikace míry rizika.

Kategorie 1: Srovnávací metody

Jsou to metody Process/System Checklist, Safety Audit/Review, Relative Ranking - Dow and Mond Hazard Indices. Pracují většinou na základě porovnávání a aplikování provozních zkušeností získaných z provozu nebezpečných zařízení a doplněné prohlídkou zařízení. Jejich cílem je odhalení slabin nebezpečného zařízení a seřazení systémů, skupin, uzlů podle subjektivního posouzení jejich podílu na příčinách a průběhu nebezpečné události.

Tyto metody upozorní na potenciálně nebezpečné části hodnoceného zařízení. Nejsou však schopny číselně kvantifikovat pravděpodobnost selhání jednotlivých systémů, nedefinují podíl jednotlivých komponent nebezpečného zařízení na pravděpodobnosti vzniku nebezpečné události. Pomocí těchto metod nelze vyčíslit míru rizika.

Kategorie 2: Analytické metody založené na deterministickém přístupu

Tato kategorie zahrnuje Preliminary Hazard Analysis, Hazard Operability Studies (HAZOP), "What if" Analysis a Failure Mode and Effect Analysis. Tyto metody již systematicky analyzují příčiny nastání nebezpečných událostí a scénáře rozvoje nebezpečné události. Pro definované nebezpečné události vypracují seznam poruch systémů, komponent a chyb obsluhy, které k těmto událostem vedou. Dávají dobrou představu o chování nebezpečného zařízení.

Jejich zásadní nedostatek, společně sdílený s metodami kategorie 1, spočívá v neschopnosti postihnout pravděpodobnost výskytu nebezpečných jevů, pravděpodobnost selhání pro bezpečnost důležitých komponent, systémů a zásahů obsluhy. Proto tyto metody selhávají při řízení pravděpodobnostní složky rizika a neumožňují důslednou prevenci nebezpečných událostí.

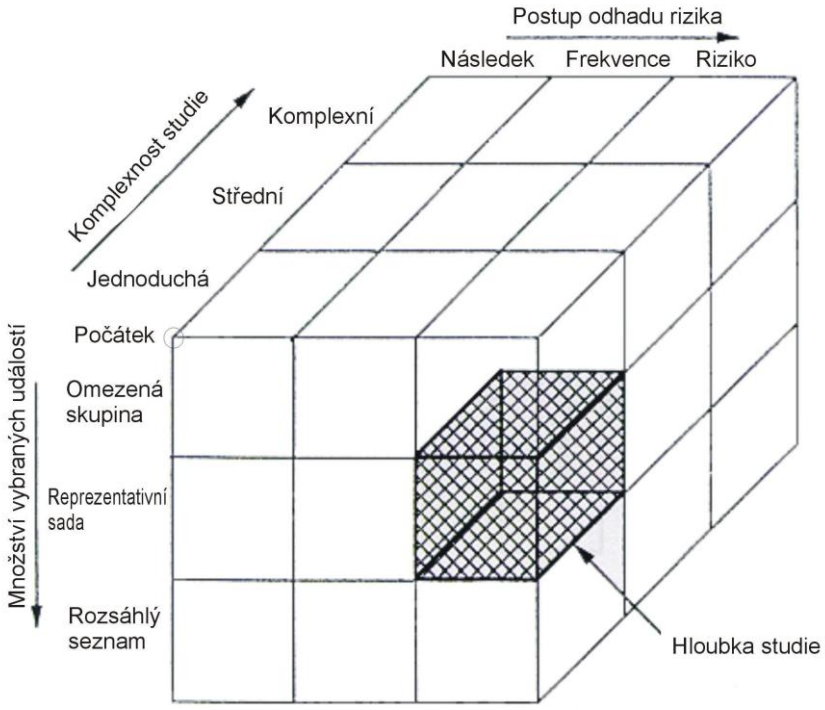
Kategorie 3: Analytické metody založené na pravděpodobnostním přístupu

Při hodnocení rizika spojeného s provozem jaderných zařízení bylo v polovině 70. let ustoupeno od analytických hodnocení založených na pouhém vyhledání příčin a následků selhání systémů, komponent a obsluhy (viz metody kategorie 2). Vyvstala potřeba číselného hodnocení podílu těchto jevů na nastání nebezpečné události a potřeba vyjádření pravděpodobnosti výskytu nebezpečné události. Proto na základě sledování poruchovosti systémů, komponent a omylů lidského činitele se pomocí matematicko statistických metod počaly kvantifikovat pravděpodobnosti příčin nebezpečných událostí.

Obdobně jako u metod kategorie 2 se na základě provedených analýz vzniku a rozvoje nebezpečné události sestaví seznam primárních jevů (poruch komponent, systémů, chyb obsluhy, nepříznivých externích vlivů), které samostatně nebo v kombinacích vedou ke vzniku nebezpečné události. K těmto primárním jevům jsou přiřazeny pravděpodobnosti jejich výskytu a vypočítává se pravděpodobnost vzniku nebezpečné události. K nejznámějším analytickým metodám, které pracují s pravděpodobnostním hodnocením, lze řadit metody stromu poruch/událostí (Fault/Event Tree Analysis), blokové diagramy, orientované grafy, Markovské procesy. Pro pravděpodobnostní hodnocení bezpečnosti/rizika jaderných elektráren (PSA/PRA studie - Probability Safety/Risk Assessment) jsou nejpoužívanější metodou stromy poruch/událostí. Jsou pro ně proto vyvinuty mezinárodně standardizované výpočtové programy, komerčně dostupné, často spojené s databázemi pravděpodobnosti poruch komponent technologických, řídicích a elektrických systémů.

K uvedenému přehledu metod je třeba podotknout, že vyčíslit riziko jsou schopny pouze metody založené na pravděpodobnostním přístupu k hodnocení rizika. Tyto metody byly nejprve používány v jaderné energetice. Obecně jsou známy pod označením **pravděpodobnostní hodnocení rizika** (PRA - Probability Risk Assessment, respektive PSA - Probability Safety Assessment). Představují souhrn metod používaných pro stanovení pravděpodobnosti úniku radioaktivních látek a jeho následků (PSA studie 1. - 3. stupně). V ostatních nebezpečných průmyslových oborech se častěji používá termínu **kvantifikované hodnocení rizika** (QRA - Qauntified Risk Assessment). V chemickém průmyslu jsou tyto metody označovány jako CPQRA - Chemical Process Quantitative Risk Analysis. Jde o metody plně zvládnuté a běžně aplikované.

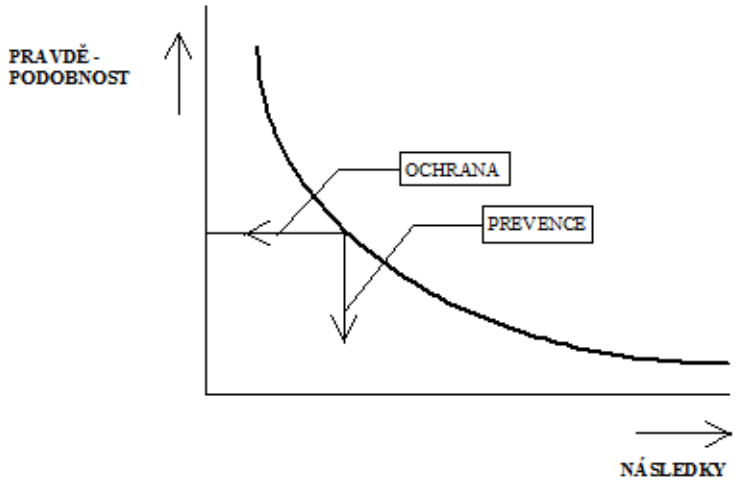
Volba postupů hodnocení rizika je dána složitostí řešeného problému, úrovní podrobnosti analýzy a dostupností údajů. Znázornění možné podrobnosti studie rizika je zjednodušeně uvedeno na obr. 4.



Obr. 4: Znázornění úrovně podrobnosti hodnocení rizika

5 ZPŮSOBY ŘÍZENÍ RIZIKA, OPTIMALIZACE RIZIKA

Charakter rizika vhodně vystihuje riziková funkce, která popisuje funkční závislost mezi jednotlivými složkami rizika (pravděpodobností výskytu a následky nežádoucích událostí). Příklad průběhu rizikové funkce je uveden na obr. 5.



Obr. 5: Riziková funkce

Z uvedeného příkladu je zřejmé, že řízení rizika lze provádět jak snižováním pravděpodobnosti výskytu nežádoucí události (prevence), tak snižováním závažnosti následků nežádoucí události (ochrana).

V úzce pojatém smyslu se riziko plynoucí z průmyslové výroby vztahuje pouze k životu a zdraví člověka. Při tomto pohledu se hodnocení rizika odehrává v rovině identifikace a hodnocení nebezpečných nežádoucích událostí (viz obr. 1) a regulace rizika je předmětem zájmu orgánů státní správy. V moderním řízení velkých průmyslových podniků se však ve světě stále více prosazuje komplexní pojímání rizika. Riziko pak není vázáno jen k životu a zdraví člověka, hodnocení a řízení rizika se děje na množině nežádoucích událostí. Tato množina nežádoucích událostí není pojímána pouze z čistě technického hlediska, ale zahrnuje i řadu dalších nepříznivých jevů, které na průmyslový provoz působí (poruchy dodavatelsko-odběratelských vztahů, fluktuace pracovníků, disponibilita finančních zdrojů, hospodářsko-politická nestabilita regionu apod.).

Je přirozené, že jiný přístup k posuzování rizika spojeného s průmyslovým provozem má vlastník průmyslového provozu (podnikatelský subjekt) a jiný orgán státní správy příslušný k schvalování jeho provozu. Úkolem orgánu státní správy není šetření veškerého rizika plynoucího z průmyslového provozu (ze všech nežádoucích událostí). Nezastupitelnou roli však má orgán státní správy při regulaci rizika, které průmyslový provoz znamená pro zdraví a životy obyvatelstva (viz nebezpečné nežádoucí události), s přihlédnutím ke škodám na majetku ostatních subjektů (některé z bezpečných nežádoucích událostí). Pro orgán státní správy je proto zásadní hodnocení rizika plynoucího z nebezpečných nežádoucích událostí, které porovnává s přijatými standardy rizika, tedy zdravotními limity rizika.

Celospolečenská kontrola rizika prostřednictvím orgánu státní správy má za následek, že odpovídající rozhodování přestává být v rukou těch, kteří tato rizika podstupují. Dochází k rozdělení rizik tak, že někteří lidé jsou jimi zatíženi více, přičemž na výhodách se podílejí

i ti, které riziko nepostihuje. Například obyvatelé obce s nebezpečným průmyslovým provozem nesou vyšší riziko než zbylí občané státu. Ve vyspělých zemí odpovídá distribuci rizika i distribuce kompenzací a výhod. Ve Francii mají kupříkladu obyvatelé sídlící poblíž jaderných elektráren levnější elektrickou energii.

Přijatelná úroveň rizika se odvozuje z rizik, kterým jsou vystaveni lidé v běžném životě z přirozených příčin. Nejnižší úmrtnost z přirozených příčin je dána pro skupinu dětí ve věku 10 - 15 let hodnotou 1.10^{-4} osoba^{-1}.rok^{-1}. Proto je například v Nizozemí stanoven pro nové průmyslové provozy zdravotní limit rizika jako jedno procento této úmrtnosti. Znamená to, že nebude povolen průmyslový provoz, který by přispěl vyšší hodnotou než 10^{-6} osoba^{-1}.rok^{-1} k individuálnímu riziku obyvatele Nizozemí. Rizika průmyslových provozů s hodnotou menší než 10^{-8} osoba^{-1}.rok^{-1} se považují za zanedbatelná neboť se pohybují na úrovni (případně pod úrovní) rizik přírodních jevů. Pro průmyslové provozy, jejichž míra rizika se pohybuje v oblasti 10^{-6} - 10^{-8} osoba^{-1}.rok^{-1}, se požaduje doložit analýzou poměru vynaložených nákladů k výslednému přínosu (CBA - Cost-Benefit Analysis), že je zajištěna rozumně dosažitelná bezpečnost provozu.

Další kritérium, které se v Nizozemí používá, je odvozeno od maximální výše sociálního rizika. Kritérium limituje frekvenci nebezpečné nežádoucí události s ohledem na možný počet úmrtí při nehodě následovně:

- úmrtí více než 10 lidí - frekvence nižší 1.10^{-5} rok^{-1}
- úmrtí více než 100 lidí - frekvence nižší 1.10^{-7} rok^{-1}
- úmrtí více než 1000 lidí - frekvence nižší 1.10^{-9} rok^{-1}

Při regulaci rizika musí orgány státní správy rovněž uvážit velikost následků nebezpečných nežádoucích událostí průmyslového podniku s ohledem na jeho finanční schopnost tyto následky krýt. Následky velké průmyslová havárie mohou totiž přesáhnout možnosti krytí podnikem a náklady na jejich likvidaci pak nese stát. Této eventualitě čelí orgány státní správy požadavkem povinného krytí rizika pojištěním a cena pojistného je pak zahrnuta do nákladů průmyslového podniku.

V České republice je řízení rizika spojené s využíváním jaderné energie pokryto zákonem č. 18/1997 Sb. (atomový zákon) a vyhláškami s tímto zákonem souvisejícími. Pro jadernou energetiku jsou důležité zejména vyhlášky č. 214/1997 Sb. (o zabezpečování jakosti), č. 215/1997 Sb. (o kritériích na umísťování), č. 219/1997 Sb. (o zajištění havarijní připravenosti), č. 106/1998 Sb. (o zajištění jaderné bezpečnosti) a nařízení vlády č. 11/1999 Sb. (o zóně havarijního plánování). Přestože ani v jedné z vyhlášek není taxativně stanovena hodnota rizika z provozu jaderného zařízení, je zajištěna minimalizace rizika předepsáním činností, které je třeba dodržovat. Požadavek na dodržení těchto činností vede k respektování pravděpodobnostních bezpečnostních cílů uvedených v dokumentu IAEA "Basic Safety Principles for Nuclear Power Plants" (Safety Series No. 75-INSAG-3 Rev.1) a k ochraně personálu a obyvatelstva před následky nebezpečných událostí vhodnou havarijní připraveností. Podle tohoto dokumentu by hodnota pro kumulativní četnost poškození aktivní zóny reaktoru měla být někde pod 10^{-4} na jeden rok provozu reaktoru pro provozované jaderné elektrárny a neměla by být větší než přibližně 10^{-5} na jeden rok provozu reaktoru u budoucích jaderných elektráren. Z dokumentu pak nepřímo vyplývá, že u nových jaderných elektráren má být kumulativní četnost překročení limitního úniku menší než 10^{-6} na jeden rok provozu reaktoru a havarijní sekvence, které představují velké úniky z reaktoru v kombinaci se závažným poškozením kontejnmentu, musí mít kumulativní četnost podstatně menší než předchozí cíl 10^{-6} na jeden rok provozu reaktoru. Tomu odpovídá i hodnota uvedená v nařízení vlády č. 11/1999 Sb. (o zóně havarijního plánování), kde v § 1 se požaduje zóna

havarijního plánování v případě, že nelze vyloučit radiační havárii s pravděpodobností větší nebo rovnou 1.10^{-7} rok^{-1}.

Dále je v České republice riziko z nejaderných aktivit regulováno zákonem č. 353/1999 Sb. (o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami a chemickými přípravky) a návaznými vyhláškami, zejména vyhláškou č. 8/2000 Sb. (zásady hodnocení rizik závažné havárie). Přijatelná hodnota rizika je určována prostřednictvím přijatelné četnosti F_p ohrožení života jedné nebo více osob N:

pro stávající zařízení

$F_p = 1.10^{-5}$, resp. $F_p = \frac{1.10^{-3}}{N^2}$

pro nové zařízení

$F_p = 1.10^{-6}$, resp. $F_p = \frac{1.10^{-4}}{N^2}$

Vzhledem k postupně získávaným zkušenostem s hodnocením rizika podle této legislativy a nepřesnostem, které vyhláška č. 8/2000 Sb. obsahuje (např. pro ohrožení života více osob vychází v případě počtu do 10 osob přijatelná četnost vyšší než pro ohrožení života jedné osoby), se předpokládá brzká novelizace těchto dokumentů

Obecně se za komplexní řízení rizika průmyslového provozu pokládá realizace účinných opatření ke zmírnění rizik plynoucích z množiny všech nežádoucích událostí. Hodnocení rizika z nebezpečných nežádoucích událostí je pouze prvním krokem vyžadovaným orgány státní správy. Podstatná a často rozhodující část rizika průmyslového provozu je však spojena s bezpečnými nežádoucími událostmi. Bezpečné nežádoucí události představují u průmyslového provozu řádově četnější množinu událostí, než je množina nebezpečných nežádoucích událostí.

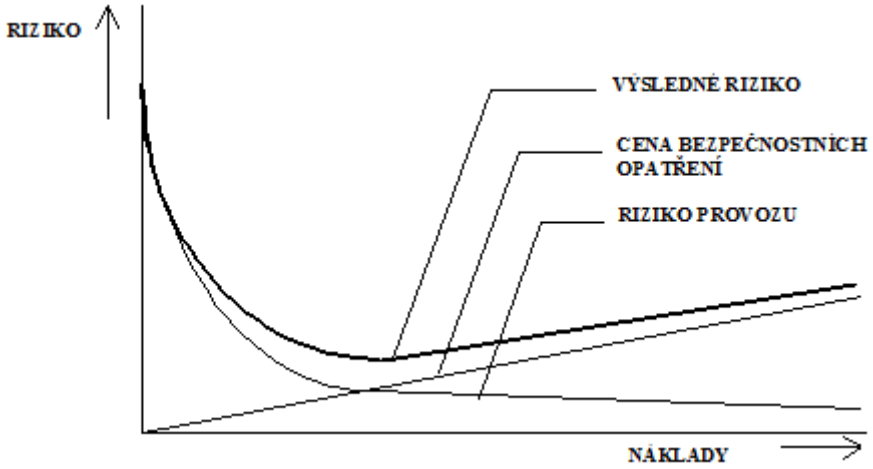
Pro krytí rizika nebezpečných a bezpečných nežádoucích událostí (vyjádřených velikostí a roční četností ekonomických ztrát) vytváří průmyslový podnik vlastní finanční rezervy nebo volí formu krytí vybraných typů rizika pojistkou. Při znalosti výše rizika je možné zjednodušeně posoudit výhodnost pojistky takto:

míra rizika podniku > pojistné ... pojistka zvýhodňuje průmyslový podnik,
míra rizika podniku = pojistné ... oboustranně vyrovnaná pojistka,
míra rizika podniku < pojistné ... pojistka zvýhodňuje pojišťovnu.

Při řízení rizika krytého pojistkou (jedná se zpravidla o riziko spjaté s výskytem nebezpečných nežádoucích událostí) je prvním krokem stanovení přiměřenosti pojistné částky k míře rizika jednotlivých nebezpečných, případně bezpečných, nežádoucích událostí. Ve druhém kroku se provádí prostřednictvím nápravných opatření cílené snižování rizika průmyslového podniku se záměrem dalšího snížení pojistného. Efektivnost nápravných opatření se vyhodnocuje postupy CBA.

Z obecného principu řízení rizika vyplývá, že riziko je nutné snižovat až na úroveň, kdy výdaje na snížení rizika se stávají neúměrnými ve srovnání s příslušným omezením rizika. Tento požadavek se v odborných publikacích definuje jako princip ALARA (as low as reasonable achievable) - riziko se požaduje snížit na úroveň tak nízkou, jak je rozumně dosažitelné. Pro stanovení efektivnosti vynakládaných opatření se aplikuje analýza poměru vynaložených nákladů k výslednému přínosu (CBA - Cost-Benefit Analysis). Metodu CBA lze vhodně objasnit na příkladu řízení rizika nebezpečných nežádoucích událostí, kde je třeba definovat rozumnou mez bezpečnosti. Je zřejmé, že cíleným vynakládáním prostředků na ochranná a zabezpečovací zařízení průmyslového provozu klesá míra rizika plynoucího z výskytu nebezpečných nežádoucích událostí. Pokles rizika vztaženého na vynaložené

finanční prostředky je zpočátku značný. V pozdější fázi, kdy jsou jednoduchá a finančně nenáročná opatření vyčerpána, se dosahuje poklesu rizika vynaložením vyšších nákladů na dokonalejší bezpečnostní zařízení. Rovněž výroba bezpečnostního zařízení však přináší riziko ohrožení zdraví a života osob. Pro výrobu bezpečnostního zařízení je nutno těžit suroviny, vyrobit energii, dopravovat polotovary atd. Veškeré tyto činnosti mají svoji míru rizika. Existuje tedy přímá závislost mezi cenou zabezpečovacího zařízení (a obecně cenou veškeré produkce) a mírou rizika spojenou s jeho výrobou. S rostoucími náklady na zabezpečovací zařízení se toto riziko zvyšuje a v určitý moment převýší riziko spjaté s výrobou bezpečnostního zařízení přínosy ze zvýšení bezpečnosti průmyslového provozu (obr. 6). Totéž platí pro hodnocení nákladů a přínosů bezpečných nežádoucích událostí, kdy náklady na nápravná opatření pro snížení rizika z bezpečných nežádoucích událostí přesáhnou přínosy z omezení jejich rizika.



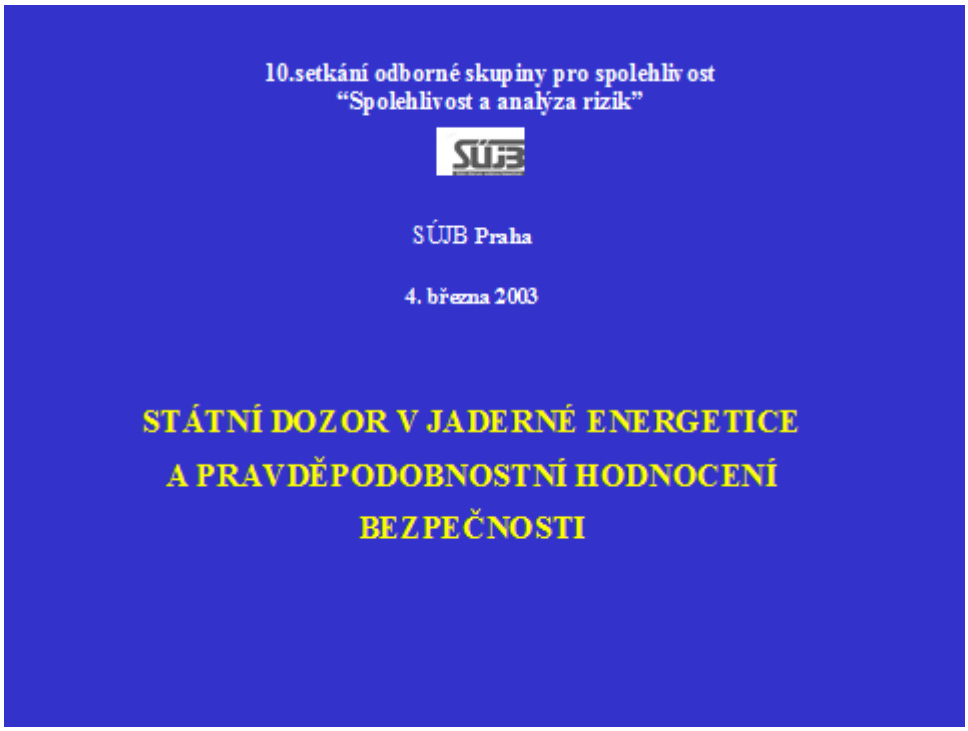
Obr. 6: Optimalizace snižování rizika

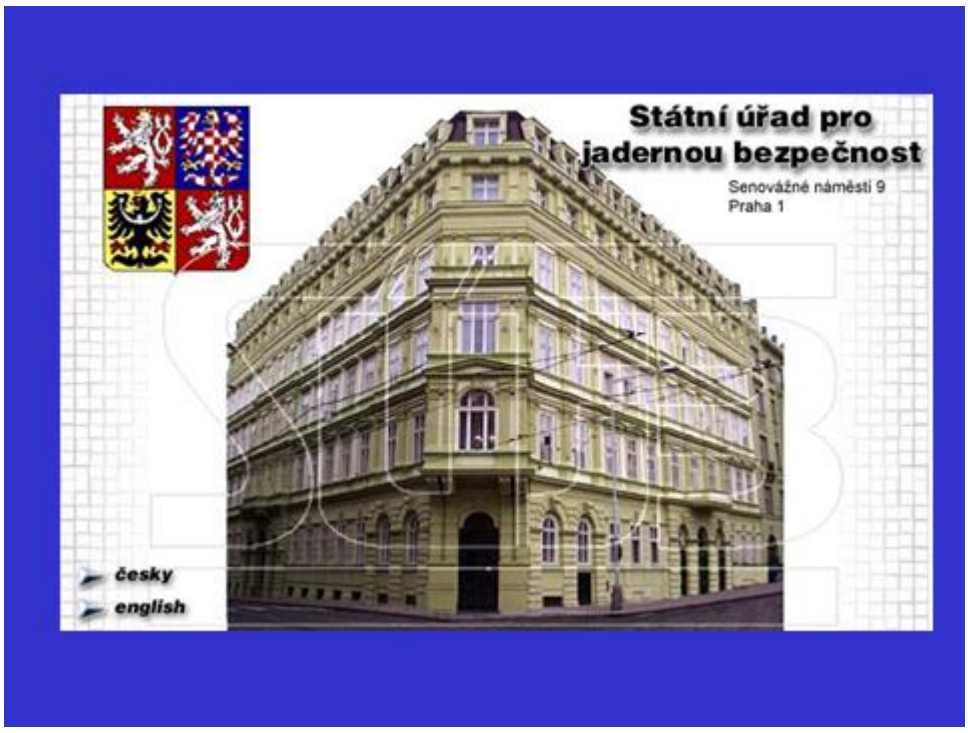
6 ZÁVĚR

Z uvedeného přehledu je patrná šíře problematiky týkající se hodnocení a řízení rizik. Významná úloha při hodnocení a řízení rizik náleží oboru spolehlivosti. Je to dáno jednak skutečností, že ze své podstaty je zaměřen na analýzu a hodnocení jevů spojených s rizikem selhání technických zařízení (poruchy komponent a jejich následky na systém, náklady spojené s poruchami zařízení). Dále pak skutečností, že představuje přirozenou informační a datovou základnu pro ty rizikové analýzy, kde nežádoucí události jsou spojeny s činností technického zařízení. Je proto logické, že analýza a hodnocení tohoto rizika je součástí metod a postupů používaných ve spolehlivosti a uváděných v normách managementu spolehlivosti, tj. v normách řady ČSN IEC 300-x-x (viz např. ČSN IEC 300-3-9: 1997 Management spolehlivosti - Část 3: Návod k použití - Oddíl 9: Analýza rizika technologických systémů).

STÁTNÍ DOZOR V JADERNÉ ENERGETICE A PRAVDĚPODOBNOSTNÍ HODNOCENÍ BEZPEČNOSTI

Ing. Josef Dušek, CSc., Státní úřad pro jadernou bezpečnost





Přehled prezentace

- Postavení SÚJB
- Legislativa
- Co je to PSA?
- Vývoj PSA ve světě a v ČR
- Stav analýz PSA v ČR
- Uplatnění PSA v práci dozoru nad jadernou bezpečností
- Strategie SÚJB v oblasti PSA

Postavení SÚJB ve státní správě České republiky (1)

Státní úřad pro jadernou bezpečnost je ústřední orgán státní správy ve smyslu z. č. 2/1969 Sb.

V jeho čele stojí předseda, který je jmenován vládou ČR. Úřad má samostatný rozpočet a je přímo podřízen vládě ČR.

SÚJB vykonává státní správu a dozor při využívání jaderné energie a ionizujícího záření a v oblasti radiační ochrany.

Postavení SÚJB ve státní správě České republiky (2)

Do působnosti SÚJB, dané zákonem č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon), zejména patří:

Povolování výkonu činnosti podle zákona č. 18/1997 Sb., např. k umísťování a provozu jaderného zařízení a pracoviště s velmi významnými zdroji ionizujícího záření, nakládání se zdroji ionizujícího záření a radioaktivními odpady, přepravě jaderných materiálů a radionuklidových zářičů;

Schvalování dokumentace, vztahující se k zajištění jaderné bezpečnosti a radiační ochrany, stanovené atomovým zákonem, limitů a podmínek provozu jaderných zařízení, způsobu zajištění fyzické ochrany, havarijních řádů k přepravám jaderných materiálů a vybraných radionuklidových zářičů, vnitřních havarijních plánů jaderných zařízení a pracovišť se zdroji ionizujícího záření;

Stanovení podmínek a požadavků radiační ochrany obyvatel a pracovníků se zdroji ionizujícího záření (např. stanovení limitů ozáření, vymezení kontrolovaných pásem), stanovení zóny havarijního plánování a požadavků havarijní připravenosti držitelů povolení dle atomového zákona;

Postavení SÚJB ve státní správě České republiky (3)

Sledování stavu ozáření obyvatelstva a pracovníků se zdroji ionizujícího záření;

Koordinace činnosti radiační monitorovací sítě na území České republiky a zajišťování mezinárodní výměny dat o radiační situaci;

Vedení státního systému evidence a kontroly jaderných materiálů, státních systémů evidence držitelů povolení, dovážených a vyvážených vybraných položek, zdrojů ionizujícího záření, evidence ozáření obyvatelstva a pracovníků se zdroji ionizujícího záření;

Odborná spolupráce s Mezinárodní agenturou pro atomovou energii (IAEA)

Poskytování údajů o hospodaření s radioaktivními odpady obcím a okresním úřadům na jimi spravovaném území a přiměřených informací o výsledcích činnosti úřadu veřejnosti a vládě ČR.

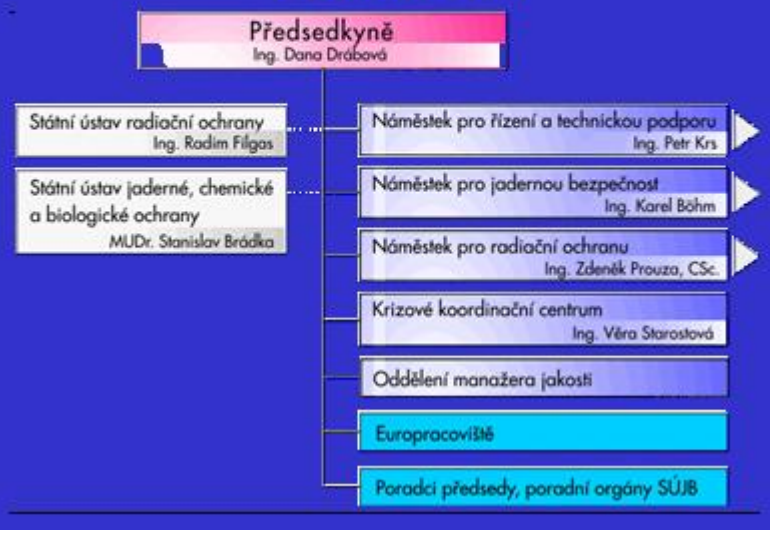
Postavení SÚJB ve státní správě České republiky (4)

SÚJB plní ve smyslu zákona č. 19/1997 Sb. ve znění zákona č. 249/2000 Sb. úkoly v oblasti dozoru nad zákazem chemických zbraní.

Ve smyslu usnesení vlády ČR č. 306/2000 vytváří SÚJB národní orgán vůči úmluvě o zákazu biologických (bakteriologických) a toxinových zbraní.

Usnesením vlády č. 431 ze dne 2. května 2001 plní koordinační a informační funkci vůči úřadu 1. místopředseda vlády a ministr práce a sociálních věcí.

Postavení SÚJB ve státní správě České republiky (5)



Současná legislativa České republiky (1)

Atomový zákon č. 18/1997 Sb.

o mírovém využívání jaderné energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění zákona č. 83/1998 Sb., zákona č. 71/2000 Sb., zákona č. 132/2000 Sb. a zákona č. 13/2002 Sb.

Obecné podmínky pro vykonávání činností souvisejících s využíváním jaderné energie (§4)

(2) ***Každý, kdo využívá jadernou energii*** *nebo provádí činnosti vedoucí k ozáření nebo zásahy k omezení přírodního ozáření nebo ozáření v důsledku radiačních nehod,* ***musí dbát na to, aby toto jeho jednání bylo odůvodněno přínosem, který vyváží rizika,*** *která při těchto činnostech vznikají nebo mohou vzniknout.*

(3) ***Každý,*** *kdo provádí činnosti související s využíváním jaderné energie nebo radiační činnosti, je povinen postupovat tak,* ***aby byla přednostně zajišťována jaderná bezpečnost a*** *radiační ochrana.*

Současná legislativa České republiky (2)

Atomový zákon č. 18/1997 Sb.

o mírovém využívání jaderné energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění zákona č. 83/1998 Sb., zákona č. 71/2000 Sb., zákona č. 132/2000 Sb. a zákona č. 13/2002 Sb.

Obecné podmínky pro vykonávání činností souvisejících s využíváním jaderné energie (§4)

(4) ***Každý,*** *kdo využívá jadernou energii nebo provádí činnosti vedoucí k ozáření,* ***připravuje nebo provádí zásahy k omezení havarijního,*** *přetrvávajícího nebo přírodního* ***ozáření, je povinen dodržovat takovou úroveň jaderné bezpečnosti,*** *radiační ochrany, fyzické ochrany a havarijní připravenosti,* ***aby riziko ohrožení života, zdraví osob a životního prostředí bylo tak nízké, jak lze rozumně dosáhnout*** *při uvážení hospodářských a společenských hledisek.* ***Prováděcí předpis stanoví*** *technické a organizační požadavky a směrné hodnoty ozáření, které se považují za dostatečné k* ***prokázání rozumně dosažitelné úrovně, nebo postup, jak jinak tuto úroveň prokázat.***

Pravděpodobnostní a deterministický přístup k jaderné bezpečnosti

Deterministický přístup k jaderné bezpečnosti, vychází z vybraných projektových havárií jaderného zařízení, proti nimž se používají projektová opatření na likvidaci, či minimalizaci jejich účinků.

Pravděpodobnostní hodnocení bezpečnosti (PSA - Probabilistic Safety Assessment) analýzy deterministického přístupu doplňuje a rozvíjí.

PSA oceňuje riziko, které se obecně chápe jako **míra pravděpodobnosti vzniku a závažnosti nežádoucích důsledků**

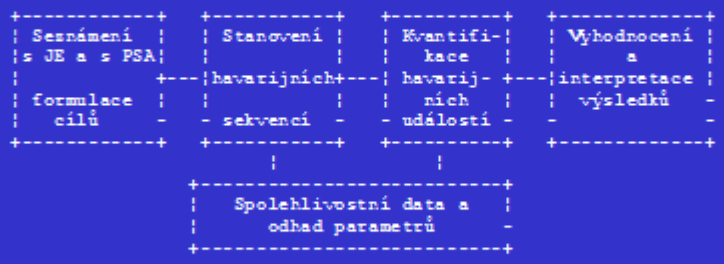
Pravděpodobnostní hodnocení bezpečnosti (PSA)

PSA je metodou analýzy bezpečnosti jaderného zařízení (JZ), která identifikuje a váže kombinace událostí vedoucích k vážným haváriím, stanovuje pravděpodobnost vzniku každé kombinace a určuje její následky.

Metoda PSA tak systematicky a velmi realisticky **spojuje** do jednotného rámce **všechny aspekty bezpečnosti:** projektové charakteristiky, provozní postupy a zkušenosti, spolehlivost systémů, výkonnost člověka, fyzikální procesy při haváriích a potenciální zdravotní účinky na obyvatelstvo v okolí JZ od uvolněných radioaktivních látek.

PSA se provádí ve třech úrovních, z nichž první vyhodnocuje pravděpodobnost tavení aktivní zóny, druhá pravděpodobnost uvolnění zdrojového členu do okolí JZ a třetí pravděpodobný účinek na obyvatelstvo.

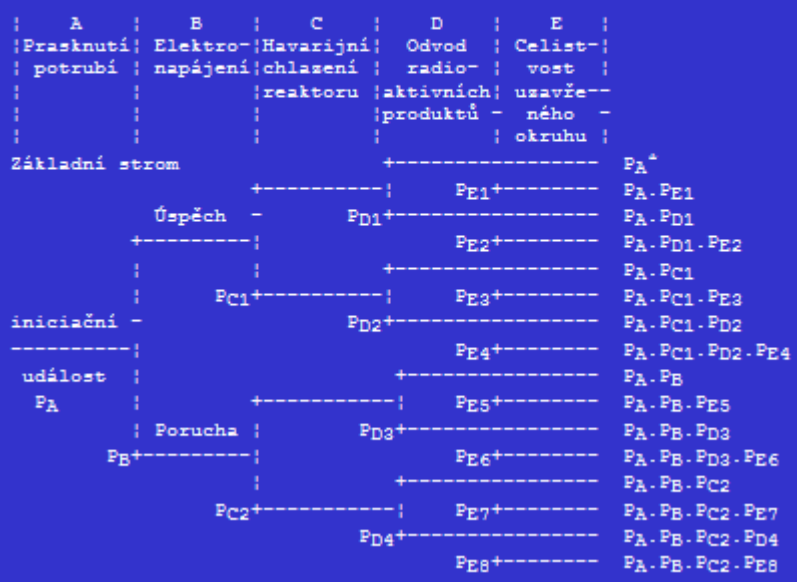
Základní požadavky na provedení PSA studie



Metoda stromu událostí

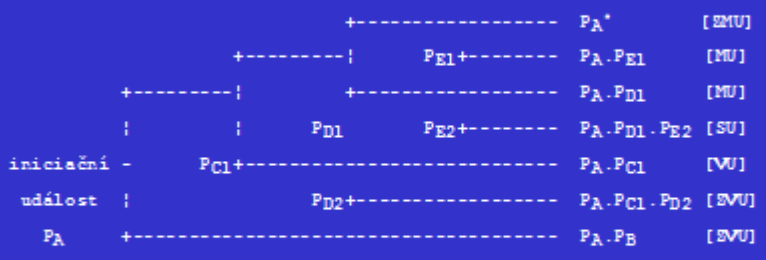
Strom událostí se zakládá na binární logice, dle níž událost se buď stala nebo nestala a zařízení buďto pracuje nebo nepracuje. **Začíná se vždy určitou iniciační událostí po níž následuje větvení podle následků. Každé větvi je přisouzena určitá pravděpodobnost výskytu stanovená např. aplikací metody stromu poruch**. Výsledkem je výčet sekvencí, z nichž každé je přiřazena určitá pravděpodobnost jako součin pravděpodobností předchozích jevů a určité následky.

Ukázka stromu událostí



Redukce stromu událostí

Redukovaný strom

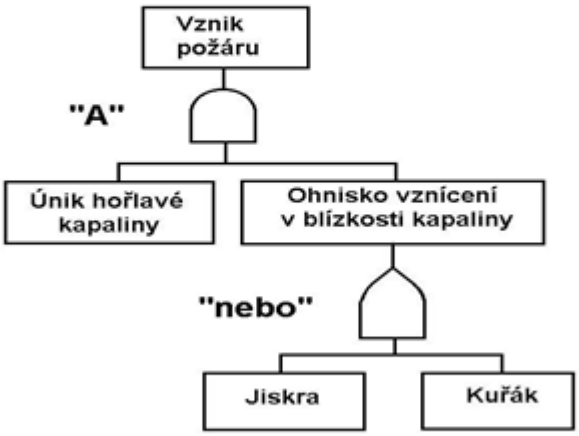


(* výraz je přibližnou hodnotou přesného výrazu
$P_A(1-P_B)(1-P_{C1})(1-P_{D1})(1-P_{E1})$;
všechna P jsou velmi malá, analogické přiblížení je použito i dále;
Z - značně; M - malá; S - střední; V - velká; U - únik)

Metoda stromu poruch

Metoda stromu poruch je deduktivní, tj. s opačnou logikou než stromy událostí. Na základě jedné nežádoucí události, nebo též vrcholové události (TOP event) **hledáme opět binární logikou postupné příčiny této události.** Konečné příčiny nazýváme zpravidla **primární události.**

Příklad použití logických hradel "A" a "NEBO" ve stromu poruch



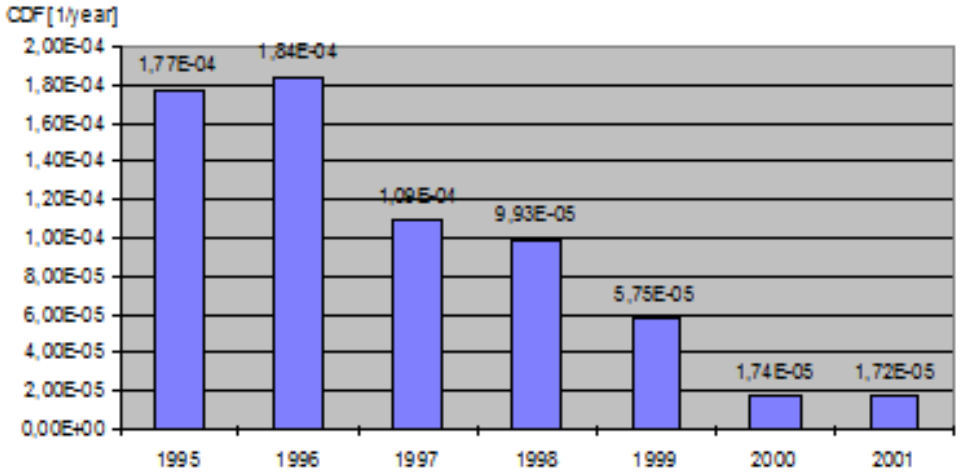
PSA studie jaderné elektrárny Dukovany (VVER440/V 213)

PSA-1.úroveň "domácí"	1993	ÚJV Řež - St.úkol - ČSKAE
PSA-1.úroveň "západní"	1994	SAIC+ÚJV (Risk Monitor SAS)
Záplavy, požáry, ATWS	1994	ÚJV Řež
PSA level 1 "upgrade"	1995	ÚJV Řež
Zhodnocení L&P	1995	SAIC
Hodnocení modifikací	1995	ÚJV Řež
Požáry	1996	ÚJV Řež
PSA - 2.úroveň	1998	SAIC
PSA - 1.úroveň "living"	1998	IPERS-MAAE (ÚJV)
SPSA (nevýkonové stavy)	1999	ÚJV Řež
Risk Monitor™	2000	SCIENTECH

PSA studie jaderné elektrárny Temelín (VVER 1000)

PSA-1.úroveň – (NUS+JE+ÚJV)	1995
IPERS-MAAE	1995
PSA-1.úroveň (požáry, záplavy seismicita aj.)	1995
IPERS – MAAE	1996
PSA-2.úroveň	1996
IPERS – MAAE	1996
Aktualizovaná PSA-1.úroveň - vnitřní iniciátory	únor 2002
Aktualizovaná PSA-1.úroveň - vnější iniciátory	listopad 2002
SPSA (nevýkonové stavy)	červen 2002
Aktualizovaná PSA-2.úroveň	prosinec 2002
PSA - Safety Monitor™	prosinec 2002

Frekvence tavení aktivní zóny (CDF) [1/rok]
Vývoj výsledků studie PSA-1 pro JE Dukovany



Výsledky PSA studie JE Temelín (předběžné z r.1995)

CDF pro 100% výkon

- vnitřní iniciátory 9.0E-5/rok
- vnitřní požáry 1.8E-5/rok
- záplavy 2.3E-6/rok

seismicita+ostatní vnější události méně než 1.0E-7/rok

CDF pro nízkovýkonové a odstavné stavy (shutdown)

ztráta chlazení paliva při odvodu zbytkového tepla 9.0E-5/rok

ztráta chlazení bazénu paliva 2.6E-5/rok

Iniciativy dozoru v oblasti PSA

Iniciace přípravy první PSA studie pro JE Dukovany (1989-1993) v rámci st. plánu

Výstupy ze smluv dozoru s firmou SAIC:

- **Příprava Risk Monitoru pro EDU (1995-1997),**
- **Zhodnocení limit a podmínek EDU na základě znalosti rizika s návrhem úprav (1995),**
- **PSA studie druhé úrovně pro EDU (1998).**

Využití a aplikace PSA

- **návrhy úprav na základě rizika** (modifikace zařízení, úprava předpisů, školení personálu aj.)
- **posuzování přínosu modifikací zařízení**
- **stanovení priorit modifikací**
  (v EDU např. soubor rekonstrukcí pro zvýšení odolnosti zařízení PoE +14,7 m, opatření proti zanášení sacích jímek TQ, drenážní trasa z A301 do A201)
- **podpora při zpracování nových předpisů** (LMS, LAS)
- **Risk Monitor** – víceúčelové využití

Aplikace PSA – Monitor rizika

- hodnotí **úroveň okamžitého rizika JE** v reálném čase, umožňuje **výpočet okamžitého rizika** při neprovozu-schopnosti jedné nebo více komponent
- **je dynamickým nástrojem** pracujícím s **okamžitým stavem komponent** (provozuschopnost – provoz, stand-by / neprovozuschopnost – porucha, údržba, test)
- **PSA** je nástrojem **statickým** pracujícím se **středními hodnotami**

Aplikace PSA – Monitor rizika (funkce)

- **výpočet okamžitého rizika** při neprovozu-schopnosti jedné nebo více komponent
- **výpočet povolené doby neprovozuschopnosti** jedné nebo více komponent
- **hodnocení Limit a podmínek** provozu na základě rizika
- **doporučení** ke zprovoznění komponent (priority)
- **variantní výpočty** (různé kombinace komponent)
- **míra rizika**: sledování pravděpodobnosti tavení aktivní zony reaktoru a/nebo pravděpodobnosti úniku RaL z boxů v průběhu provozu jaderné elektrárny

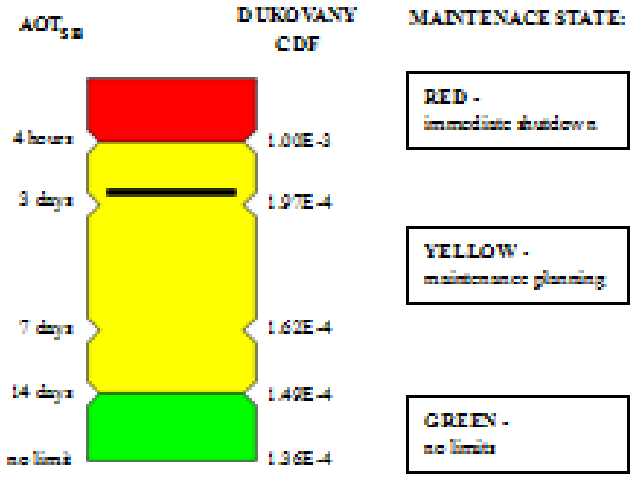
Aplikace PSA – Monitor rizika (využití)

- **vyhodnocování** provozu JE, vlivu na JB
- **podpora** při rozhodování v JE pro řízení JB
- **optimalizace** denního plánu provozu
- **posouzení** povolené doby neprovozuschopnosti zařízení v různých režimech uvedených v LaP
- **optimalizace** HMG prací během odstávky
- **posouzení** možnosti údržby zařízení během provozu
- **dokladování** bezpečného provozu JE

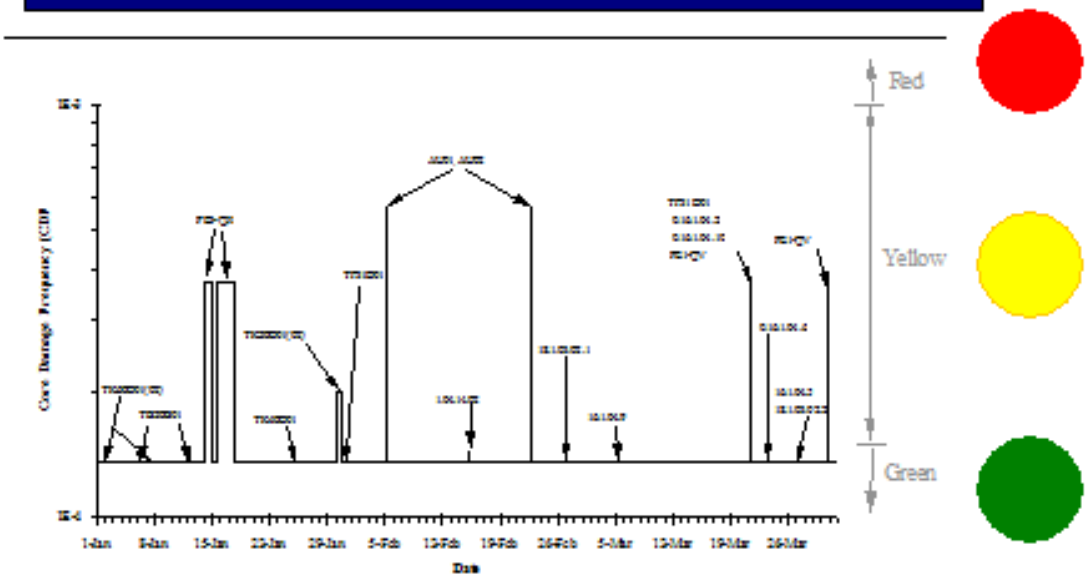
Monitor rizika EDU - historie

- **1995** instalace monitoru rizika SAS na SÚJB a EDU (grant DOE - iniciativa SÚJB)
- **1995 - 1997** provoz SAS v EDU (i v SÚJB):
- zahrnutí výsledků analýz do LaP
  - monitorování provozu EDU
- 3x podklad pro povolení dočasné změny LaP
- **1998 - 1999** SAS nevyhodnocován pro rozdíly mezi modelem SAS a upravenými modely PSA
- 2000 **instalace nového monitoru s nově upraveným modelem na EDU a SÚJB (obdobného jako je plánován pro ETE)**

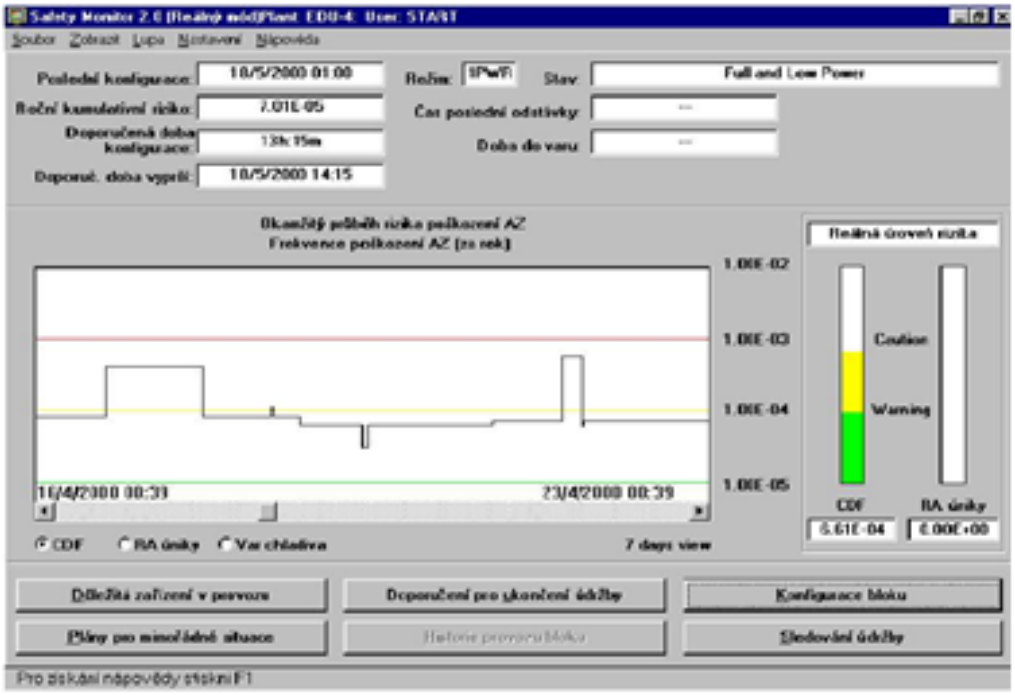
Risk monitor v JE Dukovany



Zkušenosti s Risk monitorem v JE Dukovany 1995-1997



Risk monitor ™ v JE Dukovany



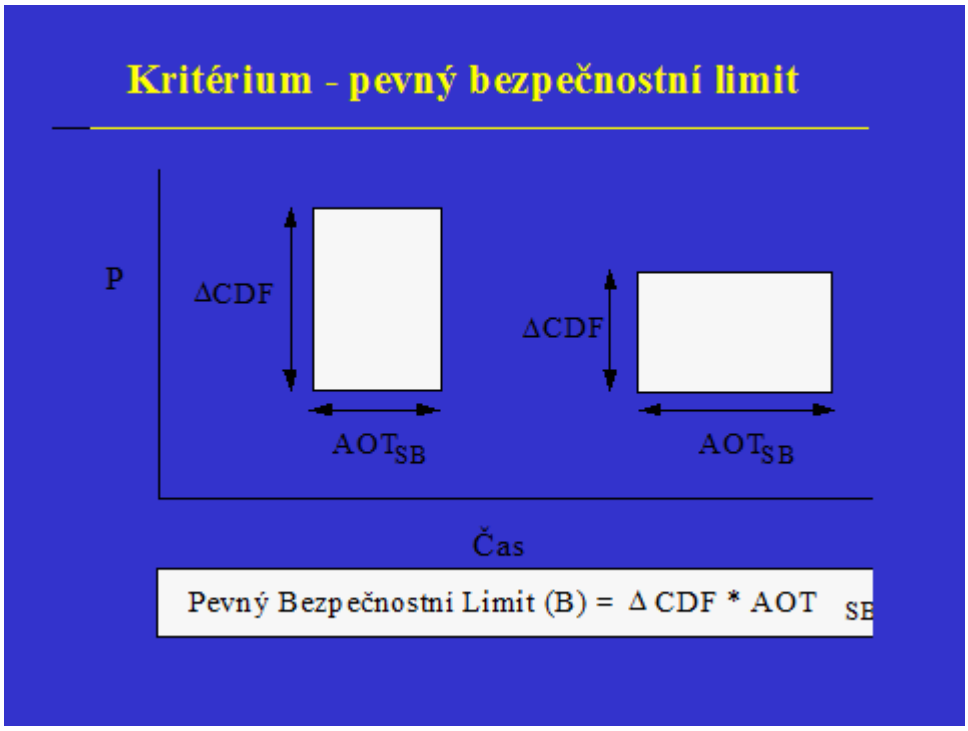
Pravděpodobnostní kritéria

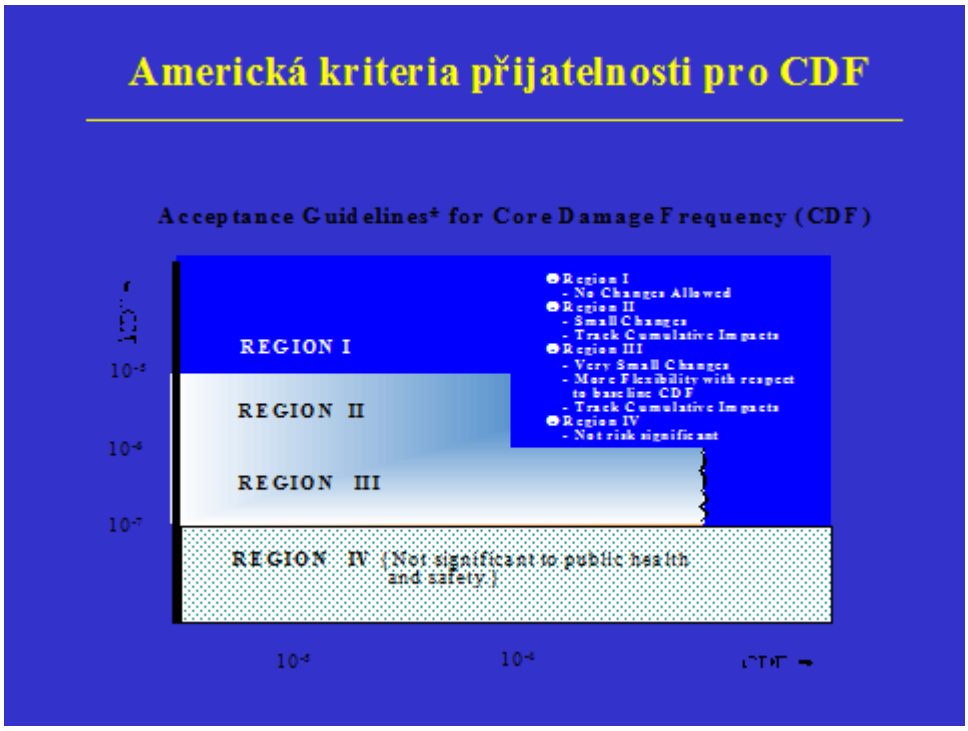
- Maximální riziko – dle risk monitoru (červené pole)
- X -% limit pro prodloužení povolené doby odstavení (AOT) komponenty nebo systému (např. 25% limit, možné využití zejména u deterministicky stanovené AOT)
- Roční limit příspěvků rizika (LEAOT) z povolených dob odstavení (banka rizika) – např. 5*E-6

$$LEAOT = \sum_{i} \frac{CDF_i * EAOT_i}{8760}$$

- Pevný bezpečnostní limit na jednotlivý příspěvek rizika (vícenásobné vyřazení komponent) – např. 5*E-7

B (bezp.limit) = přírůstek CDF * AOT (bezp.stanovený v [hod.])


Kritérium - pevný bezpečnostní limit
P
ΔCDF
ΔCDF
AOT$_{SB}$
AOT$_{SB}$
Čas
Pevný Bezpečnostni Limit (B) = Δ CDF * AOT SB


Americká kriteria přijatelnosti pro CDF
Acceptance Guidelines* for Core Damage Frequency (CDF)
REGION I
REGION II
REGION III
REGION IV (Not significant to public health and safety)
Region I
- No Changes Allowed
Region II
- Small Changes
- Track Cumulative Impacts
Region III
- Very Small Changes
- More Flexibility with respect to baseline CDF
- Track Cumulative Impacts
Region IV
- Not risk significant

Living PSA pro EDU

- **Living PSA musí modelovat skutečný stav bloku,** t.j. modifikace zařízení, změny předpisů a způsob provozování zařízení
- **Rozsah PSA je třeba periodicky doplňovat** a zpřesňovat na základě nových analýz (např. doplnění analýz nízkovýkonových režimů a odstávky, připomínky mise IPERS)
- **Sběr** specifických **dat** na JE **umožňuje zpřesňovat výsledky**
- **Pravidelná aktualizace PSA** - roční cykly

Living PSA pro EDU v r.1999 – tři etapy (1)

- **modelovány změny PSA modelu na základě modifikací projektu a předpisů, které byly v EDU provedeny**
- **aktualizace dat komponent a iniciačních událostí za období 1995-98,**
- **zahrnuta první část doporučení mise IPERS**
- **výsledky nových analýz a programu kvalifikace zařízení**

  Provedené modifikace zařízení a aktualizace dat se projevily velice pozitivně snížením CDF, zahrnutí doporučení mise IPERS ohledně událostí s prasknutím parovodů na PoE +14,7 m a zahrnutí výsledků kvalifikace elektropohonů armatur však způsobilo naopak nárůst CDF.

- **vyhodnocení přínosu připravovaných modifikací zařízení.**

Living PSA pro EDU v r.1999 (2)

Změny v I.etapě (původní CDF = 9,93E-05)	Nové CDF	Změna
A) Instalace nových HNČ	9,79E-05	-1,7%
B) Analýzy PTS (zatím provedené)	9,68E-05	-2,8%
C) Ředění H3BO3 (PH2.08/95)		0%
D) Změna tlaku v hydroakumulátorech	9,49E-05	-5,0%
E) Úprava automatiky AVV 400 kV		0%
F) Rekonstrukce ZN I. kategorie		0%
G) Změna intervalu zkoušek OaB zařízení PO&SO		0%
H) Změna chlazení VT čerpadel SAOZ		0%
I-1) Aktualizace dat iniciačních událostí	9,07E-05	-8,0%
I-2) Aktualizace dat komponent (1995-98)	7,62E-05	-22,7%
Po I. etapě	7,21E-05	-27,6%

Living PSA pro EDU v r.1999 (3)

Změny v II.etapě (původní CDF = 7,21E-05)	Nové CDF	Změna
Ověření frekvence IU LI(TF10) *(IPERS)*		0%
Doplnění IU „ztráta 6 kV rozvaděče ZN II“ *(IPERS)*		0%
Úpravy modelu: podchlazení PO, SU T5 a T2.5 *(IPERS)* a T12, doplnění falešné otevření OVKO *(IPERS)*, zahrnutí TVD a CCHV 2. bloku, odvodu páry, zpřesnění odst.koncentr.		0%
Úprava signálů HO, SOB, TOPG (dle analýz)	7,20E-05	- 0,1%
Zpřesnění nepohotovostí „opravy“ a „testy“	7,23E-05	+ 0,3%
Potřeba znovuotevření RL..S06	7,64E-05	+ 6,0%
Úprava modelu roztržení potrubí páry a napájecí vody na PoE +14,7 m dle výsledků PH 2.02/95	4,75E-05	- 34,1%
Změna modelování závislostí komponent na PoE +14,7 m (výsledky kvalifikace, doporučení IPERS)	1,40E-04	+ 94,2%
Zahrnutí IU „výpadek všech linií TVD“ *(IPERS)*		0%
Po II. etapě	1,03E-04	+42,9%

Living PSA pro EDU v r.1999 (4)

III.etapa – Modifikace (původní CDF = 1,07E-04 *)	CDF [1/rok]	Změna CDF
Přeložení potrubí SHNČ	4,63E-05	- 57 %
Instalace omezovačů švihnutí na PoE +14,7 m	7,57E-05	- 29 %
Výměna elektropohonů armatur PoE +14,7 m	6,32E-05	- 41 %
Nová ochrana „roztržení HNK nebo HVK“	5,81E-05	- 46 %
Zodolnění zařízení SKŘ na PoE +14,7 m	1,01E-04	- 6 %
Instalace nátrubků požár. vody na potrubí SHN	1,03E-04	- 4 %
Provoz armatur RR..S01 v otevřené poloze	5,77E-05	- 46 %
Všechny modifikace PoE dohromady	2,97 E-05	- 72 %
Drenážní trasa z A301 do A201	8,59E-06	- 71 %
Všechny modifikace dohromady	8,59E-06	- 92 %

*) Pozn. Rozdíl oproti CDF II.etapy vlivem použití zjednodušeného modelu

Projekt Shutdown PSA pro EDU (SPSA)

- odstávkách, spouštění a odstavování bloku do 55 %
- projekt byl zahájen v r.1996 a ukončen v pol. r.1999.
- v projektu byly využity výsledky projektu Shutdown PSA pro EBO V-2 (PH2. zahrnuje nízkovýkonové režimy a odstávku - provoz při 09/95)

Pravděpodobnost poškození AZ	CDF = 1,10E-04 /rok
Pravděpodobnost poškození paliva (mimo AZ)	FDF = 2,27E-05 /rok
Celková pravděpodobnost poškození paliva	TFDF = 1,33E-04 /rok

Výsledky SPSA pro EDU - příspěvky

	Název skupiny iniciačních událostí (IU)	Příspěvek k TFDF
1	Ztráta přirozené cirkulace	29,5 %
2	Pád těžkých předmětů	18,0 %
3	Výpadek systému dochlazování	12,0 %
4	Studené přetlakování	8,6 %
5	LOCA způsobená manipulacemi	7,8 %
6	Výpadek rozvaděčů zajištěného napájení	7,4 %
7	Malá LOCA	5,1 %
8	Výpadek linky 400 kV	2,6 %
9	Střední nebo velká LOCA	2,2 %
10	Vnitřní záplavy	1,8 %
11	Prasknutí HPK nebo parovodů	1,4 %

Výsledky SPSA pro EDU – návrhy úprav

Cíl: Zlepšení výsledku Shutdown PSA.

1. **Zpracování předpisu pro likvidaci abnormálních stavů (LAS) též v režimech odstávky**, resp. doplnění stávajících postupů (především postupy pro obnovu přirozené cirkulace a pro ztrátu odvodu tepla na SO, likvidace LOCA v režimu odstávky, postupy pro nouzové chlazení bazénu skladování, spolehlivější detekce varu chladiva)
2. **Optimalizace některých postupů koordinace údržby** (optimalizace drenáže TVD, sladění oprav SHNČ a údržby elektrických systémů)
3. **Modifikace projektu** – bez nových požadavků, pouze potvrzení významu již probíhajících prací (ochrana proti studenému natlakování PO, odvzdušnění reaktoru a primárních kolektorů PG).

Aplikace PSA ve světě (NRC) (1)

Změna přístupu NRC k hodnocení bezpečnosti provozu JE od 1.1.2000

- **Deterministický přístup hodnocení SALP** (Safety Assessment of Licence Performance) a systém jednání řídících pracovníků dozoru a elektráren SMM (Senior Management Meetings) – hodnocení třístupňovou stupnicí **byl nahrazen novým systémem.**
- **Nový přístup vyžívá výsledku PSA** a srovnává hodnoty vybraných indikátorů a výsledků inspekcí se stanovenými hodnotami (result-based)

SALP 12 – 24 měsíců*Nový systém - čtvrtletně**

Aplikace PSA ve světě (NRC) (2)

Cíl:

- **zvýšení objektivity** a předpověditelnosti provozu
- **zvýšení účinnosti** hodnotícího procesu
- **snížení** nepotřebného **zatížení** provozovatele požadavky dozoru, kde to není nezbytné
- **zvýšení průhlednosti** celého procesu

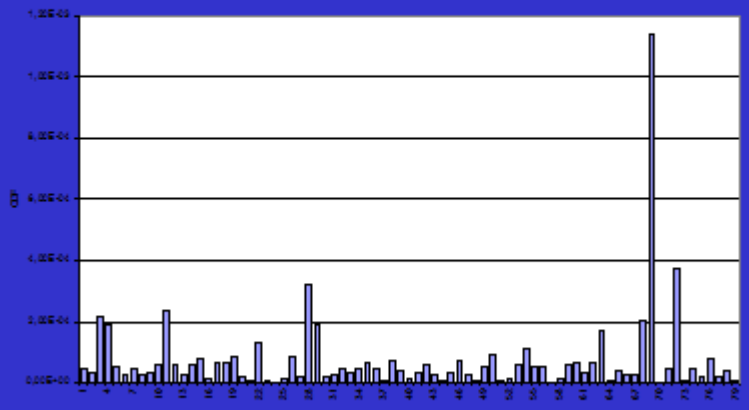
Strategické cíle (v oblasti JB, RB a bezp.ochrany) jsou charakterizovány tzv. **základními kameny** ZK (cornerstones)

V oblasti JB např. počet IU narušujících statiku provozu a vyžadujících činnnost BS, spolehlivost a provozuschopnost BS, integrita fyzických bariér, kvalita a dostatečnost havarijní připravenosti

Aplikace PSA ve světě (NRC) (3)

- **Každý ZK je reprezentován souborem několika provozních indikátorů** (PI) – celkem **asi 20** např. počet neplánovaných odstavení, odstavení s problémem odvodu tepla, přechodových procesů za 7000 hod.).
- Pro všechny indikátory jsou stanovena **pásma přijatelnosti**
- Model rozeznává z hlediska přijatelnosti **čtyři oblasti (A-zelená, B-bílá, C-žlutá a D-červená)**.
- Na základě vyhodnocení stavu všech ZK následuje dle tabulky akce dozoru. **Vyhodnocení náleží do jedné z pěti kategorií specifikující odstupňovaně činnost dozoru** (kontakt, požadavky na provozovatele, inspekční činnost dozoru, schvalovací proces).

Výsledky PSA analýz amerického programu IPE



Mezinárodní doporučení

INSAG-12
(revidovaný 75-INSAG-3, Basic Safety Principles for Nuclear Power Plants, A Report of the International Safety Advisory Group, IAEA Vienna 1999).

Cílem technické bezpečnosti pro havárie by měla být havarijní prevence, management (řízení) a omezující opatření prováděné takovým způsobem, ***aby celkové riziko bylo velmi malé a žádná havarijní sekvence, ať už s malou nebo velkou pravděpodobností, nepřispívala k riziku nadměrně ve srovnání s jinými sekvencemi.***

Strategie státního dozoru v oblasti pravděpodobnostního hodnocení bezpečnosti (1)

Strategie SÚJB je zpracována v souladu s působností Státního úřadu pro jadernou bezpečnost, který dle §3, odst.2a a odst.2e Atomového zákona ***vykonává státní dozor nad jadernou bezpečností a schvaluje dokumentaci, programy, seznamy, limity a podmínky***.

Pravděpodobnostní hodnocení bezpečnosti (PSA) hraje důležitou roli i v souvislosti s působností SÚJB danou §3, odst.2g Atomového zákona, dle kterého SÚJB ***stanovuje zónu havarijního plánování, případně její další členění a schvaluje vymezení kontrolovaného pásma***.

Strategie státního dozoru v oblasti pravděpodobnostního hodnocení bezpečnosti (2)

Strategie vychází ze stávajícího stavu této problematiky a klade si za úkol stanovit způsob, priority a rozsah aktivit a dále časové rozmezí a lidské zdroje pro její další rozvoj v rámci kompetencí a iniciativ státního dozoru nad jadernou bezpečností.

Zásady strategie PSA (1)

- PSA - podpora deterministického hodnocení
- Rozvoj PSA v úrovni první, druhé a třetí (vybrané dílčí analýzy)
- PSA - nedílná součást bezpečnostních analýz a periodického hodnocení bezpečnosti.
- Pravidelné revize PSA analýz jaderných zařízení s JR
- Možnosti uplatnění PSA u všech jaderných zařízení a při přepravách a skladování

Zásady strategie PSA (2)

- Nepředpokládá se stanovení kvantitativních kritérií (respektování doporučených kritérií MAAE, EU, OECD, mezinárodních dohod aj.)
- Jednotný postup a metodika provádění PSA
- Vytváření podmínek pro vývoj PSA (V&V, zakázky, projekty, programy, mise aj.)
- Mezinárodní spolupráce v PSA (dozorné orgány)
- Neočekává se, že SÚJB vytvoří samostatný tým pro revize PSA v plném rozsahu (širší tým specialistů orientující se v PSA, dozor a kontrola provádění aplikací)

Zásady strategie PSA (3)

- Provedení revizí PSA studií (IPSART - MAAE, vybraní experti, zahraniční dozorné orgány)
- Uplatnění PSA v hodnotící, inspekční a povolovací činnosti (směrem k RiDM)
- Rozvoj možných aplikací PSA
- Využívání risk monitoru (povolování výjimek z LaP, variantní hodnocení rizika při různých konfiguracích, příp. hodnocení poruchových stavů dlouhodobé monitorování ukazatelů rizika)
- Součinnost PSA s vývojem LaP (rizikově orientované, dostatečně konzervativní)

Zásady strategie PSA (4)

- Podpora aktivity držitelů povolení při využívání aplikací PSA (údržba, stárnutí, priority aj.), návrhy opatření, implementace změn ke zvýšení jaderné bezpečnosti
- Aktivita v informační a osvětové činnosti o PSA (veřejnost a orgány státní správy)
- SÚJB zpracuje plán prací v oblasti PSA, který bude variabilním, „živým“ dokumentem, sloužícím v průběhu tří termínovaných období, dlouhodobého (> 4 roky) střednědobého (> 1 rok) a krátkodobého horizontu.

Rozhodující úkoly první etapy Strategie PSA

- 1) Zvýšení znalostí pracovníků dozoru o PSA a jeho možných aplikacích v práci dozoru (diferencovaný program)
- 2) Zavedení PSA do legislativního rámce ČR (vyhláška SÚJB č.195/1999)
- 3) Stanovení aplikací PSA ve kterých se bude pokračovat a aplikací, které by bylo žádoucí rozvíjet
- 4) Vymezení role SÚJB v rozvoji PSA v rámci ČR.

Návrh na změnu vyhlášky SUJB č.195/1999

§2

Pro účely této vyhlášky se rozumí

o) deterministickou metodou metodu, která užitím analýz předvídá průběh událostí a jejich následků, ukazuje odezvu jaderného zařízení a jeho bezpečnostních a ochranných systémů a splnění bezpečnostních cílů.

p) pravděpodobnostní metodou metodu, která komplexně a strukturálně oceňuje pravděpodobnost vzniku poruchových scénářů a jejich následků.

§3

Ochrana do hloubky a její ověření

(1) Jaderná bezpečnost jaderného zařízení ...

(2) Pro ověřování jaderné bezpečnosti jaderného zařízení se musí používat metod podle dosažené úrovně vědy a techniky.

(3) Deterministickými metodami se ověřují projektové nehody, havarijní podmínky a události, které mohou nepříznivě ovlivnit bezpečnost jaderného zařízení.

(4) Pravděpodobnostní metody se užívají k ocenění rizika vztahujícího se k projektovému řešení i provozu jaderného zařízení.

Závěry Strategie PSA

SÚJB bude pravděpodobnostní analýzy pro jaderná zařízení diferencovaně vyžadovat, bude využívat jejich výsledků pro zvyšování jaderné bezpečnosti a bude podporovat jejich rozvoj. Výsledky analýz by ve většině případů měly sloužit jako podpora, příp. součást deterministických analýz a v oprávněných případech i pro bezpečnostní rozhodnutí na základě rizika.

Závěry

- Použití metody PSA je v ČR široce rozvinuto a využíváno jak pro potřeby provozovatelů JE tak pro potřeby státního dozoru
- Při bezpečnostním hodnocení je uplatňován deterministický přístup s podporou metod PSA
- Dosavadní výsledky přispěly v mnoha případech k významnému zvýšení jaderné bezpečnosti

POSTUPY PSA VYUŽÍVANÉ V ÚJV ŘEŽ

RNDr. Jaroslav Holý, ÚJV Řež a.s.

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Analýzy spolehlivosti a bezpečnosti v ÚJV Řež

RNDr. Jaroslav Holý
Oddělení analýz spolehlivosti a rizik
V Praze, 4. března 2003

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Cíle prezentace

- **obecná témata využití *pravděpodobnostního přístupu* k řešení otázek spolehlivosti a bezpečnosti**
- **profil Oddělení analýz spolehlivosti a rizik ÚJV Řež**
- **metody analýzy spolehlivosti a rizika (užívané při studiu projektu a provozu technologií pracujících na měřitelné úrovni rizika)**
- **typické současné ukazatele rizika v jaderné energetice**

Pozice pravděpodobnostního hodnocení v analýze provozu moderní technologie

- stále širší uplatnění je součást neodvratného procesu vývoje přístupů k zabezpečení požadavků na provoz moderní technologie
- využívá se paralelně s deterministickým přístupem, využití souvisí s poznáním hranic možností deterministické analýzy

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Základní oblasti využití pravděpodobnostní analýzy

- nejistota deterministických (fyzikálních) modelů (aplikace pravděpodobnostní analýzy zůstává přímou součástí modelu)
- ryze statistická analýza dat (zpracování údajů o daném prvku technologie, bez systémových vazeb)
- analýza spolehlivosti systému
- *analýza bezpečnosti* (rizika) provozu systému

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Specifické rysy analýzy spolehlivosti

- modelování *vazeb* mezi spolehlivostí systému a spolehlivostí jeho prvků
- libovolný počet úrovní přechodu od spolehlivosti prvku nižší úrovně ke spolehlivosti prvku vyšší úrovně, dynamicky volitelná struktura modelu reprezentující architekturu systému
- postup pravděpodobnostní charakteristiky *a její nejistoty* od nejnižší úrovně modelu až k úrovni vrcholové

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Specifické rysy analýzy bezpečnosti

- podobný charakter prostředků analýzy jako u analýzy spolehlivosti, z technického hlediska jiné cíle
- je možné zavést pojem rizika a kvantifikovat ho jako součin pravděpodobnosti a následků
- do pravděpodobnostního modelu je nutné integrovat *lidský faktor*

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Vývoj užití metodiky pravděpodobnostního hodnocení rizika - historie

- **šedesátá léta - vznik termínu PRA (Probabilistic Risk Assessment, pravděpodobnostní hodnocení rizika), v "neamerické" verzi PSA (Probabilistic Safety Assessment, pravděpodobnostní hodnocení bezpečnosti)**
- **šedesátá léta - vojenská oblast, kosmonautika**
- **sedmdesátá léta - jaderná energetika (WASH-1400 Study)**
- **osmdesátá léta - výrazný rozvoj ve všech běžných oblastech aplikací po známých havarijních událostech (Three-Mile Island, Černobyl)**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Vývoj užití metodiky pravděpodobnostního hodnocení - devadesátá léta

- **rozšíření na další technologie (chemické výroby, transport)**
- **rozšíření cílů a využitelnosti analýzy pro již pokryté technologie (propojení s ekonomikou provozu ve spojení se spolehlivostí (RCM) nebo bezpečností (RBM))**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Vývoj užití metodiky pravděpodobnostního hodnocení - stávající dekáda

- dochází k zásadním změnám v přístupu uživatele k metodice pravděpodobnostního hodnocení znalosti organizace a řízení
- analýzy se rozšiřují na další oblasti a zákazníky
- analýzy se počínají stávat *součástí legislativních požadavků*

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Spolehlivost a bezpečnost

- dvě úzce propojené, nicméně rozdílné úlohy
- cílem zvyšování *spolehlivosti* je zabezpečení lepšího plnění funkce systému (zvýraznění *pozitivního* výsledku práce systému)
- cílem zvyšování *bezpečnosti* je eliminování nežádoucích následků činnosti systému na jeho tvůrce (omezení *negativních* projevů práce systému)
- společný atribut - v obou případech závisí úroveň hodnocení systému na dosažené úrovni práce jeho prvků a zlepšení/zhoršení práce prvku vede k efektu stejné orientace u systému
- příčina odlišností v řešení úlohy - *okruhy prvků* zásadně ovlivňujících spolehlivost a bezpečnost systému mohou být *jiné*.

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické rysy současného pravděpodobnostního modelu průmyslové technologie

- rozklad systému na elementární prvky, jejichž úroveň práce lze popsat na základě provozní zkušenosti
- *jednoduché* pravděpodobnostní modely *elementárních* prvků
- *složitý* obsáhlý komplex elementárních prvků jako model systému
- vysoká spolehlivost elementárních prvků

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Cíle pravděpodobnostního hodnocení - spolehlivost

- ocenění spolehlivosti naplnění funkce systému ve vybraných místech soustavy
- dokumentování trendů vývoje spolehlivosti
- porovnání spolehlivosti (intra - jednotlivých bodů soustavy navzájem, inter - s jinými zástupci technologie)
- *operativní zásahy* do systému pro zabezpečení nejvyšší *okamžité* spolehlivosti
- spolehlivostně orientovaná údržba

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Cíle pravděpodobnostního hodnocení - bezpečnost

- prokázání dostatečně nízké úrovně rizika provozu (v porovnání s jinými zástupci technologie, s jinými zdroji rizika nebo s obecně akceptovatelnými riziky)
- hledání slabých míst systému z hlediska rizika (prověření hypotéz), eliminace slabých míst, prokázání zvýšené bezpečnosti
- rizikově orientovaná údržba

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - počátky existence

- předchůdcem bylo oddělení jaderné bezpečnosti ÚJV, které se soustředilo na aplikace deterministického přístupu a realizovalo široké spektrum termohydraulických analýz
- počátkem osmdesátých let minulého století se objevují v jaderné energetice první "klasické" analýzy spolehlivosti systémů
- v polovině osmdesátých let jsou realizovány první analýzy bezpečnosti a rizika v ÚJV, na úrovni jednotlivých systémů jaderné elektrárny
- od roku 1988 probíhá pětiletý úkol státního plánu zaměřený na pravděpodobnostní hodnocení bezpečnosti JE Dukovany
- řešení spolehlivostní problematiky podpořeno v osmdesátých letech regionálními projekty MAAE

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - devadesátá léta (1)

- do roku 1993 řešen úkol státního plánu, činnost oddělení kompletně financovaná státem
- od roku 1994 převážná část prostředků získaná na komerční bázi
- základem činnosti oddělení v tomto období vývoj a aplikace pravděpodobnostních modelů pro obě české jaderné elektrárny
- intenzivní transfer know-how od kooperujících organizací (NUS, SAYC)
- kursy a stáže MAAE, zapojení do mezinárodní spolupráce

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - devadesátá léta (2)

- druhá polovina devadesátých let typická značným rozšířením záběrů analýzy
- revize PSA studií z první poloviny devadesátých let
- PSA druhé úrovně
- PSA provozu na nízkém výkonu a odstávky
- monitor rizika
- oceňování modifikací projektu a provozu elektrárny
- hodnocení Limit a podmínek provozu elektrárny
- detailní analýza procedurálního popisu havarijních scénářů

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - devadesátá léta (3)

- záběr analýz rozšířen mimo oblast jaderné energetiky
- pravděpodobnostní hodnocení bezpečnosti výzkumného reaktoru LVR-15
- bezpečnostní analýzy ve Spolaně Neratovice
- hodnocení kritických míst potrubních systémů MERO
- příprava managementu spolehlivosti v TRANSGAS a.s.
- v oblasti jaderné energetiky široká účast na grantových projektech MPO

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - devadesátá léta (4)

- PSA studie slovenských jaderných elektráren Jaslovské Bohunice V-2 a Mochovce
- PHARE projekty (regionální banka dat, ředění chladiva primárního okruhu)
- projekty US DOE (Department of Energy - sběr dat na plnorozsahovém trenažéru, monitor rizika)
- projekty MAAE (projekty porovnání harmonizace PSA studií pro jaderné elektrárny VVER-440 a VVER-100, hodnocení PSA studií jiných elektráren - mise IPSART, regionální projekty)
- činnost pracovních skupin OECD NEA (PWG1 - provozní události, PWG-5 - analýzy rizika, SEGHOF - organizační faktory)

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Oddělení analýz spolehlivosti a rizik ÚJV Řež - Reference

- výsledky analýz spojených s PSA studiemi publikovány každoročně v obsáhlé dokumentaci projektu PSA
- interní zprávy v rámci jednotlivých projektů
- příspěvky ke studiím MAAE (IAEA TECDOC)
- referáty na zahraničních i českých odborných konferencích (PSA99, NUSIM, ESREL, PSAM)
- příspěvky do odborných časopisů (Bezpečnost jaderné energie, Nucleon, Reliability Engineering)

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Pravděpodobnostní model bezpečnosti provozu jaderné elektrárny

- složitá struktura založená na Booleovské logice zahrnující několik tisíc elementárních prvků
- každý elementární prvek vybaven jednoduchým spolehlivostním modelem

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typy primárních událostí

- intenzity poruch komponent (kontinuálně pracující komponenty, vyčkávající komponenty)
- pravděpodobnosti selhání komponent na vyzvání
- pravděpodobnosti lidských selhání
- pravděpodobnosti residuálních násobných poruch se společnou příčinou
- nepohotovosti komponent z důvodu údržby
- speciální události

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Kvantifikace parametrů primárních událostí

- generická data
- specifická data
- Bayesovský přístup, Bayesova věta, aplikace konjugovaných systémů apriorních rozdělení
- expertní odhad
- analytické metody (pravděpodobnosti lidských selhání)

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Modelování poruchovosti komponent

- pro poruchy vznikající náhodně v čase se využívají zjednodušující předpoklady - Poissonovský proces, exponenciální rozdělení doby mezi poruchami, lineární aproximace, komponenta nestárne, konstantní intenzita poruch
- pro poruchy na vyzvání přímý odhad
- u vyčkávajících komponent se řeší otázka poměru poruch s latentním efektem a poruch vznikajících při šokové změně stavu

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

(Reziduální) poruchy se společnou příčinou

- architektura hodnocených systémů typická vysokou úrovní zálohovanosti, ale obvykle omezenou diverzibilitou
- funkční závislosti řešeny přímo v logice modelu daného systému
- zbytkové závislosti ošetřeny pomocí speciálních událostí reprezentujících společná selhání skupin komponent
- kvantifikace založena na předpokladu velmi silné korelace mezi frekvencí nezávislých selhání a násobných poruch

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Modelování spolehlivosti člověka

- základní předpoklad: spolehlivost člověka lze analyzovat, popsat a kvantifikovat
- odlišný typ zpracování informace než u spolehlivosti hardware
- mnohem vyšší variabilita lidských selhání
- vyšší dynamika změny podmínek ovlivňujících lidskou spolehlivost
- kromě stálých externích podmínek závisí lidská spolehlivost mnohem více na atributech aktuální situace
- k odhadu spolehlivosti nelze využít přímé statistiky

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Modelování spolehlivosti člověka (2)

- na rozdíl od spolehlivosti komponent neexistuje konsensus v otázce metodiky
- různé metody založené na ocenění typu činnosti a bezprostředně působících externích faktorů (THERP, TCR, metody rozhodovacích stromů)
- metody založené na přímém využití expertního odhadu přes panel expertů (APJ, SLIM), specifické rysy daného úkolu
- problémy s modelováním spolehlivosti kognitivních činností fyziologické vlivy
- druhá generace metod analýzy spolehlivosti obsluhy (pojem EFC - error forcing context) - ATHEANA, CREAM, zčásti řeší problematiku kognitivních akcí, zavádí dělení na "errors of omission (EOM)" a "errors of commission (EOC)"

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Clayton Tunnel Collision

- těžká havárie vlaků v tunelu, 25.srpna 1861, 23 mrtvých a 176 těžce zraněných
- na svou dobu velmi sofistikovaný systém prevence havárie, avšak ve svém důsledku podílející se na vzniku havárie
- typická kombinace selhání automatiky, vzniku EFC a vícečetného selhání obsluhy, primárně spojeného s kognitivní činností
- klíčové selhání obsluhy patří do kategorie EOC
- dodatečná kvantifikace frekvence vzniku havárie prokazuje, že zdánlivě odolný systém byl typický relativně vysokým potenciálem pro vznik havárie během svého provozování

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Kvantifikace PSA modelu jako celku

- z hodnot parametrů primárních událostí se dle pravidel Booleovské logiky odvodí odhad pravděpodobnostní charakteristiky vrcholové události
- jde o náročný proces, který byl do nedávné doby na osobních počítačích obtížně zvladatelný
- pro kvantifikaci se používá v podstatě výhradně komerční software (RISK SPECTRUM, NUPRA, IRRAS), velmi náročné požadavky na kapacitu a na rychlost (je nutné kombinovat tisíce základních prvků modelu a počet kombinací extrémně rychle narůstá)
- ke zvládnutí výpočtu je nutné vhodně definovat úroveň přesnosti analýzy (úroveň pro odseknutí nevýznamných havarijních scénářů ze souboru výsledků)

Analýza nejistot

- každý parametr spolehlivostního modelu primární události je popsán nikoli bodovou hodnotou, ale pravděpodobnostním rozdělením a jeho parametry
- součástí kvantifikace PSA modelu je kombinování pravděpodobnostních rozdělení a postupná propagace nejistoty až k nejistotě odhadu pravděpodobnostní charakteristiky vrcholové události

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Analýza nejistot (2)

- základní metodou pro kombinování pravděpodobnostních rozdělení při postupu nejistoty logikou PSA modelu je simulace Monte Carlo
- odhad každého spolehlivostního parametru vstupujícího do PSA modelu se řídí zásadou být na konzervativní straně
- omezené možnosti analýzy vedly v minulých obdobích rozvoje PSA k relativně velké *konzervativnosti* modelu, zlepšení podmínek analýzy v současné době má za následek přechod k *best-estimate* odhadům v některých oblastech

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické výstupy studie PSA

- **frekvence vzniku nežádoucí události**
- **pravděpodobnostní rozdělení modelující nejistotu odvozené frekvence vzniku vrcholové události**
- **seznam minimálních kritických řezů**
- **importanční míry dle zadání analýzy**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Importanční míry

- **Fussell-Vesely**
- **risk-increase faktor**
- **risk-decrease faktor**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické hodnoty rizika provozu jaderné elektrárny (CDF)

- 10^{-3} - ***nevyhovující***, **zcela nepřijatelná úroveň rizika**
- 10^{-4} - ***běžná*** **úroveň rizika v** ***osmdesátých*** **letech, především u** ***starších reaktorů*** **nebo reaktorů méně progresivních tříd (RBMK s kladným koeficientem reaktivity), tuto úroveň rizika měly i československé reaktory před přijetím velkého množství nákladných opatření ke zvýšení bezpečnosti**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické hodnoty rizika provozu jaderné elektrárny (2)

- 10^{-5} - **současná úroveň rizika jednotlivých bloků obou českých jaderných elektráren, obecně přijímaná úroveň rizika pro reaktory z minulých desetiletí s perspektivou několika desetiletí provozu**
- 10^{-6} - **nízká úroveň rizika, prokázání možností dosažení této úrovně se vyžaduje u nových projektů jaderně-energetických bloků**

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Charakter výstupů spolehlivostní (bezpečnostní) analýzy

- přirozeným výstupem pro provoz s kvalitně ošetřenou spolehlivostí a bezpečností je rozdělení potenciálu pro selhání do většího množství přispěvatelů
- omezený počet silně dominujících scénářů indikuje slabiny v projektu nebo provozování
- první fáze využití pravděpodobnostního hodnocení se soustřeďuje na identifikaci a korekci konečného počtu výrazných slabin, na konci této fáze dochází k výraznému zvýšení bezpečnosti a/nebo spolehlivosti systému
- v další fázi využití je dynamika zvyšování spolehlivosti systému nižší, je však žádoucí udržet jistý trend zlepšování spolehlivosti

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické hodnoty spolehlivostních parametrů

- frekvence iniciačních událostí - velká variabilita, od řádu $5x10^{-1}$ (jednou za dva roky, zásah havarijní ochrany se všemi systémy dostupnými) až po řád 10^{-5} (prasknutí potrubí primárního okruhu velkého průměru)
- intenzita poruch významných komponent - od řádu $5x10^{-3}$ (poruchy běhu havarijních čerpadel) až po řád 10^{-7} (intenzita vzniku poruchového mechanismu selhání relé, zpětné klapky)
- podmíněná pravděpodobnost poruchy jedné větve bezpečnostně významného systému při požadavku na zásah po vzniku iniciační události - řádu 10^{-3} - 10^{-4}
- podmíněná pravděpodobnost poruchy celého bezpečnostně významného systému při požadavku na zásah po vzniku iniciační události - řádu 10^{-4} - 10^{-5}

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické hodnoty spolehlivostních parametrů (2)

- nepohotovost jedné větve bezpečnostně významného systému z důvodu údržby - řádu 10^{-3} (poměrně malý rozptyl hodnot)
- podmíněná pravděpodobnost vzniku násobné poruchy se společnou příčinou za předpokladu, že došlo k poruše nejméně jedné komponenty ze skupiny podléhající potenciálu pro znásobení poruchy - řádu $5x10^{-2}$, pro násobnou poruchu většího množství komponent řádu 10^{-3}
- pravděpodobnost selhání obsluhy - (od řádu 10^{-1} do řádu 10^{-4} podle aktuálních vnějších podmínek)
- chybový faktor pro odhad nejistoty bodového odhadu modelované lognormálním rozdělením (podíl 95%ního kvantilu a mediánu rozdělení) - 2-3 pro komponenty s relativně dobrou statistikou, 5 pro pravděpodobnosti selhání obsluhy, 8-10 pro násobné poruchy větších skupin komponent a frekvence málo pravděpodobných iniciačních událostí

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Typické vlastnosti spektra scénářů dominujících riziku

- dominují havarijní scénáře zahrnující lidské chyby a násobná selhání
- během posledních deseti let došlo k mnoha změnám v příspěvku konkrétních scénářů způsobených 1)změnami projektu a provozu elektrárny 2)změnami v přístupu k PSA
- v počátečním období rozvoje PSA se pozornost soustředila na maximální projektové havárie (velká LOCA)
- další období je charakteristické postupným objevováním slabin projektu a provozu JE a soustředěním pozornosti na zcela odlišné (obecně komplikovanější) scénáře (současná ztráta prostředků pro odvod zbytkového tepla sekundárním okruhem)
- v posledním období jsou již na řadě JE přijata opatření eliminující rizikový příspěvek slabin projektu (přeložení kolektoru systému superhavarijního napájení na EDU) a do popředí se dostávají další scénáře (malá LOCA)

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Otázky využití výstupů analýzy spolehlivosti a rizika

- současné výsledky analýz spolehlivosti a rizika mají relativně vysoký kredit
- metoda PSA přestává být chápána jako doplněk "deterministické analýzy" a stává se plnohodnotným zdrojem podkladů pro rozhodování managementu
- podpora metody vychází z osobní zkušenosti špičkových specialistů elektrárny, jejichž rozsah aktivit přesahuje do oblastí spojených s rizikem provozu
- metoda je přinejmenším využívána jako podpora prosazení smysluplných argumentů vedoucích ke snížení rizika provozu
- v současné době je tento typ analýz již využíván i při klasickém decision-making problému - výběru z několika alternativ

Ústav jaderného výzkumu Řež a.s.
Oddělení analýz spolehlivosti a rizik

Změny v přístupu uživatele k metodice pravděpodobnostního hodnocení

- *první fáze* - pravděpodobnostní analýza je neověřenou *novinkou*, zajímavou, ale spornou investicí
- *druhá fáze* - pravděpodobnostní analýza je *úkolem* - prostředkem naplnění konkrétních požadavků
- *třetí fáze* - pravděpodobnostní analýza je *procesem* - stále přítomnou součástí řízení provozu
- *čtvrtá fáze* - pravděpodobnostní analýza je společným *způsobem myšlení* analytika a uživatele