ČESKÁ SPOLEČNOST PRO JAKOST

Novotného lávka 5, 116 68 Praha 1

SPOLEHLIVOST LIDSKÉHO ČINITELE PŘI PROVOZU MODERNÍ TECHNOLOGIE

Materiály z 44. setkání
odborné skupiny pro spolehlivost

Praha, září 2011

OBSAH:

VÝVOJ A SOUČASNÝ STAV PŘÍSTUPŮ K ŘEŠENÍ PROBLEMATIKY LF PŘI PROVOZU SLOŽITÝCH TECHNOLOGIÍ S VYSOKOU MÍROU AUTOMATIZACE

RNDr. Jaroslav Holý, Ústav jaderného výzkumu Řež

Mgr. Jan Kubíček, Ústav jaderného výzkumu Řež

1. Úvod

Provoz jaderných elektráren v České Republice i ve světě je v éře jaderné energetiky teprve se vyrovnávající s událostmi v japonské Fukušimě typický ještě větším důrazem na zajištění bezpečnosti. Obsluha jaderné elektrárny hraje při řešení bezpečnostních aspektů klíčovou roli svou účastí na bezprostředním řízení provozu, organizování a inženýrské podpoře procesů zde probíhajících, údržbě a testech zařízení a vytváření obecné perspektivy a vize naplnění účelu jaderné elektrárny jako efektivního a bezpečného zdroje energie. Zvyšování bezpečnosti provozu jaderné elektrárny jako typického zástupce moderní složité technologie, pracující na měřitelné a někdy vysoké úrovni rizika, se proto nemůže obejít bez detailní analýzy vlivu lidského prvku a zformulování, přijetí a realizace opatření vzniklých na jejím základě.

Význam obsluhy pro zajištění bezpečnosti provozu byl chápán a zdůrazňován v celé historii jaderné energetiky. Existuje řada jednotlivých témat a oblastí **projevů** lidského faktoru a vytváření co nejlepších **podmínek** pro kvalitní a bezpečnou práci obsluhy, které byly od samotného počátku provozování českých jaderných elektráren intuitivně chápány jako důležité a zvládány k relativní spokojenosti, jako například výběr zaměstnanců, jejich výcvik a vzdělávání, rozdělení funkcí a odpovědnosti nebo tvorba kvalitního, uživatelsky přátelského prostředí pro interakci operátora se zařízením elektrárny.

Jaderná elektrárna je však nesmírně složitý organismus a celosvětová provozní zkušenost jaderné energetiky postupně přináší závažné příklady toho, že ani dobré zvládnutí všech intuitivně vytipovaných oblastí zajištění kvalitní práce obsluhy nemusí přinést dostatečnou míru prevence výskytu mimořádných poruchových stavů s těžkými potenciálními následky, na nichž se lidský faktor podílí výraznou měrou. Proto se v širším záběru řešení různých otázek bezpečnosti celého jaderně-energetického komplexu, při hledání prostředku co nejobjektivnějšího spojení všech podstatných složek zajištění bezpečnosti do jediného integrovaného modelu, umožňujícího co nejlépe postihnout všechny podstatné souvislosti a interakce, identifikovat pokud možno všechny scénáře narušení bezpečnosti a definovat priority pro vyrovnání se s nimi dle jejich očekávané závažnosti, jako nástroj uplatňují metody pravděpodobnostního hodnocení bezpečnosti (*probabilistic safety assessment*, PSA).

2. Lidský faktor jako součást pravděpodobnostních modelů bezpečnosti provozu jaderné elektrárny

Metody PSA se opírají o dva fundamentální pojmy, které znamenají výrazné zobecnění tradičního deterministického přístupu k zajištění bezpečnosti - primárně o pojem **pravděpodobnosti** a zprostředkovaně, s využitím pravděpodobnosti, o pojem **rizika**. „*Riziko*“, tj. pojem, který je pro moderní hodnocení bezpečnosti elektrárny i role lidského faktoru klíčový, lze s využitím pravděpodobnostní míry definovat následovně

RIZIKO = PRAVDĚPODOBNOST x NÁSLEDKY.

PSA model jaderné elektrárny je koncipován jako prezentace souboru scénářů (ne)vedoucích na postulovanou nežádoucí událost - poškození aktivní zóny reaktoru. Poškození reaktoru je komplikovanou a nepravděpodobnou událostí vyžadující si narušení celé řady bariér, záměrně nebo implicitně vystavěných proti jejímu vzniku. Proto se nepředpokládá, že by k takové události došlo ad hoc, neočekávaně, ale naplnění její definice je podmíněno postupným výskytem řady událostí, počínaje prvotní, **iniciační událostí**, přes sekvenci dalších **selhání** zařízení nebo **obsluhy**, až k finálnímu negativnímu důsledku. Lidský faktor se v tomto schématu může objevit v negativní roli (přibližující vznik nežádoucí události) nebo i pozitivní roli (správným zásahem přetrhnuvší řetězec jevů k nežádoucí události vedoucích) v podstatě na libovolném místě havarijní sekvence událostí, počínaje iniciační událostí a konče úspěchem nebo neúspěchem akce poslední záchrany (obvykle spojené se zajištěním kritické bezpečnostní funkce) rozhodující o poškození aktivní zóny. Navíc mohou mít lidská selhání i vnější a latentní vlivy na havarijní scénáře, pokud v průběhu testu nebo údržby během normálního provozu nebo při odstávce elektrárny vedou ke skrytému poruchovému stavu zařízení, který přetrvá až do eventuálního požadavku na jeho funkčnost ve specifických podmínkách havarijního scénáře.

Analýza lidského faktoru, která je v kontextu PSA studie, využívající pravděpodobnostních a rizikových pohledů, nazývaná „analýzou spolehlivosti lidského činitele“ (*human reliability assessment*, HRA), je víceméně součástí všech složek pravděpodobnostního hodnocení bezpečnosti. Na počátku PSA studie je definováno spektrum prvotních iniciačních událostí, které při shodě nepříznivých okolností v havarijní sekvenci dalších událostí mohou vést až k poškození aktivní zóny, a lidský faktor může být původcem řady z nich. Zde se poměrně výrazně odlišuje PSA studie reaktoru při provozu na nominálním výkonu (*full power PSA*, FPSA), kde je převážná většina funkcí zařízení elektrárny při výrobě elektrické energie zajišťována automaticky a podíl obsluhy, pouze kontrolující správnou funkci zařízení, bezprostředně na vzniku iniciačních událostí je spíše malý, a PSA studie provozu při změnách výkonu, odstavování, odstávce a najíždění reaktoru na výkon (*low power and shutdown PSA*, LPSD PSA), kde je zapojení obsluhy do řídící a regulační činnosti mnohem větší a narůstá i potenciál pro vznik iniciační událostí obsluhou způsobené.

Selhání funkce libovolného elementu účastnícího se sekvence událostí v havarijním scénáři, včetně selhání obsluhy při konkrétní akci, je v PSA modelu elektrárny zastoupeno tzv. primární událostí (*basic event*, BE). Příkladem lidského selhání může být nenastartování čerpadla havarijního chlazení (jehož důsledkem je nedodání potřebného množství chladiva do primárního okruhu po prasknutí některého segmentu jeho potrubí) nebo neodtlakování vybrané části potrubí sekundárního okruhu. Každá primární událost v PSA modelu, tedy i událost modelující selhání obsluhy, je opatřena pravděpodobnostním ukazatelem - číselnou hodnotou pravděpodobnosti výskytu. V pravděpodobnostním modelu elektrárny jsou primární události spojeny pomocí základních logických operátorů „A“, „NEBO“, eventuálně „NEGACE“ do větších celků - stromů poruch. Stromy poruch pak tvoří vstupy do nejvyšších úrovní složitého modelu elektrárny - stromů událostí, jejichž logika modeluje možnou posloupnost jevů v havarijních sekvencích. Primární události modelující lidská selhání jsou v PSA modelu elektrárny prvky stromů poruch i stromů událostí, význam lidských selhání modelovaných ve vrcholové logice stromů událostí přitom logicky bývá větší.

Role HRA počíná systematickým zahrnutím lidského prvku do pravděpodobnostního modelu elektrárny, protože bez něj by byl model málo vypovídající. Poměrně náročná analýza zahrnuje **identifikování** všech důležitých akcí obsluhy, jejichž přítomnost ve formě

primárních událostí je v realistickém PSA modelu nezbytná, optimální strukturování činností obsluhy a vhodné umístění jejich **reprezentace** ve formě primárních událostí na „správná“ místa PSA modelu tak, aby byly co nejlépe zohledněny všechny důležité vazby a závislosti. Na vstupní „poziční“ část analýzy navazuje část **matematická**, odvození pravděpodobností selhání, vycházející z komplexní analýzy konkrétních podmínek každého modelovaného lidského zásahu (dostupnost specifických i obecných informací o stavu zařízení pro obsluhu, úroveň výcviku a zkušenosti obsluhy s daným scénářem, kvalita procedurální podpory, očekávaný stres obsluhy a dynamika vývoje procesů, na které musí obsluha reagovat atd.). Výsledkem této fáze analýzy je soubor primárních událostí modelujících spolehlivost lidského činitele, svým umístěním v modelu dobře reprezentující realitu očekávaných dějů, a vzájemně vyvážených číselných hodnot pravděpodobností jejich vzniku.

Vytvořením vstupů popisujících v PSA modelu roli lidského prvku však končí pouze kapacitně i metodicky náročná *první část* analýzy spolehlivosti lidského činitele. Hlavní vypovídací potenciál analýz HRA se totiž uplatní až následně, kdy je s pomocí speciálního software odhadnuto celkové riziko provozu elektrárny, je identifikována váha všech rizikových přispěvatelů (mimo jiné i všech jednotlivých akcí obsluhy) a jsou nalezeny kritické kombinace prvků modelu, jejichž výskyt vede ke vzniku nežádoucí události, ve formě tzv. minimálních kritických řezů (*minimum cut sets*, MCS). Jedná se o nejmenší množiny událostí, jejichž společný výskyt v havarijním scénáři vede ke vzniku vrcholové nežádoucí události, a při absenci jakékoli události z této množiny již vrcholová událost (poškození aktivní zóny reaktoru) nenastane. Logickým důsledkem důležité role obsluhy při řešení scénářů odezvy na vznik iniciační události, kdy se v rozhodující většině možných scénářů předpokládá, že obsluha by měla mít možnost správným korektivním činem zablokovat další rozvoj mimořádného stavu, je to, že téměř každý minimální kritický řez obsahuje alespoň jednu primární událost spojenou se selháním lidského prvku (scénáře, které by žádnou takovou událost neobsahovaly, jsou lidským prvkem nekontrolované).

Mnohé minimální kritické řezy obsahují nikoli jednu, ale více primárních událostí zastupujících selhání lidského činitele. V takovém případě je vždy nutné vzít (alespoň dodatečně) v úvahu možnou závislost mezi těmito selháními, protože příslušné činnosti jsou realizovány v časové posloupnosti společného scénáře a **neúspěch akcí prováděných dříve vždy teoreticky ovlivňuje potenciál pro zvládnutí těch následujících**. Jestliže **P(A)** je pravděpodobnost selhání lidského zásahu **A**, **P(B)** pravděpodobnost selhání lidského zásahu **B** a **P(AB)** pravděpodobnost selhání **obou** zásahů v rámci jednoho výskytu konkrétního havarijního scénáře, neplatí obecně v praxi vztah

P(AB) = P(A) x P(B)

ale spíše vztah

P(AB) > P(A) x P(B) nebo dokonce **P(AB) >> P(A) x P(B),**

kde nalezení hodnoty rozdílu

P(AB) - P(A) x P(B)

je bohužel v praxi často velmi obtížné a nebývá součástí běžného vybavení metodických postupů aplikovaných při analýzách HRA (v podstatě jediný alespoň částečně sofistikovaný návod pro kvantifikaci pravděpodobností selhání závislých akcí je součástí klasické metodologie **[1]**). Mechanismy závislosti, zvyšující hodnotu součinu pravděpodobností P(A) a

P(B) odvozenou za předpokladu nezávislosti akcí A, B, lze v kontextu analýzy interpretovat dvěma způsoby:

- selhání první akce A se ani nemusí projevit na evidentním přímém zhoršení podmínek pro akci B, ale již to, že k němu (jako relativně velmi málo pravděpodobnému jevu) došlo, prokazuje existenci jistého skrytého problému, u kterého není garantováno, že se neprojeví u následující akce B (náhlá „skrytá“ indispozice operátora)
- selhání první akce A zatíží podmínky provádění následující akce B dodatečnými negativními faktory a zvýší pravděpodobnost selhání akce B oproti případu, kdy by k selhání akce A nedošlo (typickým případem je zvýšení stresu po selhání se všemi jeho negativními dopady).

Pravděpodobnosti závislých selhání jsou dle metodiky v **[1]** víceméně dominantně určeny úrovní závislosti na předchozí selhavší akci a jen v malé míře ovlivněny novými skutečnostmi specifickými pro akci B a nepřítomnými při provádění selhavší akce A. Pravděpodobnosti selhání vycházející ze závislostí jsou přitom relativně vysoké - od hodnot řádu 10^{-2} pro velmi nízkou úroveň závislosti přes cca $5x10^{-2}$ pro střední závislost až k hodnotám o velikosti $5x10^{-1}$ pro silnou závislost. Při maximální míře závislosti, tzv. *úplné závislosti* nebo také *kompletní závislosti*, je pravděpodobnost selhání závislé akce přirozeně rovna jedné.

Dalším velmi důležitým výstupem softwarového zpracování PSA modelu je přidělení důležitosti (importační míry, *importance measure*) každé primární události. Klasický algoritmus sestavení množiny minimálních kritických řezů a odvození pravděpodobnosti nežádoucí události poskytuje určitý odhad relativní důležitosti každé primární události modelu (primární událost je důležitá, když je přítomná v minimálních kritických řezech zatížených největšími frekvencemi výskytu). Tento jednoduchý princip však neposkytuje dostatek materiálu pro kompaktní analýzu celého souboru událostí a vzájemné srovnání jeho prvků, zejména neumožňuje seřadit jednotlivé primární události podle jejich skutečného významu pro riziko provozu jaderné elektrárny, který je kromě číselné hodnoty pravděpodobnostního parametru ovlivněn především umístěním v hierarchii logiky modelu elektrárny. Protože je celý PSA model elektrárny velmi složitý a rozsáhlý organismus, není práce s ním při kvantifikování důležitosti jednotlivých komponent triviální.

3. Přístupy uplatňované k analýze spolehlivosti lidského činitele v ÚJV Řež

Analýzy spolehlivosti lidského činitele se v ÚJV Řež opírají o multi-metodický, hybridní přístup, založený na dobré znalosti většiny nejpoužívanějších metodických postupů (THERP, ASEP, SLIM, HEART, NARA. Decision trees, ATHEANA, CREAM) a výběru vhodné metody analýzy **na míru** hodnoceným akcím obsluhy (viz **[2]**, **[3],** **[4]**, **[5]**, **[6]**, **[7]**, **[8]**, **[9]**). Výběr vhodné metodologie a její aplikace je pouze jednou stránkou analýzy HRA, jejíž naplnění ještě nepostačuje k zajištění dostatečné kvality analýzy. Minimálně stejně důležitou a časově mnohem náročnější součástí analýzy je získání představy o technickém pozadí hodnocených akcí obsluhy. Jako zdroje informace se zde nabízejí procedurální postupy upravující činnost obsluhy (v provozu a při různých druzích výcviku), konzultace se specialisty elektrárny a informace o příbuzných událostech z evidované provozní historie. Teprve v prostředí bohaté informace o všech aspektech činnosti prováděné obsluhou mohou vyniknout silné stránky vhodně zvolené metody HRA a zpracovatel analýzy může obdržet věrohodný soubor výsledků, na němž lze založit rizikově orientované rozhodování.

Hlavním cílem převážné části prací realizovaných ve studiích HRA je získání vstupů pro kvantifikaci primárních událostí modelu PSA zastupujících projevy lidského faktoru a jejich vhodné umístění do logiky modelu. Pravděpodobnosti selhání akcí obsluhy jsou výsledkem míry ovlivnění vlastními podmínkami akce a vnějšími podmínkami podporujícími nebo ztěžujícími realizaci činností. Z faktorů výrazně se projevujících při práci obsluhy na českých jaderných elektrárnách lze uvést například interpretaci procedur, vyšší úroveň stresu v náročných podmínkách mimořádného stavu, dynamičnost scénářů a interakci obsluhy se zařízením na rozhraní člověk-stroj. Na druhé straně umožňují tyto analýzy vyzdvihnout i pozitivní rysy podmínek práce obsluhy snižující potenciál pro selhání - dobrou úroveň výcviku, kvalitně pracující systém zpětné vazby nebo vhodné načasování scénářů bez extrémních požadavků na rychlost činnosti.

Odvozené pravděpodobnosti selhání se u činností obsluhy českých i zahraničních jaderných elektráren pohybují ve velmi širokém rozmezí daném rozsahem možných typů akcí a vnějších podmínek jejich provádění - od akcí s pravděpodobností selhání větší než 10^{-1}, které jsou však nepříliš četným prvkem modelu PSA, přes „běžné“ pravděpodobnosti selhání řádu 10^{-2} u relativně náročných činností, k pravděpodobnostem řádu 10^{-3} u činností jednoduchých, s dobrou vnější podporou a pravděpodobnostem řádu 10^{-4} u málo náročných činností, na jejichž realizaci je řada hodin. Vzhledem k obecnému pojetí pravděpodobnostních modelů bezpečnosti rizikových technologií, preferujících konzervativní pohled na věc, a vzhledem k permanentně přítomným závislostem mezi selháními v celém průběhu havarijního scénáře není užití pravděpodobností selhání menších než 10^{-4} v drtivé většině případů pro akce obsluhy jaderné elektrárny ospravedlnitelné.

4. Příklady projektů analýzy spolehlivosti lidského činitele v ÚJV Řež

Kromě využití při tvorbě PSA modelů, kdy je cílem HRA především zabezpečit **podklady** pro modelování a kvantifikaci lidského vlivu na bezpečnost provozu elektrárny, je HRA ve spojení s obecnějšími kvalitativními principy analýzy lidského faktoru (*human factor analysis*) využívána i k přímým aplikacím podporujícím procesy každodenního bezpečnostního a rizikově orientovaného rozhodování, řešení otázek a priorit provozu, výběru z konkrétních alternativ zajištění podmínek práce obsluhy atd. Z analýz realizovaných v poslední dekádě v Oddělení analýz spolehlivosti a rizik ÚJV Řež pro JE Dukovany lze vybrat například:

- systematické analýzy ergonomie symptomově založených procedur **[10]**
- analýzy specifických projevů faktorů a vnějších podmínek přímo ovlivňujících práci obsluhy **[11]**
- analýzy projevů lidského faktoru v provozní historii elektrárny **[12]**
- analýzy komunikace v provozu elektrárny **[13]**
- periodické hodnocení bezpečnosti pro Oblast 12 - lidský faktor **[14]**
- návrh metodiky pro výběr témat pro výcvik obsluhy BD na trenažéru **[15]**
- hodnocení návrhu sloučení lokálních dozoren do větších celků **[16]**
- hodnocení návrhu pro redukci obsazení směny EDU **[17]**
- vývoj výpočetního prostředku pro semi-automatickou kvantifikaci pravděpodobností selhání obsluhy při provozu elektrárny **[18]**.

Vývoj PSA modelů českých JE pokračoval i v posledních letech a spolu s ním byl dále zdokonalován způsob modelování i kvantifikace pravděpodobností selhání akcí obsluhy. Jako nejdůležitější aktivity lze v tomto směru uvést tyto projekty:

- revize analýzy spolehlivosti lidského činitele v rámci PSA modelu JE Dukovany, revize analýzy spolehlivosti lidského činitele v rámci PSA modelu JE Temelín, inženýrskou podporu provozu českých JE
- lidský faktor ve scénářích seismické události – pro seismickou pravděpodobnostní studii bezpečnosti JE Dukovany
- lidský faktor ve scénářích externích přírodních událostí (v reakci na události na JE Fukušima)
- vliv plánovaných modifikací, navržených s cílem zefektivnit provoz elektrárny, na lidský faktor (analýza lidského faktoru jako část *management of change*).

Významným zdrojem potenciálu pro budování inženýrské podpory řešení problematiky lidského faktoru na českých JE v posledních letech je grantový projekt MPO „Výzkum nástrojů a metod řízení pro zvyšování spolehlivosti lidského činitele v provozu JE“, který byl zahájen koncem roku 2008 a bude ukončen v roce 2011. Tento projekt řeší problematiku lidského faktoru ve čtyřech etapách:

- Etapa E1: vytvoření české báze znalostí o problematice lidského faktoru
- Etapa E2: vývoj koncepce podpory operátora současné blokové dozorny
- Etapa E3: sběr dat na trenažéru blokové dozorny jako vydatný datový zdroj pro analýzy lidského faktoru
- Etapa E4: organizační faktory a prezentace lidského faktoru a rizika provozu jaderné elektrárny veřejnosti.

Specialisté ÚJV Řež se v poslední dekádě rovněž postupně stali vyhledávaným partnerem pro mezinárodní projekty rizikově orientované analýzy lidského faktoru. Mezi nejvýznamnější projekty z oboru s účastí ÚJV patří například:

- spolupráce s mezinárodní atomovou agenturou ve Vídni (MAAE) na regionálních projektech zaměřených na harmonizaci projektů PSA pro reaktory VVER (viz **[19]**, **[22]**)
- spolupráce s IFE Halden na využití experimentálních dat pro specifikaci a hodnocení faktorů ovlivňujících spolehlivost obsluhy **[23]**
- účast na aktivitách pracovních skupin CSNI NEA (WGRISK, WGHOF, WGOE), která poskytla náplň například pro prezentaci **[25]**
- mezinárodní empirická studie HRA pro porovnání metod kvantifikace lidské spolehlivosti koordinovaná IFE Halden a U.S. NRC **[20]**
- projekt MMOTION 7.rámcového programu EU, organizačně zajišťovaný EdF – roadmap budoucích aktivit v oblasti lidského faktoru v Evropě **[21]**
- americká „follow-up“ studie pro další porovnání metod analýzy lidské spolehlivosti **[24]**.

V průběhu let 2006-2009 byl v oddělení analýz spolehlivosti a rizik v ÚJV Řež vyvinut v prostředí Access 2003 nástroj určený k analýze spolehlivosti lidského činitele v podmínkách provozu jaderných elektráren **[18]**. Cílem jeho vytvoření bylo získat prostředek umožňující rychlou a snadnou kvantifikaci pravděpodobností selhání lidského činitele pomocí

výpočetních modulů vycházejících z různých celosvětově užívaných metod analýzy spolehlivosti lidského činitele a zautomatizovat tak řadu činností v procesu kvantifikace, aby se specialisté na problematiku lidského faktoru mohli o to více soustředit na technickou podstatu analýzy.

Z množství v současnosti nejčastěji používaných metod kvantifikace pravděpodobností selhání činností obsluhy bylo vybráno a do kalkulátoru implementováno následujících pět metod:

- THERP **[1]** jako fundamentální, klasická metoda pokrývající velkou část rozsahu a variability projevů lidského faktoru v práci obsluhy na jaderné elektrárně
- ASEP **[7]** jako zjednodušená varianta metodiky THERP vhodná pro rychlou orientační kvantifikaci pravděpodobností selhání
- HEART **[3]** jako specifická metoda pomáhající kvantifikovat činnosti obsluhy probíhající za speciálních podmínek, metodou THERP obtížně postižitelných
- Metoda rozhodovacích stromů **[4]** jako moderní transparentní, relativně přesná metoda pro činnosti obsluhy realizované s dobrou procedurální podporou, nejčastěji se opírající o symptomově založené procedury
- CREAM **[6]** jako metoda nové generace umožňující hodnotit pravděpodobnost selhání akcí vyžadujících výrazné zapojení kognitivních funkcí (bez procedurální podpory).

Zahrnutí širšího spektra metod dává analytikovi jednak možnost validace uskutečněné analýzy pomocí jiné nezávislé metody a jednak velice zajímavé porovnání výsledků užití odlišných přístupů. Takový postup není ani v současné době ve světě zcela běžný (bez ohledu na kvalitu a hloubku analýzy HRA týmy obvykle používají jedinou metodu) a začíná se prosazovat až v posledních letech pod termínem *hybridní*. HRA kalkulátor je použitelný pro hodnocení všech typických kategorií selhání obsluhy jaderné elektrárny - činností údržby s latentním efektem na pozdější pohotovost zařízení, příspěvků selhání obsluhy ke vzniku iniciační události i selhání obsluhy v rámci odezvy na takovou událost.

Samotná kvantifikace pravděpodobností selhání se nutně opírá o charakter a podmínky analyzované činnosti obsluhy a a o generická data, která jsou součástí užitých metodik. Tyto informace jsou uloženy v **databázi** kalkulátoru, která umožňuje flexibilně doplňovat informaci ze všech analýz realizovaných tímto nástrojem a tím dále obohacovat zdroje dat pro následné analýzy. Kromě toho, že zde jsou uloženy vstupy pro vlastní kvantifikaci pravděpodobností selhání, bude mít databáze výhledově další významný úkol - s využitím Bayesovského přístupu umožní přímou explicitní aktualizaci generických dat specifickými daty z provozu JE či výcviku obsluhy blokové dozorny na simulátorech. To je zajištěno mimo jiné archivací všech analyzovaných a kvantifikovaných lidských zásahů v přehledné a strukturované formě s možností rychlého a snadného vyhledání libovolného zásahu dle široké škály parametrů.

Z dalších funkcí kalkulátoru lze uvést možnost automatického exportu všech nebo jen vybraných dat do celé řady běžných nástrojů práce s daty (MS Word, MS Excel...). Pro účely pravděpodobnostního hodnocení bezpečnosti byl vyvinut také export dat vyfiltrovaných záznamů přímo do programu RiskSpectrum, který je v této sféře základním nástrojem často komplikovaných výpočtů. Pro účely prezentací nástroje a jeho výstupů na mezinárodním poli byla vytvořena kompletní anglická verze. Tato anglická mutace byla mimo jiné využita

v rámci Mezinárodní empirické studie HRA zaměřené na porovnání jednotlivých HRA metodik. Vývoj kalkulátoru byl završen praktickým testováním a odzkoušením při analýze cca 400 lidských zásahů modelovaných v PSA studiích jaderných elektráren Dukovany a Temelín.

5. Závěr

Analýza spolehlivosti lidského činitele byla v celé své historii nedílnou součástí projektů pravděpodobnostního hodnocení bezpečnosti provozu jaderných elektráren. S narůstajícím uplatněním pravděpodobnostního hodnocení bezpečnosti se přirozeným způsobem zvyšuje i význam správného kvalitativního a kvantitativního podchycení role lidského prvku ve spektru přispěvatelů k riziku provozu elektrárny. Rozšiřující se možnosti aplikací PSA modelu při rizikově orientovaném rozhodování zasahují ve stále větší míře i do procesu vytváření co nejlepších podmínek pro kvalitní práci obsluhy. V tomto směru mají metody HRA velkou perspektivu v hodnocení a ovlivňování provozu a projektu nejen jaderné elektrárny, ale i řady dalších moderních technologií, jejichž provoz je zatížen nezanedbatelným rizikem.

Literatura

[1] Swain A.D., Guttman H.: „Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications“, NUREG/CR-1278, 1983

[2] Hannaman G.W., Spurgin A.J.: "Systematic Human Action Reliability Procedure (SHARP)“, EPRI-NP-3583, Electric Power Research Institute, Palo Alto, 1984

[3] Humpreys P.(editor): „Human Reliability Assessors Guide“, 1988, RTS 88/95Q, UKAEA

[4] Holý J.: „Nové směry v analýze spolehlivosti lidského činitele zaměřené na rozhodující faktory předcházející selhání obsluhy JE“, revize 1, ÚJV Řež, 1998

[5] „Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)“, NUREG-1624, Rev. 1, 2000

[6] Hollnagel E.: „Cognitive Reliability and Error Analysis Method (CREAM)“, Elsevier, 1998

[7] Swain, A.D.: "Accident Sequence Evaluation Program Human Reliability - Analysis Procedures", NUREG/CR-4772, 1987

[8] Spurgin J., A., Bareith A., Moieni P.: “A Computerized Safety Improvement System for Nuclear Power Plant Operator Training”, Brookhaven National Laboratory, 1996

[9] Kirwan B.: “Nuclear Action reliability Assessment (NARA): a Data Based HRA Tool”, Safety and Reliability, Vol.25 (2), 2005

[10] Holý J.: “Hodnocení nových procedur JE Dukovany z hlediska spolehlivosti lidského činitele, Ústav jaderného výzkumu Řež, 1998

[11] Kubíček J., Holý J.: “Metodika vyhodnocování provozních událostí ve spojení s řešením otázek lidského faktoru”, zpráva ÚJV 12273T, Ústav jaderného výzkumu Řež, 2005

[12] Holý J., Kubíček J.: “Lidský faktor v provozních událostech na JE Dukovany - metody, analýzy, závěry a doporučení”, zpráva ÚJV Z1594T, Ústav jaderného výzkumu Řež, 2004

[13] Holý J., Kubíček J.: "Detailní analýza způsobů a podmínek komunikace při provozu EDU - rozbor, závěry a doporučení", zpráva ÚJV Z1595T, Ústav jaderného výzkumu Řež, 2005

[14] Holý J., Kubíček J.: "Pilotní fáze periodického hodnocení bezpečnosti EDU", zpráva ÚJV Z 1548T, Ústav jaderného výzkumu Řež, 2005

[15] Holý J., "Metody hodnocení kvality práce obsluhy BD na základě dat získaných při sledování cvičení na plnorozsahovém trenažéru", zpráva ÚJV 11825T, Ústav jaderného výzkumu Řež, 2003

[16] Kubíček J., Holý J.: "Hodnocení ergonomie řídících pracovišť pomocných objektů EDU a jejich sdružování, zpráva ÚJV 12648 T, Ústav jaderného výzkumu Řež, 2006

[17] Kubíček J., Holý J., "Role managementu při zajištění bezpečného provozu JZ se speciálním zaměřením na management změny", zpráva ÚJV 12417T, revise 2, Ústav jaderného výzkumu Řež, 2006

[18] Kubíček J., Škrabal P., Holý J,: "Analytický nástroj hodnocení spolehlivosti lidského faktoru", Ústav jaderného výzkumu Řež, 2008

[19] Working material from IAEA workshop on Harmonization of PSA Methodology Approaches for WWER-1000 Reactors and Comparison of PSA Results, TC Project RER/9/068, 2002, Berlin

[20] International HRA Empirical Study - pilot phase report, OECD Halden Reactor Project, HWR-844, 2008

[21] Man-Machine-Organization Through Innovative Orientations for Nuclear (MMOTION) grant agreement, Annex 1 - description of work, 2008

[22] Manna G., Kuzmina I., Holý J., Outcomes of an International Initiative for Harmonization of low power and shutdown probabilistic safety assessment, Nuclear technology radiation protection, Vol.XXV., No.3 (2010), p.222-228

[23] Kubíček J., Holý J., Simulator data collection in the Czech Republic, OECD Halden Reactor Project Workshop on Human Performance Measurement, 31.5-1.6. 2011, Halden

[24] Kubíček J., Application of CBDT+ASEP method in frame of U.S. HRA Empirical Study, U.S. HRA Empirical Study Workshop, 21.-23.6. 2011, Washington

[25] Holý J., Fukushima lessons regarding NPP operation risk caused by human factors, Nuclear Safety and Security Summit, 27.-28.9. 2011, Vídeň

NOVÉ ASPEKTY APLIKACE METOD DRUHÉ GENERACE ANALÝZY SPOLEHLIVOSTI LIDSKÉHO ČINITELE

New aspects of second generation HRA methods application

Radim Doležal
Oddělení spolehlivosti a rizik, Technická univerzita v Liberci, Studentská 2, 461 17 Liberec 1
radim.dolezal@tul.cz http://risk.rss.tul.cz

Abstrakt:
Metody druhé generace nejsou ve své podstatě moc rozdílné. Způsob s jakým čelí lidskému výkonu se mnohdy nazývá různými způsoby, přesto v konečném důsledku nakládají s rozhodovacím procesem podobně. Dá se předpokládat, že skutečné průmyslové uplatnění sebou přinese hybridní užití poznatků více metod druhé generace. V následujících letech budou soupeřit především s přirozeným odporem proti změně a odporem k zhoršeným kvantitativním ukazatelům spolehlivosti člověka. Jejich nasazení bude také vyžadovat delší, složitější a ekonomicky náročnější analýzy.
Klíčová slova: *Analýza spolehlivosti člověka, HRA, Metody druhé generace.*
Abstract:
Second-generation methods are not inherently much different. The way in which asset human performance mechanism is often called in different ways, but ultimately the decision-making process is handled similarly. It is assumed that the actual industrial application will bring the use of hybrid methodwith knowledge of more second generation methods. In next year's they will compete primarily with natural resistance to change and resistance to the impairment of quantitative indicators of the human reliability. Their deployment will also require a longer, more complicated and economically demanding analysis.

Úvod

Lidské zásahy jsou neoddiskutovatelnou součástí operací řízení a údržby všech typů průmyslových a dopravních aktivit. Lidé jsou schopni zajistit bezpečnost a ekonomičnost procesů přijmutím proaktivních (předběžných) opatření a v případě porušení normálních nebo požadovaných dějů mohou jednat reaktivně. Přijmout opatření k nápravě dějů, nebo alespoň k zmírnění negativních následků nežádoucích jevů. Občas se říká, že není chyba systému, které by člověk nedokázal zabránit. Na druhou stranu jsou lidé také vlastním zdrojem chyb a mnohdy do dějů vstupují tak, že jsou prvotní příčinou, nebo urychlují průběh události a zhoršují možné negativní následky.

Je tedy potřeba neustále posuzovat riziko spojené s lidskými chybami a hledat cesty k redukci zranitelnosti systémů a následků lidských chyb. To jsou hlavní cíle analýzy spolehlivosti člověka - Human Reliability Analysis (v am. terminologiiHuman Reliability Assessment) - HRA. Ta může také svými důsledky zvýšit výdělečnost a pohotovost systému. Přesto je hlavním důvodem a vývojem aplikací HRA především řízení rizika.

Vývoj nástrojů HRA byl mnoho desetiletí poměrně pomalý a na okraji zájmu. Po nehodě Three Mile Island (1979) se do tohoto odvětví však vrhlo mnoho úsilí. To přineslo existenci mnoha HRA nástrojů - nejvíce v oblasti jaderného průmyslu. V období 80.- 90. let 20. století se vývoj v oblasti HRA soustředil především na kvantifikaci pravděpodobnosti lidské chyby (Human Error Probability - HEP). Ta je definována následovně:

$$HEP = \frac{počet nastalých chyb}{počet příležitostí k chybě} \qquad (1)$$

Používání terminologie „HEP" je mnohými odborníky zpochybňováno - například Hollnagel (1998) označuje HEP jako "legendární a iluzorní" s tím, že nikdo nemůže skutečně určit pravděpodobnost naprosto specifické akce.

Pravděpodobnost úspěšného provedení dané úlohy člověkem (HSP - Human SuccessProbability) je daná analogicky:

$$HSP = 1 - HEP \quad (2)$$

Toto soustředění na kvantifikaci v metodách HRA bylo přirozené, protože je výhodně použitelná v metodách hodnocení rizika, které jsou samy o sobě pravděpodobnostní (základními výstupy a srovnávacími kritérii jsou pravděpodobnosti nastoupení určitých jevů). Tyto pravděpodobnostní výsledky jsou porovnávány s podnikovými nebo vládními kritérii jednotlivých zemí pro danou oblast průmyslu a riziko je pak označeno za akceptovatelné nebo neakceptovatelné. Pakliže není akceptovatelné, musí být rizikové faktory redukovány přijatelným způsobem, v opačném případě musí být provoz ukončen.

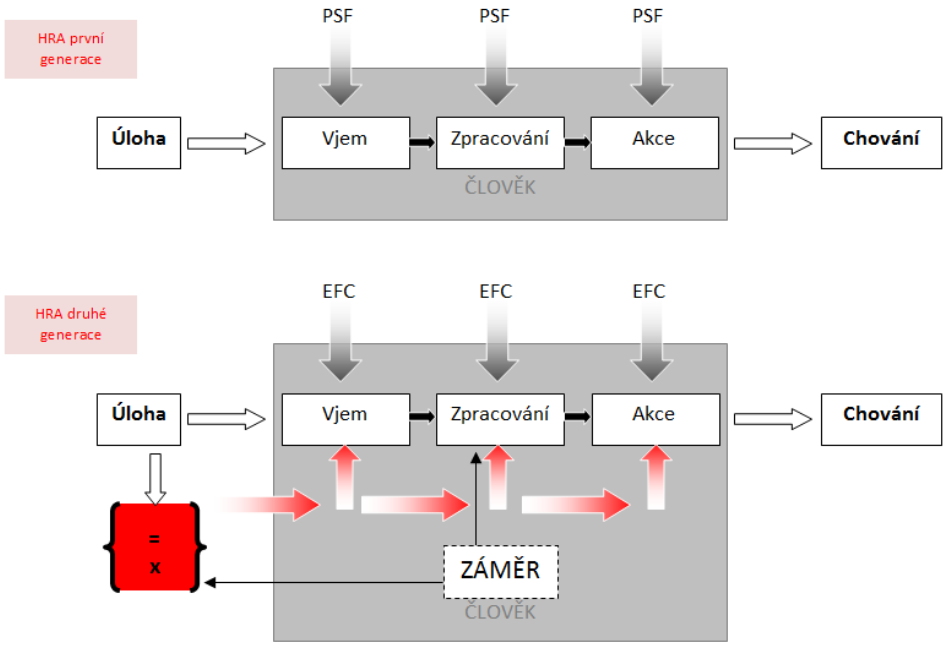
Metody první generace

O prvních studiích lidské spolehlivosti v klasickém formátu HRA můžeme mluvit od roku 1975, kdy byl vydán dokument WASH 1400. V tomto dokumentu byla analyzována bezpečnost nukleárního reaktoru, v jejímž rámci byl analyzován i příspěvek člověka. Metody první generace se snažily být v podstatě atomistické - podporovaly hodnotitele, aby rozbil úkol do malých částí a u nich hodnotil potenciální dopad faktorů, jako je nedostatek času, konstrukce zařízení, stres atd. Kombinací těchto elementů mohl hodnotitel určit pravděpodobnost lidské chyby. Hlavním zástupcem metod první generace je metoda THERP (Swain & Guttmann, 1983).

Metody druhé generace

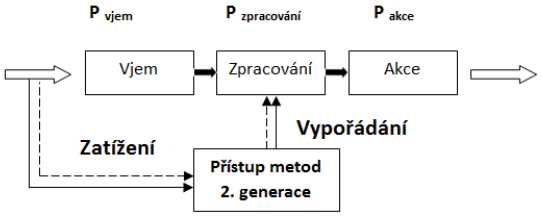
Vývoj metod druhé generace začal v devadesátých letech dvacátého století a prozatím nebyl ukončen. Charakteristickým znakem metod druhé generace je nechuť k termínu „lidská chyba". Ten je obvykle pokládán za odsuzující. Proto se napříč novými metodami vžilo užití termínu „HFE“ - událost lidského selhání (Human FailureEvent) pro událost, která vede k selhání nějaká funkce procesu a na které se určitým způsobem podílel člověk. Stejně tak se začal široce používat další nový pojem: EFC - kontext vyvolávající chybu (Error ForcingContext).

Mnohdy se může stát, že metody druhé generace nepřinášejí nové nebo lepší odpovědi na naše otázky, než metody první generace. Je to způsobeno rozdílnou filozofií, kterou je třeba přijmout, nebo alespoň akceptovat. Důsledkem toho je, že metody druhé generace nás v podstatě nutí pokládat si nové a podrobnější otázky. Už to je jejich velký přínos.Nejčastěji citovanými metodami jsou ATHEANA, CREAM, MERMOS, CESA a CAHR.



Obrázek 1 - Model lidského zpracování informací - rozdíl mezi dvěma generacemi HRA

Metody druhé generace nejsou ve své podstatě moc rozdílné (snad pouze ATHEANA zůstala v některých ohledech na půl cesty). Způsob s jakým čelí lidskému výkonu se mnohdy nazývá různými způsoby, přesto v konečném důsledku nakládají s rozhodovacím procesem podobně. Dá se předpokládat, že skutečné průmyslové uplatnění sebou přinese hybridní užití poznatků více metod druhé generace. Shrnutí podobností i rozdílností jednotlivých částí metod druhé generace je na následující tabulce:



	Zatížení	Vypořádání	Základ kvantifikace	Matematické nástroje
ATHEANA	Kontext vyvolávající chybu - EFC (PSF + podmínky výroby)	Mechanismus chyb	Expertní úsudek	Expertní kalibrace
MERMOS	← CICA	CICA →	Expertní úsudek	-
CREAM	Hlavní podmínky výkonu	Kognitivní režimy řízení	THERP Databáze	-
CAHR	Kognitivní párování & Interakce bariér	Kognitivní mechanismy řešení (Tendence)	Reálná data provozu	Kalibrace
CESA	Použitelné akce & Důležitosti & Nepříznivé podmínky	Kognitivní tendence	Reálná data provozu	Bayesovské metody

Obrázek 2 - Podobné mechanismy metod druhé generace

Pozn:
Kontext - z latinského contextus - souvislost. Komplexní souhrn vnitřních i vnějších vzájemných minulých i přítomných souvislostí a vlivů.

Kognitivní - z latinského cognitivus - poznávací. Používá se především jako přívlastek kladoucí důraz na poznávací (myšlenkovou, rozumovou) stránku činnosti, oproti stránce emotivní, praktické apod. Např. kognitivní psychologie je teorie zaměřená na zpracování informací, získávání obecných poznatků a procesů chápání.

Charakteristiky vybraných metod druhé generace jsou:

ATHEANA

ATHEANA je metoda úzce zaměřena na sektor jaderných elektráren. Některé její částí jsou nejasné. Metoda neposkytuje jasně formulované kroky jakými postupovat. V dokumentaci jsou užity nevhodné příklady nebo jsou jako příklady označeny i tabulky obsahující části metody.Nevýhodou je i rozdílný přístup dvou hlavních dokumentů metody (NUREG 1880 x NUREG 1624).Hlavní výhodou metody je skutečnost, že přináší spoustu nových poznatků a pohledů na problematiku spolehlivosti člověka. Metoda nutí k pokládání některých důležitých otázek.

ATHEANA je obecně považovaná za metodu druhé generace. Přesto nevykazuje všechny rysy dalších metod jako CAHR a CREAM. V podstatě se ani nesnaží pochopit kognitivní rozměr pozorování a chování operátora. Metoda rozšiřuje přístup THERP o systematické hledání EOC. Soustředí se na hledání odchylek od normálního provozu a průběhu operací. Inherentně pobízí k opakované aplikaci v několika iteračních krocích. Metoda je vnitřně kontextová - a v tomto přístupu je velmi dobrá. Dokáže najít kontext ovlivňující jednotlivé pravděpodobnosti neúspěchu v dílčích krocích a různé odlišné průběhy nehod. Ukazuje jaké možné EOC z těchto podmínek mohou vzniknout. Kvantifikační část je bohužel velmi závislá na odborném odhadu. Od kognitivní části výkonu člověka si však drží stejný odstup jako metody první generace.

MERMOS

Jde o vlastní metodu vyvinutou EDF (Electricité de France - Francouzská národní energetická společnost).Metoda byla vyvíjena velmi dlouhou dobu, většinu času rostla intuitivně pro potřeby EDF v rámci starších HRA přístupů, až se vyvinula ve vlastní HRA metodu.Je založena na velkém množství vyšetřených nehodových scénářů v reálné praxi EDF a dále na ještě větším množství dat získaných ze simulovaných scénářů.Přestože autoři metody publikovali velké množství článků o metodě MERMOS, velká část její skutečné aplikace je neznámá.Důležitým prvkem užitým v metodě jsou takzvané "CICA". Překlad by mohl být "konfigurace/orientace systému". CICAs jsou tedy kombinací možných reakcí na různé události. Dlouhý a detailní seznam všech CICAs by měl pokrývat všechny možné důležité mimořádné události a jejich okolnosti - včetně popisu výkonu operátora, EOC, atd. Mezi hlavní nevýhody patří především to, že je metoda podrobně popsána pouze ve francouzštině. Není veřejně nepřístupný úplný seznam CICA. Jde o interní metodu EDF,spíše než jasný a otevřený vědecký přístup.Výhodou je ohromná základna EDF - velký počet elektráren pro zpětnou vazbu aplikace metody a jednoduchý přístup k simulaci nových scénářů. Jde o jedinou skutečně zavedená a validovanou metodu druhé generace.

CREAM

CREAM a jeho filozofii popisuje sám autor takto (Hollnagel, 1998):

Lidská práce může být charakterizována na škále od „dělání" až k „myšlení". Některé úkoly, jako je manuální dovednosti a dodržování pevného postupu vyžadují více „dělání" a méně „myšlení", zatímco jiné, jako jsou diagnostika, plánování a řešení problémů, vyžadují mnohem více „myšlení" a trochu „dělání". Vývoj moderních technologií změnilo povahu lidské práce z uplatňování převážně manuálních dovedností k provádění intenzivní funkcí na základě vzdělání a zkušeností (tj. kognitivní úkoly). V současný průmyslové prostředí se množství „myšlení" zvyšuje, zatímco množství „dělání" snižuje. Tento stav má důsledky jak pro návrh systému, tak pro analýzy spolehlivosti. V návrhu systému například musí být konvenční ergonomické aspekty (např. fyzické vlastnosti ovladačů) nahrazeny kognitivní ergonomií.

Obecný způsob predikce lidského výkonu metodou CREAM má šest kroků. Prvním je detailní analýza úkolů včetně kognitivních vlastností. Druhým krokem je popsání kontextu a hlavních podmínek výkonu (CPC - Common Performance Condition). Zároveň by mělo dojít k vybrání možných chybných módů a pravděpodobných příčin. Třetím krokem je vyjasnění iniciační události - tedy startovního místa odkud budeme různé scénáře událostí analyzovat. Čtvrtým krokem je kvalitativní predikce výkonu, která odpovídá vytvoření

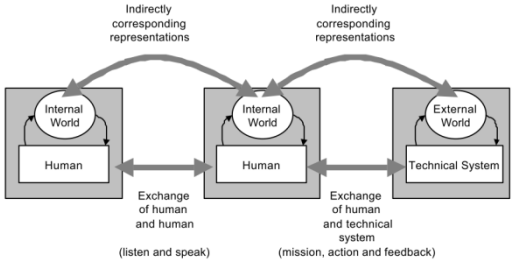
nejpravděpodobnějšímu stromu událostí, nebo soubor stromů. Pátým krokem je identifikace kroků úlohy nebo událostí, které vyžadují další analýzu. Šestým krokemje kvantifikace předpovězeného výkonu.
Celá metoda je především založena na mnoha tabulkách vytvořených podle tzv. třídícího schématu (Classificationscheme). Zde jsou jednotlivé módy chyb popsány ve vztahu tzv „předchůdce“ a „následníka“ (antecedent &consequent). Pomocí kombinace těchto tabulek je postupně vytvořen celý řetěz pravděpodobných skutečností podílejících se na daném módu chyby. Důležitou skutečností je, že se CREAM nesnaží o uplatnění mechanických pravidel při kombinaci těchto tabulek. Nejsou tak daná jasná pravidla a mantinely. To je také hlavním nedostatkem této metody.

CESA

Jde o mladou metodu ze Švýcarska. Je postavena na podobných základech jako CAHR. Dá se říci, že obě metody jsou vyvíjeny paralelně a v neustálém kontaktu. Je dost možné, že do budoucna obě metody splynou v jedinou obecnou metodu.

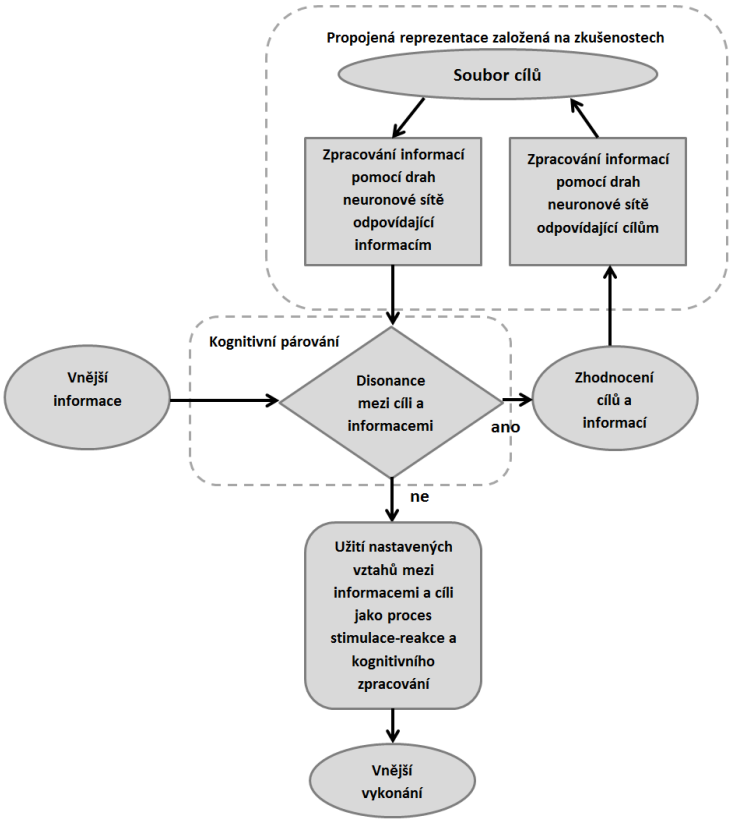
CAHR

Propojené posouzení lidské spolehlivosti (ConnectionismAssessment of Human Reliability) je mladou metodou vyvinutou v Německu profesorem Sträterem. Její princip je známý přes deset let, přesto jsou některé praktické nástroje (např. zjednodušená analýza úkolů) metody stále ve vývoji, nebo jsou zdokonalovány. Metoda stojí na podobných psychologických základech jako CREAM. Některé její prvky byly přejaty dalšími autory a jsou nadále rozvíjeny v rámci dalšího vývoje nových metod - například americká iniciativa okolo přístupu HERA.
Metoda se snaží vypořádat s kognitivním aspektem výkonu člověka. Podobně jako jiné metody se zajímá především o roli člověka v interakci s technickým systémem. Výměna informací mezi člověkem a strojem se děje za určitých psychických okolností a určitých podmínek dané situace. To samé platí i pro výměnu informací mezi více lidmi. Teoretické pozadí metody CAHR pracuje s myšlenkou kognitivního výkonu, který je velmi ovlivněn vnitřním světem pracovníka. Výměnu informací zobrazuje následující obrázek (Sträter, 2005):



Obrázek 3 - Vazby systému člověk-člověk a člověk-stroj

Lidský mozek neustále sbírá informace a porovnává je s vnitřní reprezentací světa(Sträter, 2000). Totose děje občas vědomě, ale většinu času jako naprosto nevědomý proces. Občas je tento proces nazýván jako tzv. kognitivní mlýn (CognitiveMill). Toto metaforické přirovnání může být využito při vysvětlení, jakým způsobem funguje tzv. kognitivní párování (CognitiveCoupling) a propojovací část metody CAHR. Obrázek ukazuje, jak kognitivní párování a reprezentace propojování vytvářejí předpověď o kognitivním chování. Aplikace tohoto modelu také ukazuje, že dovoluje zohlednit konkrétní podmínky dané situace, pro kterou výkon zkoumáme a výsledné chyby v lidském chování(Sträter, 2005).



Obrázek 4 - Smyčka kognitivního zpracování - koherence mezi kognitivním párováním a znalostmi

Metoda je založena na datech (v angličtině výraz „data-driven“). Přístup k vhodné databázi se tak stává jedním z hlavních problémů celé aplikace metody. Originální úplná a nejvhodnější databáze není veřejně přístupná - obsahuje citlivé údaje skutečných událostí jaderného provozu. Je možné zakoupit hrubá data bez konkrétních popisů - tedy použitelnou licenci. Dalším řešením je tvorba vlastní databáze. To může a nemusí být složité. Provozovatelé nebezpečných provozů jsou povinní vyšetřovat své nehody a shromažďovat o nich informace. Pokud by se rozhodli pro metodu CAHR a nasadili ji do svých procesů, tak by zakrátko mohli mít užitečnou databázi použitelnou pro HRA analýzu. Přesto je tvorba databáze časově náročná - databáze autora metody byla odhadnuta jako výsledek 1200 hodin práce jednoho člověka.Tvorba databáze pro perspektivní analýzu bez možnosti získat dostatek dat z podobných provozů se může stát velmi problematická a výsledná data takmohoubýt zavádějící.

CAHR přináší velký vhled do skutečných příčin lidských chyb. Oprostila se od manifestace chyb, ale zaměřila se na kognitivní aspekty lidského výkonu. Ohromnou výhodou aplikace metody je její databáze, která se zřekla jednoduchých vysvětlení komplexní interakce různých faktorů a přinesla praktický nástroj pro kvantifikaci pravděpodobností. Z dnešního pohledu jí tedy můžeme vytýkat pouze menší zaměření na kontext a možné odlišnosti v zadaném scénáři a jeho počátečních podmínkách. Dále pak absenci oficiálního dokumentu metody s jasnými pravidly, jaký nabízí například metody zveřejňované ve zprávách NUREG.

Nové aspekty aplikace metod druhé generace

Metody druhé generace přinášejí celou řadu užitečných zjištění s praktickým dopadem na analýzu. Pomocí zapojení kognitivního rozměru dokáži vysvětlit mnohem větší záběr lidského chování. Zároveň se však analýza stává několikanásobně složitější. K jejímu úspěšnému zvládnutí je potřeba získat mnohem větší znalosti a využívat buď velké databáze, nebo tabulky s mnohem větším rozsahem než u metod první generace. Užití těchto dat je také obvykle méně jasné. Zatímco metody první generace přinášejí jednoduše aplikovatelný

přístup, který je popsán krok za krokem v jasnéproceduře - metody druhé generace se obvykle zdržují pevně daných pravidel.
Metody druhé generace jsou také charakterizovány přístupem, který se snaží zohlednit kontext, které metody první generace přehlíželi a hledáním chyby z přidání (Error Of Commission - EOC). Výhody a přínosy těchto metod nebyly doposud dostatečně oceněny a tak nejsou bohužel často zaváděny. Základním důvodem malého uplatnění metod druhé generace zůstává nechuť k užití rozdílné filozofii oproti starším metodám a především pak strach z výsledků, které mají horší kvantitativní ukazatele.

Závěr

Přestože mnoho studií skutečných lidských zásahů ukázalo, že výsledky metod první generace jsou přílišně optimistické - k urychlenému nasazení lepších metod to nevedlo. Metody druhé generace stále čekají na své široké uplatnění. V následujících letech budou soupeřit především s přirozeným odporem proti změně a odporem k zhoršeným kvantitativním ukazatelům spolehlivosti člověka. Jejich nasazení bude také vyžadovat delší, složitější a ekonomicky náročnější analýzy.

Vazba na projekt

Tato práce vznikla za podpory MŠMT ČR v rámci studentské grantové soutěže 7650-SGS - *Inovativní metody hodnocení spolehlivosti a rizika* fakulty mechatroniky, informatiky a mezioborových studií na Technické univerzitě v Liberci.

Použitá literatura

Forester, J., et al. 2007. *ATHEANA User'sguide. Final Report*. 1. vyd. U.S. Nuclear Regulatory Commission. NUREG/CR-1880.
Hollnagel, E. 1998. *Cognitive Reliability and Error Analysis Model* (CREAM). 1. vyd. Elsevier. ISBN 978-0-08-042848-2.
NRC. 2000. *TechnicalBasis and ImplementationGuidelines for A Technique for Human Event Analysis (ATHEANA).*1. vyd. U.S. Nuclear Regulatory Commission. NUREG/CR-1624.
Sträter, O. 2000.*Evaluation of Human Reliability on theBasis of OperationalExperience. GRS-170.* 1. vyd. GRS. ISBN 3-931995-37-2.
Sträter, O. 2005.*Cognition and Safety.* 1. vyd. Ashgate. ISBN 0-7546-4325-5.
Swain, A. D., Guttmann, H. E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications - Final Report*. 1. vyd. U.S. Nuclear Regulatory Commission & Sandia National Laboratories. NUREG/CR-1278.
Swain, A. D. 1987. *AccidentSequenceEvaluation Program Human Reliability Analysis Procedure.* 1. vyd. U.S. Nuclear Regulatory Commission & Sandia National Laboratories. NUREG/CR-4772.

Zdroje dat pro hodnocení spolehlivosti člověka a jejich efektivní využití

Jan Kubíček

Ústav jaderného výzkumu Řež
Oddělení analýz a rizik

Praha, 14.září 2011

Obsah prezentace

- Využití dat z HERA databáze pro ocenění vlivu PSF faktorů na práci obsluhy JE
- Mezinárodní HRA empirická studie
- Americká HRA empirická studie
- Sběr dat na simulátoru jaderné elektrárny Dukovany

Motivace

- Analýza spolehlivosti lidského činitele (HRA) je v rámci PSA významným zdrojem nejistot – snahy o eliminaci těchto nejistot
- Problém: nedostatek relevantních dat týkajících se lidské spolehlivosti
- V současnosti existuje celá řada národních programů věnovaných sběru dat, ale žádný společný mezinárodní program
- Mezinárodní HRA databáze by zvýšila statistickou věrohodnost sbíraných dat a poskytovala by přesnější data týkající se LF nejen pro účely PSA

HERA databáze

- Jedná se o databázi americké NRC sloužící pro sběr a analýzu informací o lidském faktoru v provozu amerických jaderných elektráren (JE)
- Aktuálně obsahuje 395 lidských zásahů z 22 provozních událostí
  - 244 (62%) lidská selhání
  - 151 (38%) úspěšné lidské zásahy
- Modifikovaná verze HERA databáze použita pro sběr dat na plnorozsahovém simulátoru HAMMLAB v norském Haldenu
- Aktuálně obsahuje 254 lidských zásahů z 2 projektů na simulátoru
  - 33 (13%) lidská selhání
  - 221 (87%) úspěšné lidské zásahy

PSF faktory

- PSF (Performance Shaping Factors) faktory jsou faktory, které ovlivňují práci obsluhy
- Pro kvantitativní ocenění vlivu těchto faktorů na práci obsluhy bylo vybráno 7 faktorů představujících průnik mezi oběma použitými datovými zdroji:
  1. Dostupný čas
  2. Stres a stresory
  3. Složitost úkolu
  4. Zkušenost a trénink
  5. Procedurální podpora
  6. Ergonomie a rozhraní člověk-stroj
  7. Pracovní postupy

Příklad zásahu v databázi HERA

- Pracovníci, kteří objevili požár, se nedrželi havarijních předpisů a nespustili požární alarm
- Následující 3 PSF faktory negativně ovlivnily tuto jejich akci:
  - Vysoký stres (způsobený požárem daných kabelů)
  - Špatný trénink požární připravenosti a havarijních postupů (dotčený personál vůbec neprošel příslušným školením)
  - Špatné pracovní postupy (nedodržování havarijních předpisů)

Tabulka: Příklad sekvence popisující tuto akci

PSF	*Dostupný čas*	*Stres a stresory*	*Složitost úkolu*	*Zkušenost a trénink*	*Procedury*	*Ergonomie a MMI*	*Pracovní postupy*
Sekvence	*0*	*-1*	*0*	*-1*	*0*	*0*	*-1*

Porovnání dat

- Celkem 649 lidských akcí
  - 277 (43%) lidských selhání
  - 372 (57%) úspěšných zásahů

	Dostupný čas	Stres a stresory	Složitost úkolu	Zkušenost a trénink	Procedurální podpora	Ergonomie a MMI	Pracovní postupy	Celkem	%
Špatná (-1)	100	275	232	161	171	40	254	1233	27%
Nominální (0)	540	374	374	344	428	609	221	2890	64%
Dobrá (1)	9	0	43	144	50	0	174	420	9%

Odvození multiplikativních koeficientů pro jednotlivé PSF faktory

- Výsledná post = PSF koef. X základní post
- Pro výpočet PSF koeficientů použity 2 různé přístupy
- Metoda „závislých sekvencí“ byla aplikována pouze na data ze simulátoru
- Výsledné PSF koeficienty
  - Dostupný čas: M = 2.5
  - Stres a stresory: M = 4.7
  - Složitost úkolu: M = 6.4
  - Zkušenost a trénink: M = 8.6
  - Procedurální podpora: M = 3.2
  - Ergonomie a MMI: M = 2.7
  - Pracovní postupy: M = 4.2

Mezinárodní HRA empirická studie

- Projekt zaměřený na empirické testování HRA metod
- Cíl: Identifikace silných a slabých stránek HRA metodik a porovnání výsledků s empirickými daty
- Období: 2007-2009
- Technologie: Plnorozsahový simulátor BD (3-smyčkový tlakovodní reaktor firmy Westinghouse) na pracovišti Hammlab v norském Haldenu

Mezinárodní HRA empirická studie (2)

- Účastníci: 18 organizací z 10 zemí
  - Operátoři - 14 obsluh švédské jaderné elektrárny Ringhals
  - 13 HRA týmů (USA, Korea, Francie, Finsko, Švédsko, ČR, Švýcarsko)
- Použito 12 různých HRA metod (a jejich modifikací)
  - ASEP, CBDT, ATHEANA, CESA, CREAM, HEART, KHRA, MERMOS, PANAME, SPAR-H, THERP
- Scénáře:
  - Prasknutí trubky parogenerátoru (2 varianty obtížnosti)
  - Ztráta napájecí vody (2 varianty obtížnosti)

Americká HRA empirická studie

- Projekt zaměřený na empirické testování 4 vybraných HRA metod
- Cíl: Identifikace silných a slabých stránek vybraných metodik, jejich vzájemné porovnání a porovnání s empirickými daty
- Období: 2010-2011
- Technologie: Plnorozsahový simulátor BD (4-smyčkový tlakovodní reaktor firmy Westinghouse) americké JE South Texas

Americká HRA empirická studie

- Účastníci:
  - Operátoři: 4 obsluhy americké jaderné elektrárny South Texas
  - Analytici: 9 HRA týmů
- Použité HRA metody: CBDT, ATHEANA, THERP/ASEP, SPAR-H
- Scénáře:
  - Ztráta napájecí vody následovaná prasknutím trubky parogenerátoru
  - Ztráta chlazení ucpávek hlavních cirkulačních čerpadel
  - Prasknutí trubky parogenerátoru

Sběr dat na simulátoru EDU

- Grantový projekt zaměřený na sběr dat pro účely analýzy spolehlivosti LF
- Cíle:
  - Získání informací o LF za účelem přesnější kvantifikace jeho spolehlivosti v rámci PSA
  - Poskytnutí doporučení elektrárně na zlepšení symptomově založených procedur a nového MMI (zvyšování výkonu a modernizace SKŘ)
  - Získání informací o faktorech ovlivňujících práci obsluhy:
    - Trénink obsluhy
    - Dostupná časová okna
    - Složitost úkolu
    - Úroveň stresu
    - …

Sběr dat na simulátoru EDU (2)

- Technologie: Plnorozsahový simulátor BD (6-smyčkový tlakovodní reaktor VVER-440) JE Dukovany
- Účastníci: všech 30 obsluh blokové dozorny JE Dukovany
- Časový harmonogram:
  - 2010: Příprava projektu (příprava metodiky a výběr sbíraných parametrů a indikací o stavu zařízení)
  - 2011:
    - Společnost OSC vytvořila sběrný modul pro sběr vybraných parametrů
    - Ve spolupráci s tréninkovými instruktory vybrány scénáře
    - Zahájení sběru 3.10.
  - 2012: Analýza a vyhodnocení nasbíraných dat
- Scénáře (1 abnormální, 3 mimořádné stavy):
  - Únik na trase na ucpávky HCČ 4 (10 t/h)
  - Velká netěsnost na HNK (3000 t/h)
  - Prasknutí víka prim. kol. PG (300 t/h) a otevření PVPG
  - Požár na RRCS (Systém řízení regulačních kazet) vedoucí k ATWS

Ústav jaderného výzkumu Řež a.s.

www.ujv.cz

Děkuji Vám za pozornost

ÚJV

www.ujv.cz

SPOLEHLIVOST LIDSKÉHO ČINITELE PŘI PROVOZU MODERNÍ TECHNOLOGIE
(sborník přednášek),
kolektiv autorů
počet stran: 26
1. vydání,
rok vydání: 2011
druh vazby: brožovaná

ISBN 978-80-02-02342-5