TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky, informatiky a mezioborových studií

Studijní program: B2612 – Elektrotechnika a informatika

Studijní obor: 1802R022 – Informatika a logistika

Kvantitativní hodnocení spolehlivosti lidského faktoru

Quantitative assessment of human contribution to risk

Bakalářská práce

Autor: **Jan Pišta**

Vedoucí práce: Ing. Radim Doležal

V Liberci 17. 5. 2011

ZADÁNÍ

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce.

Datum

Podpis

Poděkování

Touto cestou bych chtěl poděkovat především vedoucímu bakalářské práce Ing. Radimu Doležalovi za odborné vedení, trpělivost a pomoc při zpracování této bakalářské práce.

Samozřejmě mé díky patří také celé mé rodině za všestrannou podporu při mém vysokoškolském studiu.

Kvantitativní hodnocení spolehlivosti lidského faktoru

Abstrakt

Bakalářská práce se zabývá problematikou teoretických poznatků z oblasti spolehlivosti a hodnocení rizika lidského faktoru. Dále hodnotí různé kvantitativní metody využívané při analýze spolehlivosti člověka.

Dále porovnává různé způsoby získávání vstupních dat pro kvantifikaci spolehlivosti člověka.

Na závěr je zhotoven návrh simulačního a měřícího prostředku využitelného při výuce.

Klíčová slova: lidský faktor, spolehlivost, kvantitativní hodnocení, simulační prostředek

Quantitative assessment of human contribution to risk

Abstract

The Bachelor Thesis deals with theoretical knowledge of reliability and risk assessment of the human factor. Further, evaluates the various quantitative methods used in human reliability analysis.

Further, different methods of obtaining input data for quantification of human reliability are compared.

At the conclusion there is made the design of the simulation and measuring device usable in the education.

Keywords: human factor, reliability, quantitative assessment, simulation device

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

ASEP..... Program hodnocení sledu nehod (Accident Sequence Evaluation Program)

ATHENA..... Technika analýzy lidské chyby (A Technique for Human Error Analysis)

BWR ..... Varný reaktor (Boiling Water Reactor)

CAHR ..... Posouzení lidské spolehlivosti (Connectionism Assessment of Human Reliability)

CREAM ..... Metoda analýzy spolehlivosti poznání a chyby (Cognitive Reliability and Error Analysis Method)

EF..... Chybový faktor (Error Factor)

ESAT ..... Expertní systém pro úkoly (Expertensystem zur Aufgaben)

ETA..... Metoda stromu událostí (Event Tree Analysis)

FMEA ..... Analýza způsobů a důsledků poruch (Failure Mode and Effects Analysis)

FMECA..... Analýza způsobů, důsledků a kritičnosti poruch (Failure Mode, Effects and Criticality Analysis)

FTA..... Metoda stromu poruchových stavů (Fault Tree Analysis)

HAZOP ..... Studie nebezpečí a provozuschopnosti (Hazard and Operability Study)

HEP..... Pravděpodobnost lidské chyby (Human Error Probability)

HERA..... Uložiště a analýzy lidských událostí (Human Event Repository and Analysis)

HRA..... Analýza spolehlivosti člověka (Human Resource Analysis)

HRC ..... Lidská spolehlivost poznání (Human Cognitive Reliability)

HSP..... Pravděpodobnost lidského úspěchu (Human Success Probability)

INL..... Americká národní laboratoř v Idaho (Idaho National Laboratory)

NASA..... Americký národní úřad pro letectví a kosmonautiku (National Aeronautics and Space Administration)

NRC ..... Americká jaderná regulační komise (U. S. Nuclear Regulatory Commission)

NUCLARR ..... Počítačová knihovna pro posuzování spolehlivosti jaderného reaktoru (Nuclear Computerized Library for Assessing Reactor Reliability)

PC..... Metoda výpočtu bezporuchovosti z dílů (Path County)

PHA ..... Předběžná analýza nebezpečí (Process Hazard Analysis)

PRA..... Posouzení pravděpodobnosti rizika (Probabilistic Risk Assessment)

PSF..... Faktory ovlivňující výkon (Performance Shaping Factor)

PWR..... Tlakovodní reaktor (Pressurized Water Reactor)

SLIM..... Metoda indexu možnosti úspěchu (Success Likelihood Index Method)

THERP..... Technika pro předpovídání intenzity lidské chyby (Technique for Human Error Rate Predicition)

VVER..... Tlakovodní reaktor, obvykle vnímán ruské konstrukce (Vodo-Vodyanoi Energetichesky Reactor)

°C ..... Stupeň Celsia

g/kg ..... Gramů v kilogramu

kg/s..... Kilogramů za sekundu

m ..... Metr

MPa..... Megapascal

MWt..... Megawatt

Úvod

V dnešní době se neustále zvyšují požadavky na analýzu člověka. Tyto požadavky s sebou přinášejí nutnost získávání kvantitativních dat o lidském výkonu. Dostupnost vhodných dat je neustálým problémem všech odborníků z oblasti lidského faktoru. O důležitosti spolehlivosti člověka pro bezpečný provoz průmyslových zařízení není pochyb. U velkého počtu všech velkých průmyslových havárií je na vině právě selhání lidského faktoru, nebo je lidský příspěvek jedním z důležitých faktorů nehodového scénáře. Jeho zkoumáním však můžeme předcházet dalším chybám.

Prvním z cílů této bakalářské práce je získat teoretické poznatky z oblasti spolehlivosti a hodnocení rizika lidského faktoru. V teorii spolehlivosti se budeme zabývat etapami životního cyklu, objekty, typy zapojení a metodami analýzy spolehlivosti. V základech z oblasti rizika se především zaměříme na management rizika, následovat bude pojednání o lidském faktoru.

V další části budou zhodnoceny používané kvantitativní metody a porovnat různé způsoby získávání dat pro kvantifikaci spolehlivosti člověka. Z kvantitativních metod budeme rozebírat metody TESEO a THERP/ASEP. Dále bude pozornost zaměřena na získávání dat z databank či simulátorů.

Následně porovnáme přístupy využívání simulátorů ve světě a v České republice. Simulátory jsou důležité pro získávání dat stejně jako pro praktickou ukázku reálných technologií. Další část bakalářské práce bude zaměřena na návrh simulátoru, který by mohl být zdrojem kvantitativních dat.

Výsledkem bude zhotovení návrhu simulačního a měřícího prostředku využitelného při výuce, včetně jeho možné grafické podoby.

1 Spolehlivost

1.1 Úvod

Vzhledem k rostoucí složitosti výrobků a technických soustav bylo nutné z důvodu ohrožení společnosti zavést pojem spolehlivost. Jako první se spolehlivost začala uplatňovat ve čtyřicátých letech 20. století v oblasti vojenské techniky. Konkrétně se jednalo o vývoj raketové techniky v Německu. Od raket se očekává, že doletí k určenému cíli a zasáhnou ho s co největší pravděpodobností. Bohužel dřívější postupy vývoje a následné výroby raket splnění požadavku nezaručovaly. Proto byli projektanti přinuceni se systematicky zabývat spolehlivostí těchto raket. A následně vznikla první definice spolehlivosti, která definovala spolehlivost jako pravděpodobnost, s jakou bude objekt schopen plnit bez poruchy požadované funkce po stanovenou dobu a v daných provozních podmínkách [1].

S dalším rozvojem se však ukázalo, že zmiňovaná definice spolehlivosti je nepřesná, neboť pojednává pouze o bezporuchovosti. Hlavně se to ukázalo u složitých opravovaných systémů, které se v daném okamžiku mohly nacházet v různých provozních stavech a tyto stavy se s časem mohly náhodně měnit. V angličtině je tato spolehlivost označována pojmem Reliability. Proto vznikla historicky druhá definice spolehlivosti, která se začala používat od přelomu šedesátých a sedmdesátých let. Spolehlivost chápe jako obecnou schopnost výrobku plnit požadované funkce po stanovenou dobu a v daných podmínkách, která se vyjadřuje dílčími vlastnostmi, jako jsou bezporuchovost, životnost, opravitelnost, pohotovost apod. [1]

Oproti první definici se již nevyskytuje pojem pravděpodobnost, s jakou bude objekt schopen plnit požadované funkce, ale obecně schopnost plnit dané funkce. Druhá definice byla rovněž rozšířena o další vlastnosti a nehovoří tedy pouze o bezporuchovosti. Spolehlivost tedy byla definována jako obecná vlastnost, která se vykazuje konkrétními číselnými ukazateli dílčích vlastností. V angličtině se ovšem i nadále používal pojem Reliability. Tudíž to s sebou přinášelo jisté terminologické problémy, kvůli nimž byla vypracována další a zatím poslední definice spolehlivosti. Podle terminologické normy ČSN IEC 50 (191) je spolehlivost definována takto: Spolehlivost je souhrnný termín používaný pro popis spolehlivosti a činitelů, které ji ovlivňují: bezporuchovost, udržovatelnost a zajištěnost údržby. Tato definice především

reagovala na fakt, že schopnost objektu plnit požadované funkce je ovlivněna i vnějšími činiteli, jako je zajištění požadované údržby.

Se zavedením poslední definice spolehlivosti došlo i k významným terminologickým změnám. Pojem Reliability se již používá pouze pro označení bezporuchovosti. A pro označení spolehlivosti se zavedl termín Dependability [2].

V praxi se často můžeme setkat s různými přívlastky pojmu spolehlivost. Nejpoužívanějšími přívlastky jsou inherentní, provozní a odhadovaná neboli predikovaná. Inherentní spolehlivost je spolehlivost vložená do objektu v průběhu jeho návrhu a výroby. Tato spolehlivost nebere ohledy na zhoršující se vlivy provozních podmínek, podmínek prostředí či lidského faktoru. Naopak provozní spolehlivost vlivy provozních a dalších podmínek bere v potaz. Odhadovaná (predikovaná) spolehlivost je spolehlivost, která je výsledkem metod odhadu, vstupních informací o spolehlivosti prvků, schopností a možností analytika provádějícího odhad a další.

V dnešní době je spolehlivost chápána jako součást schopnosti uspokojovat stanovené a předpokládané potřeby uživatele. Tato schopnost se nazývá jakost a kromě spolehlivosti obsahuje i další vlastnosti objektu, jako například technická funkčnost, bezpečnost, ekonomičnost, ekologičnost, estetičnost atd.

Objekt, který posuzujeme, bývá nejčastěji charakterizován dvěma stavy. A to provozuschopný stav nebo stav poruchy. Porucha nastane při přechodu z provozuschopného stavu do stavu poruchy. V případě, že objekt opět začne plnit požadované funkce, jedná se o jev obnovy [2].

Veličiny, které ve spolehlivosti sledujeme, souvisí s náhodným výskytem sledovaných jevů. Sledují se veličiny spojené s dobou a proběhem. Jedná se například o dobu provozu, dobu provozu do poruchy, dobu provozu mezi poruchami, dobu údržby, dobu opravy apod. Funkce využívaná pro popis náhodného procesu se nazývá ukazatel spolehlivosti.

1.2 Etapy životního cyklu výrobku

Životní cyklus je časový interval od stanovené koncepce výrobku až po jeho likvidaci [2]. Životní cyklus výrobku můžeme rozdělit do několika etap. Každá etapa je specifická a má různý vliv na celkovou spolehlivost výrobku.

- Etapa koncepce a stanovení požadavků
    - V první etapě se rozhoduje, k čemu bude výrobek sloužit, a současně se specifikují jeho cíle. Z hlediska výkonnostní funkce výrobku má tato etapa největší vliv.

- Etapa návrhu a vývoje
    - Druhou etapou je etapa návrhu a vývoje. V této etapě dostává výrobek konkrétní podobu. Současně se provádí dokumentace o výrobku za účelem usnadnění výroby.

- Etapa výroby
    - V této etapě dochází k výrobě produktu.

- Etapa instalace
    - V průběhu etapy se výrobek ukládá na místo svého provozu.

- Etapa provozu a údržby
    - Výrobek vykonává činnost, pro kterou byl vyroben. Současně se na něm provádí údržba tak, aby mohl být stále v provozu. Pokud ovšem v průběhu provozu nastane situace, že se zvýší náklady na údržbu až na takovou míru, že se nevyplatí dále investovat do údržby, tak užitečný život produktu končí.

- Etapa vypořádání
    - Jinak nazývána etapou likvidace. Jedná se o poslední etapu životního cyklu, během které se ukončí používání výrobku. To znamená, že se výrobek musí demontovat a následně zničit, případně recyklovat.

1.3 Objekty

1.3.1 Obecný popis

Systém je funkční celek, který se dělí na jednotlivé objekty [2]. Objektem nazýváme jakoukoliv součást, systém, zařízení, přístroj, se kterým je možné se samostatně zabývat. Objekty můžeme nazývat např. funkční blok, součástky, komponenty atd. Objekt se dělí na opravovaný objekt a neopravovaný objekt. Opravovaný objekt je opravitelný objekt, který se po poruše skutečně opravuje. Neopravovaný objekt je objekt, který se po poruše neopravuje.

1.3.2 Stavy objektu

Provoz je stav, kdy objekt plní požadovanou funkci. Prostoj je stav, kdy objekt neplní požadovanou funkci. Nevyužitý stav je prostoj objektu v použitelném stavu v době nepožadované funkce. Pokud je objekt neschopný plnit z jakýchkoliv důvodů požadovanou funkci, tak se jedná o stav provozu neschopný.

1.3.3 Porucha

Porucha je jev znamenající ukončení schopnosti objektu plnit požadovanou funkci. Poruchový stav je stav objektu charakterizovaný neschopností plnit požadovanou funkci, kromě neschopnosti během preventivní údržby nebo jiných plánovaných činností, nebo způsobený nedostatkem vnějších prostředků. Zmíněné informace se nevztahují na objekty, které se skládají pouze ze softwaru.

Příčina vzniku poruchy může být pestrá. Od konstrukční nebo výrobní poruchy přes nesprávné použití a zacházení až po opotřebení. Poruchy můžeme charakterizovat několika způsoby. Prvním je rychlost vzniku poruchy (náhlá nebo postupná), druhým rozsah důsledků (havarijní, úplná, částečná), dále podle místa vzniku (v provozu nebo při zkoušce).

Poruchy můžeme rozdělit do několika kategorií. Prvním rozdělením jsou podstatné a nepodstatné poruchy. Druhé dělení jsou započitatelné a nezapočitatelné poruchy. Do podstatných poruch spadají občasné a periodické poruchy. Dále neověřené a vzorové poruchy. V nepodstatných poruchách jsou zahrnuty poškození zařízení, špatné zacházení, porucha zařízení způsobená přetížením z vnějšku nad rámec požadovaných zkušebních hodnot či poruchy způsobené selháním člověka.

Každá porucha může vzniknout náhodně v čase. Při větším počtu zařízení lze vypočítat střední dobu do poruchy.

1.3.4 Funkce objektu

Každý objekt můžeme charakterizovat několika funkcemi. První z nich jsou funkce hlavní. Ty jsou definovány zamýšlenými funkcemi daného objektu. Druhými jsou funkce vedlejší, které vytváří potřebu pro zajištění hlavní funkce. Následují funkce zajišťující, které mají za cíl především zajistit ochranu osob a prostředí před možným poškozením. Případné poškození může nastat v případě selhání hlavní nebo vedlejší funkce. Rovněž slouží k běžnému zajištění bezpečnosti. Informační funkce spojují monitoring, měření nebo diagnostiku a jsou reprezentovány různými indikátory či displeji. Vše ukončují funkce rozhraní, které jsou představovány rozhraním mezi posuzovaným objektem a ostatními objekty. V praxi to jsou různé ovládací prvky, spínače, vypínače, kabeláže atd.

1.4 Typy zapojení

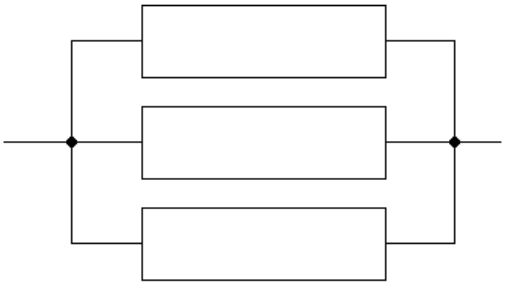
1.4.1 Sériové zapojení

Komponenty jsou řazeny za sebou. Porucha každého prvku vyvolá poruchu celého systému. Jedná se o nejhorší možné zapojení z hlediska spolehlivosti. Systém je v bezporuchovém stavu jen tehdy, pokud v bezporuchovém stavu jsou všechny komponenty.

Obrázek 1.1: Schéma sériového zapojení

1.4.2 Paralelní zapojení

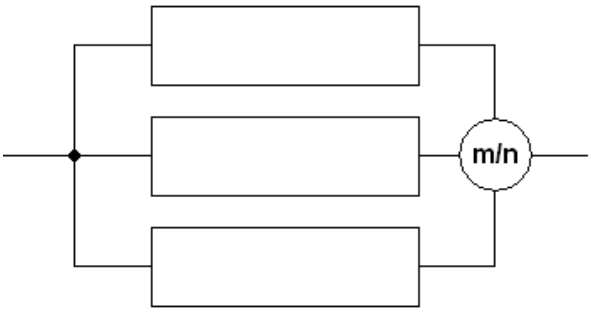
Porucha všech prvků vyvolá poruchu celého systému. Je to nejlepší možné zapojení z hlediska spolehlivosti. Systém se nachází v bezporuchovém stavu, je-li v bezporuchovém stavu alespoň jedna jeho komponenta.



Obrázek 1.2: Schéma zapojení paralelního zapojení

1.4.3 Systém m z n

K poruše systému dojde při poruše minimálně m prvků z n. Nejčastěji se používá u čidel. Nevýhodou je ovšem nákladnější projekt a realizace.



Obrázek 1.3: Schéma zapojení systému m z n

1.4.4 Ostatní

Další variantou zapojení je sérioparalelní zapojení. Systém tak obsahuje jak sériové, tak paralelní kombinace zapojení.

Každé obecné zapojení lze rozdělit na sériové, paralelní či m z n zapojení.

1.5 Metody analýzy spolehlivosti

1.5.1 Úvod

Pro provádění systematické a reprodukovatelné analýzy spolehlivosti systému je nutné používat jednotné postupy [2].

Pro konkrétní případ je nutno zvolit vhodnou analytickou metodu, která umožňuje modelovat a hodnotit spolehlivostní problémy v širokém rozsahu. Dále provádět přímou, systematickou, kvalitativní a kvantitativní analýzu a také předpovědět číselné hodnoty ukazatelů spolehlivosti. Žádná jednotlivá metoda není natolik vyčerpávající, aby zvládla všechny modely konkrétního systému.

1.5.2 Metoda výpočtu bezporuchovosti z dílů (PC)

Jedná se o induktivní metodu, která je vhodná k odhadu přibližné intenzity poruch systému [2]. Předpokládá se, že porucha je způsobena libovolnou komponentou. Obvykle se používá během časných etap návrhu, především pro elektronická zařízení. Předpověď bezporuchovosti systému je na přijatelné úrovni přesnosti. Výpočet se provádí tak, že se celý systém rozloží na jednotlivé základní komponenty a matematicky se zjistí intenzita poruch každé komponenty. Ze zjištěných intenzit poruch všech komponent se zjistí intenzita poruch celého systému.

Výhodou této metody je možnost odhadnout parametry bezporuchovosti již v době návrhu. Metoda rovněž dává nejlepší odhad parametrů bezporuchovosti v případě, že neexistují žádná data z praxe.

V případě, že nejsou známa data z provozu, je nutné pro zjištění výsledku sestavit tým odborníků schopných odhadnout frekvenci poruch komponent. A to se dá považovat za nevýhodu této metody.

1.5.3 Metoda stromu poruchových stavů (FTA)

Jedná se o deduktivní metodu, která byla poprvé využita v roce 1962 při příležitosti vývoje bezpečnosti startovacího systému rakety Minuteman [3]. V současné době je to jedna z nejrozšířenějších metod analýzy spolehlivosti, bezpečnosti, odhadu možných příčin poruch a hodnocení rizika a z nich vyplývajících důsledků poruch.

Představitelem metody FTA je logický diagram. Logický diagram znázorňuje logické vztahy mezi vrcholovou událostí a mezi příčinami vzniku této události. Příčiny

mohou být jak v provozních podmínkách, tak běžných očekávaných poruchách prvků systému, dále pak v chybách obsluhy, odchylkách provozních parametrů prvků atd. Diagram reprezentuje všechny kombinace poruch prvků, které mohou vést ke vzniku vrcholové události.

Tato metoda vyžaduje od tvůrce stromu představivost. Je nutné si uvědomit a popsat logiku rozvoje poruchy v systému a současně odhalit všechny kauzální vazby mezi prvky a poruchou. Posuzují se příčiny poruchového stavu a hledají se odpovědi na otázky: Co? Kde? Kdy? Proč? Výhodou tak je, že většina slabých míst může být odhalena již v etapě návrhu a vývoje systému.

Samotná realizace metody představuje provedení logické posloupnosti kroků, kterou lze rozdělit do pěti základních částí – přípravná část, tvorba stromu poruchových stavů, kvalitativní analýza stromu poruchových stavů, kvantitativní analýza stromu poruchových stavů a vyhodnocení analýzy.

V přípravné části musíme nejdříve shromáždit nezbytné informace o systému. Nezbytnými informacemi se rozumí konstrukční uspořádání systému, popis jednotlivých funkcí systému, předpokládané provozní režimy systému, předpokládaný systém údržby či vliv lidského faktoru na činnost systému atd. Pokud máme informace shromážděné, musíme definovat vrcholové události. Vrcholová událost je událost představující neschopnost systému plnit požadované funkce. Rovněž může znamenat začátek vzniku nebo existenci nebezpečných podmínek.

Druhým krokem je tvorba stromu poruchových stavů, která vždy začíná od vrcholové události. Další rozvoj stromu se děje analýzou vztahu mezi vrcholovou událostí a jejími příčinami. Při této analýze si pokládáme dvě základní otázky. Co by mohlo být příčinou vrcholové události? A jaká je logická vazba mezi vrcholovou událostí a jejími příčinami? Hledáme tedy všechny události, které by mohly být bezprostředními příčinami vrcholové události. Vzájemná logická vazba mezi událostmi a bezprostředními příčinami se vyjadřuje pomocí hradel. Nejpoužívanější hradla jsou hradlo AND a hradlo OR. Hradlo AND představuje událost, která nastane jen tehdy, pokud současně nastanou všechny vstupní události. Hradlo OR představuje událost, která nastane v okamžiku, kdy se na vstupu objeví kterákoliv vstupní událost.

Cílem třetí části – kvalitativní analýzy stromu je nalezení množiny minimálních kritických řezů. Případně ještě nalezení minimálních úspěšných cest. Kritickým řezem stromu poruchových stavů rozumíme takovou konečnou množinu základních, dále

nerozvíjených a jinde analyzovaných událostí, která nastane-li současně, vede ke vzniku vrcholové události. Minimálním kritickým řezem stromu poruchových stavů rozumíme takovou konečnou množinu elementárních událostí, která je sama kritickým řezem, ale současně žádná její vlastní podmnožina kritickým řezem není [3].

Předposledním krokem je určit číselné hodnoty ukazatelů charakterizujících vrcholovou událost. Ukazateli kvantitativní analýzy tak mohou být například pravděpodobnost, že vrcholová událost nastane (nebo nenastane) v zadaném intervalu provozu systému, střední doba do nastoupení vrcholové události atd. Pro výpočet těchto hodnot můžeme použít metodu přímého výpočtu, metodu minimálních kritických řezů či nějakou simulační metodu (např. metoda Monte Carlo).

Výstupem analýzy může být soupis možných kombinací provozních podmínek, podmínek prostředí, chyb lidského faktoru, či provozních poruch prvků, které by mohly vést ke vzniku nežádoucí vrcholové události. Dalším výstupem bývá pravděpodobnost, s jakou může nežádoucí vrcholová událost nastat.

V dnešní době existuje řada softwarových produktů, které značně zjednodušují praktické použití metody.

1.5.4 Metoda stromu událostí (ETA)

Jedná se o induktivní metodu, v níž se využívá grafického logického modelu (strom událostí), který identifikuje a kvantifikuje koncové stavy nehody po iniciační události [3]. Iniciační událostí může být například lidská chyba, určitá porucha zařízení apod. Stromy událostí se tedy užívají pro identifikaci scénářů nehod. Sekvence nehod zobrazené ve stromu událostí představují logické AND (a zároveň) kombinace událostí. Analýza ETA je zejména vhodná tam, kde se vyskytují složité procesy. Především se tím rozumí procesy, které mají více úrovní bezpečnostních systémů.

Výsledkem jsou scénáře nehody graficky znázorněné pomocí stromu událostí a jsou vyjádřeny jak kvalitativně tak i kvantitativně. Kvalitativní výstup obsahuje soubor poruch nebo chyb vedoucích k nehodě. Kvantitativní výstup stanoví jejich pravděpodobnosti (frekvence). V kombinaci s metodou stromu poruchových stavů (FTA) je tato metoda využívána i ke zjišťování příčin a jejich důsledků určitého jevu.

Strom událostí systematicky pokrývá časové sekvence vývoje události [2]. Tuto metodu můžeme rozdělit na další dva způsoby hodnocení. Na pre-nehodovou a post-nehodovou metodu.

Pre-nehodová metoda sleduje sérii činností bezpečnostního systému a zásahů operátora. Vyhodnocují se systémy zabraňující vzniku nehodové události.

Post-nehodová metoda má za úkol sledovat možné koncové stavy nebo následky. Post-nehodový strom událostí může být připojen do větví pre-nehodového stromu událostí, jejímž výsledkem je selhání systému.

Následky mohou být přímé nebo nepřímé. Typickým příkladem přímého následku je požár. Nepřímý následek představuje událost, která spustí nějakou další událost. Událost, která následuje po iniciační události, je podmíněna výskytem předchozích událostí. Výsledky událostí mají ve většině případů binární podobu. To znamená, že si na ně odpovíme ANO/NE. Existují ovšem i možnosti, kde se vyskytuje více výsledků. Například procento, s jakým reguluje určitý regulační prvek.

Samotná konstrukce stromu událostí, kterou můžeme rozdělit do 7 základních kroků, se kvůli přehlednosti a logice provádí zleva doprava směrem od iniciační události. Postupně se přidávají všechny bezpečnostní funkce, se kterými se zabýváme. Každá větev stromu událostí tak představuje samostatnou sekvenci událostí a koncový stav. V prvním kroku je potřeba rozpoznat iniciační událost. Iniciační událost je děj nebo stav, který iniciuje škodlivý potenciál nebezpečí v rámci scénáře jeho uplatnění [4].

Frekvence iniciační události se určuje z historických záznamů nebo analýzou FTA. V druhém kroku se identifikují bezpečnostní funkce nebo nebezpečí podporující faktory. Bezpečnostní funkce jsou vlastně zařízení nebo činnosti, které mohou přerušit sekvenci od iniciační události po nebezpečné koncové stavy. Nebezpečí podporující faktory mohou změnit koncový stav sekvence. Příkladem nebezpečí podporujícího faktoru může být zapálení úniku hořlavé látky, exploze výbušné látky, ale i meteorologické podmínky či denní a noční doba. Závěrem druhého kroku se určí výsledky jednotlivých sekvencí. Ve třetím kroku se provádí samotná konstrukce stromu událostí a to do všech významných výsledků sekvencí. Je doporučeno používat větev úspěch (ano) směrem nahoru a větev neúspěch (ne) směrem dolů. V dalším kroku se výsledky sekvencí roztřídí do kategorií podle podobných výsledků. V další analýze rizika pracujeme jen s důležitými koncovými stavy. V pátém kroku provádíme odhad pravděpodobnosti každé větve stromu událostí. Zdrojem dat pro odhad pravděpodobnosti mohou být historické záznamy, provozní data, data o lidské spolehlivosti, expertní odhady apod. V předposledním kroku provádíme kvantifikaci

výsledků sekvencí. Frekvenci konečného koncového stavu sekvence dostaneme tak, že vynásobíme frekvenci iniciační události a podmíněné pravděpodobnosti podél každé cesty vedoucí ke koncovému stavu sekvence. Správnost výsledků můžeme zkontrolovat tak, že pokud sečteme frekvence všech koncových stavů sekvencí, tak se musí rovnat frekvenci iniciační události. Posledním krokem je otestování výsledků sekvencí. Přesněji řečeno ověření reálnosti výsledků zdravým rozumem a proti historickým záznamům. Tuto činnost by měl provést nezávislý kontrolor – osoba, která se nepodílela na konstrukci stromu událostí.

1.5.5 Analýza způsobů a důsledků poruch (FMEA)

Jedná se o induktivní metodu, ve které strukturovaná kvalitativní analýza slouží k identifikaci způsobů poruch systémů, jejich příčin a důsledků [2].

Zkoumá se, jakým způsobem mohou objekty na nižší úrovni selhat a jaký důsledek mohou mít tato selhání pro vyšší úrovně systému.

Cílem metody je posoudit důsledek a posloupnost jevů pro každý zjištěný způsob poruchy prvku. Porucha může mít jakoukoliv příčinu, a to na různých funkčních úrovních systému.

Nejčastěji se tato analýza uplatňuje v etapě návrhu a vývoje jako součást přezkoumání návrhu. Dále při modifikaci a modernizaci systému či při změnách provozních podmínek. Existují tři základní způsoby, jak analýzu aplikovat. Prvním je konstrukční FMEA, druhým procesní neboli výrobní FMEA a třetím systémová (výrobková) FMEA.

Výsledky analýzy se následně mohou využít pro návrh konstrukčních změn systému, pro formulaci požadavků na provádění zkoušek či pro návrh diagnostických postupů a systémů údržby.

V případě složitých systémů je analýza složitá, pracná a časově náročná. Musí se na ní podílet odborníci z různých oborů. Analýza nezahrnuje důsledky chyb lidského činitele.

1.5.6 Analýza způsobů, důsledků a kritičnosti poruch (FMECA)

Jde o metodu FMEA rozšířenou o odhad kritičnosti důsledků poruch a pravděpodobnosti jejich nastoupení. Jedná se o semikvantitativní analýzu.

Rozdílem oproti metodě FMEA je určit významnosti nebo kritičnosti každého způsobu poruchy vzhledem k požadované funkci systému s uvážením důsledků na bezporuchovost nebo bezpečnost procesu [2]. Každý zjištěný způsob poruchy se klasifikuje podle toho, jak obtížně ho lze zjistit, testovat, diagnostikovat případně provádět kompenzační a provozní opatření. Tím se rozumí například oprava nebo údržba.

Využití výsledků analýzy je totožné s využitím výsledků analýzy FMEA.

1.5.7 Studie nebezpečí a provozuschopnosti (HAZOP)

Jedná se o jednu z nejjednodušších a nejrozšířenějších metod k identifikaci nebezpečí. Byla vyvinuta společností ICI - Petrochemicals Division ve Velké Británii a v současné době představuje uznávaný standard při posuzování nebezpečí a zajišťování bezpečnosti složitých chemických zařízení [5].

Tato metoda se používá v chemickém průmyslu pro posuzování nově projektovaných, rekonstruovaných i stávajících provozů. Metoda je vhodná jak pro velké organizační celky, tak i pro malé společnosti. Při této studii provádí kritické posouzení projektu (provozu) nevelký tým odborníků. V tomto týmu jsou zastoupeny dva typy odborníků. V tom prvním jsou techničtí odborníci. Jejich přínos spočívá v tom, že přispívají znalostmi o zařízeních, procesu, regulaci či měření. Ve druhé skupině jsou zařazeny odborníci reprezentující metodickou a konzultační činnost.

Každý úsek je posuzován systematicky s použitím série klíčových slov, které se používají tak, že si členové týmu mohou okamžitě vytvořit představu a podle toho identifikovat pravděpodobné odchylky od normálních podmínek. Dále je nutné určit, zda existuje podmínka, při níž by mohlo k odchylce dojít. Pokud tato příčina existuje, je třeba zkoumat její důsledky.

Při hodnocení metodou HAZOP se používají následující klíčová slova:

- žádný (není) ve významu, že žádné části účelu nebylo dosaženo
- více (vyšší), méně (nižší) ve vztahu k množství a vlastnostem
- rovněž (také) při situaci, že všech navržených účelů bylo dosaženo společně
- jiný než v případě, že žádná část z původního účelu nebyla dosažena

Při použití metody se nejprve musí popsat funkce (účel) systému. Následně se popíší odchylky od požadovaného účelu s využitím klíčových slov. V dalším kroku se provádí

nalezení příčin nebo kombinací příčin vedoucích k odchylce. V předposledním kroku se stanoví možné důsledky a provozní potíže. Na závěr se doporučí vhodná opatření.

1.5.8 Předběžná analýza nebezpečí (PHA)

Jedná se o induktivní metodu, která má za úkol identifikovat nebezpečí, nebezpečné situace a události, které mohou způsobit při dané činnosti poškození nebo újmu [2]. Nebezpečí se vztahuje jak k bezprostřednímu okolí systému, tak i k nebezpečí s širší sférou vlivu. Pod tím si můžeme představit například nebezpečí pro životní prostředí. Analýza se nejčastěji provádí v rané etapě vývoje produktu, kdy je k dispozici málo informací o podrobnostech návrhu. Metoda se dá rovněž uplatnit i při analyzování již existujících systémů, tam kde okolnosti brání použití pokročilejších metod.

Výsledky analýzy se následně využívají pro návrh opatření konstrukčních změn systému, formulují požadavky na provedení zkoušek. Dále identifikují nebezpečné provozní režimy a přinášejí návrh diagnostických postupů a systému údržby.

Nedostatkem této metody může být složitost, pracnost a časová náročnost v případech, když mají systémy mnoho funkcí či se sestávají z mnoha komponent. Rovněž je nutná dokonalá znalost charakteristik, práce a reakce různých komponent systému na různé provozní podmínky a podmínky prostředí. Metoda také nezahrnuje důsledek lidského faktoru.

2 Riziko

2.1 Úvod

Definovat přesně pojem riziko je obtížné. Proto zde uvedu několik možných definic. První z nich nám říká, že riziko je možnost dopadu určité události na zamýšlený plán. Podle významového slovníku je to vyhlídka na špatné následky. V ekonomii a pojišťovnictví se používá pojmu matematického očekávání, peněžní hodnoty poškození způsobených nebezpečným zdrojem. Riziko jako takové neexistuje, pokud neexistuje interakce mezi zdrojem rizika a objektem, jež má k tomuto zdroji určitý vztah. Pojem riziko se obvykle používá pouze v těch případech, pokud existuje reálný předpoklad výskytu alespoň jednoho negativního důsledku. Matematické vyjádření míry rizika je následující:

$$R = P \times D \tag{2.1}$$

Kde R značí míru rizika, P je pravděpodobnost nastoupení rizika a D je následek události.

V některých situacích můžeme ovšem matematické vyjádření rozšířit o expozici, neboli vystavení, a opatření, čili redukci. Rovnice má pak tento tvar:

$$R = \frac{P \times D}{O} \times E \tag{2.2}$$

Kde expozice má symbol E a opatření symbol O.

2.2 Management rizika

Management rizika má na starosti koordinovat aktivity pro dohlížení a řízení určité organizace při zacházení s rizikem. Management rizika obvykle zahrnuje hodnocení rizika, opatření pro snížení úrovně rizika, přijatelnost rizika a komunikaci o riziku. Často užívané termíny v managementu rizika jsou:

- Událost

  je výskyt určitého souboru okolností nebo dopadů. Událost může být jistá nebo nejistá a může být prezentována buď jediným svým výskytem anebo se může jednat o sérii výskytů.

- Důsledek

  je výstupem z události a dělí se na zisky nebo ztráty. Každá událost ovšem může mít více důsledků, které mohou být jak negativní tak pozitivní. Může být vyjádřen kvantitativně i kvalitativně. Důsledky by měly být chápany jako okolnosti, které jsou vztaženy k cílům organizace.

- Řízení

  je proces, politika, zařízení, postup či jiný druh aktivity, který je veden k minimalizaci negativních dopadů rizika nebo ke zvýšení pozitivních příležitostí.

- Frekvence

  je ukazatel počtu výskytů za jednotku času či jinou procesní jednotku.

- Zisk

  je každý pozitivní důsledek nebo možnost jeho výskytu.

- Ztráta

  je každý negativní důsledek nebo nepříznivý dopad či možnost jeho výskytu.

- Pravděpodobnost

  ve smyslu obecného pojmu (anglický ekvivalent likelihood) pro popis pravděpodobnosti (anglicky probability) a frekvence. Stupně přesvědčivosti pravděpodobnosti mohou být voleny jako třídy nebo stupně. Například řídký / nepravděpodobný / průměrný / pravděpodobný / skoro jistý. Nebo nemožný / nepravděpodobný / vzdálený / občasný / pravděpodobný / častý.

  Pravděpodobnost, v anglickém významu probability, nám vyznačuje možnost výskytu určité události. Norma ISO 3534-1:1993 tuto pravděpodobnost popisuje jako reálné číslo v intervalu od 0 do 1 vztažené k náhodné události. Tato hodnota bývá vztažena k dlouhodobé relativní četnosti výskytu nebo ke stupni přesvědčení, že daná událost nastane. Pro vysoké stupně přesvědčení je tato hodnota 1. Ovšem při posuzování rizika se může častěji vyhodnocovat frekvence než pravděpodobnost.

- Nebezpečí

  je zdroj možného způsobení škody.

- Monitorování

  nám popisuje kontrolu, dohled, pozorování kriticky a současné stanovení opatření v procesu činnosti, akce nebo systému na regulární bázi ve smyslu identifikace změny.

2.3 Pohledy na hodnocení rizika

Hodnocení rizika můžeme provádět několika přístupy. Jedním z nich je posuzovat individuální riziko. To je takové riziko, jemuž je vystaven pouze jedinec nebo objekt. Jednotlivci mohou zvýšit vlastní bezpečnost tím, že změní svůj přístup k potenciálnímu zdroji rizika. Dalším přístupem je riziko společenské. Při takovém hodnocení se posuzuje riziko, jemuž je vystavena skupina osob nebo systém. Společnost je schopna něco udělat, aby zabránila katastrofám.

Při nedobrovolném riziku je riziko uvaleno na riskující osobu (objekt) bez ohledu na možnost prospěchu či volby. Takže osoba, která je riziku vystavena, z toho nemá žádný zisk, protože neexistuje žádné vyvážení ve smyslu zisku. Naopak při dobrovolném riziku je riskující osoba (objekt) motivována dosáhnout cíle. Tudíž osoba podstupující riziko má prospěch přímo z dané události a proto je schopna vyvážit míru eventuální ztráty s mírou potenciálního zisku a určit, zda by mohla předpokládat riziko. Absolutní riziko je takové riziko, jehož základem je zkoumání přirozeného rizika, jemuž je osoba (objekt) vystavena, a kterému se nelze žádným způsobem vyhnout.

2.4 Složky managementu rizika

2.4.1 Komunikace a konzultace

Úlohou této složky je posoudit každý element v procesu, přičemž je potřeba zahrnout všechny zúčastněné strany. Proto je vhodné vytvořit komunikační plán a ustanovit osoby odpovědné za proces. Hlavním záměrem je porozumět riziku a managementu rizika.

Při komunikaci o riziku dochází k výměně či sdílení informací o riziku mezi hodnotitelem rizika a investorem. Tyto informace mohou být vztaženy k existenci, povaze, formě, pravděpodobnosti, závažnosti, přijatelnosti a dalším aspektům rizika.

2.4.2 Sestavení vnitřního a vnějšího kontextu

V této složce se určuje kontext, v rámci kterého musí být management rizika aplikován. Stanovuje se zde podstata činnosti v oblasti managementu rizika. V kontextu si musíme ujasnit organizační cíle a identifikovat prostředí, kde jsou zmiňované cíle sledovány. Dále musíme specifikovat obsah procesu, okrajových podmínek a obecných charakteristik pro ošetření rizika. V dalším kroku stanovíme kritéria, vůči kterým bude riziko a vlastní následné ošetření rizika posuzováno. Na závěr definujeme adekvátní metody a struktury pro identifikaci rizika, analýzu, hodnocení a ošetření.

2.4.3 Identifikace rizika

Ve třetí složce managementu rizika musíme provést jednoznačné určení rizika, které může ovlivnit dosažení požadovaného cíle. Proto se provádí identifikace zdroje rizika, identifikace nastalé události, identifikace a specifikace všech možných důsledků. Na závěr se určí reálné možnosti pro řízení rizika.

2.4.4 Analýza rizika

Tato složka by měla poskytnout detailní porozumění úrovni rizika a jeho povaze. Je základem pro následné ošetření rizika. Důkladná analýza nám umožňuje rozhodnout o nutnosti ošetřit riziko s předběžným odhadem nákladů a výhodnosti. Vhodnou kombinací důsledků a pravděpodobnosti získáme úroveň rizika. V analýzách rizika se systematicky využívají informace pro odhad rizika. Tyto analýzy jsou základem pro hodnocení rizika a vedou k opatřením ke zmírnění rizika. Informace mohou obsahovat historická data, teoretické analýzy, expertní odhady, názory odborníků či názory zainteresovaných stran. Výsledný odhad rizika v sobě zahrnuje identifikaci rizika, analýzu rizika a hodnocení rizika.

2.4.5 Vyhodnocení rizika

Podstatou této části managementu rizika je provedení rozhodnutí založených na analýze rizika a také na tom, zda riziko potřebuje ošetřit, či ne. Rovněž slouží ke

stanovení dalších priorit. Vyhodnocení rizika zahrnuje porovnání úrovně rizika s kritérii stanovenými pro riziko a může být podkladem pro rozhodnutí o nutnosti provedení dalších analýz.

2.4.6 Ošetření rizika

Úlohou ošetření rizika je identifikovat rozsah možností pro ošetření rizika, posoudit tyto možnosti a dále připravit a implementovat plány na ošetření rizika. Je představováno aktivním přístupem a hledáním. Založeno je na posouzení vhodných a nevhodných postupů a možností uspět. Směruje na intenzivní působení a změny spojené se závažnostmi důsledků a zvýšení pozitivních výstupů. Důležité je sdílet všechny dostupné možnosti.

Výsledkem by měla být optimalizace rizika, což je proces pro minimalizaci negativních důsledků a maximalizaci důsledků pozitivních a jejich příslušných pravděpodobností. Optimalizace rizika nám ovšem nevylučuje zbytkové riziko. Proto musíme rozhodnout o přijatelnosti rizika, která závisí na stanovených kritériích.

2.4.7 Monitorování a posuzování rizika

Poslední proces by měl odrážet postupy učiněné ve výše zmiňovaných fázích managementu rizika. V případě zjištěných nedostatků je potřeba provést znovu hodnocení rizika.

3 Lidský činitel

3.1 Chyba lidského činitele

Selhání obsluhy je jednou z nejčastějších příčin vzniku mimořádné události ve výrobním procesu. Selhání lidského činitele je podle odhadů příčinou asi 30% všech mimořádných událostí, k nimž dochází v průmyslových provozech. Jiné zdroje ovšem uvádějí až 50%. A v jaderné energetice dokonce až 90% [6]. Jedná se o jednu z hlavních příčin nehod, které většinou není věnována přiměřená pozornost.

Podle statistik, které byly vytvořeny na základě údajů získaných ve francouzských energetických závodech, patří mezi nejčastější příčiny nehod omyl, koroze, porušení svárů, chyba při údržbě, chybná identifikace zařízení (např. záměna zařízení) či opomenutí určitě činnosti. Dalšími příčinami jsou chyby v pracovních postupech a uživatelských příručkách, poruchy ze společných příčin, jazyková bariéra, chyby v nastavení a měření, chyby v důsledky nedostatku zkušeností, vliv prostředí, nedostatek informací, stres nebo nedostatečná motivace [6].

Za chybu lidského činitele se dá považovat událost, při níž plánovaná sekvence duševních nebo fyzických činností nemá požadovaný efekt a kdy výsledné selhání nelze přičíst působení nějakého náhodného činitele [6]. Podle této definice se dá za chybu považovat i například porucha zařízení. A to proto, že člověk dané zařízení navrhl a vyrobil. Jelikož při aplikaci tohoto přístupu docházelo ke zkreslování hodnocení úrovně připravenosti personálu obsluhující dané zařízení, byla navržena přesnější definice chyby obsluhy.

Tato definice zní: Chyba obsluhy je chyba v jednání zaměstnance, který neúmyslně, omylem nebo opomenutím přivede zařízení do abnormálního stavu [6]. Zmíněná definice přesněji vystihuje, co lze považovat za chybu lidského činitele, a co ne. Mezi chyby se i přes fakt, že jedná o selhání lidského faktoru, nezařazují úmyslné poškození zařízení, náhlá indispozice zaměstnance, porucha zařízení, teroristický čin apod.

3.2 Četnost lidských chyb

Stanovit přibližný rozsah pravděpodobnosti selhání obsluhy zařízení můžeme na základě Rasmussenovy taxonomie lidských chyb [6]. Podle typu vykonávané činnosti rozlišujeme tři typy činností:

- Činnosti založené na dovednostech

    - Obsluha zde automaticky vykonává pouze nacvičené úkony, nemusí se na ně vědomě soustředit
    - Pravděpodobnost vzniku chyby je asi 10^{-4} až 10^{-2}
- Činnosti založené na pravidlech
    - Obsluha zde využívá dobře známých pravidel, při klasifikaci nastalé situace se musí soustředit a vzpomenout si na správný postup.
    - Pravděpodobnost vzniku chyby je asi 10^{-3} až 10^{-1}
- Činnosti založené na znalostech
    - Obsluha zde nemá definovaný postup činností a musí tedy reagovat a vymýšlet nová pravidla, jak problém vyřešit s využitím analytického myšlení a znalostí
    - Pravděpodobnost vzniku chyby se pohybuje přibližně v rozsahu 10^{-2} až 1

3.3 Redukce vlivu chyb lidského činitele

Závažnost a četnost chyb obsluhy můžeme omezit třemi cestami. První z nich je eliminace. Eliminovat danou rizikovou činnost můžeme jednoduše tím, že se nebude vůbec vykonávat. Dalším způsobem eliminace může být zvolení jiného principu vykonávání. Metoda eliminace je nejúčinnější, ovšem pokud daná činnost prostě musí být vykonána, tak tato metoda není řešením.

Druhou cestou je cesta prevence chyb. V praxi to znamená vytvoření souboru technických a organizačních opatření, která mají za úkol snížit pravděpodobnost vzniku chyby. Z toho vyplývá zvýšení spolehlivosti lidského činitele. Pro tuto cestu je vhodné aplikovat metodu Poka-Yoke, jejíž předností je jednoduchost a nízké náklady.

Poslední cestou je cesta represe. Hlavním úkolem represe je omezit následky selhání lidského činitele. Tato metoda se uplatňuje v případech, kdy nebyla prevence dostatečně účinná. Představitelem represe je například tzv. donucovací funkce, která přeruší určitou činnost až do okamžiku, kdy dojde k vyřešení problému.

Jelikož člověk není tvor neomylný, tak dělá chyby. Povinností zaměstnavatele je proto snaha o eliminaci nebo alespoň snížení pravděpodobnosti jejich vzniku. U každé činnosti je vhodné zvážit a zmírnit negativní vlivy na spolehlivost obsluhy.

4 Analýza spolehlivosti člověka

4.1 Historie a vývoj

Počátky rozvoje oblasti, která se zaměřuje na spolehlivost lidského činitele, lze nalézt na počátku 20. století ve Spojených státech amerických. Přesněji se jednalo o rok 1911, kdy pánové Gilbreth a Taylor položili základy pro rozvoj složitějších analytických nástrojů. Byly definovány taxonomie dovedností založené na psychometrické konstrukci, které se staly myšlenkovým základem pro většinu dnešních analytických metod [7].

Další rozvoj v oblasti posuzování spolehlivosti lidského činitele zapříčinila druhá světová válka. Konkrétně se jednalo o obor letecké techniky. Konstruktéři letadel přemýšleli nad tím, proč mají nováčkové potíže s ovládáním stroje. V jedné chvíli bylo dokonce na straně spojenců ztraceno více letadel v důsledku chyb pilotů, než bojových akcí nepřítele [7]. Díky podrobné analýze činností pilotů došli odborníci ke zjištění, že je nutné změnit ovládací a sdělovací systém tak, aby více vyhovoval lidské přirozenosti. Tímto krokem byly položeny základy systematického přístupu, který se již nesoustřeďoval parciálně jen na některé faktory a prvky, ale integrálním přístupem zohledňoval vazby mezi strojem a člověkem od jeho samotného návrhu, přes konstrukci až k ovládání a užívání.

Po skončení 2. světové války byla hlavní oblastí zkoumání oblast jaderného průmyslu. V této oblasti vznikly počátkem 50. let první aplikace skutečně rozvinutých analýz lidského činitele. V USA se jednalo o techniky zaměřené na předpověď vzniku lidské chyby, které byly zpočátku vyvíjeny jako kvalitativní kontrolní metody. V roce 1972 vytvořil A. D. Swain Techniku pro předpověď míry lidské chyby. V anglickém znění Technique for Human Error Rate Predicition, nejčastěji se používá ve formě zkratky THERP. Práce A. D. Swaina byla následně rozšířena i o lidské chyby při úkolech řízení provozu se zvláštním zřetelem na provoz jaderných reaktorů. Zmiňované rozšíření se využilo v Rasmussenově zprávě, která je známa jako WASH-1400. Tato zpráva se stala základem pro metody rozvíjené právě pro potřeby jaderné energetiky.

V průběhu 70. a 80. let se vyvíjela tzv. kognitivní psychologie (kognitivní znamená mající poznávací) [7]. Teorie a poznatky aplikované při analýze lidské spolehlivosti s sebou přinesly změny v náhledu na člověka. Člověk byl nyní posuzován jako černá skříňka k využití poznatků, že jednotlivci mají určité úmysly a že jejich akce jsou ovlivňovány budoucími cíli a plány. Zmiňovaný přístup lze uplatnit především na

činnosti plánování a jednání v mimořádných situacích. Tento přístup je nejúplnější z hlediska hodnocení příčin chyb, které jsou v pozadí jevové stránky. To znamená, že je obzvláštně relevantní pro analýzu opakujících se chyb a pro predikci specifických chyb, které mohou mít závažné důsledky, což je součást analýzy bezpečnosti [7].

Poněvadž se velmi často ukazovalo, že velká část nehod a havárií v chemickém průmyslu byla způsobena chybou člověka, tak se zájem o téma spolehlivosti lidského činitele přenesl i sem. Dnes se uvádí, že chybou lidí bylo způsobeno až 80% nehod a havárií. Spouštěcí událostí byla havárie chemického provozu švýcarské firmy Givaudan v italském Sevesu v roce 1976. Zde se vyráběl herbicid TCP a během havárie do ovzduší unikly asi 2 kg dioxinu, které zamořily téměř 2 000 hektarů půdy v okolí. Na následky otravy onemocnělo asi 200 lidí. V reakci na havárii byla vypracována a v roce 1982 schválena evropská směrnice 82/501/EEC týkající se prevence a minimalizace negativních účinků průmyslových havárií. Tato směrnice je známa jako Direktiva SEVESO I. V prosinci 1996 ji nahradila podrobnější směrnice 96/82/EC, nazývána jako Direktiva SEVESO II. V ní jsou definovány požadavky na vypracování rizikových analýz, které spolehlivost lidského činitele zahrnují. V České republice byla tato směrnice přijata až v roce 1999 v podobě zákona o prevenci závažných havárií (353/1999 Sb.). Později byl nahrazen zákonem č. 59/2006 Sb [7]. Pro účely zákona jsou provozovatelé objektů nebo zařízení s rizikem vzniku závažné havárie povinni vypracovávat posouzení vlivu lidského činitele v souvislosti s významnými zdroji rizik. Posouzení musejí zpracovat jak pro normální provozní podmínky, tak i pro mimořádné provozní podmínky.

4.2 Filozofie HRA

4.2.1 PSF

Faktory, které přímo ovlivňují schopnost lidí spolehlivě plnit úkoly, nazýváme faktory ovlivňující výkon. Zmíněné faktory se liší v závislosti na vnitřních a vnějších podmínkách. Každý člověk ovšem na jednotlivé podmínky reaguje jinak. Podmínky se rovněž liší v čase. Ve složitějších systémech je mnoho faktorů, které lidský výkon ovlivňují. Tyto faktory mohou mít jak pozitivní vliv, kde výkonu pomáhají, tak vliv negativní, při kterém brání úspěšnému vykonání úkolu. Podle publikace Human Factors in Safety and Reliability [9] můžeme PSF rozdělit na dva typy:

- Vnitřní PSF

Můžeme rozdělit na schopnost výkonu a připravenost (pohotovost). Tyto faktory představují fyziologické a psychologické rozdíly mezi osobami. Tím se rozumí lidská omezení a rozdíly ve velikosti a síle, rozdíly ve zkušenostech, dovednostech, talentu, znalosti. Dále jsou to psychické změny a motivační faktory. Zahrnuje se sem charakteristika obsluhy. Patří mezi ně zkušenosti, úroveň výcviku (proškolení), obeznámenost s úkolem, zdravotní stav či motivace.

- Vnější PSF

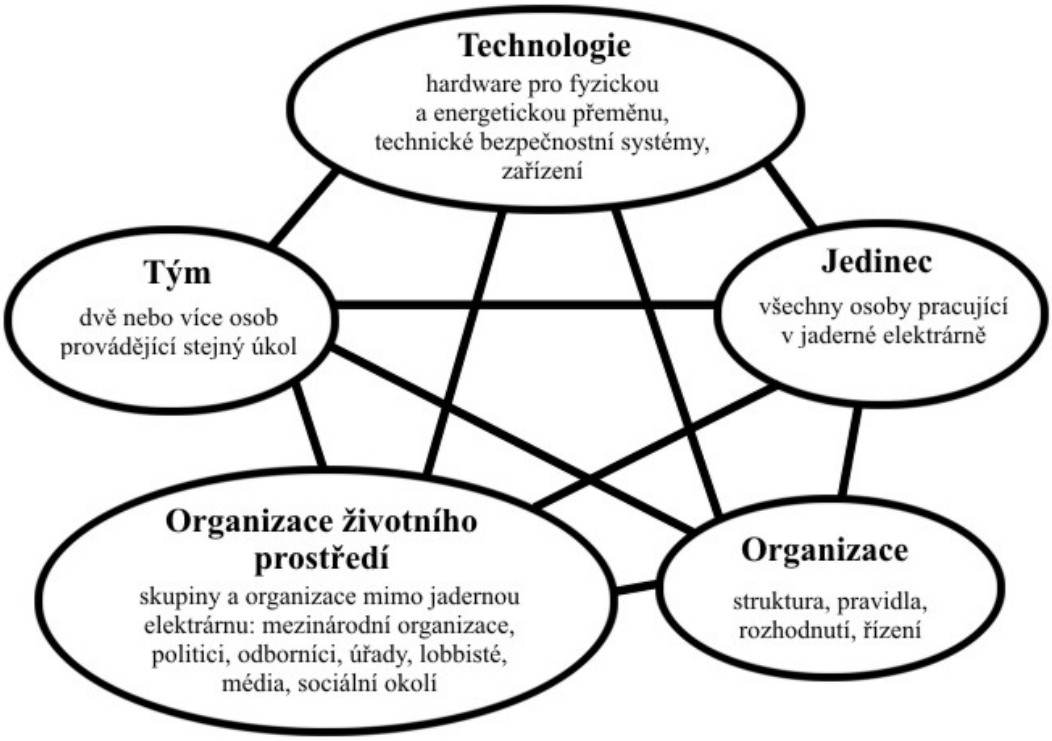
  Jsou výsledkem organizačních a technických předpokladů. Organizační předpoklady mohou být často popsány kvalitativně. Technické předpoklady, včetně návrhu zařízení na straně jedné a životní prostředí na straně druhé, bývají nejčastěji popsány kvantitativně. S přihlédnutím k významu vnějších vlivů můžeme obvykle rozlišit lidské chyby v rámci analýzy hlavních příčin a latentní chyby. Některé faktory chápeme jako reakci člověka na navrhované změny:

  - Změna v rozhraní člověk – systém: Změnily požadované změny významně rozhraní člověk – systém, jenž pracovníci potřebují k plnění úkolů?
  - Změna v postupech: Změnily požadované úpravy významně plnění úkolů nebo pro plnění úkolu nejsou definovány postupy?
  - Změna ve výcviku: Změnily požadované změny významně odbornou přípravu nebo úkoly, které nejsou součástí výcviku?

Latentní chyby představují nejvyšší hrozbu pro bezpečnost ve složitých systémech. Vznikají totiž z událostí, které nemají nic společného s přímou kontrolou a slučují se s dalšími faktory. Rozlišujeme následující skryté chyby: řízení, systémové, komunikační, návrhové, technické, regulační, chyby hlášení, údržby, postupu, hardwaru, školení [9]. V případě těchto chyb jedna příčina nikdy nevede k nehodě. K nehodě dojde pouze ve spojení s jinými faktory.

Celkový výkon komplexního systému je určen rozhraním mezi člověkem, technologií a organizací. Člověk musí sledovat individuální

parametry jako je pozornost a způsobilost. Dále pak požadavky na pracovní pozici jako je složitost úloh nebo časový tlak, aspekty týmové práce, sociálních vztahů. Člověk rovněž musí zohlednit organizační podmínky (komunikační struktura, organizační kultura, dostupnost a vhodnost postupů).



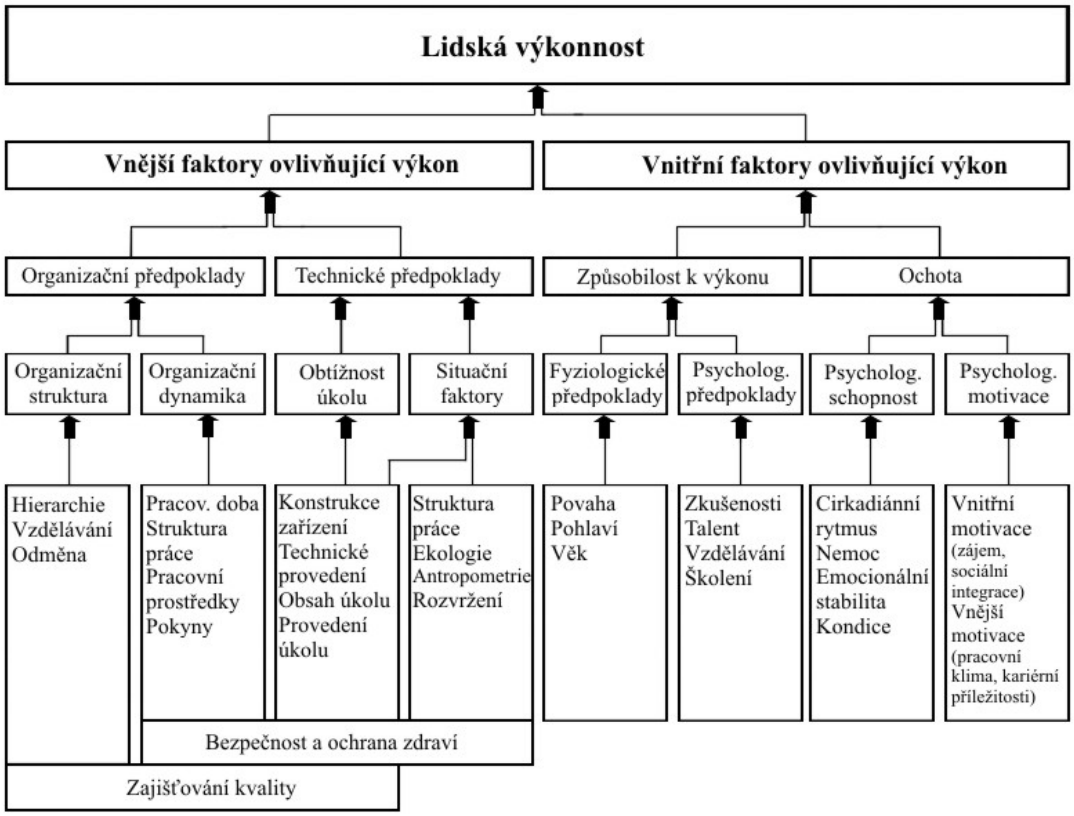
Obrázek 4.1: Subsystémy lidského faktoru [9]

Při analýze lidské spolehlivosti musíme uvažovat především následující faktory:

- Kvalitu řízení (postupu, metody, procesu)
- Kvalitu rozhraní v systému člověk – stroj (kontrolní pomůcky, indikátory atd.)
- Úroveň vzdělání obsluhy, operátora (výcvik, školení, praxe)
- Složitost úkolu (odbornost obsluhy, pravidla postupu)
- Úroveň stresu operátora
- Čas k dispozici nebo časová naléhavost (obojí možné kombinovat se stresem)
- Podmínky (pracovního) prostředí (hluk, osvětlení, teplota apod.)
- Komunikace mezi pracovníky
- Předchozí reakce

Dále je důležité poznamenat, že řídící a organizační faktory mohou být důležitými faktory ovlivňující výkon. Avšak při analýze lidské spolehlivosti obvykle nejsou explicitně uvažovány. Vliv těchto faktorů se zahrnuje u faktorů, jako jsou kvalita řízení (postupu, metody, procesu), školení personálu, kultura bezpečnosti či rozhraní systému člověk – stroj.

Přímým začleněním řídících a organizačních faktorů do analýzy lidské spolehlivosti se zabývá například studie v publikaci NUREG/CR-5752 [12].



Obrázek 4.2: Faktory ovlivňující lidský výkon [8]

4.2.2 Proces analýzy HRA

Pro určení pravděpodobnosti chybného provedení úlohy je nutno přesně definovat případy a stavy lidského selhání. Pravděpodobnosti lidských chyb jsou úzce spjaty s pravděpodobnostními událostmi a výskytem závad u hardwarových či softwarových komponent a okolními podmínkami.

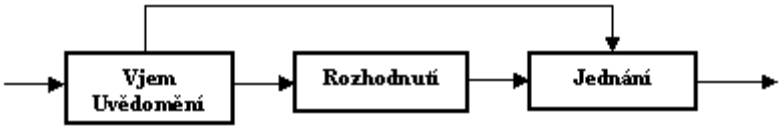
Pro pravděpodobnostní odhad lidské spolehlivosti existuje několik metod. Mezi nejznámější pak patří:

- THERP (Technique for Human Error Rate Predicition)
- SLIM (Success Likelihood Index Method)
- HRC (Human Cognitive Reliability)
- ESAT (Expertensystem zur Aufgaben)

Metody můžeme následně rozdělit do dvou generací.

Metody HRA první generace jsou založeny na hypotéze, že chyba v systému je určena interpretací a průběhem alarmu, druhem a charakterem lidského jednání [11]. Tyto metody jsou v dnešní době používány především v provozech jaderných elektráren, v chemických či vojenských oblastech. Do metod HRA první generace řadíme THERP, SLIM a ASEP (Accident Sequence Evaluation Program).

Pro zmiňované metody je charakteristický model procesního rozhraní. Tento model má tři základní prvky.



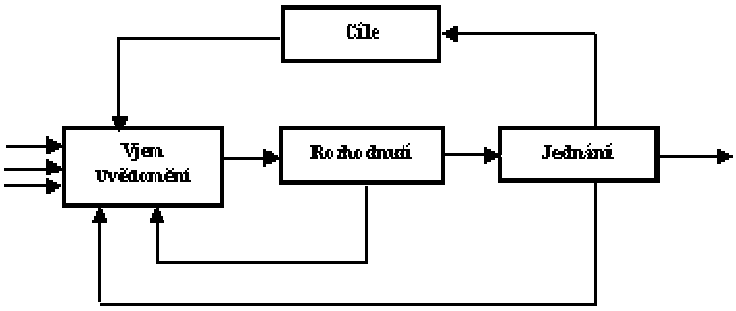
Obrázek 4.3: Model zpracování informace – postupy analýzy první generace metod HRA [11]

Jak lze z obrázku 4.3 vypozorovat, tak lidské jednání je v tomto případě založeno na přesném pořadí jednotlivých procesů. To znamená, že člověk reaguje na událost, vjem nebo pozorovaný signál. Pokud vynecháme proces rozhodování, což je možné, tak dostaneme zkrácený proces lidské reakce. Z mnoha odvětví můžeme slyšet, že existuje pouze jediná správná reakce člověka na alarm nebo neočekávaný výpadek. Tato správná reakce následně vede k uvedení systému do bezpečného stavu. Pokud ovšem člověk nezareaguje podle předem daného scénáře, tak je jeho chování vyhodnoceno jako chybné. V tom případě nese plnou zodpovědnost za konečné selhání systému.

Metody HRA druhé generace posuzují lidskou spolehlivost na pozadí. A to z pohledu lidských vlastností, schopností a cílů, které významně ovlivňují lidské chování při chybě nebo poruše systému člověk – stroj [11].

Do této skupiny metod HRA patří například metody ATHENA (A Technique for Human Error Analysis), CAHR (Connectionism Assessment of Human Reliability),

CREAM (Cognitive Reliability and Error Analysis Method). Uvedené metody mimo jiné zohledňují kognitivní (poznávací) chování člověka.



Obrázek 4.4: Model zpracování informace – postupy analýzy druhé generace metod HRA [11]

Člověk se vyznačuje mnohem větší variabilitou a komplexitou, než má technika. To prakticky znamená, že se člověk ve stejné situaci nechová vždy stejným způsobem. Takže stejnou úlohu nebo činnost provádí různými způsoby, aniž by to mělo na bezpečnost systému vliv. Právě z důvodu různé reakce a činnosti obsluhy je obtížné stanovat pravděpodobnostní odhad lidské chyby.

Parametry a znaky lidské spolehlivosti jsou podobné jako při výpočtech spolehlivosti zařízení. Pro kvantitativní určení spolehlivosti lidského chování se nejběžněji používá parametr odhadu pravděpodobnosti lidské chyby, který má zkratku HEP (Human Error Probability). Jeho hodnota je dána jako poměr počtu sledovaných chybných úkonů n vůči celkovému počtu N provedených úkolů, viz následující vztah:

$$HEP = \frac{n}{N} \tag{4.1}$$

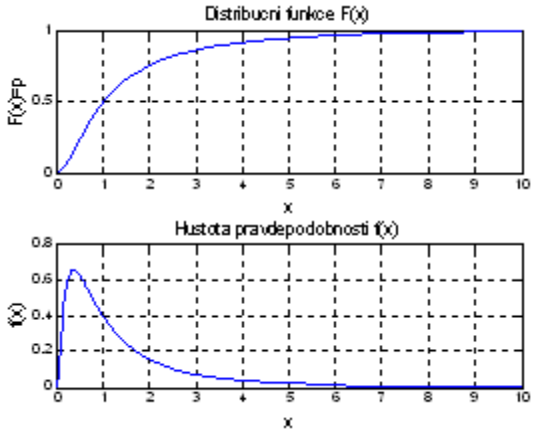
Stejně jako u technických systémů, kde určuje pravděpodobnost poruchy a pravděpodobnost bezporuchového stavu, tak i zde lze vypočítat pravděpodobnost úspěšného provedení dané operace člověkem. Pro toto vyjádření se využívá zkratky HSP (Human Success Probability) a vypočítá se podle následujícího vztahu:

$$HSP = 1 - HEP \tag{4.2}$$

Pravděpodobnost lidské chyby je uváděna jako spojitě náhodně rozdělená veličina, která je popsána typem svého rozdělení. Pro vyhodnocování pravděpodobnosti lidských chyb se velmi často používá logaritmické rozdělení LN(μ, σ^2). Přirozený logaritmus ln x

náhodné veličiny X se řídí logaritmickým normálním rozdělením s hustotou pravděpodobnosti f(x) podle vztahu [11]:

$$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} exp\left[-\frac{(\ln x - \mu)}{2\sigma^2}\right] \tag{4.3}$$



Obrázek 4.5: Logaritmicko-normální rozdělení [11]

Při zjišťování spolehlivostních parametrů μ a σ^2 mohou ovšem nastat problémy, zvláště v případech, kdy je pozorování prováděno pouze v jediném systému člověk – stroj. V tom případě je totiž počet vysledovaných chybných lidských činností omezený. Dalším problémem může být nedostatečná významnost takto získaných dat. Proto je vhodné provádět pozorování ve více systémech, které jsou srovnatelné. Tím vznikne větší datová databáze, která zároveň bude více objektivní. Srovnatelnost systémů však musí být jednoznačně prokazatelná.

Postupy metod HRA je možné vystihnout pomocí tzv. postupových kroků. Tyto kroky na sebe navazují v různých rovinách spolehlivostní analýzy lidského jednání.

POSTUPOVÉ KROKY	OBSAH
Určení zkoumaného systému	
Identifikace a stanovení úloh pro člověka zakomponovaného do (v) systému	• Popis zkoumaných a hodnocených lidských komplexních jednání, chování, činů. • Stanovení rozsahu, okrajových podmínek a kvalitativních parametrů analýzy
Kvantitativní analýza činností a úloh	
Sběr informací	Sběr informací o úkolu, roli nebo činnosti člověka v hodnocené situaci
Analýza hodnoceného úkolu	• Analýza průběhů jednotlivých elementárních činností • Kvalitativní a kvantitativní hodnocení činností podle zvoleného modelu
Identifikace možného chybného jednání	Hodnocení jednotlivých činností analyzované úkoly se zřetelem na potenciálně chybné lidské jednání
Identifikace faktorů *PSF*	Faktory PSF tvoří soubor parametrů modelu, které dovolují přizpůsobování spolehlivostních parametrů
Identifikace možných oprav či korektur chyb	Chybná chování mohou být kompenzována pomocí systémových nebo procesních charakteristik

Tabulka 4.1: Způsob postupu při analýze lidské spolehlivosti HRA [11]

Při kvantitativních analýzách se používá kvantifikace vztažená k jednotlivým elementárním činnostem. Toho využívá metoda THERP, jenž má vypracovanou příručku, ve které je obsažen seznam více jak 100 typů konkrétních hodnot pravděpodobností chyb HEP.

4.3 Metoda TESEO

Jedná se o metodu specifickou a odlišnou od ostatních metod analýzy lidského činitele. Ze všech metod je tato metoda nejjednodušší a vyžaduje nejmenší materiální a kapacitní zdroje. K odhadu spolehlivosti lidského činitele metoda využívá pět klíčových faktorů. Tyto faktory byly oceněny jako nejdůležitější mezi všemi faktory ovlivňující pravděpodobnost lidské chyby.

Klíčové faktory jsou:

- Typ realizované aktivity (K_1)
    - Faktor typu činnosti

- Čas, který je k dispozici pro provedení aktivity (K_2)
    - Stresový faktor běžných činností, případně stresový faktor mimořádných činností

- Charakteristika personálu (K_3)
    - Faktor operátorských kvalit

- Psychický stav personálu (K_4)
    - Faktor úzkosti a stresu

- Místní pracovní podmínky (K_5)
    - Ergonomický faktor

Výsledná pravděpodobnost lidské chyby při realizaci dané aktivity se vypočítá jako:

$$P(HEP) = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5 \quad (4.4)$$

Konkrétní numerické hodnoty jednotlivých faktorů K_i lze získat z tabulek. Pokud součin všech pěti faktorů dosáhne numerické hodnoty větší než 1, předpokládá se, že pravděpodobnost lidské chyby je rovna jedné.

Nevýhodou metody TESEO je nedostatečné teoretické ověření numerických hodnot jednotlivých uvážených faktorů i jejich vlastního výběru pro některé specifické případy.

Naopak výhodou metody je její rychlost a snadnost jejího použití. Metodu je vhodné použít pro srovnávací výpočty.

Typ činnosti	**K_1**
Jednoduchá, rutinní	0,001
Vyžadující si pozornost, rutinní	0,01
Neobvyklá	0,1

Tabulka 4.2: Numerické hodnoty faktoru K_1 [2]

Doba pohotovosti pro běžné činnosti [s]	**K_2**
2	10
10	1
20	0,5

Tabulka 4.3: Numerické hodnoty faktoru K_2 [2]

Doba pohotovosti pro mimořádné činnosti [s]	**K_2**
3	10
30	1
45	0,3
60	0,1

Tabulka 4.4: Numerické hodnoty faktoru K_2 [2]

Operátorovy kvality	**K_3**
Pozorně zvolený, expert, dobře školený	0,5
Průměrné znalosti a školení	1
Malé znalosti, chabé školení	3

Tabulka 4.5: Numerické hodnoty faktoru K_3 [2]

Činnost faktoru úzkosti a stresu	**K_4**
Stav vážného nepředvídaného případu	3
Stav vážného potenciálně nepředvídaného případu	2
Normální stav	1

Tabulka 4.6: Numerické hodnoty faktoru K_4 [2]

Činnost ergonomického faktoru	**K_5**
Vynikající mikroklima, vynikající koordinovanost s provozem	0,7
Dobré mikroklima, dobrá koordinovanost s provozem	1
Rušené mikroklima, rušená koordinovanost s provozem	3
Rušené mikroklima, chabá koordinovanost s provozem	7
Špatné mikroklima, chabá koordinovanost s provozem	10

Tabulka 4.7: Numerické hodnoty faktoru K_5 [2]

4.4 Metoda THERP/ASEP

Metoda THERP (Technique for Human Error Rate Prediction) je nejvíce uspořádaná, podrobná a široce využívaná metoda analýzy lidské spolehlivosti v oblasti jaderné energetiky. Pánové Swain a Guttman definovali THERP jako metodu k předpovědi pravděpodobnosti lidské chyby a ohodnocení degradace systému člověk – stroj způsobenou buď pouze lidskou chybou, nebo v souvislosti se špatnou funkcí zařízení, provozními postupy a praxí či dalšími lidskými vlastnostmi ovlivňující chování systému [9]. Využívá se zde klasické spolehlivostní techniky s možností počítat s větší variabilitou, nepředvídatelností, zahrnovat faktory ovlivňující výkon a vzájemné propojení lidského výkonu a výkonu daného zařízení. Základní model THERP umožňuje v daném prostředí získat pravděpodobnost lidského selhání. Rovněž nám umožňuje zjistit stav mysli jedince, případně celé skupiny, vykonávající úkoly. Faktory ovlivňující výkon jsou odpovědné za změny v pravděpodobnosti lidské chyby. THERP se skládá z následujících klíčových prvků:

- Analýza úkolů

  Metoda THERP je na něm silně závislá. Je důležité jej provézt podrobně a řádně. Výsledkem rozboru událostí je logický strom událostí.

- Model odezvy alarmu (ARM)

  Pro události, které jsou signalizovány po nehodě prostřednictvím alarmu či jiné signalizace.

- Křivka časové spolehlivosti (TRC)

  Pro případy, které jsou silně časově závislé a kdy se především reaguje na základě diagnózy nebo rozhodovacího procesu.

- Obnova mechanismů

  V analýze lidské spolehlivosti by se ve spojení se stromem událostí měly objevovat faktory jako je kontrola druhými osobami, přijetí nových indikací či alarmů, údržbové kontroly, příchod nových pracovníků.

Pro všechny úlohy se základní pravděpodobnost lidské chyby odhaduje. Podmínkou odhadu je vhodné pracovní rozpoložení (např. optimální stres, dobře vyškolený pracovník, odezva rozumově založená na pravidlech atd.). U všech základních pravděpodobností lidských chyb uvažujeme logaritmické rozdělení. Medián a EF (chybový faktor – error factor) jsou používány pro všechny základní pravděpodobnosti lidských chyb. Korekční koeficienty pro silnější nebo slabší faktory ovlivňující výkony se upravují a vycházejí z odchylek od průměrné hodnoty základních pravděpodobností lidské chyby. Závislost modelu je vyvinuta pro popis potenciální závislosti mezi více úkolů. Závislost mezi dvěma úkoly je rozdělena do pěti úrovní [9]:

a) Nulová závislost
b) Nízká závislost
c) Střední závislost
d) Vysoká závislost
e) Úplná závislost

Nulová závislost se vztahuje na případ, ve kterém vykonání nebo nevykonání prvního úkolu nemá žádný vliv na provedení úkolu druhého. Nízká závislost představuje takový stupeň závislosti, ve kterém je větší než nulová, ale není moc vzdálená od kontinua závislosti. Střední závislost leží mezi nízkou a vysokou závislostí. Vysoká závislost je závislost, která je přibližně uprostřed mezi střední a úplnou závislostí na kontinuu závislosti. A úplná závislost představuje takovou závislost, kdy selhání provedení prvního úkolu bude mít za následek selhání vykonávání dalšího úkolu.

Metoda ASEP (Accident Sequence Evaluation Program) je vlastně zjednodušená verze THERP pro předběžné hodnocení s pesimistickou tendencí. Kritické úkoly jsou rozčleněny na dílčí úkoly. Ty jsou následně uspořádány podle lidské výkonnosti do stromu událostí. Pravděpodobnosti lidských chyb pro dílčí úkoly jsou získány z tabulek uvedených v publikaci NUREG/CR-4772 [10].

V uvedené směrnici [10] je také uvedeno použití pro pravděpodobnosti lidských chyb v závislosti na faktorech ovlivňujících výkon. Standardizovaný postup rozkladu metodou ASEP se provádí na kritické činnosti a diagnostiku poruch v případě potřeby. Rovněž je doporučeno pro každou kritickou činnost uvést pravděpodobnost lidské chyby s tím, že podrobný odhad pro rozhraní člověk – stroj není požadován. Křivky časově související diagnostiky pravděpodobnosti lidské chyby jsou založeny na základě dohody odborníků. Ty umožňují rychlý předvýběr důležitých úkolů.

Metodu ASEP je vhodné použít v případě, že potřebujeme rychlý odhad.

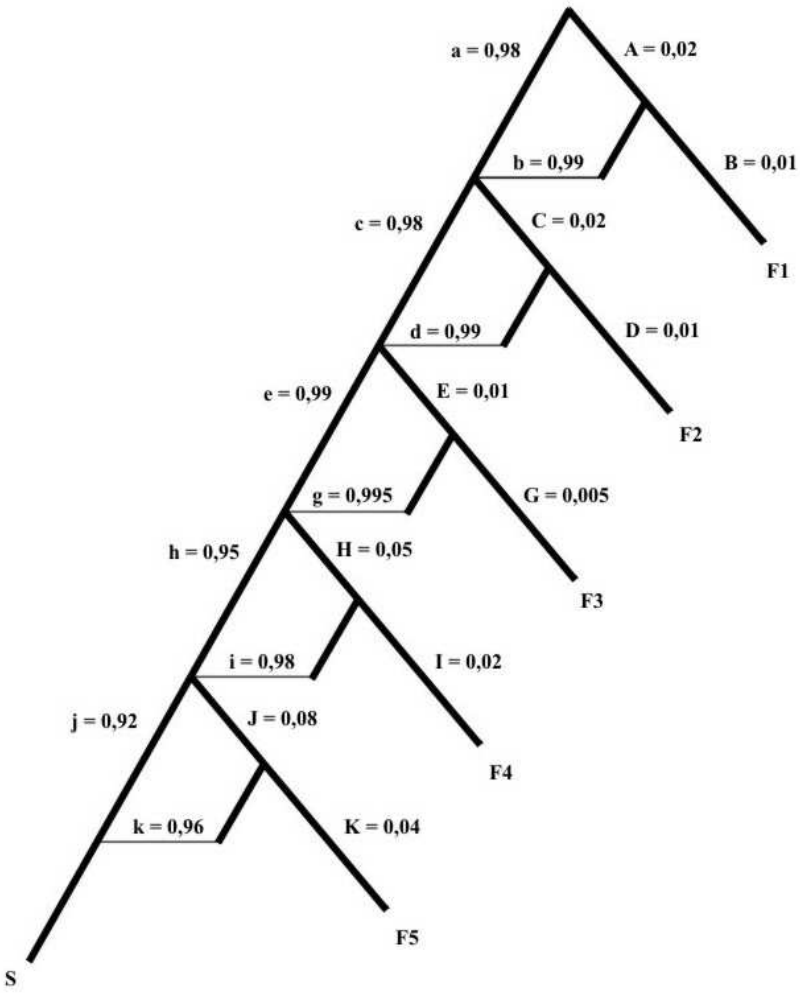
Jednoduchý ilustrační příklad - soustružení:

Uvažujme pracoviště, na kterém se nachází soustruh. Na soustruhu pracuje jeden zaměstnanec - dělník, kterému je činnost určována vedoucím pracovníkem – mistrem. Mistr se zdržuje ve stejné místnosti jako dělník. Proto se na něho dělník může obrátit v případě nejasností či problémů.

Jednotlivé podúlohy (včetně jejich pravděpodobnostních charakteristik) procesu výroby součásti:

1. Pochopení technického výkresu součásti. Pravděpodobnost, že dělník špatně pochopí technický výkres je (událost A) 0,02. Pokud by dělník měl pocit, že výkres špatně pochopil, tak se obrátí na mistra, čímž sníží pravděpodobnost nepochopení výkresu (B) na 0,01.
2. Stanovení technologického postupu výroby. Pravděpodobnost, že dělník zvolí špatný postup výroby (C) je 0,02. Pokud postup vyvstalý problém projedná s mistrem, sníží pravděpodobnost špatného postupu (D) na 0,01.
3. Správné upnutí nástroje a obrobku. Pravděpodobnost toho, že nástroj nebo obrobek bude špatně upnut (E) činí 0,01. I v tomto případě je možná konzultace s mistrem. Tím dojde opět ke snížení pravděpodobnosti (G) na 0,005.
4. Správná volba řezných podmínek. Pravděpodobnost, že dělník nastaví špatné řezné podmínky (H) je 0,05. Zásah mistra (I) sníží pravděpodobnost chyby na 0,02.
5. Kontrola rozměrů posuvným měřítkem. Pravděpodobnost špatného změření výrobku dělníkem (J) činí 0,08. Pravděpodobnost špatného změření výrobku mistrem (K) je 0,04.

Strom pravděpodobností pro soustružení vypadá takto:



Obrázek 4.6: Strom pravděpodobností pro úlohu práce na soustruhu

Celková pravděpodobnost úspěšného vyrobení požadované součástky je:

$S = (a + Ab)(c + Cd)(e + Eg)(h + Hi)(j + Jk) =$ $(0{,}98 + 0{,}02 \cdot 0{,}99)(0{,}98 + 0{,}02 \cdot$ *0,990,99+0,01·0,9950,95+0,05·0,980,92+0,08·0,96=0,9998·0,9998·0,99995·0,999·0,996* 8 ≅ 0,99535 (4.5)

Pravděpodobnost neúspěchu pak je:

$F = (1 - S) = 1 - 0{,}99535 = 0{,}00465$ (4.6)

Jednotlivé pravděpodobnosti lidských chyb byly zvoleny náhodně. Příklad především slouží k demonstraci použití stromu pravděpodobnosti.

5 Vstupní data pro kvantitativní hodnocení pravděpodobnosti lidské chyby

5.1 Databanky

Od prvopočátků HRA byla snaha shromažďovat data k tomu, aby bylo možné HRA vyjádřit kvantitativně. Toto úsilí pokračuje i v dnešní době v podobě systému úložiště a analýzy lidských událostí (HERA – Human Event Repository and Analysis). Pro NASA a Velkou Británii byla vyvinuta databáze lidských výkonů, která nese označení CORE [9].

Údaje o lidském faktoru se obvykle shromažďují s využitím empirických pozorování. Například se jedná o pozorování, jak sledovaná osoba reagovala na vzniklý problém. Na základě této analýzy můžeme předpokládat, které projevy povedou k chybě a které k úspěchu. Důležitým aspektem analýzy je, že se pomocí PSF zkouší odpovídat, proč se konkrétní výkon projevuje. Analýza spolehlivosti člověka se jednoznačně snaží zodpovědět otázku, jak často chyba nebo úspěch nastane.

V lidských činitelích jsou zahrnuty následující typy údajů [9]:

a) Normativní údaje

   Vychází z názorů vizionářů a teoretiků, kteří formulují hranice rozhraní výpočetních technologií. Vedoucímu projektu předkládají, které funkce by se měly zařadit do další verze software. Vedoucí projektu tyto funkce seřadí podle důležitosti a rozhodne, které budou zařazeny. Normativní intuice může omezit, rozšířit nebo vyjasnit problém lidských faktorů. Rovněž může přispět k nápravě chybných úvah.

b) Sebepozorující údaje

   Jsou odvozeny z představ o vlastních duševních procesech. Využívají se při navrhování designu, kde se rozhodujeme, zda konkrétní rozhraní je použitelné a bezpečné. Sebepozorující data jsou často získaná prostřednictvím protokolu analýzy. Při jeho vyplňování je uživatelům systému doporučeno myslet nahlas. Tím je hodnotiteli umožněno pochopit, zda je systém intuitivní, nebo není.

Normativní a sebepozorující údaje jsou striktně údaji o jakosti. Abychom u nich dospěli k závěrům, není nutné u nich použít numerické či statistické

rozbory. To se netýká následujících třech typů, které jsou v první řadě kvantitativní. U nich je před závěrem nutné nějakou analýzu, zpracování dat, provést.

c) Údaje získané pozorováním

Jsou kvantitativní údaje, které jsou dostupné bez obtěžování uživatele. Tato metoda se často nazývá přirozené pozorování. Zahrnuje v sobě minimální manipulaci s podmínkami prostředí. Výzkumník jednoduše sleduje přirozeně se vyskytující interakce mezi uživatelem a systémem. Údaje získané pozorováním jsou nicméně náchylné k chybám způsobené vlivem prostředí, což, může občas dělat výsledky výzkumu neprůkaznými.

d) Experimentální údaje

Byly získány za pečlivě kontrolovaných podmínek. Specifický aspekt interakce mezi uživatelem a technologickým systémem je manipulovatelný. Vlivy obsluhy jsou pečlivě měřeny. Následně je možné porovnat efekt obsluhy s kontrolní podmínkou. Pokud nastane rozdíl v interakci, tak za příčinu té interakce je považována obsluha. Z historických důvodů jsou experimentální údaje základem psychologie poznání, a proto jsou poměrně rozšířeny v oblasti lidských faktorů.

e) Vymodelované údaje

Tato forma údajů je obměnou experimentálních dat. Hlavní rozdíl spočívá ve zdroji dat. Experimentální údaje jsou do jisté míry závislé na lidských účastnících, kdežto vymodelované údaje výslovně lidské účastníky nepotřebují. Údaje jsou získávány výpočtem metodou lidského faktoru. V některých případech se výsledky porovnávají s výsledky skutečné lidské výkonnosti, v jiných případech pak s výsledky jiných simulací. Výsledkem je míra úspěšnosti simulace vůči odpovídajícím lidským interakcím s technologickými systémy.

Pro závod jaderné elektrárny je specifické, že lidské spolehlivostní údaje se skládají z odborného mínění, simulace a v několika případech i skutečných životních zkušeností.

Ve výzkumu lidské spolehlivosti není hlavní pozornost kladena na údržbu, a to přesto, že zanedbání údržby a testování se podílelo na nehodách v Černobylu a Three Mile Island. V publikaci An analysis of maintenance failures of a nuclear power plant [14] jsou obsaženy statistické závěry o vlastnostech poruch způsobených nesprávnou údržbou. Je zde využita velká databáze z jedné jaderné elektrárny.

Vybavení a elektrické součásti uvedené v databázi byly často ovlivněny údržbářskými zásahy. Je to především kvůli zranitelnosti, složitosti a velkému množství takového vybavení. V HRA je nutné klást větší důraz na studování vybavení a kontrolu elektrických součástí v bezpečnostních systémech. Ve zmiňované publikaci [14] se mimo jiné porovnává množství údržby během odstávek a při výpadku provozu. Větší počet závad byl odhalen při odstávkách. Bezpečnostní význam jednotlivých závad způsobených člověkem byl malý. Přesto některé závislé chyby byly shledány jako významné. Statistické informace o lidské činnosti mohou být vygenerovány na základě historie údržby. To představuje výjimku z kvantitativních údajů HRA. **Údaje z údržby zařízení jsou jedny z mála zdrojů skutečných historických informací o účincích lidského výkonu na technické systémy.** Z toho důvodu by k těmto účelům měly být využívány častěji.

5.1.1 NUCLARR

NUCLARR je počítačový software analýzy rizik a uživatelská příručka. Byl vyvinut americkou Jadernou regulační komisí (NRC) z důvodu podpory bezpečnostní analýzy operací jaderných elektráren. Tento software a doprovodná dokumentace pomáhá uživateli prostřednictvím jednoduchých postupů instalace najít konkrétní soubor jednotlivých datových záznamů, shromáždit hodnoty, vytvořit z nich graf a uložit data do souboru či z nich vytvořit zprávu.

Zahrnuje v sobě i celou řadu PSF, včetně druhu zařízení, stručného popisu chyby a zdroje dokumentace. Příklady datových zdrojů pro lidské selhání jsou následující: posouzení pravděpodobnosti rizika specifické pro aktuální zařízení, údaje vycházející z jednotlivých zařízení, vědeckých zpráv a studie simulátorů. V současné době databáze obsahuje více než 2500 jednotlivých datových bodů. Polovina z nich popisuje selhání lidského faktoru. Druhá polovina pak selhání u mechanických či elektrických komponent nacházejících se v jaderných elektrárnách. Databáze se každým rokem rozšiřuje a očekává se, že se velikost uložiště zvětší o velmi užitečná data. Na univerzitě

George Masona (Washington D. C.) se snaží vymyslet algoritmus, který by umožnil HEP zjištěná v jiných závodech vložit do systému klasifikace NUCLARR.

V INL (Idaho National Laboratory) byl složen tým odborníků z oblastí lidských faktorů, analýzy rizik a software, který měl posoudit proveditelnost zavedení databanky, kterou již dříve vyvinuly v NRC a General Physics Corporation. Tým INL uznal, že plně funkční knihovna jaderné spolehlivosti by neměla být proveditelná bez pomoci počítačových nástrojů pro správu a manipulaci s datovými zdroji. Rovněž prozkoumal dokumentaci zavedených databázových systémů, včetně specifikací uvedených ve zprávách NRC. Mnoho z těchto vlastností bylo zapracováno do specifikací NUCLARR a jsou uvedeny v NUREG/CR-4010. Kromě toho byly stanoveny tři specifikace týkající se písemného zadávání dat do NUCLARR: dva pro vstup pravděpodobnosti lidských chyb a jeden pro data o selhání hardware. Po naprogramování byl software NUCLARR testován a vyhodnocen.

K dnešnímu dni je v databázi zastoupeno více jak 60 veřejných či soukromých zdrojů. Jsou jimi například NUREG a provozní zkušenosti se zařízeními.

Systém NUCLARR využívá různých algoritmů pro přijetí vybraného souboru datových záznamů. Údaje následně sloučí do jediné souhrnné hodnoty. Výstupem jsou horní a dolní mez spolehlivosti. V některých případech je však vypočtena horní a dolní mez tolerance, což je 90% interval spolehlivosti. Limit pro hardwarové selhání komponenty je horní hranice tolerance.

V systému se nacházejí následující typy automatizovaných datových agregací:

- Funkční skupinové shrnutí HEP (lidské činnosti spojené s hlavní skupinou zařízení)
- Druhový HEP (lidské činnosti spojené s více specifickými zařízeními)
- Úkolové HEP (podobné situace pro lidské činnosti a související zařízení)

V závislosti na uložených údajích jsou vždy vypočteny 4 průměrné nebo úhrnné hodnoty HEP. Konkrétně jsou HEP vypočítávány samostatně pro opomenutí (vynechání, přehlédnutí) a příkaz (uvádění do provozu, vykonání). Současně se HEP považující se za obnovovací akce nikdy nesmí kombinovat s HEP, které nepočítají s obnovením.

Tyto datové shluky jsou automaticky počítány během procesu zadávání dat a jsou uloženy pro pozdější použití. HEP pro celou buňku vznikne tak, že se sloučí veškeré HEP pro zařízení a pro lidské činnosti. Buňka je přitom definována jako vztah mezi lidskou činností a vlastností zařízení uvnitř matice HEP, kde jsou lidské činnosti definovány jako sloupce a vlastnosti přístrojů jsou definovány jako řádky [13].

Uživatel však má možnost datové shluky manuálně upravit. To je vhodné v případech, kdy za účelem zkoumání potřebujeme shromáždit sadu záznamů. Při zkoumání záznamů jsou totiž získaná data řízená uživatelsky. Shluk vybraných záznamů totiž poskytuje uživateli velmi cenný souhrnný přehled o povaze a druhu dat, která byla při zkoumání získaná. Shluky se zpravidla vypočítávají přímo bez dodatečných žádostí o vstup a jsou založeny na statisticky homogenní podmnožině záznamů v datovém zásobníku. Pokud taková podmnožina nemůže být v datovém zásobníku umístěna, tak musíme učinit rozhodnutí, které HEP bude představovat soubor dat. V tom případě budeme automaticky vyzváni k zadání referenčního bodu. Faktory, které ovlivňují vhodnost referenčního bodu, jsou:

- Hodnota N (počet příležitostí – vhodnější je velké N)
- Referenční bod HEP (vyšší hodnota je více konzervativní)
- PSF (vhodnější jsou faktory reprezentující standardní podmínky)
- Kvalita (v analytickém pohledu na specifický referenční bod)

5.2 Měření simulátorů

Pod pojmem simulátor se obecně myslí něco, co nám umožňuje co nejrealističtěji napodobit nějakou činnost. Simulátory se často využívají v odvětvích, kde je potřeba naučit uživatele obsluze a řízení složitějších strojů, technologického zařízení apod. Simulátory se rovněž používají i v zábavním průmyslu ve formě počítačových simulátorů (silniční, vlakové, letecké).

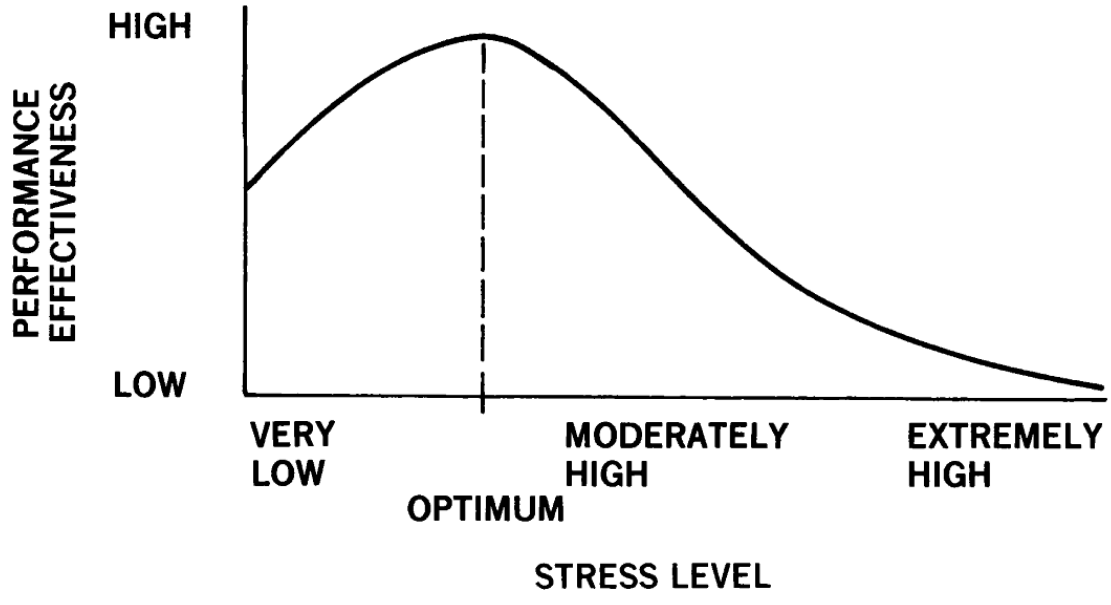
Simulace se staly efektivním způsobem, jak vybrat vhodného zaměstnance. Jsou totiž odlišené od jiných testů, jelikož vyžadují, aby uchazeč fyzicky a slovně reagoval na situace, které jsou typické pro práci, o nichž se uchází. Způsob, jakým se uchazeč chová při simulovaném cvičení, poskytne dobrou informaci o tom, jak se bude chovat na dané pozici. Simulace můžeme rozdělit do dvou různých skupin. Prvním z nich jsou vysoce přesné, druhou pak méně přesné.

Vysoce přesné simulace využívají velmi realistická zařízení. Méně přesné pak využívají zařízení a vybavení, které se od simulované situace velmi liší. Jednoduchým příkladem může být situace, kdy má kandidát popsat, jak by se zachoval v určité pracovní situaci. U vysoce přesné simulace má k dispozici zařízení, které je shodné se skutečným zařízením. Kdežto u méně přesné má slovně popsat, jak by se zachoval, tzn. jak by dané zařízení, které nemá fyzicky k dispozici, obsluhoval. Vysoce přesná simulace má ovšem i své nevýhody. První nevýhodou je, že dané zařízení (simulátor) musí být vyčleněno na zkoušku a nemůže být současně využíváno ostatními pracovníky. Dále je to potřeba personálu a vybavení, zvýšené časové nároky a zvýšené finanční náklady na údržbu.

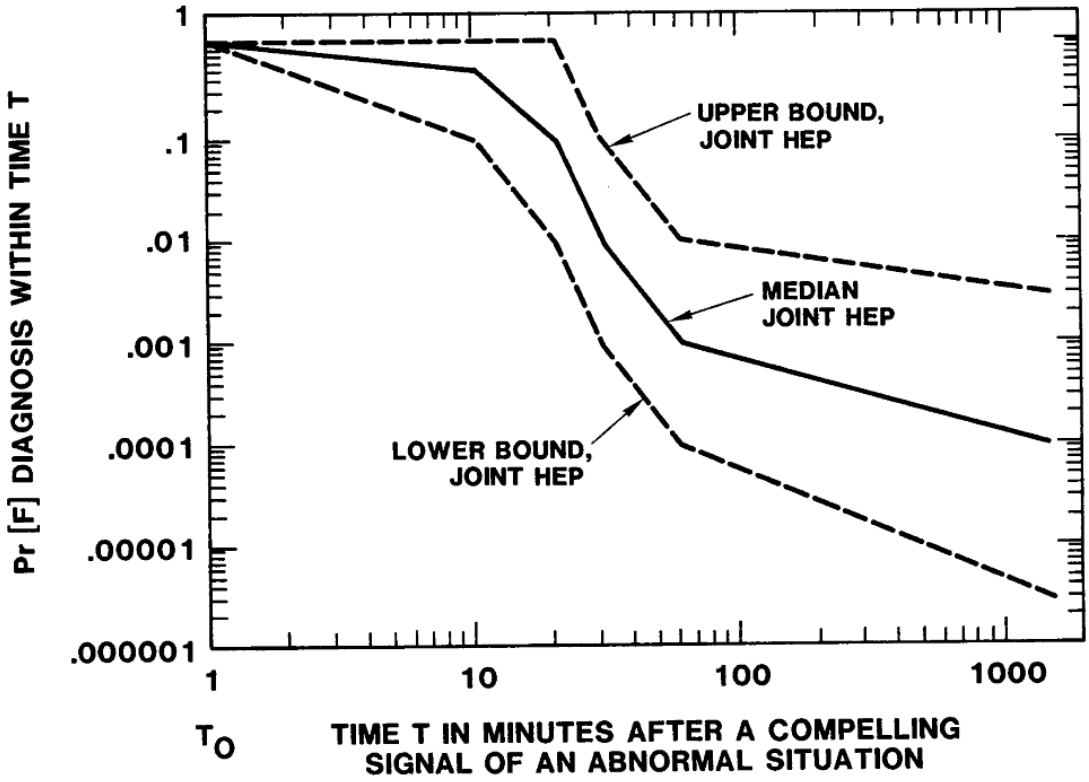
Výhodou méně přesných simulací je, že jsou levnější a nevyžadují mnoho zdrojů. U těchto testů se nevyužívá simulátoru, a ten je k dispozici zaměstnancům, kteří se na něm mohou školit [15].

5.3 Modely chování

5.3.1 Křivky pravděpodobností v závislosti na vybraných PSF



Obrázek 5.1: Efektivita výkonu v závislosti na stresu [16]



Obrázek 5.2: Křivky časové spolehlivosti (TRC) [16]

6 Cvičný simulátor

Při návrhu cvičného simulátoru vycházíme z potřeby, aby byl využitelný k mnoha účelům. Na simulátoru bude možné předvést reálnou technologii českého průmyslu. Bude zde možnost simulovat reálné nehody včetně jejich sekvencí. Dále budeme moci analyzovat chyby v myšlení operátorů. To lze využít z hlediska nových plánovaných předmětů vyučovaných na Oddělení spolehlivosti a rizik na Ústavu řízení systémů a spolehlivosti na Fakultě mechatroniky, informatiky a mezioborových studií Technické univerzity v Liberci. Samotná simulace reálného průmyslového provozu bude mít především výchovný prvek. To znamená, že si student bude moci vyzkoušet, jaké to je řídit určitý průmyslový provoz. Další důležitou funkcí bude prvek analýzy, kde budeme měřit odezvu obsluhy na vzniklé situace a zpracovávat je do grafů a tabulek.

6.1 Přístupy ve světě a v ČR

Simulátory se často využívají pří výcviku zaměstnanců v situacích, kdy je příliš drahé nebo příliš nebezpečné, aby cvičenci používali skutečné zařízení v reálném světě. Výhodou jsou chyby, které tento simulátor umožňuje nasimulovat. Simulace můžeme rozdělit do třech kategorií:

- „live“ simulace
    - lidé využívají simulovaného zařízení ve skutečném prostředí
    - ve standardizovaných testech bývají označovány jako vysoce přesné (high-fidelity) produkující vzorky pravděpodobných výkonů
- „virtuální“ simulace
    - lidé využívají simulovaného vybavení v simulovaném prostředí
- „konstruktivní“ simulace
    - lidé používají simulované vybavení v simulovaném prostředí
    - tato simulace je často označována jako válečná, jelikož se velmi podobá strategickým válečným hrám, ve kterých lidé velí armádám a pohybují s nimi po hrací ploše [15].

Publikace High Versus Low Fidelity Simulations [15] se zabývá porovnáním vysoce přesných a méně přesných simulátorů. Pro porovnání si autoři zvolili odvětví mimořádné události (požár) u hasičského záchranného sboru. Vysoce přesnou simulaci představoval požár skutečné budovy a posuzovaný hasič měl za úkol řídit záchrannou

akci. K dispozici měl veškerou běžně používanou techniku. V hořící budově byly místo lidí figuríny. Méně přesná simulace byla realizována v místnosti, ve které byl posuzovanému hasiči promítán obraz ohně. Kandidát rovněž viděl hořící budovu a na základě tohoto promítaného obrazu vydával rozkazy. Výsledky obou simulací byly překvapivě velmi vyrovnané. Dále byl s vybranými kandidáty veden rozhovor na vhodnost obou simulací. Většina se jich přiklonila k názoru, že je vhodnější využít vysoce přesnou simulaci. I když v ní nejsou pro kandidáty zaručeny stejné podmínky (počasí, rychlost šíření ohně, rozsah ohně apod.). Kandidát se ale dostane pod větší tlak, pokud si danou situaci zažije (žár, kouř atd.).

Typickým příkladem odvětví, kde se objevují simulace je energetický průmysl. Po desetiletí sloužily hlavně jako školící nástroj. V poslední době slouží i jako nástroj pro pomoc s plněním finančních a operačních cílů [17].

V dřívějších dobách byly simulátory složité a náročné na údržbu. Jelikož je vyžadováno, aby simulátor co nejvěrněji napodoboval skutečné zařízení, bylo nutné pořídit stejné řídící prvky, pracovní stanice a související logiku, jako se používá v reálném řídicím systému. V případě, že došlo k modernizaci řídicího systému, musely být vynaloženy stejné finanční prostředky k modifikaci simulátoru.

S rozvojem výpočetní techniky došlo i k technologickému pokroku v oblasti simulací. Je možné vytvořit virtuální simulátor, kde může být aplikační software řídicího systému provozován na osobním počítači. To nám umožňuje mnohem snadněji a levněji provádět údržbu simulátoru. Z toho důvodu jsou dnešní simulátory hodnotnější a praktičtější. Stále více elektráren proto specifikuje své distribuované řídicí systémy s požadavkem na schopnosti simulace. Využívají možností simulátorů jako školícího nástroje a učí na nich operátory lépe porozumět řízení závodu a ti jsou schopni řídit závod v měnicích se podmínkách, náležitě reagovat na alarmy a zvládat málo pravděpodobné provozní situace.

Simulátory se často používají k zaškolování nových pracovníků pro bezpečný a efektivní provoz závodu. Dále se uplatňují ke školení operátorů na zcela novém systému před jeho uvedením do provozu tak, aby byl zajištěn hladký přechod bez přerušení dodávky energie nebo provozu [17]. Simulátory se také využívají pro technickou analýzu, kde se například ověřuje logika řídicího systému před spuštěním systému.

Vhodným příkladem z praxe, jak simulace přispívá ke zkrácení doby potřebné pro uvedení nových projektů a modernizovaných prvků závodů do provozu, může být

projekt East River Repowering Project (ERRP) společnosti Con Edison. Cílem tohoto projektu bylo udržovat spolehlivou a cenově přiměřenou dodávku páry a elektřiny pro zákazníky společnosti v New Yorku. Aby společnost zajistila optimální provoz, chtěla své operátory školit pomocí modelů zařízení a závodu duplikujícího obnovený projekt East River ještě před vlastním uvedením do provozu a spuštěním. Společnost Noc Edison rovněž chtěla nástroj, který by jí pomohl identifikovat a validovat novou řídicí logiku před její instalací do řídicího systému závodu. Technici a operátoři společnosti Con Edison společně s týmem společnosti Emerson nakonfigurovali věrnou simulaci se skutečným softwarem pro řízení závodu a duplikáty pracovních stanic, které napodobují dispečink závodu East River [17].

Na platformě Scenario se intenzivně školili operátoři, kteří byli zvyklí na tradiční konfiguraci elektrárny s kotli a parními turbínami. Díky technologii simulace se operátoři také dobře seznámili se systémem na bázi mikroprocesorů, který umožňuje operátorům rozeznat abnormální provozní situace a reagovat na ně rychleji. Simulace nalezla své využití i při vypracování optimální metodiky práce operátorů, která je dokumentována v provozních postupech závodu. Použití simulační technologie pomohlo společnosti Con Edison zajistit, aby její investice do nové technologie byla optimalizována dobře zaškolenými operátory a přesnými řídícími prvky. Jedním z významných přínosů bylo bezpečné a efektivní spuštění závodu, které zkrátilo dobu uvádění do provozu ze čtyř měsíců na jeden. Po spuštění závodu se simulace nadále využívala pro školení operátorů a optimalizaci procesů závodu East River s cílem zvýšit efektivitu a spolehlivost.

Společnost Emerson předpovídá, že v budoucnu bude simulátor součástí samotného řídicího systému a modely simulátoru budou sledovat skutečnou řídicí logiku a provozní podmínky závodu v reálném čase. V takovém případě by simulátor fungoval jako testovací stolice a operátorům by umožnil testovat řídicí postupy na simulátoru a následně je okamžitě nahrát do řídicího systému. Výsledkem bude architektura synchronizované simulace a řízení pro simulaci elektrárny v reálném čase. Pro elektrárny toto spojení simulátoru a řídicího systému nabízí nejen příležitosti k vyšší efektivitě, ale také vyšší spolehlivost a schopnost plnit finanční cíle omezením lidských chyb, které by mohly vést k neplánovaným odstávkám. S tím, jak se elektrárny snaží vyrovnávat s konkurenčními tlaky, simulace bude nadále životně důležitým prvkem komplexní strategie dosahování lepších provozních a finančních výsledků [17].

6.1.1 HAMMLAB

HAMMLAB je mezinárodní centrum pro výzkum řízení procesů, systémů lidských interakcí a lidské výkonnosti ve složitých systémech. HAMMLAB je zařízení pro dosažení optimálního využití nových technologií ve složitých odvětvích, jako jsou jaderné elektrárny, distribuce elektrické energie či těžba ropy. Řídící centrum tohoto zařízení je flexibilní a adaptibilní, přičemž jeho vybavení a funkce mohou být využívány k navození různých experimentálních podmínek. HAMMLAB je příkladem moderního řídícího centra, jehož výsledky mohou posloužit při projektování.

HAMMLAB má dva hlavní cíle. Prvním z nich je studium lidského chování v interakci se složitým systémem. Tím druhým pak vývoj, testování a hodnocení prototypů středisek řízení včetně jejich jednotlivých systémů. To je zajišťováno s využitím moderních počítačů, experimentálních řídících místností a čtyř trenažérů. Tři jsou pro jaderné reaktory (PWR, BWR, VVER) a jeden pro výrobní proces těžby ropy na volném moři. Na rozdíl od jiných simulátorů není HAMMLAB vzdělávací nástroj. Je zaměřen na uplatňování nových technologií v rámci svého uživatelského prostředí a přinesl nové poznatky o systému lidské interakce, která má praktické využití v prostředí řízení procesů [20].

HAMMLAB se využívá déle jak 20 let a byl použit například při hodnocení počítačových postupů, hodnocení a srovnání uživatelských rozhraní, hodnocení diagnostických systémů nebo při hodnocení systémů alarmů. Jeho výsledky slouží při návrzích systémů, vývoji norem a směrnic, při hodnocení lidské spolehlivosti apod. Systém je rovněž vybaven dalšími zařízeními k shromažďování a analýze údajů. Mezi ně patří sledovač očního pohybu či audiovizuální záznam událostí a akcí operátora.

Záměrem HAMMLAB, kterého například využívají Americká jaderná regulační komise (NRC), Institut de Protection et de Sûreté Nuclaire (IPSN, Francie), OKG AB (Švédsko), Norské ropné ředitelství (NPD) a BP Amoco (Norsko), je rozšířit znalosti lidské výkonnosti ve složitých procesech a přizpůsobit nové technologie potřebám lidského operátora [20].

Experimentální řídící centrum HAMMLAB v současnosti provozuje v plném rozsahu simulátory dvou jaderných elektráren založených na rozhraní operátora. Prvním je HAMBO (HAMmlab BOiling reactor simulator), což je vlastně simulátor švédské BWR Forsmark 3 elektrárny (BWR) a využívá se od roku 2000. Druhým je FRESH (Fessenheim REsearch Simulator for Hammlab), který je simulátorem francouzské

jaderné elektrárny Fessenheim 1 (PWR). Tento simulátor se využívá již od roku 1998 [21].

6.2 Tvorba vlastního simulátoru

6.2.1 Hardware

K realizaci cvičného simulátoru bych použil klasický stolní počítač, jehož komponenty uvedu níže. Provoz simulace bych zobrazoval na 2 LCD monitorech. Ovladače virtuálního zařízení bych obsluhoval s využitím 2 dotykových obrazovek.

úhlopříčka	**rozlišení**	**cena**	**rozlišení**	**cena/Mpixel**
17"	1 280 x 1 024	3 342 Kč	1,31 Mpixel	2550 Kč
19"	1 440 x 900	3 816 Kč	1,29 Mpixel	2960 Kč
20"	1 600 x 900	3 800 Kč	1,44 Mpixel	2640 Kč
22"	1 680 x 1 050	4 416 Kč	1,76 Mpixel	2510 Kč
24"	1 920 x 1 080	6 401 Kč	1,78 Mpixel	3600 Kč
26"	1 920 x 1 200	11 263 Kč	2,30 Mpixel	4900 Kč
30"	2 560 x 1 600	28 818 Kč	4,09 Mpixel	7050 Kč

Tabulka 6.1: Porovnání LCD monitorů (rozlišení, cena)

Pro každou úhlopříčku jsem zvolil zástupce, který se v době porovnání (13. března) nacházel přibližně uprostřed cenového žebříčku e-shopu firmy AB COM Czech s.r.o. Hodnoty v sloupci cena/Mpixel jsem zaokrouhloval na desetikoruny.

úhlopříčka	výhoda	výhoda	nevýhoda	nevýhoda
17"	dobrá cena	slušný poměr ceny/Mpixel	malá velikost	
19"	dobrá cena			
20"	dobrá cena	slušný poměr ceny/Mpixel		
22"	slušná cena	nejlepší poměr ceny/Mpixel		
24"	zobrazovací plocha s vysokým rozlišením			
26"	zobrazovací plocha s vysokým rozlišením		vysoká cena	špatný poměr ceny/Mpixel
30"	obrovská zobrazovací plocha s velmi vysokým rozlišením		velmi vysoká cena	špatný poměr ceny/Mpixel

Tabulka 6.2: Porovnání LCD monitorů (výhody, nevýhody)

Na základě provedeného porovnání jsem zvolil, že v cvičném simulátoru bude vhodné použít 2 LCD monitory s úhlopříčkou 22". Konkrétně jsem vybral LCD Dell G2210 za 4 416 Kč.

Obrázek 6.1: 22" LCD monitor Dell G2210

úhlopříčka	rozlišení	cena	rozlišení	cena/Mpixel
15"	1 024 x 768	8 052 Kč	0,79	10 200 Kč
17"	1 280 x 1 024	9 444 Kč	1,31	7 210 Kč
19"	1 280 x 1 024	14 196 Kč	1,31	10 840 Kč
22"	1 680 x 1 050	12 264 Kč	1,76	6 970 Kč
26"	1 366 x 768	24 174 Kč	1,05	23 030 Kč
32"	1 366 x 768	36 918 Kč	1,05	35 160 Kč

Tabulka 6.3: Porovnání dotykových LCD obrazovek (rozlišení, cena)

Stejně jako porovnání LCD monitorů, tak i porovnání cen dotykových obrazovek jsem prováděl s využitím e-shopu stejné firmy. Zaokrouhlení v sloupci cena/Mpixel je provedeno na desetikoruny.

úhlopříčka	výhoda	výhoda	nevýhoda	nevýhoda
15"	dobrá cena		malá velikost	
17"	slušná cena	slušný poměr ceny/Mpixel		
19"			špatný poměr ceny/Mpixel	
22"	nejlepší poměr ceny/Mpixel	zobraz. plocha s vys. rozliš.		
26"			vysoká cena	špatný poměr ceny/Mpixel
32"			velmi vysoká cena	špatný poměr ceny/Mpixel

Tabulka 6.4: Porovnání dotykových LCD obrazovek (výhody, nevýhody)

Z tabulky vyplývá, že nejvhodnější bude zvolit dotykovou obrazovku s úhlopříčkou 22". Pokud ještě uvážíme, že úhlopříčka zvolených monitorů je stejná, tak je to ideální řešení. Všechny čtyři zobrazovací zařízení budou mít stejnou úhlopříčku a dosáhneme

celkového rozlišení (6 720 x 1 050; 7,06 Mpixel). Zvolené dotykové LCD obrazovky nesou označení LCD NEC V-Touch 2223w. Cena jedné obrazovky činí 12 264 Kč.

Obrázek 6.2: 22" LCD dotyková obrazovka NEC V-Touch 2223w

Komunikace s dotykovou vrstvou obrazovky probíhá přes USB port. Na počítač je nutné nainstalovat ovladače. Ovladače na CD jsou součástí balení. Součástí nákupu získáme i nadstandardní servisní balíček, který nám v případě závady zaručuje jistotu rychlé opravy.

Při návrhu počítačové sestavy musíme brát v potaz připojení 4 monitorů. Z toho vyplynula potřeba dvou grafických karet a základní deska se dvěma PCIe 16 x sloty. Jednotlivé komponenty sestavy jsem vybíral ve stejném e-shopu jako zobrazovací zařízení.

Komponenta	Produkt	Cena
Počítačová skříň	CoolerMaster Elite 330K	945 Kč
Zdroj	CoolerMaster GX 650W PFC v 2.3	1 928 Kč
Základní deska	GIGABYTE MB Sc AM3 790FXTA-UD5, AMD 790FX, 4xDDR3	3 633 Kč
Procesor	CPU AMD Phenom™ II X4 Quad-Core Black Edition 955 rev.C3 3.2GHz 8MB cache 125W socket AM3, BOX	2 704 Kč
Operační paměť	KINGSTON 4GB DDR3 1333MHz Non-ECC CL9 DIMM (Kit of 2)	900 Kč
Pevný disk	WD CAVIAR BLUE 250GB SATA/300 7200 RPM, 16MB cache	871 Kč
Grafické karty	2× GIGABYTE VGA ATI Radeon HD5770 1GB DDR5	2× 2647 Kč
Optická mechanika	LG DVD±R/±RW/RAM, GH24NS, SATA, černá, bulk	460 Kč
Čtečka paměť. karet	Čtečka karet Sweex interní ALL-IN-1 USB 2.0 černá	189 Kč
Celkem		**16 924 Kč**

Tabulka 6.5: Nejlevnější varianta počítačové sestavy

V tabulce 6.5 jsou uvedeny komponenty úsporné varianty. Na základě předpokládaných hardwarových požadavků simulátoru byly voleny tak, aby se jejich výkon držel při spodní hranici a příliš nepřevyšoval požadavky.

Naopak v tabulce 6.6 je uvedena doporučená varianta počítačové sestavy. Na této sestavě bude simulátor ideálně pracovat a bude mít i dostatečnou rezervu pro případné rozšíření simulátoru o nové hardwarově náročnější funkce.

Při vybírání jednotlivých komponent byl rovněž brán ohled na hardwarové požadavky vývojových prostředí, o kterých se hovoří v kapitole 6.2.2.

Komponenta	Produkt	Cena
Počítačová skříň	CoolerMaster Elite 330K	945 Kč
Zdroj	CoolerMaster Silent Pro Active 850 W Modular PFC v 2.3	3 066 Kč
Základní deska	GIGABYTE MB Sc AM3 790FXTA-UD5, AMD 790FX, 4xDDR3	3 633 Kč
Procesor	CPU AMD Phenom™ II X4 Quad-Core Black Edition 955 rev.C3 3.2GHz 8MB cache 125W socket AM3, BOX	2 704 Kč
Operační paměť	2× KINGSTON 4GB DDR3 1333MHz Reg ECC Module	2× 1 785 Kč
Pevný disk 1	WD CAVIAR GREEN WD10EARS 1TB SATA/300 64MB cache	1 177 Kč
Pevný disk 2	SSD 120GB Intel® 320 series High Performance 2.5"	4 606 Kč
Grafické karty	2× GIGABYTE VGA ATI Radeon HD5770 1GB DDR5	2× 2 647 Kč
Optická mechanika	LG DVD±R/±RW/RAM, GH24NS, SATA, černá, bulk	460 Kč
Čtečka paměť. karet	Čtečka karet Sweex interní ALL-IN-1 USB 2.0 černá	189 Kč
Celkem		**25 644 Kč**

Tabulka 6.6: Doporučená varianta počítačové sestavy

6.2.2 Software

Vzhledem k požadavkům vývojových prostředí, o kterých se hovoří dále, k dovednostem většiny studentů a k používanému operačnímu systému na Technické univerzitě v Liberci, se z hlediska kompatibility jeví jako nejlepší varianta využít operačního systému Microsoft Windows 7 Professional. Tento operační systém se dá pořídit za 6 271 Kč. Pokud by byl koupen v rámci licence pro školství, stál by pouze 1 730 Kč.

K naprogramování simulátoru s vizuálními prvky lze využít několik softwarových možností. Pro porovnání jsem zvolil několik možností, které se od sebe liší vývojovým prostředím a použitým programovacím jazykem.

- Visual Basic .NET
  - Jedná se o novou generaci jazyka Visual Basic postavenou na platformě .NET Framework. Je to moderní objektově orientovaný jazyk, který se neustále vyvíjí a který má velmi širokou základnu vývojářů po celém světě.
  - Výhody (oproti Visual Basic 6):
    - Kompletní objektově orientovaný model. Jsou plně podporovány třídy, dědičnosti a rozhraní.
    - Povinná deklarace proměnných. Ve starších verzích nebyla deklarace vyžadována. Bez nadeklarování se automaticky použil datový typ Variant.
    - Rychlejší kód. Programy napsané nad rozhraním .NET Framework se kompilují do jazyka MSIL, který je podobný assembleru. V tomto jazyce se kód zabalí do EXE souboru a teprve před spuštěním programu na klientské stanici se provede kompilace do strojového kódu. Velkou výhodou tedy je, že se výsledný strojový kód může optimalizovat přímo pro procesor daného počítače [18].
    - Lepší vývojové prostředí. Lze využít buď placené Visual Studio .NET, či Express Edition, která je pro komerční i nekomerční využití dostupná zdarma.
  - Nevýhody:
    - Kód není zpětně kompatibilní s aplikacemi napsanými ve Visual Basic 6.
    - Nutnost mít nainstalovaný .NET Framework. V dnešní době je součástí automatických aktualizací, a jelikož ho vyžadují i některé programy a hry, tak je pravděpodobné, že ho většina uživatelů má nainstalovaný.
- C#
  - Je vysokoúrovňový objektově orientovaný programovací jazyk. Vyvinula ho firma Microsoft zároveň s platformou .NET Framework.

Jazyk C# je založen na jazycích C++ a Java a lze jej využít k tvorbě databázových programů, webových aplikací a stránek, webových služeb, formulářových aplikací ve Windows apod.

- Jazyk je vhodný pro vývoj softwarových komponent distribuovaných v různých prostředích.
- Výhody:
  - Neobsahuje ani nepotřebuje dopřednou deklaraci. Není důležité pořadí deklarace metod.
  - Jazyk je case sensitive. Rozlišuje mezi velkými a malými písmeny.
  - Nevýhody:
  - Neexistuje vícenásobná dědičnost. Každá třída může být potomkem pouze jedné třídy.
  - Neexistují žádné globální proměnné a metody. Všechny funkce a metody tak musí být deklarovány uvnitř tříd.

- Delphi
  - Je integrované grafické vývojové prostředí firmy Borland. Je určené pro tvorbu aplikací na platformě MS Windows v jazyce Object Pascal. Obsahuje systém, který umožňuje vizuální návrh grafického uživatelského rozhraní. Na jeho základě je automaticky vytvářena kostra zdrojového kódu. To velmi urychluje vývojový cyklus.
  - Programování v Delphi je založeno na použití komponent. Komponenta je malý program, který vykonává určitou činnost. Komponenty jsou obsaženy v knihovnách.
  - Výhody:
    - Podpora systému RAD (Rapid Application Development) – vizuální návrh grafického rozhraní.
    - Založení na vyšším programovacím jazyce.
    - Možnost kompilace do jednoduchého spustitelného kódu s eliminací funkcí dynamických knihoven.
    - Rychlá optimalizace kódu pro převedení do jazyka symbolických adres.
    - Znaky objektově orientovaného programovacího jazyka s možností dědičnosti a polymorfismu v rámci objektových tříd.

- Nevýhody:
  - Nelze vytvářet nativní 64-bitové aplikace.
  - Vytvořené aplikace mohou běžet pouze v OS Microsoft Windows.
  - Výsledný kód není příliš optimalizovaný.

- Control Web
  - Je programovým systémem, který dokáže vystupovat v mnoha rolích.
  - Může například pracovat v řídicích jednotkách strojů, může spojovat výrobní technologii s informačním systémem podniku, může být datovým serverem s mnoha webovými klienty, může modelovat a simulovat procesy, dokáže vytvářet náročné vizualizace a mnoho dalšího [19].
  - Používá se v celé škále odvětví (rozsáhlé aplikace ve velkých firmách, v malých a vestavěných aplikacích, ve škole, ve vědě a výzkumu atd.).
  - Control Web je natolik bohatým a komplexním systémem, jehož veškeré možnosti a vlastnosti není možno uceleně vysvětlit. Jeho základní dokumentace má přes 2000 stran [19].

	Microsoft Visual Basic	**Microsoft Visual C#**	**Delphi**	**Microsoft Visual Studio**	**Control Web**
verze	2010 Express	2010 Express	2010	2010 Professional	2000
programovací jazyk	Visual Basic	C#	Delphi	Visual Basic, C#, C++	vlastní
požadavky na OS	Standardní [1]	Standardní [1]	Standardní [1]	Standardní [1]	Nízké [2]
požadavky na HW	Vyšší [3]	Vyšší [3]	Vyšší [3]	Vyšší [3]	Nízké [4]
cena	zdarma	zdarma	36 120 Kč [5]	21 472 Kč [5]	4 620 Kč [6]

Tabulka 6.7: Srovnání vybraných vývojových prostředí

[1] Windows XP (SP2 nebo SP3), Windows Vista (SP2), Windows 7

[2] minimálně Windows 98

[3] Procesor o frekvenci 2 GHz, 2 GB RAM, místo na harddisku 3 GB, rozlišení minimálně 1024 x 768

[4] Procesor o frekvenci 500 MHz, 128 MB RAM, místo na harddisku 100 MB

[5] http://www.sw.cz

[6] http://www.mii.cz

Z uvedeného srovnání bych k naprogramování simulátoru doporučil zakoupit Microsoft Visual Studio. Pořizovací cena je sice vyšší, ale pokud zohledníme jeho celkové možnosti ve srovnání s Express verzemi, tak bych zvolil právě Studio verzi.

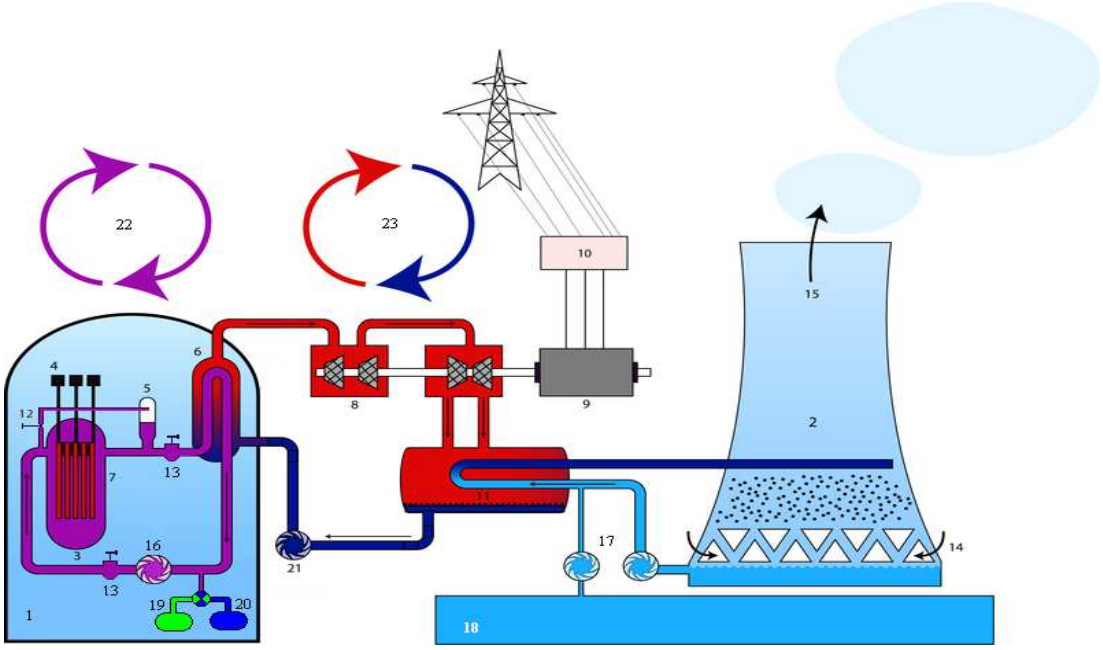
Celkové náklady na pořízení simulátoru činí při variantě s nejlevnější počítačovou sestavou 73 486 Kč vč. DPH. Při nákupu doporučené varianty počítačové sestavy jsou náklady 82 206 Kč vč. DPH.

6.2.3 Jaderná elektrárna s PWR reaktorem

Rozhodl jsem se pro simulaci provozu jaderné elektrárny využívající reaktor PWR. V dnešní době se jedná o nejrozšířenější typ jaderného reaktoru ve středoevropském regionu. Tento typ je využit i v obou českých jaderných elektrárnách. Jedná se o tepelný tlakový reaktor moderovaný i chlazený demineralizovanou vodou. V aktivní zóně (primární okruh) se nacházejí malé válečky z oxidu uraničitého, které jsou naskládané a hermeticky uzavřené v obalové trubce ze zirkoniové slitiny. Tento celek tvoří tzv. palivový proutek. Svazky zhruba tří set pravidelně uspořádaných palivových proutků vytvářejí palivové články (u reaktorů s výkonem cca 1000MWt). Z nich je sestavena aktivní zóna uvnitř tlakové nádoby reaktoru. Výměna vyhořelého paliva probíhá jednou za rok až rok a půl při odstavení reaktoru [22].

Teplo se z primárního okruhu předává přes tepelné výměníky (parogenerátory) do sekundárního okruhu. Stěny trubek parogenerátorů oddělují primární okruh od sekundárního a zabraňují tak přechodu radioaktivních látek z chladiva primárního okruhu do okruhu sekundárního.

Voda se v parogenerátorech odpaří a vznikne sytá pára, která pohání turbínu. Po průchodu turbínou je pára odváděna do kondenzátoru, kde se ochlazuje a přeměňuje ve vodu. Chlazení kondenzátorů je zajištěno vodou z chladícího cirkulačního okruhu elektrárny. Voda, která kondenzátorům teplo odebírá, je odváděna do chladicích věží, ze kterých je zbytkové teplo odváděno do ovzduší. Elektrická energie vyrobená v generátoru je přenášena do sítě vysokého napětí [23].



Obrázek 6.3: Schéma jaderné elektrárny s tlakovodním reaktorem [24]

1. Reaktorová hala, uzavřená v nepropustném kontejnmentu
2. Chladící věž
3. Tlakovodní reaktor
4. Řídící tyče
5. Kompenzátor objemu
6. Parogenerátor
7. Aktivní zóna
8. Turbína – vysokotlaký a nízkotlaký stupeň
9. Elektrický generátor
10. Transformační stanice
11. Kondenzátor sekundárního okruhu
12. Sprcha kompenzátoru objemu
13. Hlavní uzavírací armatura
14. Přívod vzduchu do chladící věže
15. Odvod teplého vzduchu a páry komínovým efektem
16. Oběhové čerpadlo primárního okruhu
17. Napájecí čerpadla chladicího okruhu
18. Napájecí nádrž chladícího okruhu
19. Nádrž s koncentrovanou kyselinou boritou
20. Nádrž s čistým kondenzátem
21. Oběhové čerpadlo sekundárního okruhu
22. Primární okruh (voda pouze kapalná pod vysokým tlakem)
23. Sekundární okruh

6.2.4 Schéma funkcí simulátorů

Matematicko-fyzikální vlastnosti jednotlivých komponent simulátoru nejsou náplní bakalářské práce. Fyzikální chování reaktoru bude například určeno z následujících parametrů: teplota, objem a teplota přítoku chladicí kapaliny, objem odtoku chladicí kapaliny, zasunutí regulačních tyčí, koncentrace kyseliny borité a teploty v předcházejícím časovém kroku.

Celý model bude dodán externě od spolupracujících odborníků z oblasti fyzikálního modelování.

a) Primární okruh

V primárním okruhu se nacházejí celkem 4 hlavní zařízení. Tím nejdůležitějším je jaderný reaktor, ve kterém probíhá štěpná reakce. Štěpnou reakci v rámci simulátoru budeme regulovat. Regulace se může provádět s využitím řídících tyčí, kde nás zajímá jejich zasunutí. Dalším regulátorem je chladicí kapalina s příměsí kyseliny borité. V tomto případě hraje nejdůležitější roli koncentrace kyseliny v kapalině.

Druhým zařízením, které nás bude zajímat, je hlavní cirkulační čerpadlo, které má za úkol udržovat chladicí kapalinu v oběhu. Třetím zařízením je kompenzátor objemu, jehož náplní je regulace tlaku v potrubí vedoucím do parogenerátoru. Posledním zařízením v primárním okruhu je parogenerátor, v němž dochází k odpařování vody a vzniklá pára putuje do sekundárního okruhu.

Vedlejšími zařízeními jsou dvě nádrže, dvě hlavní uzavírací armatury a sprcha kompenzátoru objemu. V první nádrži se nachází koncentrovaná kyselina boritá, v druhé čistý kondenzát. Hlavní uzavírací armatury jsou zde z hlediska bezpečnosti. V případě závady na potrubí lze chladicí okruh uzavřít na dvou místech.

Na základě uvedeného popisu první části simulátoru bude v rámci simulace nutné měřit následující veličiny. V jaderném reaktoru budeme měřit jeho tepelný výkon v MWt, teplotu [°C] a budeme zde mít snímače zasunutí regulačních tyčí [% zasunutí]. Na hlavním cirkulačním čerpadle budeme měřit průtok chladiva [kg/s] a jeho výkon [% výkonu]. V kompenzátoru objemu nás bude stejně jako v parogenerátoru zajímat výška hladiny [m], vnitřní tlak [MPa] a teplota [°C]. Na sprše kompenzátoru objemu budeme měřit průtok [kg/s]. Další teplotní [°C] a tlaková čidla [MPa] rozmístíme na potrubí. První měřicí bod bude mezi parogenerátorem a hlavním cirkulačním čerpadle, druhý

pak před jaderným reaktorem, kde současně budeme měřit i koncentraci kyseliny borité v chladivu [g/kg] a třetí měřicí bod bude mezi jaderným reaktorem a parogenerátorem.

b) Sekundární okruh

V sekundárním okruhu nás pro potřeby simulace budou především zajímat parní turbína, kondenzátor a oběhové čerpadlo sekundárního okruhu. V parní turbíně dochází k přeměně tepelné a tlakové energie páry v mechanickou energii. V kondenzátoru kondenzuje pára z nízkotlakého dílu turbíny a oběhové čerpadlo odtud čerpá kondenzát na chlazení parogenerátoru v primárním okruhu.

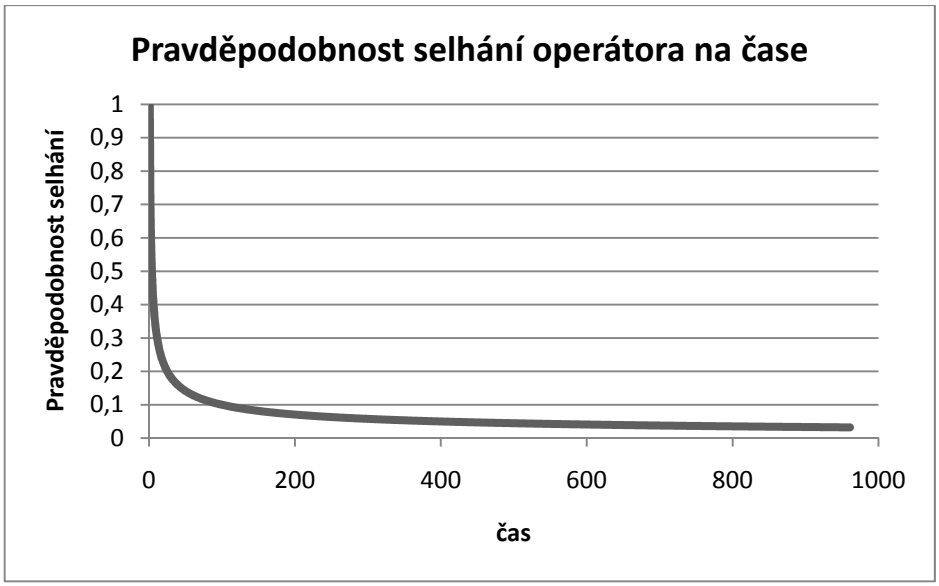
Na parní turbíně budeme měřit pouze otáčky [otáčky/min], v kondenzátoru výšku hladiny [m] a teplotu [°C]. V oběhovém čerpadle nás bude zajímat průtok kondenzátu [kg/s] a výkon [% výkonu]. Stejně jako v primárním okruhu, tak i zde umístíme čidla i na potrubí. První bude na potrubí vedoucím z parogenerátoru do parní turbíny a budeme zde měřit teplotu [°C], tlak [MPa] a průtok [kg/s]. Na potrubí z kondenzátoru do parogenerátoru nás bude zajímat pouze teplota [°C].

6.2.5 Měřené charakteristiky člověka

Pro vyhodnocování spolehlivosti lidské obsluhy využijeme 6 typů simulace. Jednotlivé simulace se budou lišit hlavním působícím vlivem. Jedná se o vlivy času, skrytých vad indikátoru, ergonomie, zkušeností a vzdělání, motivace a vyrušení jiným typem úlohy. Jednotlivé vlivy lze samozřejmě spolu kombinovat.

a) Vliv času

Simulace vlivu času na pravděpodobnost selhání operátora vychází z faktu, že čas je jediným faktorem, který můžeme jednoduše měřit a simulovat. Křivka pravděpodobnosti selhání operátora na čase v literatuře vypadá takto:



Obrázek 6.4: Křivka pravděpodobnosti selhání operátora na čase

Naše měření by mohlo tuto teoretickou křivku potvrdit nebo vyvrátit.

Scénář simulace: Z důvodu netěsnosti na potrubí v primárním okruhu dojde k poklesu tlaku v potrubí a úniku chladiva do prostoru. Důsledkem toho se začne přehřívat reaktor. Přehřívání reaktoru spustí alarm, který by měl operátora upozornit (pokud si tohoto problému dosud nevšiml) na vzniklou situaci. V této simulaci budeme měřit čas, za který operátor reaktor odstaví. Scénář simulace můžeme obohatit o netěsnosti na sekundárním okruhu. Rovněž můžeme zavést časový limit, který operátorovi poskytneme. Po uplynutí limitu můžeme na obrazovky vypsat hlášky typu: „Došlo k jaderné havárii“, „Elektrárna vážně poškozena“ apod.

b) Vliv skryté vady indikátoru

V tomto typu simulace budeme zohledňovat fakt, že měření jedné veličiny bude záměrně špatné. Tím odvedeme mysl operátora od vzniklé situace.

Scénář simulace: Bude docházet k přehřívání reaktoru, na což by obsluha měla zareagovat zvýšením koncentrace kyseliny borité. Indikátor koncentrace kyseliny borité v chladivu však bude vykazovat hodnotu na horní hranici povolené koncentrace. Ve skutečnosti se bude hodnota pohybovat na dolní hranici. Z toho můžeme usuzovat, že si

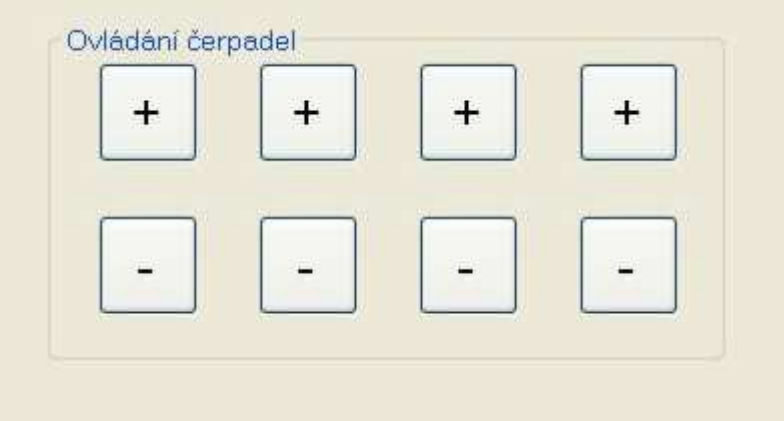
obsluha bude myslet, že koncentrace kyseliny v chladivu je dostatečná a bude zkoumat jiné příčiny přehřívání reaktoru.

Dalším možným scénářem může být vada na průtokoměru oběhového čerpadla sekundárního okruhu. Tento průtokoměr bude vykazovat nízké hodnoty, přičemž skutečná hodnota průtoku bude na 100%. V této situaci můžeme předpokládat, že si obsluha bude myslet, že čerpadlo nemá dostatečný přívod z kondenzátoru sekundárního okruhu.

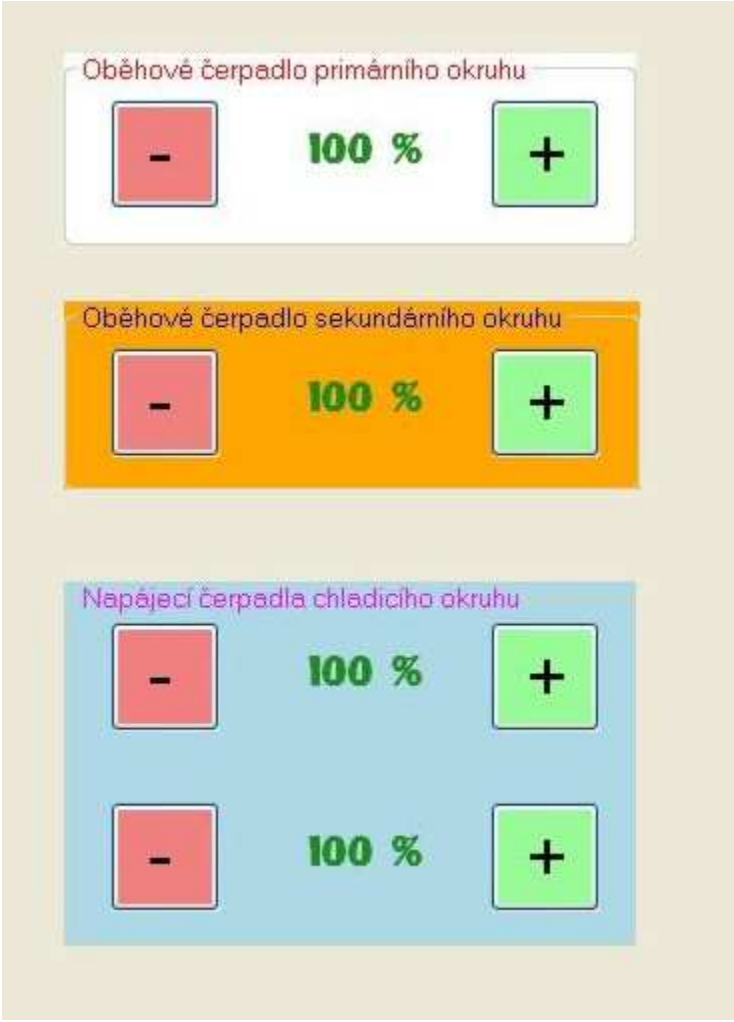
c) Vliv ergonomie

Při této simulaci budeme především vyhodnocovat chování operátora při různém uspořádání ovládacího pultu. Můžeme posuzovat vliv velikosti tlačítek, jejich popsání, resp. nepopsání, jejich rozmístění. Pro zobrazovací prvky můžeme porovnávat, zda operátor lépe reaguje na digitální či analogové zobrazení hodnot.

Scénář simulace: Úkolem operátora v tomto typu simulace bude běžná obsluha jaderné elektrárny. Prvním úkolem bude snížit koncentraci kyseliny borité v chladivu o polovinu. Zde budeme zkoumat rozdíly v přesnosti při použití digitálního a analogového ukazatele (dvě různé simulace). Druhým úkolem bude regulovat výkon jednotlivých čerpadel. Výkon oběhového čerpadla primárního okruhu ponecháme na 100%, požadovaný výkon oběhového čerpadla sekundárního okruhu bude 75%, výkon napájecího čerpadla na potrubí z napájecí nádrže bude 50% a výkon napájecího čerpadla na potrubí z chladící věže bude 60%. V tomto případě budeme sledovat vliv na rozmístění tlačítek ovládající výkon jednotlivých čerpadel a jejich popsání nebo nepopsání. Třetím úkolem bude nouzové odstavení reaktoru. Zde budeme zkoumat vliv velikosti tlačítka na nouzové odstavení, jeho umístění na ovládacím pultu a jeho možné označení.



Obrázek 6.5: Nevhodná ergonomie tlačítek ovládání výkonu čerpadel



Obrázek 6.6: Vhodnější ergonomie tlačítek ovládání výkonu čerpadel

d) Vliv zkušeností a vzdělání

Tato část má především za úkol vyhodnotit, jak důležité je kvalitní školení operátora.

Scénář simulace: Pro tento typ scénáře rozdělíme skupinu studentů (operátorů) do několika skupin. Rozdělení můžeme provést podle několika kritérií (prospěch, zájem o odvětví jaderných elektráren, fyzické předpoklady, náhodně). Následně jednotlivé skupiny proškolíme. Nejvhodnější školení by mohlo vypadat tak, že bude velmi obsáhlé. Nejprve bychom vysvětlili princip fungování jaderných elektráren včetně bezpečnostních procedur, následně bychom detailně vysvětlili rozložení ovládacího pultu simulátoru. Následovaly by příklady kritických situací s vysvětlením správného řešení, se kterými se operátoři mohou v simulátoru setkat. Ostatní skupiny bychom proškolili méně důkladně s možným zaměřením pouze na jednotlivé části (jedna skupina pouze teorie, druhá skupina pouze ovládací panel, třetí skupina pouze řešení kritických situací apod.). Je tu i možnost neškolit vůbec a skupině pouze poskytnout jakýsi manuál celého simulátoru, ve kterém by bylo vše popsané.

Po tomto různě obsáhlém proškolení bychom mohli operátorům simulovat scénáře popsané v kapitolách výše a zjišťovat jaký vliv na správné řešení má provedené školení. Můžeme předpokládat, že nejlépe si povedou jedinci se zájmem o jadernou energetiku, kteří mají lepší prospěch a současně byli nejvíce proškoleni. Rovněž můžeme předpokládat, že pokud se operátor setká s nějakou kritickou situací, tak se s ní v budoucnu lépe vypořádá.

e) Vliv motivace

Při vlivu motivace budeme posuzovat, do jaké míry je operátor schopen riskovat, aby dosáhl požadovaných výsledků.

Scénář simulace: Skupinu operátorů rozdělíme na 2 skupiny. Operátoři první skupiny budou mít za úkol vyrobit co nejvíce elektřiny. Nejlepší operátor skupiny bude odměněn. Při využití v rámci nově uvažovaného předmětu pod RSS například tím, že dostane bonusové body k zápočtovému testu. Stejnou odměnou můžeme motivovat i nejlepšího operátora druhé skupiny. Tato skupina bude mít za úkol co nejbezpečněji

řídit virtuální provoz elektrárny. Oběma skupinám můžeme simulovat události uvedené v kapitolách výše.

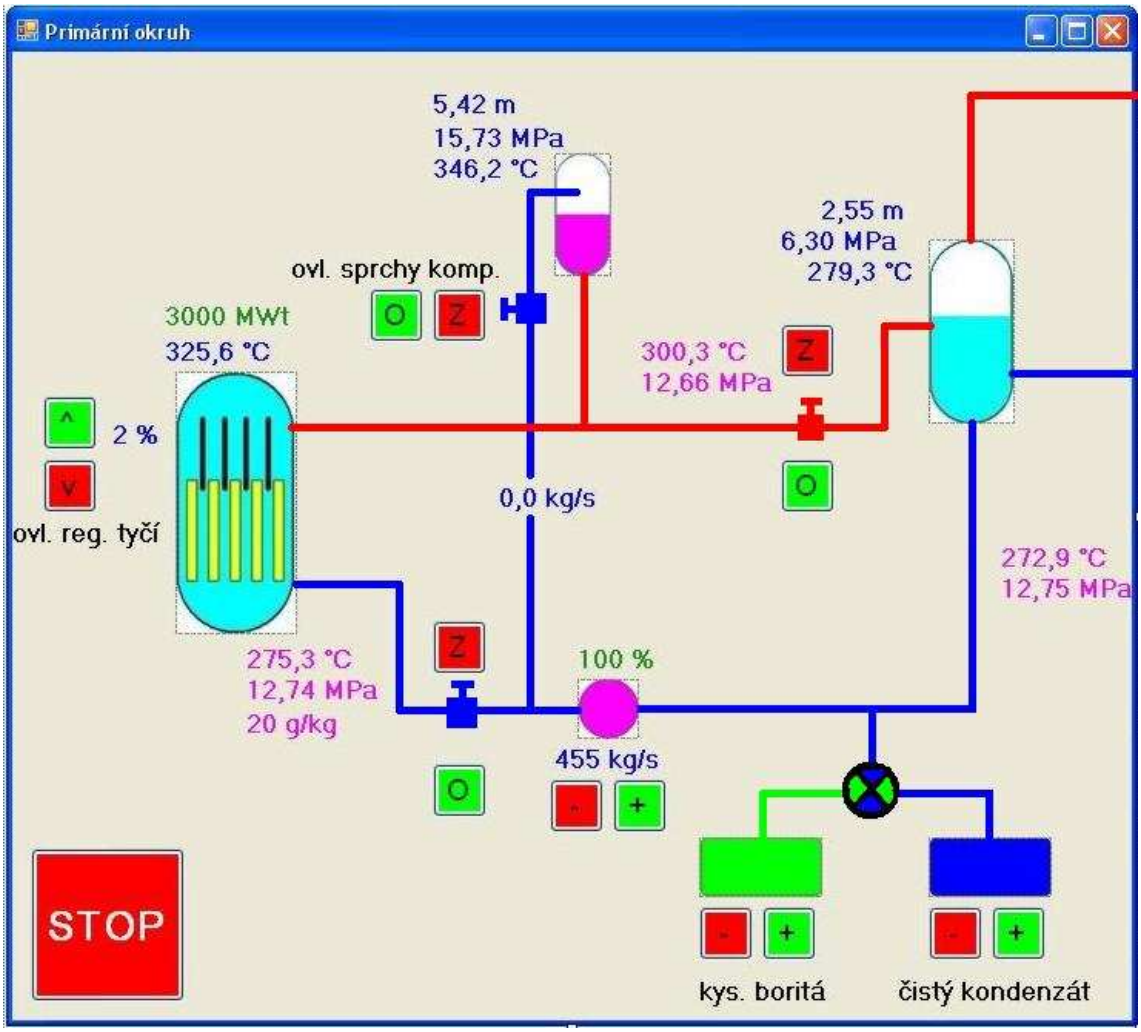
f) Vliv vyrušení jiným typem úlohy

V této části budeme obsluhu zaměstnávat dalšími úkoly, které přímo či nepřímo souvisí s obsluhou simulátoru.

Scénář simulace: Při běhu simulace budeme obsluhu zaměstnávat dalšími úkoly. Prvním z nich může být vyplňování nejrůznějších formulářů. Druhým úkolem bude telefonická konverzace, při které budou obsluze kladeny různé otázky. Vzhledem k tomu, že v simulátoru uvažujeme více monitorů, tak by dalším typem úlohy mohlo být sledování filmu, ve kterém by operátor musel najít odpovědi na předem připravené otázky. Rovněž je možné nechat operátora řadit různé kartičky podle abecedy, případně podle jiného kritéria.

7 Výsledky

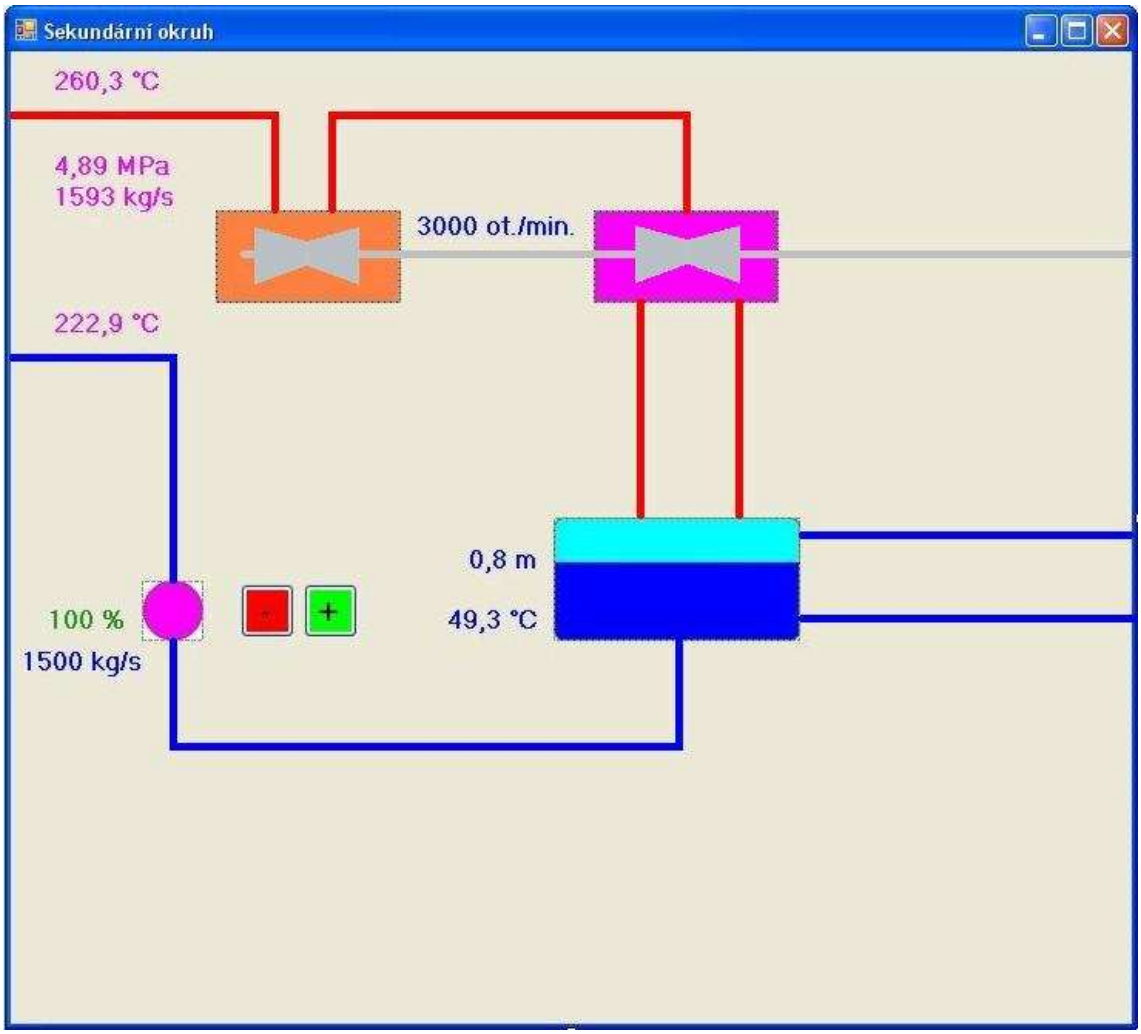
S využitím vývojového prostředí Microsoft Visual C++ byla navržena možná grafická podoba simulátoru. Na obrázku 7.1 je navrženo schéma primárního okruhu. V návrhu je uvažováno s využitím dotykových obrazovek popsaných v kapitole 6.2.1. Z toho důvodu jsou ovládací tlačítka součástí schématu tak, aby se s nimi mohl celý simulátor ovládat.



Obrázek 7.1: Možná podoba simulátoru primárního okruhu

Na obrázku 7.2 je znázorněna možná podoba sekundárního okruhu. Pro ovládání sekundárního okruhu využijeme druhou dotykovou obrazovku.

Oba grafické návrhy jsou prvotními návrhy, jak by simulátor mohl vypadat. Při samotné realizaci simulátoru předpokládáme spolupráci s odborníky na tvorbu simulátorů, odborníky z oblasti jaderné energetiky, grafiky a zkušenými programátory.



Obrázek 7.2: Možná podoba simulátoru sekundárního okruhu

Dva LCD monitory, které budou rovněž využity pro práci se simulátorem, využijeme například pro zobrazování grafů vývoje veličin, chybových hlášek, analýzy postupů operátorů apod. Rovněž mohou být využity pro některé popsané scénáře, především pro scénář vyrušení jiným typem úlohy, kdy operátor bude sledovat film či bude vyplňovat dotazníky.

7.1 Srovnání s reálnou praxí

Fyzikální chování jednotlivých částí technologie a samotný způsob ovládání elektrárny, popsaných ve scénářích v kapitole 6.2.5, bude nutné konzultovat se

zkušenými pracovníky jaderných elektráren Dukovany nebo Temelín. Tyto scénáře tedy budou změněny tak, aby co nejlépe odpovídaly reálné praxi a zároveň splňovaly naše požadavky na zjednodušený popis.

Nelze očekávat, že naměřená data bude možno bez úpravy použít pro výpočet lidské spolehlivosti v reálné průmyslové praxi. Naším vzorkem měření na simulátoru budou studenti, jejichž chování může být značně odlišné od skutečných operátorů. Přesto věříme v předpoklad, že obecné trendy vlivu PSF při řízení se podaří prokázat.

8 Závěr

První část bakalářské práce byla zaměřena na teoretické poznatky z oblasti spolehlivosti a hodnocení rizika lidského faktoru. Hlavním zdrojem informací byly zápisky z přednášek z předmětů hodnocení rizik a řízení jakosti a spolehlivosti.

Ve druhé části byly zhodnoceny základní používané kvantitativní metody. Tyto metody se nejčastěji používají pro odhad pravděpodobnosti lidského selhání. Byly popsány některé způsoby získávání dat pro kvantifikaci spolehlivosti člověka. K tomu byly využívány především publikace vydané v anglickém jazyce. Bylo ukázáno, jak jsou data o lidském výkonu získávána, shromažďována do databází a reálně užívaná. Byly ukázány praktické příklady užití analýzy spolehlivosti člověka včetně matematického výpočtu celkové pravděpodobnosti.

Na základě těchto informací doplněných o základní principy fungování nejběžnějšího typu jaderných elektráren s tlakovodním reaktorem byl získán dostatek potřebných informací pro tvorbu nového simulátoru pro Oddělení spolehlivosti a rizik. Byly vypočteny jeho finanční požadavky, byl navržen vhodný software, grafická podoba a zajímavé faktory, které by mohly být měřeny.

Tato práce je prvotním krokem k tvorbě reálného simulátoru. Jistě se ukáže, že bude potřeba dílčích změn především po konzultaci s pracovníky našich jaderných elektráren. Tyto změny by posléze měly přinést reálný simulátor, který by byl vhodný jak z hlediska měření kvantitativních dat, tak pro výuku a reálnou demonstraci obtížnosti obsluhy velkých průmyslových celků. To by mohlo být cílem mé další práce v této oblasti.

Seznam použité literatury

[1] Rudolf Holub, Zdeněk Vintr, Spolehlivost letadlové techniky, Vysoké učení technické v Brně, Fakulta strojního inženýrství, Elektronická učebnice, 2001.

[2] Pavel Fuchs, David Vališ, Josef Chudoba, Jan Kamenický, Jaroslav Zajíček, Elektronická verze přednášek předmětu Řízení jakosti a spolehlivosti, Technická univerzita v Liberci.

[3] Pavel Fuchs, Využití spolehlivosti v provozní praxi, Technická univerzita v Liberci, 2002.

[4] Vilém Sluka, Výkladový terminologický slovník některých pojmů používaných v analýze a hodnocení rizik pro účely zákona o prevenci závažných havárií, Výzkumný ústav bezpečnosti práce, 2004.

[5] Milan Říha, Integrovaný záchranný systém [online] [cit. 2010-11-20], dostupné na URL: <www.trivis.info/view.php?cisloclanku=2005112101>.

[6] Luboš Kotek, Martina Vohralíková, Jak zvyšovat spolehlivost lidské obsluhy [online] [cit. 2010-11-20], dostupné na URL: <www.odbornecasopisy.cz/index.php?id_document=37315>.

[7] Petr Skřehot, Spolehlivost lidského činitele [online] [cit 2010-11-28], dostupné na URL: <www.bozpinfo.cz/knihovna-bozp/citarna/clanky/lidsky_cinitel/spol_lid_cin06.html>.

[8] ČSN EN 62508, Návod pro lidská hlediska spolehlivosti, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.

[9] Heinz-Peter Berg, Human Factors in Safety and Reliability, SSARS 2009.

[10] Alain D. Swain, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, 1987.

[11] Marie Havlíková, Lidský faktor v systémech MMS [online] [cit 2010-11-30], dostupné na URL: <www.bozpinfo.cz/josra/josra-01-2009/havlikova_lidsky-faktor.html>.

[12] D. D. Orvis, P. Moieni, V. Joksimovich, Organizational and Management Influences on Safety of Nuclear Power Plants: Modeling Hypotheses Using PRA Techniques, NUREG/CR-5752, U.S. Nuclear Regulatory Commission, 1993.

[13] David I. Gertman, Harold S. Blackman, Human Reliability & Safety Analysis Data, 1993.

[14] P. Pyy, An analysis of maintenance failures of a nuclear power plant, 2001.

[15] Lauren C. Havighurst, M.A., Laura E. Fields, M.S., Cassi L. Fields, Ph.D., High Versus Low Fidelity Simulations: Does the Type of Format Affect Candidates‘ Performance or Perceptions?

[16] Alain D. Swain, H. E. Guttmann, Handbook of Human Reliabilty Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandia National Laboratories, 1983.

[17] Gene Abruzere, Rozmach simulací v elektrárnách [online] [cit 2011-03-22], dostupné na URL: <www.controlengcesko.com/index.php?id=47&no_cache=1&tx_ttnews%5BbackPid%5D=35&tx_ttnews%5Btt_news%5D=3064&cHash=0dbd68e232&type=98>.

[18] Tomáš Herceg, Tomáš Jecha, Web o jazyce Visual Basic .NET [online] [cit 2011-04-02], dostupné na URL: <www.vbnet.cz>.

[19] Moravské přístroje, a.s., Webové stránky společnosti [online] [cit 2011-04-02], dostupné na URL: <www.controlweb.cz>.

[20] Institutt for energiteknikk, HAMMLAB [online] [cit 2011-04-04], dostupné na URL: <www.ife.no/laboratories/hammlab/index_html-en?set_language=en&cl=en>.

[21] Institutt for energiteknikk, Jaderné simulátory HAMMLAB [online] [cit 2011-04-04], dostupné na URL: <www.ife.no/laboratories/hammlab/files/nucsimhl/view>.

[22] Lukáš Rytíř, Seznam jaderných elektráren [online] [cit 2011-04-15], dostupné na URL: <http://proatom.luksoft.cz/jaderneelektrarny/index.php?akce=reaktor&idtypbloku=2>.

[23] ČEZ, a.s., Princip funkce jaderné elektrárny [online] [cit 2011-04-15], dostupné na URL: <www.cez.cz/cs/vyroba-elektriny/jaderna-energetika/jaderne-elektrarny-cez/ete/technologie-a-zabezpeceni/4.html>

[24] Steffen Kuntoff, Generování elektrické energie [online] [cit 2011-04-15], dostupné na URL: <www.hellfirez.de/web/referate/inhalte/Physik_Energie.htm>.