ČESKÁ SPOLEČNOST PRO JAKOST

Novotného lávka 5, 116 68 Praha 1

SPECIÁLNÍ TÉMATA HODNOCENÍ SPOLEHLIVOSTI MODERNÍCH TECHNOLOGIÍ SE ZAMĚŘENÍM NA DIGITÁLNÍ SYSTÉMY KONTROLY A ŘÍZENÍ

Materiály ze 48. semináře
odborné skupiny pro spolehlivost

Praha, září 2012

Obsah

Vážení přátelé,

výbor **Odborné skupiny pro spolehlivost** České společnosti pro jakost Vás vítá na dalším semináři, zaměřeném na výměnu zkušeností s řešením problematiky spolehlivosti. Dnešní setkání je věnováno několika zajímavým tématům souvisejícím se spolehlivostí a bezpečností provozu složitých moderních technologií. Téma, jež alespoň částečně spojuje všechny tři příspěvky, které budou přednesené na semináři a jsou uvedené v tomto sborníku, je role moderních **systémů kontroly a řízení** v kontextu zajištění spolehlivého provozu technologie jako celku.

První příspěvek se bude zabývat velkou skupinou událostí, nazývanou souborně *externími* nebo *přírodními* událostmi reprezentujícími tzv. *externí hazardy*. Jeho cílem je shrnout zkušenosti z analýzy jejich, především bezpečnostních, dopadů na jaderně-energetickou technologii, které lze přímočaře přenést do oblasti **hodnocení spolehlivosti** a zobecnit i pro **další moderní technologie** provozované za náročných požadavků na spolehlivost. V souladu s tématem semináře se příspěvek bude orientovat i na příklady účinku vybraných externích (přírodních) událostí na komponenty systémů kontroly a řízení provozu technologie. Přestože rozvoj řešení témat spojených s externími událostmi byl nedávno výrazně stimulován známými událostmi na JE Fukušima a následným celosvětovým vývojem v jaderné energetice, řada závěrů je přenositelná i na jiné průmyslové technologie. V rámci příspěvku bude diskutována především odezva technologie na události typické pro lokality provozu moderních technologií v České republice, tj. extrémní vichřice, extrémně vysoké a extrémně nízké teploty, extrémní vodní a sněhové srážky atd. Příspěvek přednese RNDr. Jaroslav Holý, vedoucí Oddělení spolehlivosti a rizik ÚJV a.s., které se externím událostem intenzivně věnuje v posledních pěti letech jako jednomu z významných přispěvatelů do spektra faktorů potenciálně ovlivňujících bezpečnost provozu jaderných elektráren.

Druhý příspěvek přímo zastupuje hlavní téma odborného setkání – řešení otázek spolehlivosti moderních digitálních systémů kontroly a řízení. Příspěvek se v přehledové formě věnuje současnému stavu v oboru a specifickým rysům hodnocení spolehlivosti této kategorie komponent v porovnání s běžnými prvosledovými komponentami a systémy typickými pro strojně průmyslové technologie. Příspěvek přednese ing. Jiří Sedlák rovněž z Oddělení spolehlivosti a rizik ÚJV a.s., který se mimo jiné podílí na činnosti speciální mezinárodní pracovní skupiny OECD NEA DIGREL, zabývající se aktuálně vytvořením taxonomie poruchových módů pro digitální systémy kontroly a řízení.

Třetí příspěvek měl být původně orientován na konkrétní zajímavý případ analýzy spolehlivosti systému kontroly a řízení – spolehlivost řídicího systému vlaku. V závěrečné fázi přípravy semináře bylo v důsledku posunu jeho termínu a nutnosti zajištění nového přednášejícího rozhodnuto o jeho nahrazení obecnější verzí stejného tématu, uvedenou v tomto sborníku. Nový příspěvek se věnuje moderním způsobům zajištění bezpečného a spolehlivého provozu na železnici, v jejichž rámci se uplatňují principy funkční bezpečnosti a řízení rizik. Z časových důvodů byla pro potřeby sborníku využita pouze kopie prezentace, za což se garant semináře omlouvá.

Přírodní události a provoz složité moderní technologie a metody analýzy jejich vlivu na spolehlivost

RNDr. Jaroslav Holý, Ústav jaderného výzkumu Řež

1. Úvod – spolehlivost moderní technologie, systémy kontroly a řízení a externí události

Většina moderních technologií je v současném konkurenčním prostředí provozována s vysokými požadavky na spolehlivost a bezpečnost. Spolehlivost provozu technologie a ekonomické i další následky jejího selhání jsou výrazně ovlivněny spolehlivostí komponent a systémů zabezpečujících řízení jejího provozu.

Spolehlivost technologie je ukazatel, který je již po dlouhou dobu (několik posledních dekád) stále častěji, podrobněji a sofistikovaněji analyzován, hodnocen, porovnáván, sledován z pohledu trendů vývoje a cíleně pozitivně ovlivňován přijímanými opatřeními. Tradiční, opakovaně využívané a dále zdokonalované přístupy k hodnocení a ovlivňování spolehlivosti i *bezpečnosti* provozu se však většinou zaměřují na (z pohledu technologie) *interní* události, charakteristické selháním vlastní komponenty/systému, s různými dopady na provoz danými pozicí selhavšího prvku v logickém uspořádání struktury elementů technologie. V poslední době je však stále častěji doceňován i vliv událostí, jejichž negativní, v nejtěžších případech destruktivní účinek, má svůj původ v *externích* jevech s omezenou, v řadě případů minimální možností ovlivnění potenciálu vzniku provozovatelem dané technologie.

Zásadním rozdílem mezi typickými interními a externími událostmi v běžném pojetí jejich pravděpodobnostní analýzy zaměřené na spolehlivost nebo bezpečnost je binární pohled na vznik *interní* události (událost vzniká nebo nevzniká s danou/odhadovanou frekvencí - například daný provozní systém pracuje nebo selže ve své funkci) a *spojité pojetí* parametrizace a analýzy *externích* událostí (externí událost je vždy přítomna, ale až při jisté, vzácné hodnotě určujícího parametru z krajní oblasti spojitého spektra jeho hodnot se projeví negativními/destruktivními následky – běžný vítr nebo smysly nepozorovatelné seismické projevy nijak neovlivňují provoz technologie, ale extrémní vichřice nebo silné zemětřesení má destruktivní vliv na její komponenty, ať už přímo, nebo díky zborcení stavebních konstrukcí, ve kterých jsou umístěny).

Tento příspěvek se zabývá velkou skupinou externích událostí, nazývanou souborně *přírodními* událostmi reprezentujícími tzv. *externí hazardy*. Jeho cílem je shrnout zkušenosti z analýzy jejich, především *bezpečnostních*, dopadů na jaderně-energetickou technologii, které lze přímočaře přenést do oblasti hodnocení *spolehlivosti* a zobecnit i pro další moderní technologie provozované za náročných požadavků na spolehlivost. V souladu s tématem semináře se příspěvek bude výrazně orientovat na příklady účinku vybraných externích (přírodních) událostí na komponenty *kontroly a řízení* provozu technologií.

Požadovaná míra *spolehlivosti* provozu technologie je utvářena a silně ovlivňována požadavky na *bezpečnost a stabilitu* provozu technologie na jedné straně a snahou o *efektivní, ekonomicky výhodný* provoz technologie na straně druhé. *Veřejnost* typicky požaduje co nejvyšší *bezpečnost* provozu technologie a co nejmenší ohrožení populace a životního

prostředí jejím provozem a *provozovatel* se snaží o co nejvyšší *spolehlivost*, která mu zaručí co nejdelší a bezporuchový provoz zařízení a přiměřený *zisk*. Nereálné požadavky na bezpečnost principiálně vedou buď k zablokování projektu nové technologie nebo jejímu odstavení, popřípadě ke (z pohledu investora/provozovatele) nepřijatelnému nárůstu nákladů. Procesy budování a provozu moderní technologie by se proto měly pohybovat na optimální úrovni mezi bezpečností, spolehlivostí a ekonomikou.

Realizace podpůrných analýz pro hodnocení bezpečnosti a spolehlivosti se v současné praxi velmi často (detailně) zaměřují na různé scénáře *interního selhání* technologie, které jsou buď z vlastních nebo přejatých zkušeností pokládány za realistické, ne-li frekventované, nebo jsou sice vzácné a málo pravděpodobné, ale na základě historických zkušeností z provozu (hodnocené technologie nebo i příbuzných technologií) do projektových a provozních analýz „povinně“ zařazované. *Externí události*, které naopak z historických důvodů nebývaly tradičními subjekty takto pojatého hodnocení, se v praxi projevují vzácně a jejich absence v analýzách tak má opticky malý dopad na realitu provozu - pokud ale k výskytu dojde i s očekávanou mírou následků, jež je u "silných" externích událostí vysoká, mohou jejich efekty jednorázově vést k velkým výkyvům ve veřejném mínění a na celém trhu technologií daného druhu, podobně jako u reakce mezinárodní odborné i laické veřejnosti na události na JE Fukušima.

Komponenty systémů *kontroly a řízení* ve scénářích účinku externích událostí na moderní technologii a odezvy technologie na jejich vznik hrají ze své podstaty důležitou roli, protože téměř každý scénář nestandardní události může být pozitivně ovlivněn jejich správnou funkcí a dobrou kooperací s lidským prvkem v řízení provozu během odezvy na událost, stabilizace provozu a převedení technologie do bezpečného klidového stavu nebo naopak posílen ve svém negativním efektu ztrátou prostředků pro řízení probíhajících nestandardních procesů. Specifickým rysem selhání těchto komponent pak je dvojaký hrozící typ selhání – kromě "klasického" selhání obecně spočívajícího v tom, že daný (řídící) prvek procesu odezvy na vznik provozního problému je ve své funkci nedostupný, se rovněž významně uplatní poruchový mód spočívající ve vygenerování *falešné aktivity* řídicího systému a obecně nežádoucího požadavku na činnost některého prvku technologie řešícího v prvním sledu odezvu na mimořádný stav. Tento typ selhání systémů kontroly a řízení je typický i pro některé externí události a může pro daný typ události představovat významného přispěvatele k potenciálu pro narušení spolehlivosti a bezpečnosti provozu technologie.

Pro zajištění co nejvyšší rozumně dosažitelné úrovně bezpečnosti a spolehlivosti provozu technologie lze zobecnit tzv. princip ALARA – „*as low as reasonable achievable*“ dobře známý z provozu jaderně-energetických zdrojů do formy následujících tří postulátů:

- zabránit nekontrolovanému negativnímu vlivu technologie na lidskou populaci a životní prostředí,
- minimalizovat pravděpodobnost vzniku takových událostí, které by mohly vést ke ztrátě kontroly nad provozem technologie spojené s následky naplňujícími definici negativního vlivu v předchozím bodu
- v případě vzniku událostí dle předchozího bodu je zvládnout tak, aby byly jejich negativní následky minimalizovány.

Dodržení základních bezpečnostních a spolehlivostních cílů by mělo být být zajištěno ve všech fázích existence technologie, včetně plánování její výstavby, umisťování do lokality,

projektování, vlastní výroby a výstavby, uvádění do provozu, vlastního provozu až po vyřazení a to i se zahrnutím transportu nebezpečných materiálů a nakládaní s nebezpečnými odpady. Bezpečný a spolehlivý provoz moderní technologie je (obecně i speciálně ve vztahu k externím událostem) garantován:

- uplatňováním principu jediné, nedělitelné odpovědnosti a zajištěním vysoké úrovně kultury bezpečnosti (obecně posilujícím odolnost technologie i vůči projevům externích událostí)
- správným výběrem lokality provozu technologie (se zcela zásadním preventivním ovlivněním síly projevů a následků externích událostí)
- pečlivým projektováním při dodržení platných technických a bezpečnostních standardů, výběrem ověřených prvků pro design a provoz technologie a uplatňováním principů ochrany do hloubky (podcenění tohoto pravidla, které ve vztahu k externím událostem extrémní síly může mít zcela "logické" a "ospravedlnitelné" důvody, ve fázi výstavby technologie může znamenat velké problémy při pozdějším uplatnění legislativních požadavků na bezpečnost a spolehlivost jejího provozu)
- komplexním zajištěním jakosti při projektování, výrobě, montáži, spouštění a provozu technologie (stejná poznámka jako v předchozím případě)
- vysokou a po celý provoz technologie posilovanou kvalifikací provozního personálu (ve vztahu k následkům externích událostí působí preventivně udržováním nastavené kvality designu a provozu a je zárukou adekvátní odezvy na vznik externí události)
- důsledným ověřováním, hodnocením a kontrolou bezpečnostních zařízení a činností (s výraznou vazbou na činnosti systémů kontroly a řízení a s dostatečným prostorem vyhrazeným problematice externích událostí)
- využíváním zpětné vazby ze zkušeností pro aplikaci provozních postupů (v rámci odezvy na externí události může jít i o převzaté zkušenosti z jiných lokalit, kde je provozována příbuzná technologie)
- plněním ostatních bezpečnostních požadavků (fyzická ochrana, technická bezpečnost, havarijní připravenost, ochrana životního prostředí, požární ochrana apod.).

Ochrana do hloubky je klíčovým principem využívaným při zajištění spolehlivého a bezpečného provozu jaderně-energetické technologie (opírajícím se o základní dokument Mezinárodní atomové agentury ve Vídni INSAG – 3, respektive jeho novou rozšířenou revizi INSAG–12 [1]). Smyslem ochrany do hloubky, jako obecného principu přenositelného do provozu dalších složitých moderních technologií pracujících s vysokými požadavky na spolehlivost a bezpečnost, je zajistit prevenci proti vzniku havárií a v případě jejich vzniku zajistit zmírňování následků havárie v maximální možné míře. Primárně se ochrana do hloubky zabývá prevencí, jež je založena na fyzických bariérách a řídí se obecně následujícími principy:

- konzervativnost při návrhu, konstrukci, výrobě a montáži, dosahovaná používáním ověřených a spolehlivých metod (podporuje kvalitní odezvu na projevy externích událostí, včetně zapojení systémů kontroly a řízení do odezvy)

- program zajištění jakosti užívaný při všech provozních činnostech (s výrazným pozitivním preventivním dopadem na kvalitu odezvy na projev externí události vysoké intenzity)
- uvážení selhání lidského činitele, kdy při všech provozních i speciálních činnostech je počítáno s lidským faktorem a tomu jsou podřízena opatření k zajištění spolehlivosti a bezpečnosti provozu (v oblasti externích událostí často nebyla tato oblast historicky budována ve stejné míře jako pro interní události a je zde velký prostor pro metodický vývoj)
- spolehlivostní a bezpečnostní rozhodování (s rostoucím uplatněním spolehlivostně a rizikově orientovaného rozhodování u externích událostí)
- radiační ochrana (typické pro provoz jaderných technologií, ale s analogiemi pro prevenci účinku nebezpečných látek u dalších rizikových technologií s potenciálem ohrozit zdraví člověka a životní prostředí)
- zpětná vazba (v oblasti jaderně-energetické technologie velmi silně rozvinutá), včetně využití zkušeností z provozu výměnou informací mezi různými zástupci provozované technologie, v případě jaderné energetiky v rámci platforem MAAE /Mezinárodní atomová agentura/ či WANO /organizace provozovatelů JE/ (u obecně vzácných externích událostí vysoké intenzity velmi důležitý princip).

Pro zajištění bezpečnosti se u moderních průmyslových technologií uvažují dva progresivní typy bezpečnostních přístupů (aplikovatelné i v rámci odezvy na externí události a mající pro zvládnutí závažných externích událostí vysoké intenzity ještě větší význam než pro "standardní" události interní):

- *inherentní bezpečnost* předpokládá využití základních fyzikálních principů fungování dané technologie, které samy a priori vyloučí možnost havárie
- *pasivní bezpečnost* zmírní následky případných havárií a spolu s bariérami zabrání úniku nebezpečných látek i v případě, že by selhala veškerá aktivní bezpečnostní havarijní technika.

Inherentní systém je netečný vůči lidským chybám, úmyslným zásahům nebo vnějším vlivům. Tlakovodní jaderný reaktor má tuto vlastnost, která je dána fyzikálními vlastnostmi uranu a vody, podílejícími se na procesu jaderného štěpení. Voda, která slouží jako moderátor (zpomalovač neutronů), zvětšuje v důsledku růstu své teploty svůj objem, tj. dochází ke zvětšování vzdáleností mezi jednotlivými molekulami vody. V důsledku toho se snižuje moderační účinek vody, který je předpokladem pro vznik a existenci štěpné řetězové reakce. To má za následek pokles počtu tepelných neutronů, které jsou schopny štěpit jádra uranu, a tak dochází k útlumu štěpné reakce, což postupně může vést až k úplnému samoodstavení reaktoru. Proto ve všech případech, při kterých by došlo k růstu teploty vody v důsledku nežádoucího výkonu, se výkon tohoto typu reaktoru samovolně tlumí.

Inherentní systém může snížit závažnost selhání systémů kontroly a řízení provozu technologie. V případě jaderného reaktoru s designem podporujícím inherentní bezpečnost ani selhání několikanásobně zálohované nezávislé havarijní ochrany, odstavující reaktor v případě havárie se ztrátou chladiva primárního okruhu, nezabrání zastavení štěpné reakce díky tomu, že se v aktivní zóně reaktoru tvoří pára, ve které jsou vzdálenosti mezi molekulami řádově větší než u vody. Na bezpečnosti provozu těchto reaktorů se však podílí i samotné jaderné palivo. Uran 238, který tvoří asi 97 % paliva, zasahuje regulačně do procesu štěpení

tak, že sám absorbuje neutrony, aniž by se dále štěpil. Opět platí, že absorbuje tím více neutronů, čím je jeho teplota vyšší. Obecně mluvíme o tzv. *záporném koeficientu reaktivity* – dojde-li ke zvýšení teploty v reaktoru, dojde v důsledku horšího zpomalování neutronů k poklesu četnosti štěpení a tím k poklesu množství uvolňované energie.

Základním prvkem *pasivní bezpečnosti* u jaderného reaktoru jsou *havarijní absorpční tyče* systému havarijní ochrany. Ve scénářích s úplnou ztrátou elektrického napájení, včetně záložních zdrojů, se nevyžaduje bezprostřední aktivní zásah systému kontroly a řízení, protože tyče samovolně *působením zemské tíže* spadnou do reaktoru a zastaví štěpnou reakci. Jiným příkladem prvku pasivní bezpečnosti u jaderně-energetické technologie je vnější bariéra proti úniku radioaktivních látek, pevná železobetonová obálka nad reaktorem – kontejnment. V kontejnmentu jsou umístěny nejdůležitější části jaderné elektrárny - celý primární okruh a další bezpečnostní a pomocná zařízení. Kromě dalších funkcí kontejnment zajišťuje jejich ochranu proti *externím* událostem: odolá například pádu dopravního letadla, tlakové vlně výbuchu, vichřici, extrémním teplotám, extrémním srážkám a podobně. Uvnitř kontejnmentu je vedle reaktorové šachty umístěn bazén použitého paliva, takže i výměna paliva probíhá bezpečně v uzavřeném prostoru.

Pro projektování systémů, plnících bezpečnostní funkce ochrany do hloubky, se využívá metod opírajících se o zavedené a konzervativní inženýrské postupy, například *redundanci* (zálohování), *diverzitu* (rozličnost) nebo *fyzickou separaci*. Použití *redundance*, velmi výrazně aplikované u systémů kontroly a řízení, znamená, že se systém projektuje tak, aby plnil svoji funkci s vysokou spolehlivostí díky rozčlenění do dvou, tří nebo více identických, zcela nezávislých větví, kde správná činnost každé z nich naplní funkci systému jako celku (při bližším pohledu se však tato „úplná nezávislost“ obvykle projeví jako iluzorní). *Diverzita* je z pohledu prevence úplného selhání systému vyšším stupněm redundance, kdy jsou nezávislé větve systému samostatně zabezpečující naplnění jeho funkce založeny na odlišných projektových a funkčních principech (jako klasický příklad diversity mohou posloužit dva zálohující se způsoby havarijního odstavení - pomocí havarijních tyčí a pomocí zaplavení aktivní zóny kyselinou boritou). Externí události vysoké intenzity mohou výrazně devalvovat přednosti redundance, ale často nebudou již dostatečně silné pro poškození funkce systémů obsahujících prvky diverzity. *Fyzická separace* je v zásadě jedním z faktorů podporujících skutečnou nezávislost funkce redundantních nebo diverzifikovaných systémů. Nedostatečná fyzická separace byla vyhodnocena jako jedna z důležitých příčin nezvládnutí scénáře odezvy na tsunami při havárii na JE Fukušima. I v rámci opatření navrhovaných pro zvýšení bezpečnosti provozu evropských JE hraje fyzická separace důležitou roli.

2. Výběr externích událostí s vlivem na spolehlivost provozu moderní technologie a jejich orientační analýza

V následující tabulce je uveden seznam obecně uvažovaných externích přírodních událostí, tak jak vyplývá například z publikací [2], [3]. Jak již bylo naznačeno v úvodu, *externí* událost obecně nelze označit za *iniciační* událost ve smyslu pravděpodobnostních modelu bezpečnosti. Obecnou vlastností externích událostí je však schopnost za určitých podmínek, při vysoké hodnotě určujícího parametru události, takovou iniciační událost vyvolat. Míra rizika provozu technologie je pak dána součinem frekvence vzniku vyvolané iniciační události a pravděpodobností selhání odezvy technologie na tuto událost.

Pro *externí* události je často charakteristická relativně nízká četnost vzniku vyvolané iniciační události a vysoký potenciální negativní vliv na stav zařízení technologie, implikující vysoký potenciál pro selhání její odezvy na událost, způsobený především skutečností, že u externích událostí může dojít k současnému narušení funkce nebo vyřazení většího počtu provozních nebo bezpečnostních systémů, včetně systémů kontroly a řízení, které jsou projektovány, aby se při selhání vzájemně zálohovaly. Dalším charakteristickým znakem externích událostí je specifičnost jejich síly a charakteru pro danou lokalitu a závislost účinku na konkrétním projektovém provedení technologie.

V průběhu procesu hledání relevantních iniciačních událostí je vhodné se zabývat co nejúplnějším seznamem externích IU, a následně provádět jeho redukci v závislosti na konkrétních parametrech lokality provozu technologie a projektových a provozních charakteristikách staveb a technologických zařízení. V dalším, souvisejícím kroku analýzy je pak nutné podrobněji specifikovat jednotlivé iniciační události vyvolané případným výskytem externí události na základě hodnot parametrů, které se vztahují k velikosti ohrožení technologie a schopnosti způsobit její poškození. Například při úvahách o četnosti výskytu silné vichřice je nezbytné rozlišit větrné bouře podle síly, neboť jen ty největší větrné bouře způsobí škody a budou zřejmě předmětem zájmu spolehlivostních a bezpečnostních analýz. Pro externí událost analyzovanou v souvislosti s provozem jaderně-energetických zařízení byly například za odpovídající parametry považovány následující hodnoty:

- projektové zatížení tlakem větru: 0,69 kN/m^2
- extrémní výpočtové zatížení tlakem větru: 1,26 KN/m^2.

Na základě těchto dvou parametrů lze odvodit maximální rychlosti větru, při které lze očekávat vyvolání odpovídajícího tlaku na stavební konstrukce a vnější zařízení JE. V případě *projektového* zatížení tlakem a předpokladu o působení po dobu alespoň 10 vteřin se u jaderné elektrárny jedná o cca 46 m/s. V případě *extrémního* výpočtového zatížení tlakem větru a za stejného předpokladu o působení zátěže alespoň 10 s se pak jedná o hodnotu cca 60 m/s.

Cílem dalšího kroku analýzy je vyřadit iniciační události, jejichž četnost výskytu je tak malá, že s velkou jistotou významně neovlivní celkové riziko provozu JE. Vzhledem k charakteru iniciačních událostí vyvolaných externími událostmi (možnost velkých následků) je však nutné volit dostatečně přísné výběrové kritérium pro vyřazení iniciačních událostí z analýzy z těchto důvodů. V souladu s kritérii výběru, tak jak jsou uvedena v [4], je pro externí události použita jako nejnižší hodnota roční frekvence výskytu události, kdy je nutné událost uvažovat v rizikových analýzách jaderných elektráren, hodnota 1x10^{-7} události/rok. Nutnou podmínkou pro doporučení k podrobné analýze externí události je však kromě překročení limitní hodnoty roční frekvence vzniku i existence prokazatelných následků externí události vedoucích na vznik „skutečné“ iniciační události. Pojem iniciační události pro účely analýzy externích rizik je definován stejně jako v jiných scénářích modelovaných ve studiích pravděpodobnostního hodnocení bezpečnosti. Plánované postupné odstavování nebo snížení výkonu vyvolané externí událostí, například z důvodu administrativního odstavení v situaci, kdy hrozí porušení („přečerpání“) Limit a Podmínek provozu technologie nebo z důvodů preventivního odstavení technologie ještě před skutečným „nárazem“ externí události, není ve standardních bezpečnostních analýzách považováno za iniciační událost.

Následující tabulka podává přehled o externích událostech, které byly systematicky hodnoceny z hlediska rizikového potenciálu závažného pro provoz jaderných elektráren a

vybrané z nich podrobně analyzovány (ve smyslu definování iniciačních událostí, modelování odezvy technologie na vznik iniciační události, ocenění rizika, které iniciační a tedy i externí události přinášejí, a formulace opatření ke snížení tohoto rizika). Další informace o závěrech z těchto analýz, především z pohledu vlivu událostí na činnost komponent systémů kontroly a řízení, je uvedena v kapitole 4.

Tabulka 1: Celkový přehled externích přírodních událostí zpracovaných v rizikových analýzách pro české jaderné elektrárny a zobecnění závěrů analýz pro jiné technologie

Původ jevu	Základní jevy	Konkrétní projevy	Detaily analýzy a rizikový potenciál
Půda	*Zemětřesení (důlní činnost)*	Záchvěvy podloží o různé intenzitě	V letech 2007-2010 zpracována metodika seismické studie rizika. V letech 2011-2012 realizována kompletní seismická studie rizika pro JE Dukovany. Rizikový příspěvek seismické události odhadován díky značné geologické stabilitě podloží jako malý. **Podobný výsledek by mohl být dosažen i pro většinu průmyslových technologií provozovaných v ČR.**
	Vulkanická činnost	Výbuch sopky, výrony plynu	Analyzována historie vulkanické činnosti na území současné ČR, na základě této analýzy a vulkanologických a geologických předpokladů byla událost z další analýzy vyřazena. Odezva jaderné elektrárny na tuto externí událost neanalyzována. **Podobný výsledek je pravděpodobný i pro většinu průmyslových technologií provozovaných v ČR.**
	Změny podloží	Sesuvy nebo sedání půdy, laviny, bobtnání jílu, zhroucení krasu	Předpokládalo se, že náchylnost k měřitelnému potenciálu pro vznik takové události by odhalil geologický průzkum před zahájením výstavby elektrárny. Riziko zanedbáno, odezva elektrárny na iniciační událost neanalyzována. **Tento výsledek není přenositelný na jiné lokality a technologie.**
	Abrazivní bouře	Písečné a prašné bouře	Potenciál pro vznik iniciační události v lokalitě EDU vyhodnocen jako poměrně vysoký. Událost a odezva JE na ni detailně analyzována v roce 2008. Událost patří mezi minoritní rizikové přispěvatele. **Pro jiné technologie tento závěr obecně není přenositelný.**
Voda	*Říční záplavy*	Protržení přehrady, záplavy v důsledku deště nebo tání	Apriori vyloučeno v důsledku vzájemné výškové polohy elektrárny a přilehlých vodních zdrojů. Provedena pouze stručná přehledová analýza. Pro analýzu **odezvy** technologie na tuto externí událost je však dostupná metodologie, se kterou jsou i praktické zkušenosti, osvojené při řešení problematiky vnitřních záplav. **Výsledky analýzy jsou pro danou lokalitu zcela specifické a nepřenositelné.**
	Pobřežní záplavy	Tsunami, vysoké vlny	Tato v současnosti velmi známá externí událost je v kontextu provozu JE Dukovany zcela vyloučena v důsledku vnitrozemské polohy lokality elektrárny. **Stejný závěr platí pro všechny průmyslové technologie provozované v České republice.**

Vzduch	*Extrémní meteorologické podmínky*	Extrémně vysoká teplota	Detailně analyzována frekvence vzniku extrémního přírodního jevu v celém spektru projektových i nadprojektových událostí. Frekvence intervalů postulovaných intenzit události odvozeny extrapolací z dostupných historických dat (viz kapitola 3). Detailně analyzována odezva JE na vznik události. Událost představuje poměrně významného rizikového přispěvatele. **Lze očekávat, že tato událost bude spolehlivostně a rizikově významná pro mnoho průmyslových technologií. Data spojená s frekvencí a intenzitou výskytu události by měla pro mnohé technologie částečně přenositelná vzhledem k obdobnému charakteru rozdělení teplotních meteorologických veličin v České republice. Určující charakteristikou pro přenositelnost bude nadmořská výška. Odezva každé technologie na vznik události extrémní intenzity bude ovšem vysoce specifická. Nepřehlédnutelným faktorem, stimulujícím požadavky na analýzu této události, jsou projevy klimatických změn (nový teplotní rekord dosažený v srpnu tohoto roku znatelně překračuje současnou hodnotu intenzity této události s dobou návratu 100 roků).**
		Extrémně nízká teplota	Detailně analyzována frekvence vzniku extrémního přírodního jevu v celém spektru projektových i nadprojektových událostí. Frekvence intervalů postulovaných intenzit události odvozeny extrapolací z dostupných historických dat (viz kapitola 3). Detailně analyzována odezva JE na vznik události. Událost představuje poměrně významného rizikového přispěvatele (pro JE Dukovany ale nižšího než „příbuzná“ událost „Extrémně vysoká teplota“). **Událost může být spolehlivostně a rizikově významná pro mnoho průmyslových technologií. Data spojená s frekvencí a intenzitou výskytu události by měla být pro mnohé technologie částečně přenositelná vzhledem k obdobnému charakteru rozdělení teplotních meteorologických veličin v České republice. Určující charakteristikou pro přenositelnost bude nadmořská výška. Odezva každé technologie na vznik události extrémní intenzity bude ovšem vysoce specifická.**
		Extrémní vodní srážky	Detailně analyzována a odvozena frekvence vzniku události, na základě kvalitativní analýzy se předpokládá poměrně příznivá odezva, která nebyla dále pro lokalitu a umístění stavebních objektů EDU podrobně analyzována. Případný vývoj extrémní přírodní události vede na záplavové scénáře, pro jejichž analýzu je k dispozici metodika a praxe v jejím užití. **Závěry ke spolehlivostnímu a rizikovému vlivu dané události na provoz technologie jsou obtížně přenositelné ze dvou důvodů: 1) srážkové úhrny a dynamika jejich tvorby jsou pro danou lokalitu značně specifické (výrazněji než u extrémních teplot) 2)negativní následky této události se formují přes záplavové scénáře, jejichž potenciál je u různých lokalit v ČR vysoce individuální.**

		Extrémní sněhové srážky	Detailně analyzována frekvence vzniku extrémního přírodního jevu v celém spektru projektových i nadprojektových událostí. Frekvence intervalů postulovaných intenzit události odvozeny extrapolací z dostupných historických dat. Detailně analyzována odezva JE na vznik události. **Závěry ke spolehlivostnímu a rizikovému vlivu dané události na provoz technologie jsou obtížně přenositelné ze dvou důvodů: 1) srážkové úhrny a dynamika jejich tvorby jsou pro danou lokalitu silně specifické (výrazněji než u extrémních teplot) 2)Negativní následky této události se formují přes scénáře narušení odolnosti stavebních konstrukcí, jejichž potenciál je pro různé technologické provozy v ČR vysoce individuální (závisí především na kvalitě střešního pokrytí).**
		Námraza	Pro JE Dukovany detailně analyzována frekvence vzniku a souborně zhodnocen rizikový potenciál a možné scénáře rozvoje události. Pro hlavní důsledek - postižení systémů elektrického napájení - byla událost z další analýzy vyloučena vzhledem k jiným dominujícím poruchovým módům vedoucím ke ztrátě jejich funkce. **Závěry z analýzy jaderně-energetické technologie nejsou obecně přenositelné na jiné technologie provozované v ČR. V ČR je typickou povětrnostní situací pro vznik silné námrazy existence jihovýchodního proudění vlhkého vzduchu, kdy se námraza tvoří hlavně na Českomoravské vrchovině. Námraza se však může tvořit i při výrazném západním proudění, a to především v horských oblastech nad 1000 m nadmořské výšky.**
		Krupobití	Rizikový význam události byl odhadnut jako malý a proto nebyla detailně analyzována ani data pro odvození její frekvence. Z metodického hlediska však analýza spolehlivostních a bezpečnostních dopadů této události nevyžaduje nové postupy a nepředstavuje problém. **Závěr o malém významu není obecně přenositelný na jiné technologie, ale lze očekávat, že většina moderních technologií bude dobře odolná vůči této externí události.**
	Vítr	Extrémní vichřice	Detailně analyzována frekvence vzniku extrémního přírodního jevu v celém spektru projektových i nadprojektových událostí. Frekvence intervalů postulovaných intenzit události odvozeny extrapolací z dostupných historických dat. Vzhledem k významnému rizikovému potenciálu probíhala v letech 2010-2011 rozsáhlá diskuse k metodice odvození frekvence této iniciační události a velikost frekvence byla odvozena alternativními metodami a opakovaně přehodnocena s využitím co nejreprezentativnějšího dostupného datového souboru . **Frekvence výskytu vichřice s projektovou dobou návratu je pro ČR poměrně vysoká. Vzhledem ke specifickým prvkům jaderně-energetické technologie nejsou obecné závěry k této externí události přímo přenositelné, ale lze očekávat, že událost bude významná pro řadu lokalit a technologií v ČR.**

		Hurikány, tornáda, cyklóny	V roce 2008 detailně analyzována frekvence vzniku události „tornádo“, detailně bylo analyzováno i riziko od výskytu tornáda v lokalitě JE Dukovany (porucha venkovních linek velmi vysokého napětí). Potenciál pro vznik tropické cyklóny vzhledem k zeměpisné poloze ČR zanedbán. **Závěr o malém rizikovém významu této externí události je do značné míry přenositelný i na další provozované technologie.**
	Požáry v přírodě	Lesní požáry, požáry trávy nebo zemědělských plodin	Rizikový efekt těchto událostí byl zanedbán vzhledem k poloze JE Dukovany ve vztahu ke zdrojům potenciálního nebezpečí (lesy, osetá pole atd.). **Tento závěr není přenosný na jiné exempláře technologií provozovaných v České republice.**
	Úder blesku	Požár a eventuální destrukce zařízení.	V roce 2008 přibližně odhadnuta frekvence vzniku tohoto atmosférického jevu jako obecně vysoká. Pro jadernou elektrárnu je ale frekvence vzniku rizikově zajímavých havarijních scénářů vyvolaných bleskem výrazně redukována při uvažování (obecně vysoké) spolehlivosti bleskojistek a bleskosvodů. **Tento závěr je obecně přenositelný na mnohé technologie vzhledem k tradičně poměrně vysokým požadavkům na vybavení technologií bleskojistkami a bleskosvody. Výjimkou jsou technologie s objemnými zásobníky hořlavých a nebezpečných látek, které se v poslední době stávají subjektem rizikových a spolehlivostních analýz (viz například [5]).**
	„Severe space weather“	Elektromagnetická interference	Nový typ externí události, doposud málo analyzovaný, bez vyvinuté ucelené metodologie analýzy, s potenciálně významným vlivem na spolehlivost a riziko provozu technologie. **Při současném trendu automatizace řízení provozu technologie, využívajícím digitální systémy kontroly a řízení, jde o významný subjekt analýzy pro mnohé složité technologie.**
	Pád meteoritu	Rozsáhlá destrukce technologie.	V roce 2008 analyzována frekvence vzniku této iniciační události. Zanedbatelná frekvence dopadu 500kg meteoritu na zařízení s vlivem na bezpečnost provozu JE. **Velmi nízká frekvence této externí události dává dobré předpoklady pro přenositelnost závěru o jejím nízkém rizikovém vlivu na jiné technologie. Přes zanedbatelně nízkou hodnotu frekvence je událost již tradičním prvkem seznamu externích událostí.**
Kombinace několika externích událostí			V roce 2008 byly pro české JE systematicky analyzovány všechny možné kombinace přírodních externích událostí a byly pro ně odhadnuty četnosti výskytu. Tématika kombinace několika externích událostí je v současné době považována v rizikových a spolehlivostních analýzách JE za velmi významnou a je jí věnována stále větší pozornost.

3. Odhad potenciálu pro vznik externí události v dané lokalitě provozované technologie a pro vznik závažných následků události

Pro odhad frekvencí externích událostí by bylo ideální využít empirická data ve formě nějaké standardní statistiky výskytu za dostatečně dlouhé období. Takový postup je však komplikován obecným nedostatkem dat majícím dvě příčiny:

- úzká vazba sledovaných událostí na konkrétní lokalitu neumožňující využít příbuzná data nasbíraná z provozu dalších exemplářů dané technologie
- ultra-vysoké intenzity rizikově a spolehlivostně významných externích událostí, při kterých se tyto události běžně nevyskytují.

Zejména pro druhou příčinu je hodnota roční frekvence výskytu nežádoucí externí události velmi často zatížena poměrně velkou nejistotou a často je odvozována nikoli z reálně naměřených dat, ale extrapolací zcela mimo jejich oblast. U přírodních meteorologických jevů se preferují data z dostupných databází měření na meteostanicích a pokud postulovaná intenzita doposud naměřena nebyla, použije se vybrané vhodné pravděpodobnostní rozdělení k extrapolaci a odhadu frekvence výskytu málo četných jevů. Speciálně pro meteorologické jevy je k odhadu frekvence vzniku extrapolací doporučeno Gumbelovo rozdělení a jako případná alternativa je využíváno tříparametrické lognormální nebo Weibullovo rozdělení.

Gumbelovo pravděpodobnostní rozdělení lze definovat například následujícím způsobem (pomocí kumulativní distribuční funkce):

$$P_G(X_G) = \exp\{-\exp[-(X_G - \alpha_G)/\beta_G]\}$$

kde:

X_G je náhodná proměnná, jejíž hodnoty jsou takto rozděleny (rychlost větru, teplota apod.)

$P_G(X_G)$ je pravděpodobnost nepřevýšení proměnné X_G náhodnou hodnotou daného statistického výběru

α_G, β_G jsou parametry Gumbelova rozdělení, napočtené z dostupných meteorologických měření (pro hodnoty představující významné riziko pro provoz technologie nejčastěji extrapolací).

Pokud známe mezní hodnotu proměnné X_G, která vymezuje hranici od níž se začnou projevovat účinky externí události popsatelné jako konkrétní iniciační událost, a dále známe hodnoty parametrů Gumbelova rozdělení, můžeme vypočítat pravděpodobnost výskytu proměnné X_G o hodnotě vyvolávající tuto iniciační událost (jakákoliv hodnota vyšší než hraniční hodnota) dle následujícího vztahu.

$$P_{G(IU)}(X_G) = 1 - P_G(X_{G(\text{hraniční})}).$$

Data pro výpočet parametrů Gumbelova rozdělení pro danou technologii lze získat obvykle měřením přímo namístě nebo zkombinováním statistických dat z měření na několika blízkých meteostanicích. Vzhledem k velmi krátkému intervalu mezi dvěma po sobě následujícími měřeními na meteostanici typickému pro současná měření, produkují meteostanice velké množství (často jen velmi málo variabilních) dat. Do procesu odhadu parametrů statistického (nejčastěji Gumbelova) rozdělení (jehož finálním cílem je odhad *roční* frekvence vzniku externí události) však vstupují typicky až při prvotní statistické analýze nalezené hodnoty

ročních maxim dané meteorologické veličiny. Finálnímu transferu ročních maxim předchází i kontrola a dodatečná analýza splnění očekávaných podmínek měření.

Za dostatečně obsáhlý statistický soubor hodnot ročních maxim analyzované veličiny je v praxi považován soubor minimálně padesáti měření (tj. soubor měření reprezentující 50 let sledování dané lokality) a za minimální vyhovující soubor zahrnující alespoň třicet měření. Tyto podmínky může být problematické splnit, pokud je snahou založit odhad frekvence přírodní události na datech přímo z lokality. Provoz moderních technologií, které jsou pokládány za rizikové, často v rámci inženýrské podpory doprovází měření meteorologických charakteristik, které ale bývá obvykle zavedeno současně se zahájením provozu technologie nebo krátce před ním a k dosažení minimálního statistického vzorku je pak třeba dlouhá řada let provozu. Tento problém byl typický i pro analýzy meteorologických veličin například pro provoz JE Dukovany, kde bylo třicet kvalitních hodnot ročních maxim přímo z lokality elektrárny k dispozici až před několika lety a pro JE Temelín na podobný datový vzorek budeme ještě poměrně dlouhou dobu čekat.

V dalším kroku analýzy, zaměřeném už na modelování *odezvy* technologie na externí událost, jsou podrobně studovány pouze ty externí události, které jsou schopny vyvolat na technologii postulovanou iniciační událost. U externích událostí nás z pohledu JE zajímají pouze takové, kdy:

- nebyla možnost „včasné výstrahy“ před externí událostí a uvedení technologie do bezpečného neprovozního stavu preventivní obrany vůči následkům události
- externí událost není již zahrnuta ve frekvencích vzniku interních IU a odezva na její vznik tak analyzována jako událost interní.

U mnohých výskytů extrémních přírodních jevů je možné cíleně pravidelně organizovat jejich předpovědi nebo včas zpozorovat jejich vznik a rozvoj. V těchto případech je často možné předpokládat preventivní odstavení technologie vedoucí na snížení rizika případné havarijní události. Pokud není možné dosáhnout bezpečného stavu technologie v čase od výstrahy do ničivých projevů externí události, je nutné uvažovat vznik případných iniciačních událostí odpovídajících aktuálnímu provoznímu stavu technologie.

Některé často se opakující meteorologické jevy mohou být kořenovou příčinou poruch vedoucích například na událost typu ztráta vnějších elektrických zdrojů. V takovém případě jsou již projevy externí události součástí spolehlivostního nebo bezpečnostního modelu technologie a není tudíž nutné vytvářet pro zohlednění externí události samostatné iniciační události.

Analýza odezvy na vznik externí události je charakteristická hledáním slabých míst v JE vůči jejím negativním projevům. K tomu je potřebné mít dobrou představu o typech poškození, které mohou být způsobeny analyzovanou externí událostí. Pochopení mechanizmů poškození umožní správně definovat hraniční hodnoty fyzikálních parametrů vedoucích na poškození budov, systémů nebo komponent. Hraniční hodnoty fyzikálních parametrů vedoucích k poškození staveb, technologií a komponent jsou dány projektovými a maximálními výpočtovými parametry a jsou přímo vázány na konkrétní způsob jejich namáhání dynamickými efekty externí události.

4. Vliv externích událostí na spolehlivost komponent a systémů kontroly a řízení a celé technologie

Systémy kontroly a řízení jsou z pohledu pravděpodobnostního hodnocení bezpečnosti soubory komponent rovnocennými s prvosledovými systémy technologie a pro modelování jejich činnosti jako součásti odezvy na vznik externí (iniciační) události je užívána stejná metodologie. Specifickým rysem komponent systémů kontroly a řízení je relativně vysoká zranitelnost zatížením generovaným externími událostmi. Na druhé straně bývají tyto systémy vůči externím vlivům obvykle záměrně poměrně dobře chráněny.

Následující tabulka obsahuje stručný celkový přehled vlivu jednotlivých typů externích událostí na komponenty systémů kontroly a řízení, tak jak vyplynul ze současných analýz externích událostí, orientovaných převážně na jaderně-energetickou technologii.

Tabulka 2: Vliv externích přírodních událostí zpracovaných v rizikových analýzách pro české JE na komponenty a systémy kontroly a řízení

Externí událost	Vliv na provoz komponent a systémů kontroly a řízení
Zemětřesení	Možnost (neoprávněného) havarijního odstavení reaktoru v důsledku vygenerování falešného signálu při události nižší intenzity. Možnost ztráty některých systémů kontroly a řízení ve scénářích se ztrátou zdrojů elektrického napájení (rizikový význam vyšší vzhledem k následkům kombinovaných scénářů, ale potenciál pro vznik události malý vzhledem k zálohovanosti systémů elektrického napájení při výpadku vnější sítě).
Abrazivní bouře	Obvykle bez vlivu na systémy kontroly a řízení (měly by být "uvnitř technologie" chráněny vhodnou bariérou). U jaderné elektrárny je základním poruchovým módem zanesení sít na trasách dodávky chladiva.
Extrémně vysoká teplota	Pro míru vlivu na komponenty systémů kontroly a řízení je klíčová schopnost odvodu tepla z místností jejich lokalizace příslušnými ventilačními systémy. Ztráta ventilace může mít pro systémy kontroly a řízení fatální následky. Při variantě události s dobou návratu 10 000 let (reprezentující velmi vysokou teplotu výrazně nad 40°C) je výpadek ventilačních systémů pravděpodobný.
Extrémně nízká teplota	Vzhledem k umístění komponent systémů kontroly a řízení je vliv události na tyto komponenty zanedbatelný vzhledem k běžné velké rezervě v kapacitách pro vytápění technologie a značné tepelné setrvačnosti prostor ve stavebních objektech.
Extrémní vodní srážky	Scénáře této externí události vedou potenciálně na vnitřní záplavy technologie, u kterých je pro ocenění vlivu na komponenty systémů kontroly a řízení důležitá výšková poloha jejich komponent. Pro technologii jaderných reaktorů typu VVER je typické umístění systémů kontroly a řízení na relativně nízkých kótách s potenciálem pro významné následky eventuální záplavy.

Extrémní sněhové srážky	Spolehlivostní a rizikový efekt těchto scénářů spočívá v možné destrukci střechy objektů technologie a poškození málo chráněného zařízení. Vzhledem k umístění systémů kontroly a řízení (viz předchozí bod) na nízkých podlažích, které jim z pohledu dané iniciační události obecně zajišťuje ochranu, je vliv externí události na tyto systémy obvykle marginální. Jistý vliv může být spojen s pozdější fází havarijního scénáře, kdy může dojít k lokálním záplavám po přeměně vodního skupenství.
Námraza	Systémy kontroly a řízení jsou svým umístěním chráněny vůči projevům této externí události. Jediným možným ovlivněním jejich činnosti je konsekvenční ovlivnění po výpadku systémů elektrického napájení. Potenciál pro jejich ztrátu v důsledku dané iniciační události je obecně nízký.
Extrémní vichřice	Systémy kontroly a řízení jsou svým umístěním obvykle chráněny vůči projevům této externí události. Vzhledem k rozsáhlé postulované ztrátě systémů vnějšího elektrického napájení, včetně možného vlivu na jeho zálohy (ztráta systémů technické vody důležité a následně chlazení dieselgenerátorů) je potenciál pro ztrátu systémů kontroly a řízení JE s reaktorem VVER větší než u jiných externích událostí, kde jsou tyto systémy chráněny.
Úder blesku	Přes relativně vysokou frekvenci této externí události je potenciál pro poškození systému kontroly a řízení malý, protože tyto systémy se nacházejí (spolu s většinou bezpečnostně významných systémů) v železobetonových objektech, které jsou dle ČSN pokládány za velmi odolné vůči účinkům blesku. Rovněž konsekvenční ztráta řídicích systémů v důsledku ztráty elektrického napájení je nepravděpodobná, protože účinek blesku na soustavu elektrického napájení je (na rozdíl od jiných externích událostí – zemětřesení, extrémní vichřice atd.) poměrně krátkodobý a vnitřní zálohy zajištění elektrického napájení (dieselgenerátory) by neměl postihnout vůbec.
Elektromagnetická interference	Vliv této externí události na komponenty systémů kontroly a řízení je vzhledem k novosti tématu a vývoji těchto systémů směrem k digitalizaci a automatizaci nejasný, ale je obecně v současnosti považován za potenciálně významný.

5. Závěr

Pravděpodobnostní hodnocení bezpečnosti provozu jaderných elektráren se v uplynulých dvou dekádách stalo plnohodnotným doplňkem tradičního deterministického přístupu k bezpečnosti. Pravděpodobnostní hodnocení je filosoficky objektivizujícím zobecněním a zpřesněním deterministických závěrů. Ještě výraznějšímu uplatnění jeho role zčásti brání problém se získáním dostatečně kvalitních podkladů ve formě provozních dat a fyzikálních a termohydraulických analýz prováděných v rámci inženýrské podpory. S intenzivním rozvojem počítačového hardware a software, rostoucím objemem provozní zkušenosti a zvyšováním přesnosti modelování fyzikálních a organizačních procesů spjatých s provozem elektrárny role pravděpodobnostního hodnocení bezpečnosti dále nabývá na významu a je vyjádřena i narůstající legislativní podporou ve státech provozujících jaderně-energetické zdroje.

Pravděpodobnostní hodnocení bezpečnosti jaderně-energetické technologie je vzhledem ke složitosti a rozsáhlosti jejího designu a procesů probíhajících během jejího provozu velmi dobrou prověrkou obecné využitelnosti pravděpodobnostních přístupů k hodnocení spolehlivosti a rizik i pro další moderní průmyslové technologie. V poslední době se rychle rozvíjejí metody hodnocení spolehlivosti a stability provozu přepravních (síťových) technologií, ať již jde o technologie přepravující (nebezpečné) materiály nebo technologie přepravující přímo energii. Závěr o přenositelnosti metodologie pravděpodobnostního hodnocení vyvinuté pro podporu rizikově a spolehlivostně orientovaného rozhodování je zvláště platný pro oblast externích událostí, kde je značný objem vlastní analýzy i jejích výsledků spojen s vlastnostmi *lokality*, které jsou na dané technologii málo závislé.

Jak již bylo uvedeno v úvodní části příspěvku, aktuální hodnoty odvozených rizikových nebo spolehlivostních ukazatelů jsou pro interní (iniciační) události jaderně-energetické technologie výrazně nižší než před několika dekádami v důsledku mnohých přijatých a realizovaných doporučení ke zvýšení bezpečnosti provozu, což poměrně výrazně navyšuje význam podrobné, exaktní a systematické analýzy externích událostí pro spolehlivost a bezpečnost provozu. I tento závěr lze s velkou jistotou přenést do provozu řady dalších průmyslových technologií. V případě, že se provozovatel takové moderní technologie rozhodne uplatnit při strategickém řízení jejího provozu pravděpodobnostní přístupy, ať už orientované na spolehlivost, na bezpečnost nebo na oba fenomény, je vhodné od samotného počátku zařadit do plánovaného rozsahu analýzy i externí události.

Literatura

[1] INSAG-12, Basic Safety Principles for Nuclear Power Plants, a report by the International Nuclear Safety Advisory Group, IAEA, Vienna, 1999

[2] Safety series No. 50-P-7, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, IAEA, 1995

[3] IAEA-TECDOC-1487, Advanced nuclear plant design options to cope with external events, IAEA, 2006

[4] American National Standard, External – Events PRA Metodology, ANSI/ANS-58.21-2003, March, 2003

[5] Necci A., Antonioni G., Cozzani V., Borghetti A, Nucci C.A., Risk assessment of accidents induced by lightning strike on storage tanks, Proceedings of PSAM11-ESREL2012 Conference, 25.6.-29.6.2012, Helsinki

Spolehlivost moderních digitálních systémů kontroly a řízení

Jiří Sedlák, ÚJV Řež a.s.

Úvod

Digitální systémy kontroly a řízení (dSKŘ) pronikají stále častěji do dříve zapovězených oblastí, které vyžadovaly vysokou transparentnost řešení. Po vojenské technice, kde zvyšování schopností a účinnosti převážilo nad riziky, dochází k průlomu i v jaderné energetice, známé aplikováním konceptu „bezpečnost na prvním místě“ (Safety First). Je to především ze dvou důvodů:

1. Digitální technologie umožňují výrazně zvýšit úroveň řízení bloku, a zlepšením celkového přehledu o stavu jaderně energetického bloku kompenzují rizika spojená s implementací digitálních technologií.
2. Údržba zastaralých řídicích systémů na bázi reléové techniky je čím dál složitější a někdy i nemožná, protože na trhu začínají chybět analogové prvky shodných parametrů.

V případě elektráren typu VVER byla nízká spolehlivost instrumentace kompenzována vysokým stupněm redundance. To v případě modernizovaných řídicích systémů, tj. včetně čidel a převodníků, již není třeba, a navíc to není ani velmi účelné, neboť pozitivní účinek redundance je zčásti eliminován vysokým potenciálem poruch se společnou příčinou (CCF), který nelze u programovatelných komponent zanedbat. Navíc je zde nebezpečí, že pokud se jedná o softwarovou chybu, která jen čeká na spouštěcí podmínky (*triggering conditions*), dojde k ní ve všech kanálech ochran současně nebo s nevýznamným časovým zpožděním.

Specifické problémy digitálního SKŘ

Je zjevné, že v případě digitálních systémů kontroly a řízení je nezbytné se vypořádat s problémem chyb software. V první řadě je třeba brát se značnou rezervou tvrzení výrobců a dodavatelů řídicích systémů o bezchybnosti jejich software, většinou s odvoláním na „k chybám odolný“ (fault tolerant) software a na provedení procesu verifikace a validace. Oba tyto postupy jsou vysoce účinnými nástroji při zvyšování spolehlivosti systémů a při obraně proti CCF, nicméně neprokazují eliminaci chyb software. Software se tak vlastně stává další komponentou v rámci měřícího a ovládacího řetězce.

Digitální řídicí systémy se vzhledem ke svému dynamickému charakteru vysloveně nabízejí k využití moderních metod hodnocení spolehlivosti, jako jsou Petriho sítě, Markovské a Bayessovské řetězce. Přesto jsou současné analýzy stále ještě často založeny na metodách „klasických“ – nejde přitom jen o komplikovanost aplikace nových postupů pro rozsáhlejší logické struktury, ale i o překvapivou schopnost klasických postupů, jako jsou stromy poruch, identifikovat minimální souběh poruchových událostí, které vedou k nenaplnění mise (selhání funkce), v systémech ochran. To je dáno především jednoúčelovostí a relativní transparentností zde užívaných algoritmů v porovnání například s informačním systémem.

Moderní řídicí systémy přinášejí ovšem celou řadu dosud neobvyklých fenoménů, které při spolehlivostním modelování běžné technologie nepřipadaly v úvahu. Jedná se především o schopnost systému reagovat na vzniklou poruchovou událost a modifikovat svoje chování. Dochází tak ke změnám jejich konfigurace, a to především vlivem degradace výběrové logiky podle toho, zda je pro

danou funkci preferováno bezpečné odstavení nebo bezpečná porucha. Tyto změny konfigurace je možné provádět zpravidla automaticky i ručně, popřípadě automaticky s ručním potvrzením. Všechny tyto vlastnosti je samozřejmě možné transformovat do binárního modelu, jako je strom poruch, dochází však ke značnému nárůstu objemu a komplikovanosti modelu a je na analytikovi, aby zvolil dostatečnou aproximaci podle účelu, ke kterému má spolehlivostní model sloužit.

Nakonec to ale mnohdy není nedokonalost logického modelu věrně zahrnout všechny významné poruchové kombinace zkoumaného systému, ale naše neschopnost pochopit poruchové chování jeho jednotlivých komponent, která nám brání v adekvátním zhodnocení spolehlivosti digitálního systému řízení.

Identifikace poruchových módů

V případě relativně jednoduchých elektronických komponent, jako jsou diody, tranzistory apod. dokážeme snadno identifikovat poruchové módy jako je přerušení, zkrat atd. Složitější je to ale s určením odpovídajících pravděpodobnostních parametrů. Samozřejmě je možné se obrátit na prediktivní zdroje dat, resp. na generické databáze zkušeností z provozu, nicméně pravděpodobnost některých poruch výrazně závisí na způsobu zapojení a především dimenzování jednotlivých součástek (např. do kruhu s max. napětím 5 V je zapojena dioda zatížitelná do 48 V). Některé prediktivní zdroje úroveň naddimenzování sice respektují, nicméně jsou většinou postaveny na sběru dat pro značně zastaralou součástkovou základnu. Proto je mnohdy lepší požádat projektanta systému o inženýrský odhad poměru pravděpodobnosti mezi jednotlivými poruchovými módy.

Nejdůležitějším aspektem odhadu pravděpodobnosti poruchy pro jednotlivé poruchové módy je její závislost v čase od jejich poslední kontroly.

Spolehlivostní modely základních událostí

Nejobvyklejší model poruchového módu (tzv. základní události stromu poruch) pro technologické systémy je periodicky testovaný poruchový mód daný součinem intenzity poruch $\underline{\lambda}$ (=1/MTBF) a střední doby mezi kontrolami. Na prvek, resp. jeho poruchový mód, se v tomto případě pohlíží jako na „jako nový“ po kontrole, popřípadě opravě. Vliv stárnutí se zanedbává. Samozřejmě i zde zůstává určitá složka pravděpodobnosti poruchy, která je dána např. nedodržení postupu repase, nesprávnou kalibrací apod. Ta se obvykle buď také zanedbává, popřípadě se ve stromech poruch spolehlivostních modelů objevuje jako lidská chyba typu *chyba údržby*.

Dalšími používanými poruchovými módy jsou selhání na požadavek (konstantní pravděpodobnost poruchy, monitorovaná komponenta (oprava ihned po poruše) a selhání v průběhu plnění mise.

V případě digitálních systémů kontroly a řízení se ale provádí celá řada kontrol jednotlivých prvků a subsystémů, a to jak vlastními prostředky hodnoceného systému/komponenty (autodiagnostika), tak speciálními externími prostředky (supervizor, systémy pro údržbu apod.). Tyto kontroly mají rozdílnou periodicitu a rozdílný rozsah, přičemž se často překrývají. Je proto velmi žádoucí dokázat rozdělit poruchové módy komponent podle schopnosti jednotlivých testů je zachytit, ale ještě důležitější je identifikovat, zda existují poruchové módy, které není možné zachytit žádným periodickým testem za provozu jaderně-energetického bloku na výkonu. Navíc mohou existovat poruchové módy, které lze zjistit jen při některých odstávkách (například kalibrace měřících řetězců), a samozřejmě mohou existovat i poruchové módy, které není schopen odhalit žádný test a projeví se

až poruchovým stavem. Vzhledem k jejich předpokládané velmi nízké četnosti se nejedná o tak závažný problém, pokud nedojde k poruše se společnou příčinou v odezvě na havárii. Tento případ se samozřejmě netýká jen digitálních technologií, ale i mnoha dalších komponent. Například některé pojistné ventily je nutné po testu repasovat, a pokud dojde k chybě při repasi, není možné ji odhalit jinak, než následujícím testem. V případě digitálních komponent a systémů je ale situace přece jen poněkud komplikovanější, protože odhadnout rozsah a stupeň úspěšnosti jednotlivých testů klade na analytika značné nároky. Je zde proto nezbytné důkladné interview s projektantem systému, ale i při něm je třeba vyhodnocovat odpovědi obezřetně a nepodlehnout tvrzením typu: „*O jakékoliv poruše víme okamžitě, vždyť je to monitorované*“.

Výsledkem zkoumání poruchového chování komponent je pak soubor poruchových módů s různou periodicitou testů a s různou závislostí pravděpodobnosti poruch na čase. Obvykle je mimořádně těžké odhadnout rozdělení poruchových módů a je na úsudku a zkušenostech analytika, aby poruchové módy s nízkým příspěvkem k pravděpodobnosti poruchy zanedbal, protože jinak by byl vzniklý model příliš komplikovaný a těžkopádný.

Degradace spolehlivosti komponent v čase je bohužel velice často zanedbávaný fenomén, přestože má na výsledek velice často zásadní vliv. Zde nemáme na mysli proces stárnutí, jakkoliv i ten je velmi důležitý, ale to, zda platí úměra mezi délkou provozu komponenty a pravděpodobností její poruchy. Odpověď se samozřejmě může lišit pro různé poruchové módy. Výsledkem je téměř vždy situace, kdy pravděpodobnost poruchy komponenty má dvě složky – jednu na čase závislou vyjádřenou intenzitou poruch λ (FR = failure rate) a druhou na čase nezávislou, často nazývanou šokovou, vyjádřenou pravděpodobností selhání na požadavek (pfd = probability to fail on demand). Velmi časté řešení je takové, že méně významnou složku zanedbáváme, což má mnohdy své zcela racionální dodatečné opodstatnění. Velice často se ale analytici rozhodují nikoliv racionálně, ale na základě nedostatečně popisných dostupných dat. Výrobcům, dodavatelům a projektantům se po letech úsilí podařilo vštěpit nutnost udávat k jejich produktům i spolehlivostní data, ale tato povinnost se bohužel „smrskla“ na uvádění střední doby do poruchy (navíc hodnot mnohdy pochybného původu), resp. intenzity poruch. Pokud už se výrobci zabývají počtem cyklů, činí tak ve vztahu k životnosti a ne k bezporuchovosti. Mezi počtem cyklů do vyčerpání životnosti a středním počtem cyklů do poruchy ale nelze odvodit žádný univerzální vztah. Navíc životnostní údaje jsou prokazovány na omezeném počtu vzorků, takže jen málo odrážejí případnou zmetkovitost.

Digitální systémy kontroly a řízení obsahují kromě obvyklých komponent, které jsou trvale v provozu (např. procesor neustále provádí svůj cyklus bez ohledu na hodnoty vstupních parametrů) a v menší či větší míře jsou monitorovány, i celou řadu komponent, které změní svůj stav několikrát během kampaně jaderného reaktoru (nebo dokonce jen při odstávce). Tyto komponenty, nebo alespoň některé jejich poruchové módy, navíc objektivně není možné monitorovat. Jedná se o komponenty na vstupech měřících řetězců (např. koncové spínače, binární hladinoměry, přepínače) i na výstupech (spínací relé). Pokud například relé použijeme při kontinuálním řízení technologického procesu, a toto relé spíná několikrát za hodinu, pak jistě existuje jistá korelace mezi délkou doby provozu a pravděpodobností poruchy (v tomto případě se komponenty netestují a provozují se do poruchy nebo do vypršení životnosti). Intenzitu poruch odvozenou z takovéto aplikace komponenty ale můžeme jen stěží aplikovat na ochranné systémy jaderné elektrárny. Navíc použití takovýchto hodnot má na výsledky spolehlivostního hodnocení devastující vliv a zcela zkreslí informaci o rozložení poruchovosti ve zkoumaném systému.

Při hodnocení vlivu doby provozu od posledního testu/údržby je nutné si uvědomit i vliv prostředí. V místnostech SKŘ je v podstatě laboratorní prostředí, navíc řada prvků je zapouzdřených, někdy i v ochranné atmosféře, takže např. vliv oxidace kontaktů je téměř eliminován.

Z uvedených důvodů je podrobná identifikace poruchových módů, výběr odpovídajících pravděpodobnost-ních modelů a získání relevantních dat naprosto nezbytné.

DIGREL

Důležitost sjednocení přístupu k identifikaci poruchových módů si uvědomila i pracovní skupina WGRISK při agentuře NEA (OECD), a proto vytvořila tematickou pracovní skupinu DIGREL (DIGital RELiability). Tato skupina má za úkol vytvořit návod pro stanovení poruchových módů pro potřeby pravděpodobnostního hodnocení bezpečnosti (PSA). Taxonomie poruchových módů bude zaměřena na budoucí využití při modelování a kvantifikaci pro účely spolehlivostních a bezpečnostních analýz. Důležitým aspektem je sjednocení přístupu, který umožní sběr srovnatelných dat. Taxonomie bude zahrnovat i řídicí systémy, nicméně primárně bude zaměřena na systémy ochran jaderných elektráren. Cílem skupiny DIGREL je:

- vyvinout technicky podloženou a použitelnou taxonomii poruchových módů pro spolehlivostní hodnocení digitálních systémů kontroly a řízení (dSKŘ) v rámci PSA
- na základě nejlepších zkušeností připravit návod k aplikaci taxonomie při modelování, sběru dat a kvantifikace spolehlivosti dSKŘ.

Práce ve skupině DIGREL je vedena finským výzkumným centrem VTT a dále se jí účastní následující subjekty: Risk Pilot (Švédsko), IRSN (Francie), EDF (Francie), AREVA (Francie), GRS (Německo), KAERI (Korea), NRC (Spojené státy), Ohio State University, (Spojené státy), ÚJV Řež (Česká republika), JNES (Japonsko), VEIKI (Maďarsko), ENEL (Itálie), NRG (Holandsko), RELKO (Slovensko) a CSNC (Kanada).

Taxonomie poruchových módů je prostředek pro popis, klasifikaci a pojmenování poruchových módů souvisejících se systémem. Zatímco běžná technologická zařízení mají obvykle jasně ohraničené poruchové módy (např. čerpadla mají poruchu startu nebo poruchu běhu), počítačové systémy jsou stále v běhu, ale na základě vstupních parametrů provádějí různé algoritmy.

Taxonomie poruchových módů se v PSA využívá při systémové analýze pomocí stromů poruch. Dva základní poruchové módy na systémové úrovni jsou:

- selhání funkce
- samovolné působení.

Selhání funkce může být popsáno jako „nezafunguje“, „ztráta integrity“, „chybí výstupní signál“ apod.

Při analýze metodou stromů poruch se poruchové módy na systémové úrovni rozpadají na poruchové stavy subsystémů a komponent. Poruchové módy systémové úrovně se pak objevují jako hradla a poruchové módy komponent jako základní události stromu poruch. V zásadě je možné pro poruchové módy komponent použít stejnou taxonomii jako pro systémovou úroveň, ale u komponent je popis poruchového módu zpravidla přesnější (např. „čidlo zamrzlo“) a je blíže příčině poruchy, resp. poruchovému mechanismu. Poruchové módy komponent se využívají při analýzách způsobů poruch a jejich důsledků (FMEA).

V případě PSA nás zpravidla příliš nezajímá poruchový mechanismus (např. „došlo k přetečení registru“, „chybný CRC kód“), ale rozhodující je *projev* poruchy (např. „CPU nefunguje“). Vymezení pojmů příčina poruchy, poruchový mechanismus a důsledek poruchy se liší podle úrovně detailu zkoumání systému/komponenty, takže to co je při spolehlivostní analýze komponenty důsledek poruchy může být pro PSA poruchový mechanismus. Je tedy zjevné, že pro různé aplikace mohou existovat zcela odlišné taxonomie poruchových módů. Skupina DIGREL se zaměřuje na využití v rámci PSA, proto navrhovaná taxonomie bude relativně méně detailní než by tomu bylo v případě spolehlivostních analýz jednotlivých funkcí.

Pro dříve vyvíjenou taxonomii hardware byly odsouhlaseny následující cíle:

- podporovat aplikace v rámci PSA
- postihovat jak detekovatelné, tak nedetekovatelné poruchy
- zahrnout všechny kritické závislosti a rysy projektu
- aplikovatelnost na systémy důležité pro bezpečnost
- podporovat definici poruchových módů, nikoliv mechanismů
- vycházet z funkčního hlediska (ne komponent)
- vytvořit odpovídající základnu pro sběr specifických dat
- v nezbytné míře podporovat modelování poruch se společnou příčinou (CCF)

Některé z těchto požadavků je možné vztáhnout i na poruchové módy software. Taxonomie poruchových módů software je nicméně stále otevřenou záležitostí. Software není možné rozložit na komponenty stejně transparentním způsobem jako hardware. Navíc chyby software jsou spíše systematické chyby, nikoliv náhodné, a tak je třeba se ve zvýšené míře zabývat problematikou poruch se společnou příčinou (CCF). K tomu je třeba připočíst skutečnost, že konkrétní důsledek softwarové chyby je obvykle těžké předvídat.

Pro ilustraci použití návodu byl v rámci skupiny DIGREL připraven vzorový příklad systému kontroly a řízení bloku jaderné elektrárny. Vydání návodu jakožto publikace CSNI (OECD NEA Committee on the Safety of Nuclear Installations) je plánováno na začátek roku 2013.

Literatura:

[1] "Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants," NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris (2009)

[2] S. Authén, K. Björkman, J.-E. Holmberg. "Guidelines for reliability analysis of digital systems in PSA context — Phase 1 Status Report," NKS-230 Nordic nuclear safety research (NKS), Roskilde (2010)

[3] J.-E. Holmberg, S. Authén, A. Amri , J. Sedlak, N Thuy. Best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PRA, NPIC/HMIT Conference, San Diego (2012)

[4] J. Sedlak. Reliability Assessment of Diversity in Digital I&C Systems at Nuclear Power Plants, NPIC/HMIT Conference, Las Vegas (2010)

[5] Chu, T-L, Yue, M. A Comparison of Taxonomies of Digital System Failure Modes. 11th International Probabilistic Safety Assessment & Management Conference, PSAM 11, Helsinki, June 25–29, 2012

[6] Proceedings of the DIGREL seminar "Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA", October 25, 2011, VTT-M-07989-11, Espoo (2011)

[7] Sedlak, J. Software critical for safety in reliability models. ESREL 2009 Conference, Prague, September 7-10, 2009.

„Funkční bezpečnost – moderní způsob zajištění bezpečnosti a spolehlivosti na železnici“

Ing. Jan Famfulík, Ph.D.

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Funkční bezpečnost – moderní způsob zajištění bezpečnosti a spolehlivosti na železnici

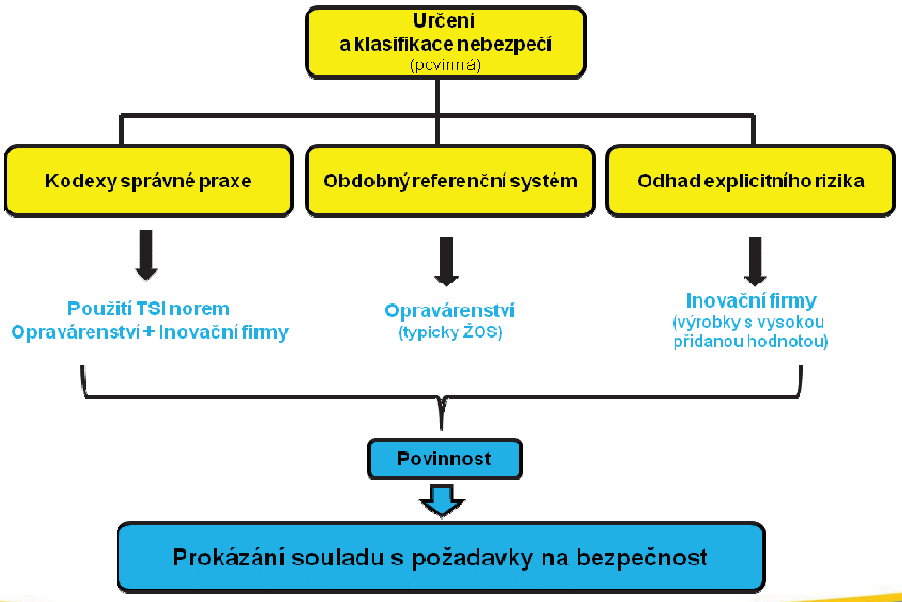
Pro železniční aplikace

- Nař. 352/2009/EU
- TSI - Interoperabilita
- ČSN EN 50126
- ČSN EN 50128
- ČSN EN 50129

vychází z ČSN EN 61508
Basic Safety Norm

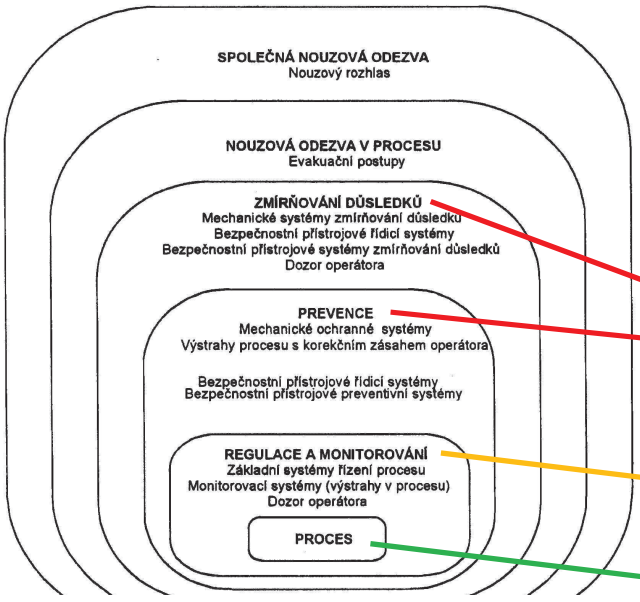
Ing. Jan Famfulík, Ph.D.

ŘÍZENÍ RIZIK - 352/2009 EU



Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Funkční bezpečnost a bezpečností funkce



Z technického hlediska je nutno zajistit, aby bezpečnostní funkce v případě nutného zásahu byla provedena spolehlivě, t.j. pravděpodobnost selhání bezpečnostní funkce musí být dostatečně nízká.

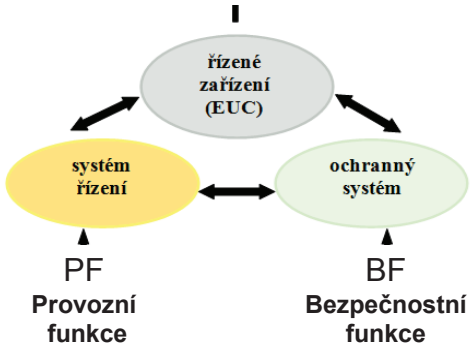
Porucha velmi vážná
BF zasahuje (vypne motor)
Aktivní odstavení zařízení

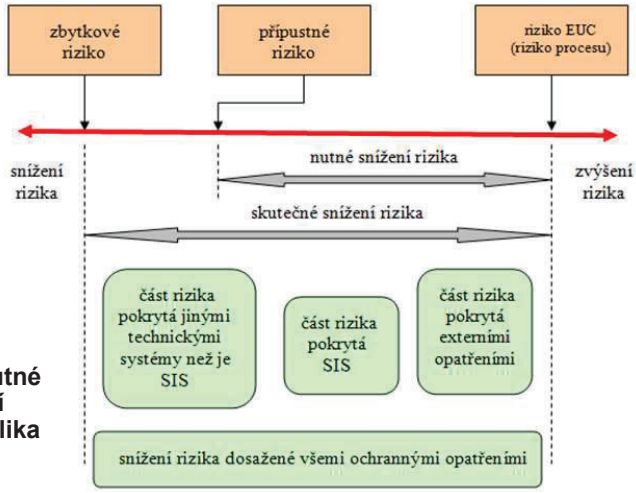
Regulátor v poruše
Je vypnut diagnostikou
BF sdělí strojvedoucímu poruchu
Ten učiní další opatření

Regulátor pracuje správně

Ing. Jan Famfulík, Ph.D.

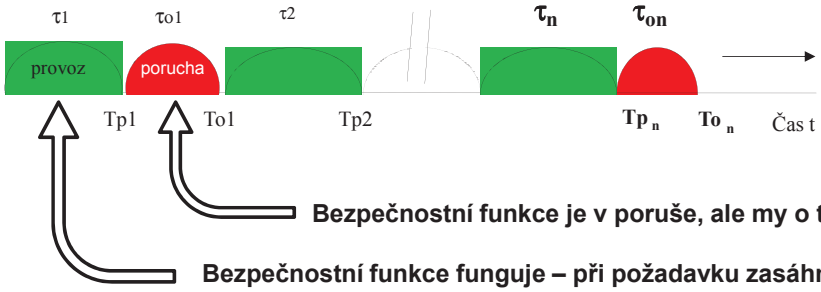
Funkční bezpečnost – snížení rizika





Pokud se riziko EUC jeví jako nepřijatelné, je nutné buď vytvořit v řídicím systému bezpečnostní funkce, nebo zařízení doplnit jedním nebo několika ochrannými (často vnějšími) zařízeními.

Problém bezpečnostních funkcí



Bezpečnostní funkce je v poruše, ale my o tom nevíme – PROBLÉM !!

Bezpečnostní funkce funguje – při požadavku zasáhne

Problém se řeší tak, že se počítá pravděpodobnost poruchy BF na hodinu provozu.

$$THR = PFHsys = \frac{PFDsys}{t}$$

THR - tolerovaná intenzita nebezpečí (h^{-1})
PFD_{SYS} - pravděpodobnost poruchy BF (-)

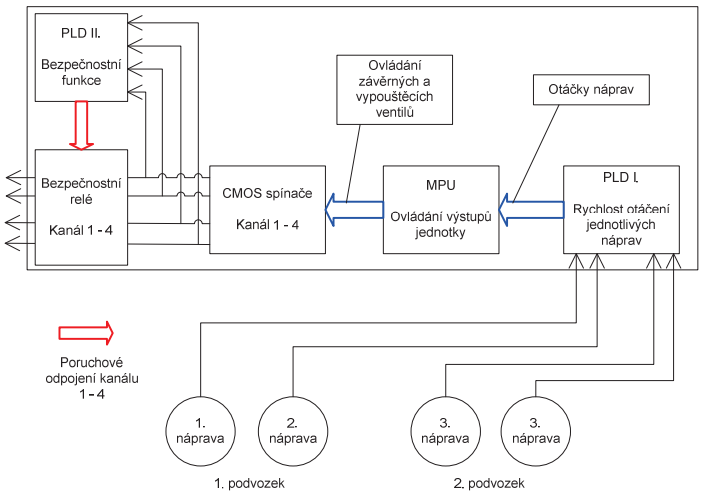
Funkční bezpečnost – součást spolehlivosti

- **Bezpečnostní funkce** – musí systém (subsystém) udržet v bezpečném stavu i v případě vzniku poruchy.
- **Vyžaduje se velmi vysoká pravděpodobnost jejího zafungování** – je hodnocena pojmem SIL.
- **SIL (úroveň integrity bezpečnosti)** – diskrétní úroveň pro stanovení požadavků na integritu bezpečnosti bezpečnostních přístrojových funkcí.
- **SIL (X)** – celkem jsou čtyři úrovně integrity bezpečnosti (nejvyšší je 4, nejnižší 1). Vyšší úroveň integrity bezpečnosti účinněji snižuje riziko.

U nově zahajovaných projektů ve smyslu Nař. 352/2009 EU je vždy nutné prokázat bezpečnost výrobku. U elektronických systémů to v praxi znamená použít postupy a principy z oblasti Funkční bezpečnosti.

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Příklad – řídící jednotka protismyku



Blokový diagram řídící jednotky protismyku

- V případě kritické poruchy bude pneumatická brzda vozidla zcela vyřazena
- Tomuto stavu musí zabránit bezpečnostní funkce
- Je nutné definovat, co mají dělat bezpečnostní funkce.
- Je nutné stanovit požadavek na úroveň integrity bezpečnosti SIL(x) pro jednotlivé bezpečnostní funkce
- Je nutné vypracovat „Důkaz bezpečnosti“ pro každou bezpečnostní funkci, HW + SW.

Ing. Jan Famfulík, Ph.D.

Záznam o nebezpečí – hodnocení řídící jednotky dle SIRF400

Nebezpečí	Popis nebezpečí - následky nebezpečí	Hodnocení nebezpečí podle SIRF400 Hazard classification acc. SIRF400						
		Škody počet (SA)	Škody zranění (SV)	Pravděpodobnost výskytu (W)	Doba vystavení (E)	Zamezení (V)	Klasifikační indikátor (I)	SIL (SAS)
Nevyžádané odbrzdění všech náprav	nelze bzdit pneumat. Brzdou. Prodloužení zábrzdné dráhy, vznik nehody.	8,00	9,00	1,70	1,30	1,70	94	3
Nevyžádané odbrzdění jedné nápravy	Snížený vrzdný účinek, malé prodloužení zábrzdné dráhy, možný vznik nehody.	3,00	4,00	1,70	1,30	1,00	27	1
Protismyk neučinkuje u všech náprav	Možnost vniku plochých míst, vznik větší hmotné škody, prodloužení brzdné dráhy, možnost nehody.	3,00	4,00	1,70	1,30	1,00	27	1
Protismyk neučinkuje u jedné nápravy	Možnost vniku plochéch míst, u jedné osy, vznik menší hmotné škody						0	0
Protismyk se nevypnul	Vybití baterie vozidla, neschopnost vozidla.						0	0
Protismyk se nezapnul	Možnost vniku plochých míst, vznik větší hmotné škody, prodloužení brzdné dráhy, možnost nehody.	3,00	4,00	1,70	1,30	1,00	27	1

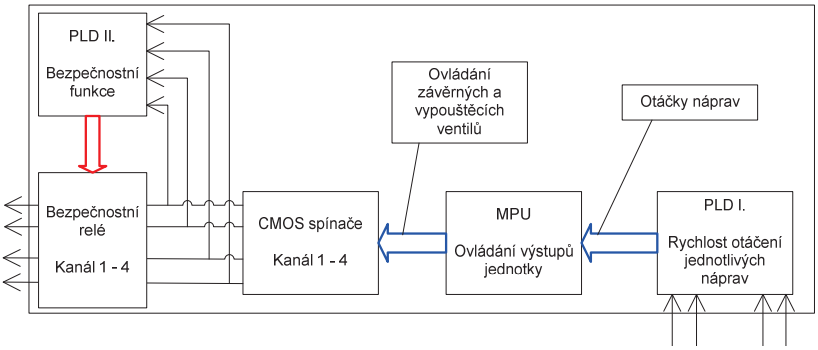
Poznámka:

SIRF 400 je standard používaný u Deutsche Bahn.

Umožňuje stanovit potřebnou úroveň SIL(X) a do značné míry odstraňuje problémy spojené s použitím Diagramu rizika dle IEC 61508-5, příloha E.

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Analýzy hardware – návrh BF



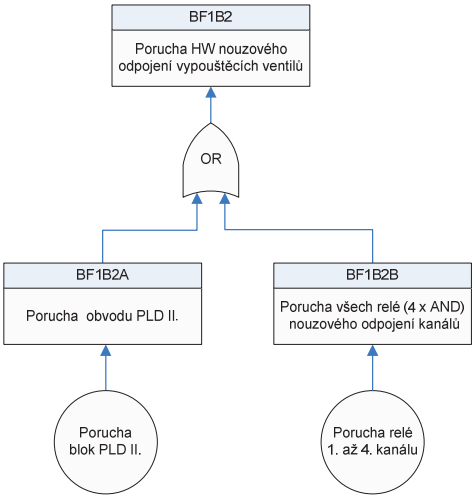
Hradlové pole PLD II a blok bezpečnostních relé realizuje BF1 až BF3. Plní funkce reaktiivní bezpečnosti.

Způsob zapojení CMOS spínačů plní funkce inherentní bezpečnosti.

Označení	Popis funkce	SIL
BF1	při překročení max. povolené doby uzavření závěrných ventilů (Tmax=5s) nouzově odpojit výstup jednotky	2
BF2	při překročení max. povolené doby otevření vypouštěcích ventilů (Tmax=2s) nouzově odpojit výstup jednotky	2
BF3	blokování nevyžádaného otevření vypouštěcích ventilů	2

Výpočet hardware – důkaz bezpečnosti

Označení součástky			Intezity poruch součástek [1/h]	
schématické	katalogové	ks	1 ks	součet
1 x PLD II. řídící logika				
U37	Obvod 1	1	8,00E-09	8,00E-09
Q108	Obvod 2	1	4,00E-09	4,00E-09
U50	Obvod 3	1	1,60E-09	1,60E-09
R245,246	odpory	2	3,00E-10	6,00E-10
Celkem intenzita 1 kanál				1,42E-08



Výpočet pravděpodobnosti poruchy při vyžádání bezpečnostní funkce bude proveden ve dvou krocích. V prvním kroku bude s využitím intenzit poruch součástek vypočítána pravděpodobnost vzniku poruchy (jev v kolečku stromu FTA), tj. pravděpodobnost vzniku elementárního jevu.

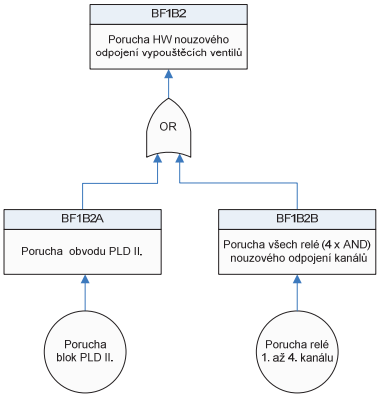
$$PFD_X = 1 - e^{-\lambda_{Du} t_{CE}}$$

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Výpočet hardware – důkaz bezpečnosti

V druhém kroku budou sestaveny rovnice řešené soustavy, které reprezentují význam použitých operátorů (OR, AND) ve stromu poruch FTA. Do těchto rovnic budou dosazeny pravděpodobnosti vzniku elementárních jevů, tak dostaneme výslednou pravděpodobnost vzniku TOP jevu.

$$PFD_{SYS} = (1 - PFD_1) \cdot (1 - PFD_2) \qquad PFH_{SYS} = \frac{PFD_{SYS}}{t_{CE}}$$



Parametr	Hodnota	
	PLD II	Relé
T1 (h)	50 000	
λ	1,42E-08	1,98E-07
DC	0,8	0,70
λdu	2,84E-09	5,93E-08
λdd	1,136E-08	1,38E-07
t_{ce}	50 000	50 000
PFD	5,68E-04	6,89E-03
PFDsys	**7,46E-03**	
PFHsys	**1,49E-07**	
SSF	**0,71**	

Požadované a dosažené hodnoty pro bezpečnostní funkce

Požadované parametry bezpečnostních funkcí řídící jednotky protismyku

Požadavek SIL:	SIL2
Poměr bezpečných poruch SFF:	60% - 90%
Požadavek PFHsys [h^{-1}]:	1 x 10^{-6} ÷ 1 x 10^{-7}
Odolnost proti vadám hardware N [-]:	0

Dosažené parametry bezpečnostních funkcí řídící jednotky protismyku

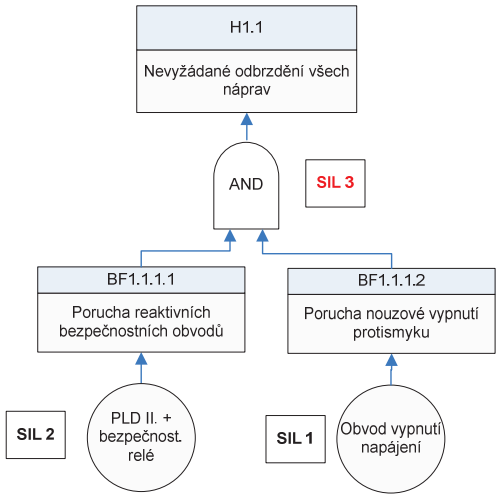
Název bezpečnostní funkce	Odolnost proti vadám HW [-]	Ekvivalentní doba prostoje [h]	PFHsys [1/h]	SSF [%]
BF1 - nouzové odpojení závěrných ventilů	0	50 000	1,49E-07	71
BF2 - nouzové odpojení vypouštěcích ventilů	0	50 000	1,49E-07	71
BF3 - blokování nevyžádaného otevření vypouštěcích ventilů	0	50 000	1,45E-08	70

Pozor!
Nebezpečí „Nevyžádané odbrzdění všech náprav“ požaduje BF na úrovni SIL(3). Avšak BF1 až BF3 splňují pouze integritu bezpečnosti na úrovni SIL(2). Jak problém vyřešit?

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta strojní, Institut dopravy

Řešení problému - použití vnějšího ochranného systému

Vnější ochranný systém umožňuje strojvedoucímu nouzově vypnout napájení řídící jednotky. Pokud je jednotka v beznapěťovém stavu, je zaveden bezpečný stav systému.
Vnější ochranný systém není součástí řídící jednotky, musí být posuzován samostatně. Pokud bude splňovat požadavky na integritu bezpečnosti SIL1, spolu s řídící jednotkou (SIL2) zajistí požadovanou úroveň integrity bezpečnosti SIL3.



Závěr:
Řídící jednotka protismyku vyhovuje požadavkům integrity bezpečnosti na úrovni SIL2 v režimu s vysokým nebo nepřetržitým vyžádáním.

Ing. Jan Famfulík, Ph.D.

Děkuji za pozornost.

Kontakt:
Ing. Jan Famfulík, Ph.D. – vedoucí ústavu Dopravní techniky
VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy
708 33 Ostrava – Poruba
Tel.: +420596994553
e-mail: jan.famfulik@vsb.cz

ISBN 978-80-02-02401-9
Speciální témata hodnocení spolehlivosti moderních technologií se zaměřením na digitální systémy kontroly a řízení,
Sborník přednášek, kolektiv autorů, 1. vydání, rok vydání 2012, vazba brožovaná, počet stran 32