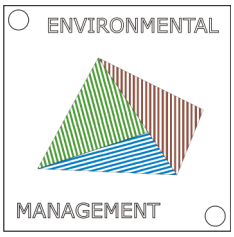
RUSKO, M. – BALOG, K. [Eds.] 2008:
Manažérstvo životného prostredia 2008 ▼▲▼ Management of Environment ´2008
Zborník z VIII. konferencie so zahraničnou účasťou konanej 5.-6.12. 2008 v Bojniciach
Proceedings of the International Conference, Bojnice, December 5 - 6, 2008.
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-34-3.



SHRNUTÍ POZNATKŮ O SPOLEHLIVOSTI, RIZIKU A BEZPEČNOSTI

DANA PROCHÁZKOVÁ

SUMMARY OF KNOWLEDGE ON RELIABILITY, RISK AND SAFETY

ABSTRAKT: *Článek obsahuje shrnutí nejnovějších poznatků z oblasti bezpečnosti, spolehlivosti a rizika prezentované na konferenci ESREL 2009 v Praze.*
Kľúčové slová: *bezpečnost, spolehlivost riziko*

ABSTRACT: *The paper contains the summary of recent knowledge of domain of safety, reliability and risk presented at the ESREL conference 2009 held in Praha.*
Key words: *safety, reliability, risk*

ÚVOD DO PROBLEMATIKY

Evropská unie se v rámci Sedmého rámcového programu zaměřila na oblast bezpečí a udržitelného rozvoje lidí, tj. cílem je bezpečné území, které je sledované v několika měřítcích, od komunity, přes region a stát až po Evropu a svět. V souvislosti s tím bezpečnost jako nástroj k zajištění bezpečí a udržitelného rozvoje nabyl vysoký kredit. V současném odborném pojetí bezpečnost zahrnuje spolehlivost a funkčnost a její úroveň závisí na řízení rizik, které se proto označuje řízení bezpečnosti, čímž se odlišuje od klasického řízení rizik, které se týká dílčích rizik a je základem technických norem, ekologických a jiných standardů a norem [1].

KONFERENCE ESREL

Ve dnech 6.-10. září 2009 se v Praze konala celosvětová odborná konference ESREL, která se zabývala spolehlivostí, rizikem a bezpečností. Za Českou republiku ji organizovala Vysoká škola báňská a Univerzita obrany. Konference se zúčastnilo přes tisíc odborníků. Byla z ní vydána stejnojmenná třídílná kniha [2] pod záštitou Evropské asociace pro bezpečnost a spolehlivost (European Safety and Reliability Association – ESRA). Kniha obsahuje 328 sdělení, které jsou rozřazeny dle teoretických a aplikačních odborných celků. Všechna sdělení byla oponována 4 recenzenty z hlediska obsahu, přínosu pro řešení sledovaných problémů a anglického jazyka. Sedmnáct českých odborníků, včetně autorky, prezentovalo výsledky a má sdělení ve vydané knize.

RUSKO, M. – BALOG, K. [Eds.] 2008:
Manažérstvo životného prostredia 2008 ▼▲▼ Management of Environment ´2008
Zborník z VIII. konferencie so zahraničnou účasťou konanej 5.-6.12. 2008 v Bojniciach
Proceedings of the International Conference, Bojnice, December 5 - 6, 2008.
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-34-3.

POZNATKY ZÍSKANÉ NA KONFERENCI ESREL

Na konferenci byly prezentovány nejnovější poznatky ze sledovaných oborů, proto si zaslouží transfer do české odborné komunity. Získané poznatky jsou dále shrnuty dle 37 tématických teoretických celků.

I. Vyšetřování nehod a havárií

1. Pro získání poučení z nehod a havárií a z hlediska aplikace správných opatření k zajištění bezpečnosti je třeba vyšetřování vést objektivně a nespoléhat na šablonu, protože podmínky vzniku nehod a havárií se mění. Je třeba prošetřovat jak proces, který vyústil v nehodu nebo havárii, tak okolnosti (tj. prostředí, ve kterém proces probíhá) a přitom posuzovat závažnost postupných jevů, které se podařilo dokumentovat.
2. Pro zajištění bezpečnosti technologických procesů je třeba používat proaktivní indikátory bezpečnosti, které se stanoví na základě analýzy scénářů kritických provozů, hodnocení vnímání rizika zúčastněnými a kvalitativní analýzou kultury bezpečnosti. Výzkum indikátorů dovoluje zvyšovat jejich spolehlivost a tím zvyšovat kulturu bezpečnosti.

II. Bayesovské metody

3. Bayesovské metody jsou vhodné pro stanovení charakteristik mezních rozložení náhodných veličin. Jsou vhodné i pro sestavování případových studií, a to hlavně těch extrémních, které vedou ke katastrofickým jevům (např. kolaps státu, kolaps nadnárodní banky apod.). V těchto případech se při modelování situací používají tři kroky:
   - identifikace důležitých proměnných (spojitých i diskrétních) a rozmezí jejich hodnot,
   - vyjádření vztahu mezi identifikovanými proměnnými, a to graficky,
   - hodnocení místních podmíněných a nepodmíněných pravděpodobností výskytu jevů.
4. Hlavním zdrojem pro odhad parametrů modelů rizika a spolehlivosti jsou expertní odhady, které jsou zatíženy jak nejistotami, tak nepřesnostmi. Používání expertních odhadů nahrazuje nedostatečná data a je relativně levné, protože kvalitní sběr a kvalitní zpracování dat vyžaduje čas a sofistikované přístupy. Kvalita expertního odhadu závisí podstatně na znalostech a zkušenostech příslušného experta. Výběr expertů však bývá značně subjektivní. Aby se snížila chyba expertního odhadu je třeba použít více expertů a jejich vyjádření vyžadovat ke strukturovanému procesu tak, že na každé úrovni struktury procesu se provede vyhodnocení a zdůvodnění tzv. „správného“ odhadu.

III. Systémy pro podporu rozhodování (DSS) a softwarové nástroje pro bezpečnost a spolehlivost

5. Riziko je obvykle spojováno s předvídatelnou náhodnou možností vzniku dopadu, který působí škody, ztráty a újmy člověku a dalším chráněným zájmům. DSS v řízení rizik je informační systém, který dovoluje rozhodovacímu subjektu získat přehled o možnostech, které se mohou vyskytnout u semi-strukturovaných a nestrukturovaných problémů. Aby DSS byl užitečný a efektivní, musí mít kvalitní databázi pro sledovaný proces, kvalitní model procesu a uživatelský příjemný způsob pro dialog mezi DSS a jeho uživatelem. Pro sestavení modelu procesu se obvykle používá Multi-Atribute Utility Theory (MAUT).
6. Integrální část analýzy rizik kritického systému je identifikace a hodnocení všech ohrožení, která významně přispívají k riziku. Analýza ohrožení generuje data pro popis scénářů rizika, definici bezpečnostních funkcí, určení skutečných úrovní rizika a pro požadovanou redukci rizika. Při analýze ohrožení je třeba odpovědět na otázky:
   - která ohrožení mohou existovat v systému,
   - proč ohrožení existuje v systému,
   - jaká je pravděpodobnost (četnost) výskytu ohrožujícího jevu,
   - jaké jsou příčiny identifikovaných ohrožení.

   HAZOP je proces identifikace ohrožení prováděný týmem.
7. Složitost systému systémů vychází z požadovaných rysů systému, a to:
   - velký rozměr,

- použito více technologií,
- složité funkční závislosti,
- velká interoperailita,
- velký výkon,
- vysoká spolehlivost a bezpečnost.

Aby byly požadované rysy zajištěny, tak inženýring (tvorba) systémů musí používat standardizované postupy. Pro bezpečnost kritických systémů se používá standard IEC 61508, který zajišťuje bezpečnost během životního cyklu.

8. Existuje řada software pro podporu rozhodování na základě mnoha kritérií založená na sofistikovaných matematických metodách, např. MCA (multi-criteria analysis) metoda, WSA (weighted sum approach), CDA (concordance, discordance analysis), TOPSIS (technique for order preference by similarity to ideal solution), IPA (ideal point analysis), AGREPREF (aggregation preferences) PROMETHEE (preference ranking organisation method for enrichment evaluations). Kamenem úrazu je kvalita a množství vstupních dat.
9. Inženyring / technika požadavků na spolehlivost vychází z požadavků techniky a z modelování systémů (hlavně založených na metodikách orientovaných na objekt, semi formálních a orientovaných na činitele), analýzy spolehlivosti, modelů selhání a z analýzy a hodnocení rizik.

IV. Dynamická spolehlivost

10. Modelují se selhání různých systémů systémů (počet ≥2) při provozu (protože při provozu se mění podmínky, tak se mění i spolehlivost, a proto se používá pojem „dynamická spolehlivost“) a hledá se objektivní přístup pro stanovení pravděpodobnosti výskytu selhání. Na základě znalostí chování dynamické spolehlivosti se vymýšlejí chování systémů taková, která budou tolerovat riziko. Používají se různé modely, např. modely založené na Petriho sítích.

V. Identifikace a diagnostika chyb

11. Pro identifikaci a diagnostiku chyb u systémů se v praxi používá několik přístupů. Nejčastěji se používají modely založené na bayesovských sítích. Často se používají indikátory sestavené na míru sledovaného systému.

VI. Lidský faktor

12. Analýza lidské spolehlivosti vychází z hodnocení lidských chyb. Pro jejich modely se nyní používají také bayesovské sítě. Identifikují se různé scénáře a stanovuje se pravděpodobnost jejich výskytu v konkrétních podmínkách. Do systému systémů tak přibývá další systém, a to sociální. Někdy se pro zvážení neurčitostí používá mlhavý bayesovský model.
13. Při nouzových situacích je důležité, aby lidé byli samostatní a aby dostali sebe i ostatní na bezpečné místo. Samostatnost se zvyšuje, když lidé znají obsah varovacích instrukcí a znají, jak se chovat. Efektivitu varovacích instrukcí ovlivňuje mnoho faktorů – osobní charakteristiky, způsob zpracování informace člověkem, chování člověka, sociální vlivy, nepřímé informace aj.
14. Ke zranitelnosti systému systémů přispívá i zranitelnost, kterou představují lidé, tj. sociální systém.

VII. Řízení integrovaného rizika a rozhodování na základě informací o riziku

15. Definice rizika jsou rozmanité. Např. riziko je míra bezpečnosti, tj. míra, která kombinuje pravděpodobnost výskytu nežádoucích jevů a důsledky těchto jevů. K nejednotnosti v definiční oblasti dochází přesto, že v oborech a oblastech, ve kterých se řízení rizik používá, jsou cíle stejné. Řízení rizika, tj. formulace činností, opatření, pokynů apod. i jejich provádění, závisí na chápání rizika. Při řízení je třeba zvažovat dobu, po kterou trvá nestabilita vyvolaná realizací rizika. Pro optimální chod rozvodných sítí je nutné sledovat proces, identifikovat příznaky nasvědčující brzké realizaci rizika a pro aktivně včasně proti riziku zasahovat. Důkazy jsou z oblasti bankovnictví, distribučních sítí pro rozvod elektřiny, vody, řízení podniků apod.
16. Při řízení podniků / organizací se doporučuje sledovat aspekty celkového rizika a přinejmenším strategické riziko, finanční riziko a provozní riziko. Dále je třeba odlišit místní dopady, dopady na systém a dopady na podnikání, které mohou být též důsledkem prvních dvou jmenovaných.

VIII. Modelování a optimalizace údržby

17. Pro zajištění bezpečnosti provozů je důležitá údržba. Ta musí být z hlediska finančního optimální. Proto je třeba vytvořit reprezentativní soubor možných scénářů údržby, určit a vyhodnotit dopady jejich rizik s ohledem na kvalitní chod provozu a z nich vybrat kvalitní, tj. průhlednou, opakovatelnou a správnou metodou ten optimální. Přitom je důležité zvažovat bezpečnost životnost a spolehlivost zařízení. Jelikož u provozů i organizací se nejedná o statické problémy, ale o problémy dynamické, je vhodné provádět řízení bezpečnosti pomocí indikátorů. Každý provoz i organizace jsou jedinečné, a proto indikátory jim musí být přišity na míru. Existuje obecný logický postup pro jejich sestavení a používání, ale použití v konkrétní praxi musí zohledňovat místní specifika.

IX. Metody Monte Carlo v systému bezpečnosti a spolehlivosti

18. Výsledky modelování pomocí různých přístupů na stejný případ, např. Monte Carlo, Petriho sítě, Markovovy řetězce atd. nejsou vždy totožné, tj. potvrzuje se známá pravda z řady oborů. To znamená, že na důležitosti nabývá interpretace výsledků a ve složitých systémech i jejich ověřování. Zmíněný fakt nabývá na důležitosti při aplikacích na řídké jevy.

X. Pracovní bezpečnost

19. Na úseku bezpečnosti práce je cílem zajistit bezpečné místo, bezpečnou osobu a bezpečné systémy. Na základě systematických a dlouhodobých studií (Makin, Winder) jsou prioritní prvky, které je třeba v dané oblasti sledovat: Na základě výzkumu platí v sestupném pořadí, že pro:
    - bezpečné místo je třeba sledovat: nouzovou připravenost; zařízení; nebezpečné látky; hluk; elektrická zařízení; základní hodnocení rizika; inspekce / monitoring; bezpečí lidí; nakládání s odpadem; stroje; úklid; systém řízení změny; preventivní údržbu / opravy; vchody / východy; ergonomická hodnocení; radiaci; biologická ohrožení; přebírání / odebírání; věci pro pohodlí / životní prostředí,
    - bezpečnou osobu je třeba sledovat: výcvik; popis práce a strukturu úkolů; schopnost poskytnutí první pomoci; osobní ochranná zařízení; konfliktní řešení a rozhodování; odhad výkonu osoby - zaměstnance; zotavení pracovníka při namáhavé práci; asistenční programy pro zaměstnance; organizace práce – únava; rovné příležitosti – opatření proti diskriminaci; pestré ubytování; zdravotní dohled; zdravotní postupy; dohled na návštěvníky a kontraktory; kritéria výběru osob; vnímavost ke stresu; revize fluktuace osob; programy odezvy / zpětné vazby; budování sociální sítě; modifikace chování,
    - bezpečný systém je třeba sledovat: řízení nehod; spolupráce s orgány pro bezpečnost práce při zvažování zdravotních aspektů; politiku a postupy orgánů pro bezpečnost práce; možnost konzultací; postupy pro bezpečnou práci; kompetentnost řízení; vytyčování úkolů; služba zákazníkům; řízení kontraktorů; alokaci zdrojů; odpovědnost; péče o záznamy – archivace; modernizaci legislativy; komunikace; soulad s kritérii orgánů pro bezpečnost práce; revize pracovních postupů / analýza mezer /nedostatků; revize systému; audity; sebehodnocení; modernizace postupů.

    Vysoké riziko pro bezpečné místo představují: nebezpečné látky; nouzová připravenost; elektrická zařízení; výrobní prostředky; přebírání / odebírání; vchody / východy; ergonomická hodnocení; základní hodnocení rizika – často se porušují.
    Vysoké riziko pro bezpečnou osobu představují: zdravotní dohled; vnímavost ke stresu; dohled na návštěvníky a kontraktory; osobní ochranná zařízení; organizace práce – únava – často se porušují.
    Vysoké riziko pro bezpečný systém představují: řízení nehod; možnost konzultací; řízení kontraktorů; alokace zdrojů; revize pracovních postupů / analýza mezer /nedostatků; odpovědnost.
20. V Evropě se data o haváriích spojených s pracovním procesem sestavují podle metodiky ESAW (European Statistics on Accidents at Work). Pro preventivní účely je třeba hodnotit rizika

pracovního procesu metodikou, která dává správné a souměřitelné výsledky. Úsilí v sestavení metodiky vyvíjí Evropská komise i EUROSTAT.

21. Bezpečnostní kontroly a audity často používají matici rizik. V matici je obvykle 5 kategorií pro četnost výskytu jevu a 4 kategorie pro závažnost důsledků. Druhou možností je použití indikátorů.

XI. Organizační poučení

22. Bezpečnost a spolehlivost organizace předurčují jak podmínky uvnitř, tak podmínky v okolí. Proto obojí musí být zvažovány při zajištění uvedených cílů. Na zajištění bezpečnosti se musí podílet všichni zúčastnění. Existuje tzv. Skandinávský model pro zapojení všech pracovníků do zajišťování bezpečnosti, který bazíruje na naplnění sloganu „co říkáš, to dělej".
23. Při zajišťování bezpečnosti je nutno přihlížet a národnostním a kulturním rozdílům. Odlišnost je obvykle v 5 oblastech: využívání energie; tolerance neurčitých situací; nerovnost pohlaví; individualismus a kolektivismus; orientace na dlouhodobé či krátkodobé cíle.
24. Při zajištění bezpečnosti důležitou roli má výcvik (trénink) a životní zkušenosti.
25. Obecně úkolem bezpečnostních inženýrů je vyšetřovat havárie a zajistit zpětnou vazbu tak, aby se snížila četnost i dopady podobných havárií.

XII Sběr a analýza dat pro bezpečnost a spolehlivost

26. Pozornosti při zajištění bezpečnosti a spolehlivosti se dnes soustřeďuje na odhalení příčin mnohočetných / hromadných škod. Metodiky používají pokrokové statistické metody pro komplexní analýzu dat s cílem odhalit příčiny mnohačetných škod a predikovat potenciální případy škod. Začíná se obvykle s technickou nebo statistickou analýzou případů. Pro vše je základem reprezentativní datový soubor (správný, homogenní, validovaný). Častou chybou v praxi je, že se neověřuje kompletnost a vypovídací schopnost datového souboru. Při získávání dat sběrem či měřením je nutno respektovat požadavky na kvalitu dat, např. podmínky měření, vzorkování dat apod.

XIII. Vytváření politiky / postupu na základě rizika a důkazů

27. K určení parametrů rizika je řada softwarových nástrojů, pro případ jevů spadajících pro Seveso se jedná např. o ALOHA, SAVE I, ROZEX, CEI, TEREX, EFFECTS. Při praktickém použití jsou hlavními nedostatky nekompletní údaje a rozdíly mezi limity (mezními hodnotami). První faktor se uplatňuje až ve 43% případů. U druhého faktoru se uplatňuje především nedostatečný popis jevů v bezpečnostních dokumentech.
28. Kritérium přijatelnosti rizika v praxi je údaj, dle kterého je riziko hodnoceno, zda je či není přijatelné. Používá se jak individuální, tak společenské riziko (křivky F-N; četnost výskytu vs. velikost dopadů / nebo jen počet obětí; oblasti nepřijatelné, podmíněně přijatelné a přijatelné riziko).

XIV. Analýza ohrožení a rizika

29. V dnešní praxi je v řízení rizik spojených s technologickými procesy snaha snížit četnost havárií optimalizací spolehlivosti bezpečnostních systémů. Velikost ohrožení lze snížit jen někde, např. snížením disponibilního množství nebezpečných látek.
30. Řada prezentovaných případů ukazuje, jak živelní pohroma (např. blesk, povodeň, zemětřesení, hurikán atd.) odstartovala velkou technologickou havárii.
31. Při určení rizik je v důsledku nekvalitních souborů dat řada nejistot a neurčitostí. Nejde o přesnost spojenou s metodou, ale o přesnost vstupních dat, která jsou často z objektivních důvodů neúplná a zatížená chybami, a to i hrubými.
32. Jelikož při vzniku kritických podmínek je nutná evakuace, existují pro různé sektory pravidla a normy pro nouzovou evakuaci. Pro evakuaci za různých podmínek a v různých sektorech platí jak obecně platná pravidla, tak specifická pravidla, která závisí jak na specifikách sektoru, tak na místě a čase, ve kterých evakuace probíhá. Jedním z faktorů, který se sleduje je doba trvání evakuace; při evakuaci z laku je např. určující počet schodů, průchodnost dveří atd.
33. Na základě mezinárodních standardů je proces hodnocení rizika složen z: plánování (definice problému, sběr dat a rozvržení prací; výběr metody pro analýzu); hodnocení rizika (identifikace

iniciačních jevů; analýza příčin a analýza důsledků; představa o riziku); vyjednávání s rizikem (srovnání alternativ, identifikace a vyhodnocení opatření na zvýšení bezpečnosti; ocenění účinnosti různých typů řízení rizik a jeho revize; rozhodnutí).

34. Při vypořádání rizik je nutno počítat také s případy, které jsou málo pravděpodobné, ale působí velké škody, ztráty a újmy. Uvedené jevy se vyskytují nepravidelně a zřídka, a proto pro jejich ocenění je potřeba používat speciální techniky.
35. Dělení dopadů pohrom zajím není sjednocené. Např. poruchy v sítích dělíme dle dopadů na dlouhodobé a krátkodobé. Dále na vnější neb vnitřní. Obé dále dělíme na ty způsobené lidskou činností, technické a přírodní. Ty spojené s lidskou činností dělíme na ekonomické, politické, geopolitické a teroristické.
36. Odolnost ve smyslu houževnatost je významnou vlastností systému při řízení bezpečnosti systému. V systémovém kontextu je definována jako schopnost systému / organizace reagovat na poruchy a zotavit se z nich ve včasné fázi tak, že dopady na dynamickou stabilitu systému jsou malé.
37. Projevy klimatické změny jsou tak velké, že někteří výzkumníci navrhují, aby se tyto zahrnuly mezi pohromy, které se používají v bezpečnostním inženýrství a systematicky se prováděla opatření proti jejich dopadům.
38. Hodnocení rizika pro potřeby bezpečnosti metodou 6 sigma zahrnuje algoritmus: definuj cíle hodnocení rizika; posuď skutečný běh procesu na základě konkrétních dat; identifikuj příčiny rizik a navrhni opatření; realizuj opatření; posuzuj účinnost opatření a prováděj korekce směřující k vyšší bezpečnosti. Algoritmus statistického hodnocení rizika je: vyhledání zdrojů ohrožení; ocenění ohrožení; odhad rizika; ocenění rizika; vyhodnocení úrovně bezpečnosti. V případě, že úroveň není dostatečná, je třeba udělat opatření a proces opakovat od odhadu rizika. Pro posouzení úrovně bezpečnosti jsou nejvhodnější indikátory.
39. Odhady pro řízení rizika musí odhadnout ztráty, škody a újmy způsobené realizací rizika v daném místě rozpočtené na časovou jednotku, aby bylo možno stanovit priority řízení.

XV. Řízení rizika v komplexním prostředí

40. Případové studie k problému budování bezpečnosti pomocí zodolnění organizace ukázaly klíčová kritéria, která je třeba v procesu respektovat. Jimi jsou: povědomí o riziku, řízení nehod a zálohování, a to i v oblasti předávání informací. Nedostatečné zálohování ve scénářích vede např. k nedostatečné informovanosti, která je potřeba jak k odezvě, tak obnově. Prosazuje se slogan „share and win (sdílej a vyhraješ)“.

XVI. Vnímání rizika a komunikace

41. K posouzení vnímání rizika se používají dotazníky a klasifikační metody. Sociální zranitelnost a odolnost vůči pohromám se obvykle chápe jako schopnost vyjednávat s pohromami, která předurčuje nový životní styl. Rizika musí být analyzována nejen z pohledu velikosti ohrožení, ale také s ohledem na sociální, ekonomické a politické procesy, které generují zranitelnost pocházející z neschopnosti společnosti vyjednávat s riziky. Vnímání rizika závisí na znalostech a na schopnosti reálně hodnotit situace v souvislostech a de facto předurčuje odezvu a hlavně kvalitu a úroveň připravenosti na odezvu.

XVII. Kultura bezpečnosti

42. Kultura bezpečnosti je součást kultury organizace, která ovlivňuje stanoviska a chování členů organizace ve vztahu ke zdraví a bezpečnosti. Organizace obvykle hledají způsob, jak posílit kulturu bezpečnosti organizace. Nástrojem je SMS a proces PSM. Oba nástroje musí být postaveny odborně správně (tj. využít teoretické základy) a musí být správně přizpůsobeny na místní podmínky.

XVIII. Systémy řízení bezpečnosti

43. Víceoborový přístup řízení rizik zavádí integrovaný systém řízení. Obvykle se dle legislativy požaduje paralelní zajišťování kvality, ochrany a bezpečnosti při práci, ochrany životního prostředí a instalace systémů řízení bezpečnosti. Protože dochází často ke konfliktům kvůli

nejednotnému konceptu jednotlivých požadovaných aktivit, je výhodnější zavést komplexní SMS a proces PSM, kterým se zajišťuje provázaná bezpečnost.

44. Petriho sítě jsou výkonné metody pro získání různých druhů diskrétních systémů jevů. Umožnění sestavení modelů statických struktur a dynamického chování. Dovolují posuzovat architekturu systému i dočasné evoluce a reakce. Proto jsou důležité pro hodnocení výkonu, bezpečnosti a spolehlivosti. Další modifikace stochastické nebo barevné Petriho sítě rozšiřují jejich použití v oblasti náhodných proměnných.
45. Při řadě rozhodování je konflikt mezi bezpečností a zvýšením zisku. Aby tento konflikt byl správně rozhodnut, je nutné posouzení přijatelnosti rizika, které vzniká při upřednostnění zisku. To lze pouze jen na základě stanovení a ocenění následků na chráněné zájmy v případě podcenění bezpečnosti a posouzení jejich přijatelnosti.

XIX. Spolehlivost software

46. Mnoho software spojených s bezpečností pracuje automaticky, aniž by informovala lidi. V některých případech, u kterých hrozí, že při selhání software nepatří, špatné formátování a anomálie obsahu. Je třeba sledovat a hodnotit procesní model nakládání s informacemi a na něm posuzovat pravděpodobnost výskytu selhání výše uvedeného typu. Problém hledání způsobu pro posuzování spolehlivosti software je starý již přes 30 let, a není doposud úspěšně vyřešen.
47. Zranitelnost software pochopitelně ovlivňuje jeho spolehlivost. Zranitelnost software je chyba ve specifikaci, rozvoji nebo konfiguraci software, jejíž realizaci vede k narušení explicitní nebo implicitní bezpečnostní politiky. Ukazuje se, že řada modelů, které hodnotí spolehlivost software neberou v úvahu zranitelnosti prvků software.

XX. Strukturální spolehlivost a normy pro projektování

48. Metody pro zajištění strukturální spolehlivosti jsou zpravidla přebírány z Eurokódů (European Standards Eurocodes) nebo z dokumentů ISO. Provádí se deterministické a pravděpodobnostní analýzy. V praxi se však také posuzuje spolehlivost historických objektů, např. mostů. Tam je třeba brát v úvahu efekty, jako je ztekucení apod., které vedou k selhání.

XXI. Analýza spolehlivosti systémů

49. Posouzení úrovně integrity bezpečnosti je součástí auditů. Požadavky na bezpečnost, funkčnost a snadné používání u moderních technických systémů rostou. Propojené systémy jsou integrovány do velkých celků. Tím se stává stále složitější i architektura elektronických systémů. ***Rostoucí komplexita vede k větší a větší roli strukturovaných metod a procesů, a to ve všech úsecích činností***, počínaje od projektování. K modelování struktur se používá analytický přístup, Markovovy řetězce a Petriho sítě. Zásadním problémem spojeným se zajištěním požadavků je provedení kvalitní analýzy rizik z pohledu funkčnosti, spolehlivosti a bezpečnosti.
50. Obecné otázky kontrolního seznamu pro analýzu rizik u software z hlediska jeho funkčnosti: jak užiji software pro různé programy? mohu ho použít v mém telefonu?; Mohu použít software v týmovém prostředí? mohu rozšiřovat projekty všem mým týmovým kolegům a dostávat od nich vyjádření?; mohu upravovat kvantifikační mechanismus tak, abych vyzkoušel nový algoritmus?; software je stále větší a větší, mohu software rozdělit na části, abych mohl použít starší počítače?
51. Požadavky na bezpečnost u moderních technických systémů jsou stanoveny zákonem. Vizualizace funkční spolehlivosti mechatronických systémů lze použít pro mapování relací na maticově orientované relace. Modelům pro komplexní systémy je třeba věnovat velkou pozornost.
52. Řešitelné jsou několikaúrovňové strukturované systémy. Funkčnost, spolehlivost a bezpečnost nestrukturovaných systémů se těžce řeší. Kritické infrastruktury, např. elektrické přenosové sítě nebo dopravní sítě jsou reprezentovány jako sítě komponent (někdy nazývanými uzly, vrcholy nebo prvky), které spolu intereagují pomocí vazeb (někdy nazývanými hranami, oblouky nebo propojeními). Struktura sítí propojení ovlivňuje robustnost a zranitelnost těchto systémů vůči selháním a útokům. Relevantním výstupem analýzy síťové struktury je identifikace nejdůležitějších skupin prvků různých rozměrů v síti. Z hlediska topologické analýzy sítě může být definována různá míra důležitosti ve spojení s důležitostí komponent, které zaujímají různé

strukturální aspekty propojených cest mezi síťovými prvky. Identifikace nejzávažnějších prvků různých rozměrů v síti je kombinatorický problém, který může být efektivně vypořádán pomocí vývojových algoritmů.

53. Plán mechatronického systému obsahující velký počet komponent z různých technologií a zahrnující noho disciplín vyžaduje spolupráci mezi různými vývojovými odborníky, aby se dosáhlo uspokojivé kvality. Největší problém představuje multidisciplinarita. Aby bylo možno vyhodnotit spolehlivost takových systémů, je důležité mít jednoduchý model a analyzovat několik konfigurací s cílem získat požadavky.Pro vyhodnocení funkčnosti, spolehlivosti a bezpečnosti složených systémů je třeba zvažovat a hodnotit interakce mezi systémy. Lze to dělat metodikou Petriho sítí. Stejné metody lze použít i na stanovení pravděpodobnosti výskytu selhání bezpečnostních systémů a opatření.
54. Bezpečnost kritických systémů může být modelovaná pomocí postupů (i ve formě software) založených na heuristických principech.

XXII. Analýza nejistot a citlivosti

55. Model je reprezentací reálného objektu a nejistoty nevyhnutelně vznikají, když jsou možné alternativní interpretace systému a jeho projevu, které všechny jsou věrohodné ve světle současného poznání systému.
56. V analýze inženýrských rizik je obvykle dělán rozdíl mezi stochastickou a poznávací / znalostní nejistotou. Rozmezí nejistot pomáhá při hodnocení různých parametrů při projektování.

XXIII. Aeronautika a kosmonautika

57. S růstem požadavků na leteckou přepravu v blízké budoucnosti je třeba očekávat přetížení leteckého prostoru. Prevence lidských chyb se stane klíčovou pro bezpečnou a spolehlivou leteckou přepravu. Pro nalezení správného způsobu řízení letové bezpečnosti je třeba udělat opatření, jak v letadlech a jeho řízení, tak v oblastí řízení leteckého provozu včetně jeho pracovníků. Pro jednotlivé úseky existují různé modely řízení letové bezpečnosti.

XIV. Biotechnologie a potravinářství

58. Pro zajištění kvalitních potravin je nutné, aby výrobní proces i celý proces nakládání s potravinami i ze surovinami pro výrobu potravin, byly spolehlivé a bezpečné. Procesy se nejčastěji modelují pomocí stromů událostí a dnes moderně pomocí variantních stromů událostí.

XXV. Kritické infrastruktury

59. Z praktických důvodů (kvůli interdependences selžou životně důležité služby pro obyvatele v území a prostoru) se dnes požadují metody pro modelování a popis SoS jako celků. Celkový model je nutný znát pro hodnocení spolehlivosti a bezpečnosti s ohledem na různá ohrožení. Pomocí metody „What-If“ je třeba vytvořit scénáře dopadů, které vzniknou nebo mohou vzniknout při výskytu pohrom. Tak se dostane materiál pro identifikaci a hodnocení interdependences. Tím se také odhalí zranitelnosti spojené se vzájemným propojením jednotlivých systémů. Integrovaný model obsahuje jak dílčí systémy, tak jejich hierarchické propojení.
60. Pro bezpečnost a spolehlivost SoS jsou důležité jak bezpečnost a spolehlivost dílčích systémů, tak především SoS. Stochastické modely založené na Markovových a Poissonových procesech je možno použít pro modelování velkých a komplikovaných systémů tak, že na jejich základě je možné predikovat chování systémů, které obsahuje nejistoty. Tyto modely však nemají schopnost kompletně vyjádřit fundamentální strukturu systému a schopnost přizpůsobit se selhání dílčích systémů, když existují silné interdependences. V současné době je nedostatek modelů, které by vyjadřovaly interakce komplexních přizpůsobivých systémů (např. pro elektrickou rozvodnou síť) a automatizační systémy. Důležitost dynamiky sítí je prokazována velkými blackouty u elektrických rozvodů a u internetu, a je důkazem vysokostupňového propojení mezi sítí a řídícími systémy – viz blackout USA a Kanada v r. 2003.
61. Recentní teoretické analýzy sítí ukázaly citlivost sítí vůči degradaci dynamiky sítí. Porušení komplexních sítí jsou často důsledkem relativně pomalé degradace systému, která eskaluje do rychlého přívalu selhání komponent vedoucích ke kompletní ztrátě služby. Nelinearita těchto

systémů je zřejmá, zatímco prvních několik výpadků může být vzájemně nezávislých, tak kauzální řetězce selhání se vyznačují jevy v kaskádovitém režimu. Jedním z hlavních systémů, který by mohl reagovat na tyto kaskádovité jevy je systém SCADA (Supervisory Control and Data Acquisition), který dovoluje systému přizpůsobit se. Další velká zranitelnost způsobená kaskádovitými jevy je u řídících (ovládacích) systémů, které mohou být potenciálním zdrojem rizik, když bezpečný provoz mohou ovlivnit špatné povely nebo nepříhodné reakce. Např. selhání potrubí chladícího systému vede k částečnému odstavení komunikačního systému. Stabilní podmínky nepožadují korekce u SCADA a důsledkem je částečné nesprávné fungování SCADA. Rozsah postižených infrastruktur nelze predikovat, což je příkladem skrytých zranitelností SoS.

62. Jedním z hlavních zájmů analýzy spolehlivosti komplexních systémů je určit stabilitu a odolnost (resilience) různých infrastruktura analyzovat působení řídících opatření na schopnost adaptace s ohledem a nepredikované změny udržující schopnost poskytovat požadované služby. Infrastruktury jsou vysoce dynamické systémy s tím, že kapacita infrastruktury se mění v čase a je rozhodující pro adaptaci vůči selháním. Dynamické vlastnosti jsou vlastní (implicitní, inherentní) topologii základních sítí a jsou řízené SCADA a / nebo systémem automatizovaných procesů. Jejich analýzy dovolují identifikovat chování a určit bezpečnostní okraje (rozmezí), které jsou potřebné k tomu, abychom se vyhnuly kaskádám a lavinám.
63. Vláda USA vydala normu „Critical Infrastructure Protection“ pro stanovení bezpečnostních rozmezí, které nedovolí výskyt kaskádovitých či lavinovitých selhání. Dnešní pravděpodobnostní modely aplikované na kritickou infrastrukturu obecně předpokládají náhodnost a nezávislost výpadků komponent, jako další včlenění mnoho závislých nízko pravděpodobných selhání je omezeno enormními výpočetními náklady. Nicméně, jednotlivé základní komponenty jsou v základu propojené a intereagují v síti každá s každou, zanedbání vzájemných vlivů selhání vede k systematickému podceňování pravděpodobnosti výskytu kaskádovitých selhání. Je proto důležité identifikovat a modelovat všechny možné závislosti, a to i takové, které nejsou zřejmé z prvotních analýz. Všudypřítomné využití ICT uvnitř dalších infrastruktur, např. u elektrické sítě, poskytuje mnoho užitků, které se stávají nepostradatelné pro provoz každodenních propojených systémů, hlavně kvůli výkonnosti, automatizaci a dostupnosti informací. Tato závislost však zvyšuje zranitelnost analyzovaných systémů vůči poruchám ICT infrastruktury.
64. Šíření řídkých a nepředvídaných, ale závislých selhání v kaskádě není hodnoceno, nebo není dostatečně hodnoceno, konvenčními hodnoceními . Hlavním důvodem je, že je těžké predikovat přesné sekvence jevů, protože je prakticky nekonečný počet možných provozních eventualit a proměn systémů, které by měly být zváženy. S ohledem na dopady je zotavení z kaskády, typu blackout, do plného provozu pravděpodobně delší než obnova specifických částí systému, které byly rozpojené.
65. Potřeba pochopit kvalitativně jednak chování systémů infrastruktur a jednak chování SCADA, ICT a řídících systémů znamená vlastně požadavek vyhodnotit rizika spojená s konkrétní infrastrukturou a tímto způsobem vyhodnotit včleněné zranitelnosti. Jeden z hlavních problémů při použití jakékoliv metody vztažené ke spolehlivosti propojených infrastruktur je dostupnost dat pro sestavení koherentního / logického modelu. Různé metody mohou poskytnout výsledky použitelné pro řešení sledovaného problému.
66. Počáteční závislosti jsou na úrovní systémů a z nich vychází interdependences. Další interdependences jsou způsobeny zranitelnostmi, které jsou fyzické, kybernetické, logické a územní. Fyzická zranitelnost vzniká tím, že infrastruktury jsou fyzicky vzájemně závislé, tj. stav jedné z nich je závislý na materiálním výstupu infrastruktury druhé. Kybernetická zranitelnost vzniká tím, že stav jedné infrastruktury závisí na informacích z jiné infrastruktury. Kybernetická vzájemná závislost předpokládá existenci informační infrastruktury. Územní zranitelnost způsobuje to, že infrastruktury jsou územně vzájemně závislé, tj. události v území mohou měnit stavy infrastruktur. Logická zranitelnost je způsobená logickou závislostí mezi infrastrukturami, tj. stav jedné infrastruktury závisí na stavu jiné infrastruktury, přičemž mechanismus propojení není

fyzický, kybernetický nebo územní. Jedná se o závislosti přenášené přes toky, kterými jsou předpisy, finance, legislativa apod., např. se může jednat o finanční trhy.

67. Kritická infrastruktura je systém systémů, tj. je komplexním systémem. Komplexní systémy mají velký počet aspektů, nelinearit, silných interakcí, neznámých nebo inherentních náhodných parametrů, a časová zpoždění v dynamické struktuře. Dalšími charakteristikami komplexních systémů je emergenční chování a smyčka zpětné vazby. Centrální otázkou je, zda existující metody pro hodnocení rizika a spolehlivosti složených systémů lze aplikovat na SoS. Kvůli vysoké dynamické proměnlivosti a nelinearitám v chování SoS tyto nemohou být plně poznatelné.
68. SoS se skládá z mnoha heterogenních, distribuovaných, občas nezávisle provozujících systémů, které jsou zakotvené do sítí o mnoha úrovních, které působí v čase. NEBO SoS jsou mnohastupňové souběžné a distribuované systémy, které jsou složené z komplexních systémů. Z uvedených definic je zřejmé, že je problémem stanovit, jak vyjednávat s komplexností a jak modelovat SoS. Když strukturální model má 3 úrovně, tak u kritické infrastruktury je to: globální úroveň SoS; střední úroveň – model interakcí mezi jednotlivými infrastrukturami (někdy též lokální systém systémů); nejnižší úroveň – systémové modely jednotlivých infrastruktur.
69. Jeden z nejpoužívanějších přístupů k hodnocení zranitelnosti kritických infrastruktur je založen na komplexní síťové teorii, která vychází z charakteristické délky cesty, funkcích výkonnosti sítě nebo výkonnosti spolehlivosti, rozšíření konceptu výkonnosti, který zvažuje spolehlivost vazeb. Avšak hodnocení je hodnoceno jako jednoduchý objektivní problém, např. určení takových síťových komponent, které mají nejdůležitější roli v systémech z hlediska zranitelnosti. Rozhodující subjekty obvykle požadují soubor řešení, které jsou, co nejvíce vhodné k dosažení jistých cílů. Např. zisk, který požaduje rozhodující subjekt lze získat z pochopení výměny mezi jevem s malým výkonem (výskytem) a vysokou cenou nebo jevem s nízkou cenou a vyšším výkonem (výskytem). V současné době v důsledku této výzvy rozhodující subjekt musí řešit několik problémů při použití jednoduchého objektivního přístupu variací skupiny omezení. V kontrastu k tomu při víceúčelové formulaci se určení Paretova rozhraní provádí přes jednoduchý problém. Pro charakteristiku Paretova rozhraní se používá např. mnohaoborový deterministický problém zranitelnosti sítě (MO-DNVP: multiple- objective Deterministic Network Vulnerability Problem), ve kterém dva nebo více cílů jsou optimalizovány na základě vývojového algoritmu. Pro optimalizaci lze např. použít algoritmy MOFA (Multiple-Objective Evolutionary Algorithms).
70. Infrastruktura podniku je klíčem pro udržitelné hospodářství a sociální blaho národa. Recentní světové jevy ukázaly, že kritické infrastruktury jsou zvláště citlivé na zvláštní nebo kompletní ztrátu způsobilosti kvůli vnitřním nebo vnějším zdrojům selhání nebo útoků. Pro zdroje vnitřních selhání nástroje představují inženýrství spolehlivosti a pro odhad, prevenci a odezvu s ohledem na jevy, které se vyskytují náhodně ve složitých systémech. Protože vnější zdroje selhání s důrazem na úmyslné útoky mohou být katastrofické pro společnost (vedou až k narušení společnosti), představují novou výzvu. Jeden z nejčastěji používaných přístupů je založen na složených konceptech sítě. Kritická infrastruktura, např. elektrická síť, je abstraktně modelována jako G síť s uzly propojenými vazbami. Některé problémy, např. důležitost komponent mohou být hodnoceny jako jednoduchý objektivní problém, jako např. určení, která síťová komponenta by měla být zodolněna, aby zranitelnost byla snížena, nebo která komponenta bude / musí být určitě poškozena, když zranitelnost bude maximální. Avšak hodnocení touto analýzou nezvažuje náklady ve spojení s výskytem jevu a zda je jev limitní. To není vhodné pro rozhodující subjekty, protože ony obvykle požadují soubor řešení, které jsou, co nejvíce vhodné k dosažení jistých cílů.
71. Sektory kritické infrastruktury, které jsou životně důležité pro společnost, se běžně sledují pomocí analýz rizik a zranitelnosti, které byly adaptovány pro potřeby kritické infrastruktury. Na základě toho vznikly různé přístupy pro hodnocení rizik a objevily se nedostatečné analýzy interdependences mezi sektory. Proto vznikl projekt DECRIS (Risk and Decision Systems for Critical Infrastructures), jehož cílem je vývoj analýzy rizik a zranitelností vůči všem ohrožením (all hazards), která bude specifická pro kritickou infrastrukturu a její sektory a bude vhodná pro

analýzy napříč sektory. V ní jsou zahrnuty aspekty jak bezpečnosti (havárie, technologická selhání atd.), tak bezpečí (úmyslné činy). Obecná případová studie pro město Oslo zaměřená na nežádoucí jevy v infrastrukturách elektrické energie, dodávek vody, dopravy a přenosu informací vyvíjela metodu analýzy napříč sektory zaměřenou na několik výzev, např. složitost systému a interdependences v infrastruktuře. Interdependences vytváří zádrhele, které v závislosti na situaci mohou zapříčinit otřesy v různých sociálních funkcích.

72. Pro studium interdependences se používají prediktivní přístupy a empirické přístupy. Prediktivní modely simulují chování skupiny propojených infrastruktur, např. hodnotí, jak jdou poruchy kaskády systémem. Empirické přístupy minulých jevů studují infrastruktury s cílem pochopit interdependences v infrastrukturách. Často je snaha najít model, na jehož základě lze dělat politická rozhodnutí, např. modely důsledků pro společnost nebo jak často se selhání šíří mezi různými infrastrukturami. Prediktivní metody dají důležité informace o specifickém systému a mohou být užitečné při pro-aktivním řízení rizika. Empirické modely mohou přispět důležitými informacemi o obecných modelech interdependences v infrastrukturách a o četnosti poruch, které se kaskádovitě šíří v systémech, a proto tvoří vhodné vstupy do prediktivních modelů. Analýza interdependences zahrnuje úkoly jako: popis scénáře havárií; identifikace interdependences; kvalitativní popis interdependence pomocí diagramu kaskády (cascade diagram) a provedení semi-kvantitativního hodnocení celkového rizika spojeného s daným scénářem; provedení detailní kvantitativní analýzy interdependence; vyhodnocení opatření na snížení rizika, aby se zredukovaly kritické interdependences. Je si nutné uvědomit, že v jednotlivých sektorech je mnoho modelů a počítačových simulací pro jednu infrastrukturu, ale žádné z nich neprovádí analýzu napříč sektory. Modely pro nové potřeby musí být schopné hodnotit velké množství dat různé povahy a dynamické chování mezi modely infrastruktur.
73. Nástroj „cascade diagram“ modeluje interdependences. Umožňuje holistické hodnocení interdependences a poskytuje systematický přehled o interdependences, jejich spřaženích a o reakčním chování.
74. Kritičnost komponent v systému sítí s ohledem na jejich příspěvek a účast v procesech kaskády selhání je třeba charakterizovat. K tomu se navrhují speciální indikátory, tj. indikátory kritičnosti.
75. Kaskádovitá selhání jsou největší hrozbou pro distribuované propojené systémy jako jsou dodávky energií, komunikační systémy aj. Tyto typy selhání jsou obvykle iniciovány, když z nějakého důvodu selže vysoce zatížená komponenta systému a její zátěž nebo tok, který prochází skrz ní, je přerozdělen na ostatní komponenty; přerozdělení může způsobit zatížení dalších komponent takové, že se přesáhne jejich kapacita, což způsobí selhání nebo spuštění ochranného mechanismu, který vede k jejímu odstavení, aby se zabránilo jejímu zničení. Proces selhání se takto šíří přes celou ovlivněnou síť. Modely a simulační nástroje navrhované k popisu procesu kaskádovitých selhání v systémech sítí jsou dosud ve výzkumné fázi: vznik a důsledky rozdělení velikostí kaskád; vztahy mezi iniciačními jevy a následnými kaskádovými jevy; jak navrhovat ochrany zabraňující šíření kaskádovitých selhání po jejich vypuknutí (tj. vhodný systém odezvy). Potřeba analýz je zvláště vysoká tam, kde dynamika kaskád je rychlá a zmírňující opatření v síti jsou žádoucí. např. kaskáda jevů vedoucích k blackoutu se vyskytne v časové stupnici minuty a hodiny a je dokončena v době menší než 1 den.
76. Modely kaskádovitých selhání závisí jak na logice rozložení zátěže od selhání, tak na iniciační události kaskády, tj. buď na náhodném selhání nebo na cíleném úmyslném útoku. Šíření kaskády se musí sledovat krok po kroku a vlastní indikátory jsou hodnoceny pro každou komponentu - sleduje se četnost její účasti v kaskádě, průměrný čas před jejím vstupem do kaskády, průměrná doba trvání a konečná velikost kaskády způsobené jejím selháním. Nakonec kritičnost komponent s ohledem na jejich příspěvek ke kaskádovitým selháním je vztažen ke klasickým opatřením topologickému hlavnímu úkolu.
77. Moderní technické systémy jsou vysoce složité a vysoce vzájemně závislé. Podstata vzájemné závislosti mezi těmito systémy nabývá dnes na důležitosti. Kromě toho tyto systémy čelí množství

pohrom různé postaty (technické, lidské, přírodní atd.). Navíc u nich není jeden vlastník, provozovatel a regulátor. Každá porucha v libovolném z vnitřně propojených systémů může způsobit kaskádu jevů. Tato kaskáda se může vyskytnout na místní, regionální nebo národní úrovni a v některých případech může překročit i národní hranice. Systémové modely SMS (SSMS) se používají k modelování interdependences kritické infrastruktury. Současným úkolem je poznat interdependences a snížit zranitelnost systému systémů s ohledem na interdependences.

78. Jedním z hlavních zájmů udržitelného rozvoje moderní společnosti je zajištění kontinuity kritických služeb a s nimi spojených infrastruktur. Fundamentální procesy a fyzické komponenty, které mají zajistit d´jednoduché servisní dodávky, mají mnoho závislostí, jak technických, tak netechnických. Kromě toho každá služba předpokládá podporu alespoň jedné infrastruktury, která je složená dalších infrastruktur, komponent a propojení, které mohou selhat, snížit úroveň služby a / nebo vygenerovat škody a obvyklá selhání. Abychom minimalizovali dopady těchto jevů je potřeba stanovit metodologii ochrany kritických infrastruktur.
79. Pro bezpečnost kritické infrastruktury, která zahrnuje i ochranu kritické infrastruktury potřebujeme integrovaný (celistvý, sjednocený) přístup pro analýzu zranitelnosti, odolnosti (houževnatosti) a adaptability infrastruktur k tomu, abychom mohli vyjednávat s riziky pro lidskou společnost spojenými s kritickou infrastrukturou.

XXVI. Elektrické a elektronické inženýrství

80. Stále se vyvíjejí optimalizační metody pro strategie rozšiřování elektrických přenosových sítí (tj. pro připojování nových linií). Cílem je vylepšit přenosovou spolehlivost při omezených investicích do údržby. Pro velké elektrické sítě existuje mnoho řešení, a proto klasické optimalizační metody nelze aplikovat. Proto se vyvíjí algoritmus MOGA (Multi-Objective Genetic Algorithm) zaměřený na globální výkonnost spolehlivosti a minimalizaci nákladů pomocí Paretova optimalizačního schématu na vyhledávání nedominantních řešení.
81. Je skutečností, že navzdory růstu počtu a úrovně standardů pro spolehlivost a významným technologickým pokrokům v minulých desetiletí neklesá četnost blackoutů v elektrické síti, ale naopak jejich velikost znepokojivě roste kvůli růstu propojení a interdependences. Proto provozovatelé elektrických sítí hledají efektivní a ekonomická technická řešení ochrany před selháními pomocí modifikací modelů a méně napjatých (vystresovaných) módů provozu, které jsou konkurenceschopné na deregulovaném trhu s elektřinou. Pro nalezení těchto řešení se provádí systémové analýzy elektrických sítí a jejich odezvy na selhání. Kvůli složitosti a vysoké propojenosti infrastruktur je systematická analýza zranitelností a robustností s ohledem na selhání obtížná, když ji provádí pouze jeden resort tradičními PSA metodami.
82. Spolehlivost elektronických zařízení je způsobena především selháními, které jsou způsobeny latentními defekty, které vznikly během výroby nebo během provozu. Hledají se proto nedestruktivní metody, kterými by se tyto latentní defekty daly odhalit.

XXVII. Výroba a distribuce energie

83. Jedním z požadavků, které jsou kladeny na elektrickou distribuční síť je zajistit spolehlivou a kvalitní dodávku elektrické energie zákazníkům. Kvůli tomu, aby distributoři nemuseli poskytovat finanční kompenzace za selhání dodávek, hraje významnou roli kvalita a spolehlivost. Systémy sou dálkově řízeny a spojitě monitorovány. To umožňuje rychlé řešení problémů, a to zvláště těch, které jsou spojené s vlastním provozem. Problémy při řízení distribuce elektřiny jsou však tehdy, když zvážíme jiné pohromy.

XXVIII. Zdraví a medicína

84. Navzdory snaze poskytovat bezpečnou a účinnou zdravotní péči nepříznivé jevy se vyskytují s jistou pravidelností. Cílem je vyvinout bezpečnější zdravotní péči, ač jsme si vědomi toho, že riziko nelze plně eliminovat. Systém zdravotní péče se modeluje pomocí Bayesovských sítí. K analýze a hodnocení systému se používají stejné postupy jako v oblasti technologických systémů. Používají se také modely založené na logické regresi.

XXIX. Informační technologie a telekomunikace

85. Při zpětné analýze spolehlivosti se používají CPN (Colored Petri Nets), které se aplikují ve dvou krocích: CPN se převede do pojmů multipikativní intuitivní lineární logiky (MILL – Multiplicative Intuitionistic Linear Logic); zkonstruují se důkazní stromy. V prvním kroku musí být respektovány vlastnosti jako sémantika spojená se symboly.
86. Systém spolehlivosti je důležitým výstupem, a to zvláště tehdy, když je aplikován na kritické oblasti. Systémy jsou ověřovány nástroji, které kontrolují soulad jejich vlastností s těmi projektovanými. Formální metody založené na lineární logice poskytují zajímavý způsob pro studium a vývoj nástrojů pro ověřování díky své precizní charakteristice modelovaného systému. Petriho sítě (PN – Petri Nets, Petri 1962) a zvláště CPN (Colored Petri Nets, Rozenberg 1991) jsou účinným modelovacím nástrojem. PN dovolují studovat statické vlastnosti díky své struktuře i dynamické díky symbolice vývoje. Další metoda je Monte Carlo (Metropolis, Ulam 1949). Uvedené metody dovolují sledovat chování modelů. Uvedené metody trpí velkým množstvím možných kombinací a velkým rozptylem výsledků.
87. Analýzy výskytu náhodných selhání komunikačních systémů, které degradují výkonnost vedou k pokroku při vytváření sítí příští generace,které budou založené na internetovém protokolu. Cílem je vyvíjet systémy, které tolerují chyby, tj. dokáží se z nich zotavit. K tomu je potřebná rychlá detekce chyby, která spustí nápravné činnosti. Takové systémy již pracují v oblasti jednoduchých oblastí. Cílem je vyvinout takové i pro složené oblasti jako jsou komplexní systémy.

XXX. Výroba

88. Systematická analýza strojů je metodologie, která poskytuje dostatek dat pro audit zařízení pro údržbu. Nákladově a přínosně řízená údržba společnosti nebo majetku podniku je absolutně podstatná pro maximální ziskovost a dlouhodobé přežití společnosti nebo podniku. Pro posouzení úrovně údržby jsou nutné dokumentace a inspekce, včetně pravidelných auditů, a to především vnějších. Podle amerických modelů funkční bezpečnost podniku či zařízení zajišťuje dostupnost (dosažitelnost) a vyžaduje integrální bezpečnost, spolehlivost a udržovatelnost.
89. Záruka je obvykle definována jako politika důvěry / jistoty vůči zákazníkům (spotřebitelům). Tato jistota je v platnosti po určitou dobu od doby prodeje. Řízení záruk kombinuje technické, administrativní a organizační činnosti během doby záruky. Strukturovaný přístup k zárukám je založen na řízení rizik spojených s vysokou zárukou. Řízení záruk zahrnuje všechny činnosti v oblasti řízení spojené s cíli, prioritami, strategiemi a odpovědnostmi a implementuje řízení ve smyslu ovládání (tj. kontrolu), dohled i vlastní řízení reklamací. Cílem je dostupnost, snížení nákladů, spokojenost zákazníků atd. proto tento druh řízení je důležitý pro každého výrobce.

XXXI. Námořní průmysl

90. Jestliže je dostatek dat např. z historických pozorování, je materiál pro hodnocení a řízení rizik. V případech nových, např. u teroristických útoků, je dat málo, a proto je nutno použít specifické nástroje pro hodnocení a řízení rizik, např. založené na metodě mlhavých množin., např. přístup označovaný FuRBaR (Fuzzy Rule-based Bayesian Reasoning). Začíná se obvykle s nástrojem IF – THEN. Parametry rizika se popisují proměnnými: bude (Will – W), schopnost poškození (Damage capability – D), obtíže při obnově (Recovery difficulty - R), pravděpodobnost poškození (Damage probability – P) a úroveň bezpečí (Security level – S).

XXXII. Přírodní ohrožení

91. Povodeň – podle funkce úmrtnosti se vydělují 3 zóny: zóna narušení - $h . v \geq 7$ m^2 /s a $v \geq 2$ m/s v je rychlost toku a h je hloubka zaplavení; zóna s rychle rostoucí hladinou vody - přírůstek vody za hodinu $w \geq 0.5$ m/hr; přírůstek vody a její rychlosti je malý. Počet obětí pro daný scénář pohromy závisí na prostorovém rozložení časových charakteristik povodně, hustotě obyvatelstva v postiženém území , na možnostech evakuace a na pravděpodobnosti úmrtí postižených lidí. Ohrožení se počítá speciálními metodami, např. pomocí zjednodušeného Bayesovského přístupu.

XXXIII. Jaderné inženýrství

92. Pravděpodobnostní hodnocení rizika požárů se často modeluje pomocí vnitřního modelu komponent technického zařízení. Obrana do hloubky poprvé použitá u jaderných zařízení je typicky realizovaná rozmanitostí bariér bezpečnosti a sítí záloh, se osvědčila i v řadě dalších oblastí. Avšak zatímco hodnota zálohy nemůže být úplně realizovaná kvůli obvyklým příčinám selhání, stejná záloha může posílit mechanismy zatajení výskytu nehod, které mohou dovést systém do nebezpečného stavu. Proto je potřeba mít kvalitní diagnostiku, aby schopnost lidí bezpečně provozovat řídit systém byla na dobré úrovni.
93. Je si třeba uvědomit, že systém obvykle odráží modely chování, které ne vždy ukazují pravdivé vnitřní podmínky (stav) systému. Typicky – vnější pozorovatel zaznamenává pouze odezvy systému a jen z jejich pozorování se pozorovatel pokouší dedukovat podmínky (stav) systému. V tomto kontextu vzniká pochopitelně otázky, zda monitoring odezev systému vždy odhaluje vnitřní podmínky systému. Moderní teorie řízení systémů říká, že tomu tak vždy není. Tento fakt je potřebné zvážit při rozhodování. Je si třeba také uvědomit, že u složitých systémů de facto přesný monitoring není možný, a proto s tím počítají řídící systémy. Systémy předpokládají latentní nebezpečné stavy jako důsledek nepozorovaných selhání během provozu systému, např. skryté selhání záložních komponent systému. Analogické situace jsou identifikovány při analýze zpráv o haváriích – faktory, které přispěly k havárii samotné nebo k její krutosti.
94. Proces diagnostiky problémů požaduje vývoj analytických nástrojů na odhad vývoje stavu systému na základě indikací od senzorů. Problém odhadu stavu je vztažen ke konceptu rozpoznatelnosti stavu v teoretickém kontextu řízení. Rozpoznatelnost stavu je skutečná vlastnost systému, která dovoluje vnějšímu pozorovateli usuzovat o stavu systému v daném čase na základě záznamů výstupů. Představa, že je to analogické k rozpoznání stavu a ve stejném čase je to přímo vztažené k provedení bezpečnosti systému, je konceptem schopnosti diagnostiky. Koncept schopnosti diagnostikovat popisuje vnitřní vlastnost systému odhalit vnějšímu pozorovateli utajené minulé chování systému, které by mohlo nepříznivě ovlivnit budoucí provedení (chování) bezpečnosti systému. V posledním desetiletí se objevila řada nástrojů, které odhalují selhání diagnostiky / detekce u dynamických systémů.
95. Vysoké úrovně zálohování mohou zvýšit celkovou spolehlivost systému, avšak na druhou stranu mohou silně degradovat schopnost systému diagnostikovat selhání a potenciálně utajit o systému, že se nachází v nebezpečném stavu. Např. selhání záložní komponenty může indikovat, že systém nepracuje bezpečně. Když se tato indikace nedostane k provozovateli systému, neprovede se žádná činnost a může dojít k havárii. Používá se argument, že tato patologická situace by měla být odhalena a odstraněna během projektování systému. To znamená, že u pokrokových systémů se musí posilovat jak spolehlivost, tak kapacita monitoringu.
96. Požární PSA se provádí v několika krocích. Začíná se screeningem (prosvícením) systému vedoucím k odhalení problémů. Pak se pokračuje za použití procesních modelů příslušného zařízení. Podstatným požadavkem pro kvalitní výstup je kvalitní databáze, protože jen pomocí ní lze stanovit četnost poškození zařízení po nežádoucích spouštěcích jevech. Tradiční modely FTA a ETA jsou statické, a proto se požadují pravděpodobnostní hodnocení, ve kterých se předpokládá stochastické chování systémů.
97. Pravděpodobnostní analýzy bezpečnosti (PSA) patří ke špičkovým nástrojům pro hodnocení bezpečnosti zařízení. PSA je obvykle prováděna pro proměnný rozsah počátečních jevů, vnitřních i vnějších. Používají se analýzy FTA, ETA nebo Monte Carlo simulace (MCS).
98. Při řízení bezpečnosti je třeba se také vyrovnat s nestacionárními náhodnými procesy, které se vyskytnou během provozu. U běžných hodnocení bezpečnosti se totiž proměnnost objektů, mechanických vlastností a fyzikálních parametrů v čase obvykle zanedbává. To znamená, že běžné pravděpodobnostní analýzy nezvažují proměnnost uvedených položek v čase.

XXXIV. Ropa a plyn u pobřeží

99. Bezpečná těžba ropy a plynu u pobřeží vyžaduje velmi mnoho komponent a systémů. Pro její řízení se používají specifické indikátory. Obvykle se používá koncept DSHA (Defined Situations of Hazard and Accident).

XXXV. Bezpečí a ochrana

100. Empirické Bayesovské modely poskytují metodu na odhad četnosti výskytu havárií na základě symptomů havárií. Zvažují řídké jevy a používají se při pravděpodobnostním hodnocen rizika zařízení. Na základě výsledků se stanovují bezpečnostní a ochranná opatření.

101. Většina rizik, kterým jsou vystaveny moderní společnosti nejsou vyhodnoceny lidskými smysly, ale jsou zjištěné z komunikace. Pohromám čelíme zřídka osobně. O nebezpečných jevech nás informují média. Proto je důležité, jak média interpretují skutečné jevy. Pro realistické pochopení rizika terorismu je třeba odpovědět na otázky: Jak je riziko terorismu popisováno a hodnoceno?; Kdo jsou teroristi a jaké jsou teroristické zbraně a motivace?; Které faktory jsou zvažovány jako příčiny růstu nebo poklesu terorismu?; Jaké jsou cíle teroristů?; Jak jsou změny v mandátu a reorganizaci PST (Police Security Service) a obrany legalizovány s ohledem na hrozbu terorismu?. Na základě odborných analýz a hodnocení je riziko terorismu společenské a katastrofické a může zasáhnout každého kdykoliv. Společnost musí být proti němu ochraňována, protože toto riziko je netolerovatelné.

XXXVI. Pozemní doprava (silniční a vlaková)

102. Aby se zajistila komplexní bezpečnost relevantních systémů, musí se používat principy bezpečnosti, aby se ušetřil čas a udržela architektura bezpečnosti. Principy jsou bezpečný život, zálohování a diversita. Systém je navrhován podle principu bezpečný život, když s velkou pravděpodobností je dostupná spolehlivá funkce bezpečnosti. K tomu je potřeba detekce všech kritických selhání a adekvátní reakce k dosažení bezpečnosti. Během této doby systém musí být dostatečně bezpečný. To vyžaduje monitoring kritických komponent (pozn. zálohování samotné není dostatečné poněvadž se musí zabránit latentním selháním). To musí být zkombinováno s vhodnou činností, která zabrání výskytu dvojitého selhání. Z tohoto důvodu je implementováno automatické zpomalení bezpečnosti na detekci kritických selhání. Tímto přístupem se zabraňuje kumulaci chyb, protože ta může být kritická pro životnost bezpečných systémů. Zálohování je přítomnost více prostředků než které jsou potřeba pro požadovanou funkci. Diversita charakterizuje situaci, při které několik subsystémů provádí stejnou funkci různým způsobem. Principy bezpečnosti dovolují obejít fázi pokusů a omylů a vytvářet bezpečnou architekturu.

103. Analýzu spolehlivosti komplexních systémů komplikuje několik faktorů. Možná nespolehlivost logistických podpůrných elementů může vést ke snížení provozního výkonu systému. Na základě toho dochází k narušení realizace úkolu a k neschopnosti sytému přijmout nový úkol.

104. Při hodnocení rizik v silničních a železničních tunelech se v Evropě používá metoda QRA. ERTMS (The European Railway Transmission and Management System) je systém, který v Evropě zajišťuje interoperabilitu provozu na železnicích.

105. Markovova analýza je statistická metoda používaná při předpovědi budoucího chování rozmanitých systémů, které mají Markovovy vlastnosti. Mít Markovovou vlastnost znamená, že daný přítomný stav a budoucí stavy jsou nezávislé na minulých stavech Exponenciální pravděpodobnostní rozložení je důležitou podmínkou pro aplikaci Markovovy analýzy.

XXXVII. Vodní doprava

106. Vodní doprava nebezpečných látek má potenciální riziko, že poškodí životní prostředí, způsobí ztráty na majetku a životech lidí. Proto vlády a mezinárodní organizace věnují zvláštní pozornost požárům a explozím, jelikož statistiky ukazují, že právě tyto dva jevy významně poškozují lodě.

ZÁVĚR

Údaje v předchozí kapitole charakterizují současnou úroveň poznání ve sledované oblasti. Nejvíce pozornosti bylo věnováno ožehavým otázkám bezpečnosti kritické infrastruktury, protože na nich závisí přežití lidí v kritických obdobích. Práce [3] shrnula zásady pro řízení bezpečnosti kritické infrastruktury takto „Bezpečnost kritické infrastruktury je integrální bezpečnost systému systémů (SoS). Model systému systémů označuje takový soubor systémů, které mohou fungovat autonomně a pro plnění funkcí v území jsou propojeny do systému, který musí být bezpečný, funkční a spolehlivý. Vzájemné propojení systémů způsobuje závislost, které se projevují vazbami a toky napříč souboru systémů a jsou příčinou kaskádovitých selhání, jak jednotlivých infrastruktur, tak souboru infrastruktur. Z pohledu technologického je řízení bezpečnosti kritické infrastruktury proces, který je zaměřen na ***takové zajištění fungování kritické infrastruktury, při kterém se plní požadované funkce a za žádných okolností nedojde k selhání při zohlednění všech možných rizik a hrozeb a nebo když k selhání dojde, tak je selhání bezpečné, tj. např. nevyvolá domino efekty***. Základním prvkem bezpečnosti je správné umístění v území, dobrý projekt, kvalitní výstavba, údržba, opravy a zálohování prioritních částí kritické infrastruktury, využití různých principů zálohování a rozmístění záloh v území, které musí být v souladu se zásadami, které se od počátku 80. let používají při projektování, výstavbě a provozu jaderných zařízení“.

POUŽITÁ LITERATURA

[1] D. Procházková: *Bezpečnost a krizové řízení*. ISBN 80-86477-35-5. POLICE HISTORY, Praha 2006, 255p.

[2] R. Briš, C. G. Soares, S. Martorell (eds): *Reliability, Risk and Safety: Theory and Application.*ISBN 978-0-415-55509-8, 2367p., CD ROM - ISBN 978-0-203-85975-9, CRC Press / Balkema, Leiden 2009.

[3] D. Procházková: *Critical Infrastructure Safety Management*. In: Reliability, Risk and Safety. Theory and Applications. ISBN 978-0-415-55509-8, CRC Press / Balkema, Leiden 2009, 1875-1882, CD ROM ISBN 978-0-203-85975-9.

ADRESA AUTORA:

Doc. RNDr. Dana PROCHÁZKOVÁ, PhD., DrSc. Univerzita Jana Amose Komenského, Roháčova 89, 130 00 Praha 3, prochazkova.dana@ujak.cz & Vysoká škola evropských a regionálních studií, Žižkova, České budějovice, prochazkova.dana@vsers.cz

RECENZENT:

RNDr. Miroslav RUSKO, PhD. Ústav bezpečnostného a environmentálneho inžinierstva, Materiálovotechnologická fakulta Trnava, Slovenská technická univerzita Bratislava, E-mail: miroslav.rusko@stuba.sk