Metodika vypracovania bezpečnostnej analýzy pre technologické dynamické systémy

Methodology for Developing a Safety Analysis for Technological Dynamic Systems

Milan Štrbo

Katedra matematiky a informatiky, Pedagogická fakulta, Trnavská univerzita v Trnave

Abstract: Safety analysis is carried out in the process of development of control systems. We suggest designing it based on models that will detect deviations between real system operation (real values) and ideal system operation (ideal values set in models). The models will be created especially for safety-critical processes of system operation that could threaten it.

Keywords: safety analysis, dynamic systems, safety-critical systems.

1 Úvod

Bezpečnosť a starostlivosť o zdravie ľudí, ich majetok a životné prostredie je dnes prvoradou podmienkou pri vývoji riadiacich systémov. Prevádzka bezpečnostne-kritických dynamických systémov predstavuje pre svoje okolie určité nebezpečenstvo, pričom intenzita škôd spôsobených vďaka nežiaducim účinkom systému môže byť obrovská. Na základe týchto poznaní sa kladie veľký dôraz pri vývoji riadiacich systémov a najmä na analýzu možných rizík.

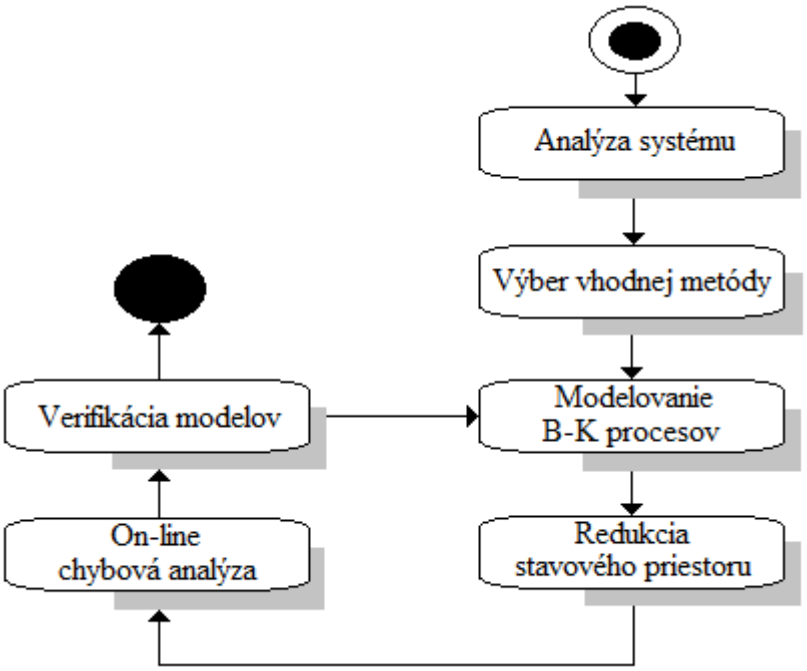
Bezpečnostná analýza rizík je návrhový nástroj, ktorý pomáha vývojárom identifikovať a riešiť nebezpečenstvo v počiatočných fázach vývoja takýchto systémov. Bezpečnosť je pojem, ktorý sa zdá byť síce zrejmý, ale postupnosť krokov, ktoré je potrebné vykonať na jej implementovanie do konkrétneho systému sú veľmi náročné. Proces bezpečnostnej analýzy je náročný a zdĺhavý proces. Cieľom príspevku je predstaviť návrh metodiky bezpečnostnej analýzy pre dynamické technologické systémy.

DOI: https://doi.org/10.31262/2585-8556/2018/2/1/23-28

2 Návrh metodiky bezpečnostnej analýzy

Návrh metodiky slúžiacej na vývoj modelov pre jednotlivé bezpečnostne-kritické procesy nachádzajúce sa v dynamických technologických systémoch zobrazuje obrázok jeden. Metodika je znázornená pomocou štandardného stavového UML diagramu a pozostáva z postupnosti šiestich nadväzujúcich krokov. Posledným krokom metodiky je verifikácia samotných navrhovaných modelov na kontrolu bezpečnostne-kritických procesov.

Ak verifikácia preukáže nedostatky pri navrhnutých modeloch, samotný proces bezpečnostnej analýzy sa vracia späť do kroku „modelovanie bezpečnostne-kritických procesov“. V tomto kroku sa odstránia nedostatky zistené pri verifikácii a proces vývoja modelov pokračuje ďalej v postupnosti podľa navrhovanej metodiky. Proces sa opakuje dovtedy, kým sa verifikáciou modelov nepreukáže správnosť vytvorených modelov, ktoré budú slúžiť na on-line kontrolu daného systému.



Obrázok 1: Metodika na modelovanie bezpečnostne-kritických stavov.

2.1 Analýza dynamického technologického systému

Cieľom prvého kroku je analýza konkrétneho dynamického technologického systému. Je dôležité uviesť, že analýza je realizovaná so zameraním na bezpečnostnú analýzu. znamená to, že je potrebné oboznámenie sa so systémom, s jeho funkciami a určenie všetkých možných stavov systému v priebehu prevádzky. Potrebné je analyzovať aktuálne podmienky a základné prevádzkové parametre, respektíve základné prevádzkové podmienky. S týmto krokom úzko súvisí analýza obmedzení pri jednotlivých stavoch, analýza nedostatkov, rizík a všetkých dostupných zdrojov systému. Dôležitou súčasťou analýzy konkrétneho systému je metóda Top-Down, ktorej nástroje umožnia rozloženie systému od globálneho pohľadu až k jednotlivým subprocesom systému.

Každý systém má určitú množinu stavov respektíve procesov. Cieľom tejto analýzy je výber a analýza tých procesov prevádzky, ktoré sú pre systém bezpečnostne-kritické a rozdelenie týchto procesov na deterministické a stochastické. Podrobnou analýzou týchto procesov získame požiadavky na meranie, funkcie kontroly priebehu procesov alebo požiadavky akčných členov regulátorov. Pre kritické procesy je potrebné vyhotoviť výber zdrojov informácií, ktoré budú obslužnému personálu podávať informácie o priebehu týchto procesov. V neposlednom rade je potrebné definovať vstupy pre jednotlivé procesy, vzájomné väzby medzi procesmi systému a samozrejme dôležitá je charakteristika týchto procesov na výstupe. Cieľom tohto kroku je takisto určiť požiadavky na bezpečnostnú analýzu respektíve kontrolu procesu z hľadiska vzniku, priebehu a vyhodnocovania kritických situácií (porúch). To môžeme chápať ako určenie jednotlivých požiadaviek na hardvér a softvér riadiaceho systému pre bezpečnostne-kritické procesy.

2.2 Výber vhodnej metódy na modelovanie bezpečnostne-kritických procesov

Podrobnou analýzou systému sa o systéme zistí všetko potrebné k vykonaniu bezpečnostnej analýzy. Na základe tejto analýzy systému je potom jednoduchšie vybrať vhodnú metódu na vytváranie modelov potrebných na automatizovanú kontrolu prevádzky dynamických systémov. Na vývoj modelov pre bezpečnostne-kritické procesy dynamických systémov navrhujeme použiť metódu SQMD.

Samotná metóda SQMD je využívaná na bezpečnostnú analýzu dynamických systémov. Je založená na kvantitatívnych a kvalitatívnych modelovacích metódach. Využíva hybridné modely na monitorovanie a detekciu reálneho času. Hybridný model obsahuje kvalitatívne a dynamické prvky a kombinuje výhody oboch metód. Takto je možné predstaviť si predstaviť on-line monitoring a diagnostiku na detekciu a lokalizovanie porúch v dynamických technologických systémoch.

Hlavnou výhodou bezpečnostnej analýzy metódou SQMD je jednoduché modelovanie dynamických systémov. Netreba zabúdať na dva dôležité aspekty. Na jednej strane už existujúce matematické modely. Tie sú kombinované s kvalitatívnymi modelmi, takže dynamické systémy môžu byť modelované a simulované. Na druhej strane, jedinou zaujímavou časťou je to, že stavy sú analyzované, čo znamená, že môžu byť ohodnotené on-line, s menšou výpočtovou silou (Fröhlich, 1996).

2.3 Modelovanie bezpečnostne-kritických procesov dynamických systémov

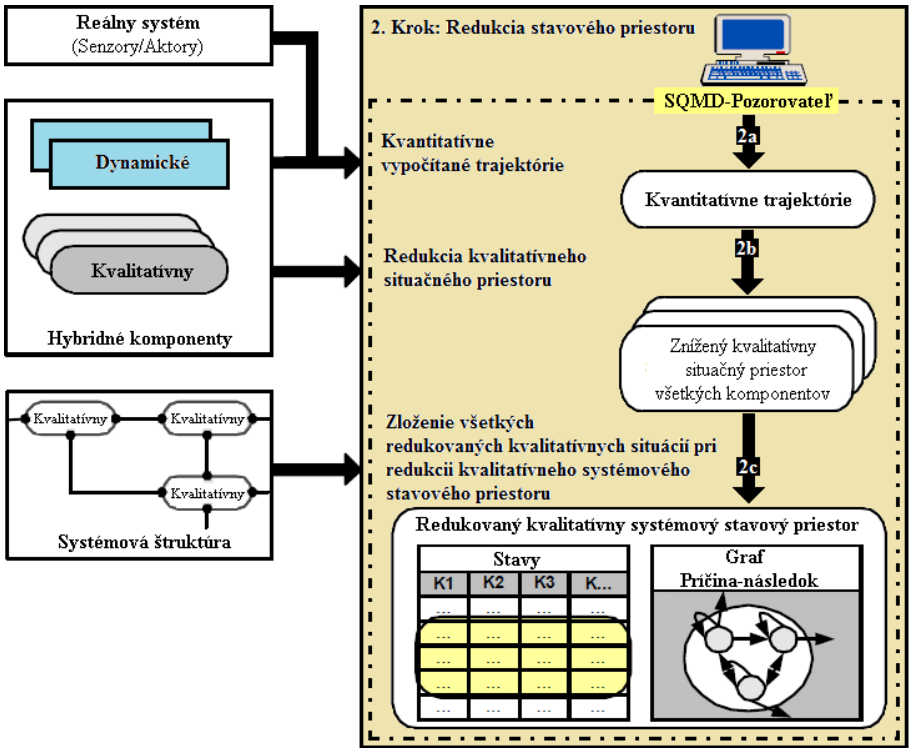
V tomto kroku je dôležité správne opísať bezpečnostne-kritické procesy konkrétneho systému pomocou modelov. Cieľom je vypracovať kvalitatívne a kvantitatívne modely v rozsahu všeobecného popisu systému. Na vytvorenie kvalitatívnych modelov jednotlivých procesov využijeme fuzzy logiku, poprípade sa môžu použiť kauzálne siete alebo pre vyložene diskrétne procesy Petriho siete. Kvantitatívne (matematické) modely zostrojíme pomocou diferenciálnych a diferenčných rovníc, keďže ide o dynamické technologické systémy.

V inom prípade môže byť ako matematický model použitý takmer každý správny matematický vzorec. Takisto je potrebné vykonať syntézu týchto modelov, vyhodnotiť ich efektívnosť a vykonať kontrolu platnosti modelov. Na automatizovanú kontrolu dynamických systémov navrhujeme použiť hybridné modely zložené práve z kvalitatívnych a kvantitatívnych (matematických) modelov. Správnosť týchto modelov bude overená ich verifikáciou v poslednom kroku metodiky.

2.4 Redukcia stavového priestoru

Ťažisko celkového konceptu bezpečnostnej analýzy sa nachádza v on-line redukcii stavového priestoru, ktorá umožňuje on-line kontrolu dynamických systémov. Po zostrojení jednotlivých modelov na automatizovanú kontrolu bezpečnostne-kritických procesov systému je potrebné vykonať redukciu stavového priestoru. Najdôležitejším dôvodom tejto redukcie je odstránenie kombinatorickej explózie a tým urýchlenie samotných výpočtov a teda celého riadiaceho systému.

Cieľom je pre vopred určený časový interval (časové okno) stanoviť redukovaný kvalitatívny stavový priestor. Tento obsahuje všetky možné stavy systému pre stanovený časový interval a následne je možné tieto stavy vyhodnotiť v nasledujúcom bode metodiky a teda v on-line chybovej analýze.



Obrázok 2: Koncept on-line redukcie stavového priestoru (Manz, 1999).

Redukciu stavového priestoru periodicky vykoná SQMD pozorovateľ (obrázok 2) v troch navzájom nadväzujúcich čiastkových krokoch 2a, 2b a 2c. Detailne obsahujú tieto čiastkové kroky nasledujúce činnosti (Lauber, Göhner, 1999):

- Kvantitatívne stanovenie trajektórií (2a).

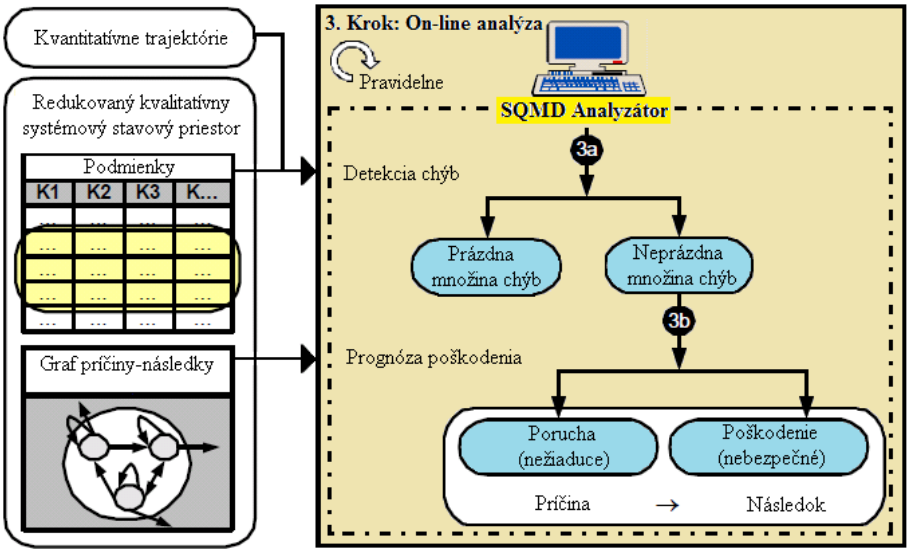
- Redukcia situačného priestoru na úrovni komponentov (2b).
- Kompozícia komponentov (2c).

Výhoda redukcie stavového priestoru na úrovni komponentov je v odstránení kombinatorickej explózie. Analýza a vyhodnotenie sa nevykonáva v celom stavovom priestore, ale len pre časový interval relevantnej časti priestoru. Ďalšou výhodou je priame vyhodnotenie dát z technického procesu na úrovni komponentov. Znamená to, že kvalitatívne veličiny sú nahradené presnými nameranými hodnotami z dát senzorov a aktorov, čím stúpa presnosť modelu (Manz, 1999).

2.5 On-line chybová analýza

V tomto kroku metodiky je potrebné analyzovať redukovaný kvalitatívny stavový priestor z predchádzajúceho kroku. Na základe toho je potom vyhodnotená prognóza poškodenia. Úlohou rozpoznania chýb je analýza kvantitatívnych a kvalitatívnych pomerov vo vnútri časového okna tak, aby bolo možné z tejto analýzy spätne uskutočniť rozhodnutie o možnom chybovom správaní systému.

Koncept on-line analýzy (obrázok 3) je možné rozdeliť na dva čiastkové kroky „Rozpoznanie (detekcia) chýb – krok 3a“ a „Prognóza škody – krok 3b“. Tieto potom dopĺňajú výpočty vykonané analyzátorom. Úlohou rozpoznania chýb je skúmanie (analýza) kvantitatívnych a kvalitatívnych pomerov vo vnútri časového okna tak, aby bolo možné z tejto analýzy spätne uskutočniť rozhodnutie o možnom chybovom správaní systému. Prognóza škody neslúži primárne k diagnóze, ale k rozpoznaniu možných škôd, ktoré sú spôsobené nepožadovaným priebehom.



Obrázok 3: Koncepcia on-line analýzy (Manz, 2004).

2.6 Verifikácia navrhovaných modelov pre bezpečnostne-kritické procesy

Úlohou verifikácie je overiť správnosť navrhovaných modelov slúžiacich na on-line monitoring prevádzky bezpečnostne-kritických procesov v dynamických technologických

systémoch. Overovanie modelov je možné uskutočniť pomocou simulačných nástrojov ako MATLAB.

Pri simuláciách sa nemôže zabudnúť na šumy, ktoré ovplyvňujú výstupy v reálnej prevádzke jednotlivých systémov. Práve tento šum je potrebné zahrnúť respektíve zapracovať do simulačného modelu. Ak by verifikácia nepotvrdila správnosť navrhovaných modelov, tak sa proces metodiky vývoja modelov vracia naspäť do bodu modelovania bezpečnostne-kritických procesov dynamických systémov, kde sa odstraňujú nedostatky zistené pri verifikácii.

3 Záver

Predstavený návrh metodiky na vykonanie modelovo-orientovanej bezpečnostnej analýzy pre dynamické technologické systémy pozostáva zo šiestich krokov, ktoré sme znázornili pomocou UML stavového diagramu.

Literatúra

1. Susanne Manz: *Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme*, January 2004, Forschungsbericht Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart.
2. P. Fröhlich: *Überwachung verfahrenstechnischer Prozesse unter Verwendung eines qualitativen Modellierungsverfahrens*, Institut für Automatisierungs- und Softwaretechnik (IAS), Universität Stuttgart, Dissertation, Universität Stuttgart, 1996.
3. Lauber, P. Göhner: *Prozessautomatisierung 1, Band 1, 3.* Auflage, Berlin Heidelberg, Springer-Verlag, 1999.
4. S. Manz: *On-line monitoring and diagnosis based on hybrid component models*, Institute of Industrial Automation and Software Engineering University of Stuttgart, Germany, 1999.
5. M. Strbo, P. Tanuska, A. Gese, L. Smolarik: *The methodology proposal for the model-oriented safety analysis of dynamical systems*, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, 2014.
6. M. Strbo, P. Tanuska, A. Gese, I. Hagara, L. Smolarik: *Safety Analysis for Complex Dynamic Systems*, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, 2014.
7. M. Strbo: *The Process of preliminary hazard analysis for safety-critical systems*, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava.

Kontakt

Ing. Milan Štrbo, PhD.

Katedra matematiky a informatiky, Pedagogická fakulta, Trnavská univerzita v Trnave
Priemyselná 4, P. O. BOX 9, 918 43 Trnava
milan.strbo@truni.sk