RIADENIE SYSTÉMU S DEFINOVANOU ÚROVŇOU RIZIKA
CONTROL OF SYSTEM WITH DEFINED RISK LEVEL

☩ **Pavol Tomašov, Martin Šuták**
Katedra informačných a zabezpečovacích systémov, Elektrotechnická fakulta ŽU v Žiline
Veľký diel, 010 26 Žilina, tel.: + 421 41 5133 262, Mail: tomas@fel.utc.sk, *sutak@fel.utc.sk*

Abstrakt V predkladanom príspevku sú prezentované základné požiadavky na riadenie systému s definovanou úrovňou rizika. Článok má byť úvodom do opisu teoretického aparátu, ktorý vznikal počas niekoľkých rokov výskumnej práce v tejto oblasti na Katedre informačných a zabezpečovacích systémov. Ide o úpravu, alebo vytvorenie úplne nových častí Teórie informácií, Teórie systémov a Teórie riadenia. Tieto časti sú potrebné pre úlohy analýza a úlohy syntézy v systémoch, kde dominantným atribútom riadenia je definovaná miera rizika. Základným problémom je vytvorenie mechanizmu na ochranu proti ohrozeniam z vnútra aj z okolia riadeného systému. Pre každý mechanizmus na redukciu rizika je potrebná nejaká nadbytočnosť, ktorá má byť do algoritmu riadenia vkladaná presne stanoveným spôsobom.

Summary In the following paper the basic requirements for system control with defined risk level is presented. The paper should be an introduction to describe of theoretical apparatus, which was created during some years of research work in the Department of information and safety systems in this area. It a modification or creation of new parts of Information theory, System theory, and Control theory means. This parts are necessary for the analysis and synthesis tasks in the systems where dominant attribute of control is defined risk level. The basic problem is the creation of protect mechanism again the threats from inside and from controlled system environs. For each risk reduction mechanism is needed some redundancy which should be into control algorithm to put by exactly determined way.

1. IDENTIFIKÁCIA PROBLÉMU

Základným problémom je usporiadanie, alebo úprava riadenia systému tak, aby sa riziko dalo redukovať (ak je väčšie ako jeho vopred definovaná úroveň). Tento problém možno dekomponovať na niekoľko problémov nižšej hierarchickej úrovne. Na dekompozíciu a riešenie jednotlivých problémov sú obvykle používané nástroje, založené na kvalitatívnom prístupe tam, kde nie je dostatok teoretických nástrojov pre kvantitatívnu analýzu, ale najmä pre syntézu.

Predkladaný článok má byť úvodom do opisu teoretického aparátu, ktorý vznikal počas niekoľkých rokov výskumnej práce v tejto oblasti na Katedre informačných a zabezpečovacích systémov. Ide o úpravu, alebo vytvorenie úplne nových častí Teórie informácií, Teórie systémov a Teórie riadenia, použiteľných pre úlohy analýza a úlohy syntézy v systémoch, kde dominantným atribútom riadenia je definovaná miera rizika.

Po špecifikácii základných problémov a nástrojov na ich riešenie budú jednotlivé časti teoretického aparátu opísané v nadväzujúcich článkoch. V úvode sa však treba ešte zastaviť pri stanovení obsahu niektorých základných pojmov.

1.1 Riadenie v zmysle control (vo všeobecnosti aj management) je cieľavedomý pohyb systému v stavovom priestore. Opis takého pohybu možno nazvať postavením úlohy riadenia. Už v tejto fáze treba stanoviť potrebu definovania úrovne rizika.

1.2 Úloha riadenia. Pre riadený systém musí byť spracovaná stratégia:

a) vymedzenie stavového priestoru,

b) spôsob (rovnica) pohybu systému v stavovom priestore,

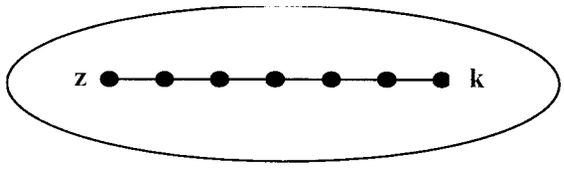
c) cieľ, kam sa má systém v stavovom priestore dostať a cena (napríklad energia) za ktorú sa tam má dostať.

Úlohu riadenia rovnako ako systém možno dekomponovať.

Úlohu riadenia možno optimalizovať podľa kritérií, ktoré sú na to vhodné (cesta v stavovom priestore, čas, alebo počet krokov, energia, alebo cena,....)

1.3 Rozhodovanie. Delí sa na kroky, alebo úseky. Ďalší postup (do ďalšieho úseku) je alebo determinovaný, ak sa podmienky „výpočtu" riadenia nemenia, alebo o ňom treba rozhodnúť pred ďalším krokom v stavovom priestore. Pritom je pohyb spojitý, alebo diskrétny, prípadne diskretizovaný. Rozhodovanie sa deje na základe úplnej, alebo čiastkovej znalosti o stave systému, prípadne spôsobom pokus – omyl.

Spôsob rozhodovania a jeho interpretácia vyplýva zo stratégie. Pre každú stratégiu treba stanoviť osobitné pravidlá pre:



Obr. 1. Stavy systému v stavovom priestore
Fig. 1. The states in the state space

a) definíciu počiatočného stavu z (analýza súčasného stavu systému) podľa Obr. 1. ,

b) definíciu konečného stavu k systému (definícia cieľa riadenia),

c) definíciu prostriedkov na dosiahnutie cieľa,

d) definíciu kritických faktorov úspešnosti stratégie,

e) definíciu trajektórie pohybu v stavovom priestore (vykonanie úlohy riadenia).

f) Pre riadenie s potrebou zvládnutia poruchy (bod x v stavovom priestore) podľa Obr. 2. treba stanoviť ďalšie pravidlá pre:

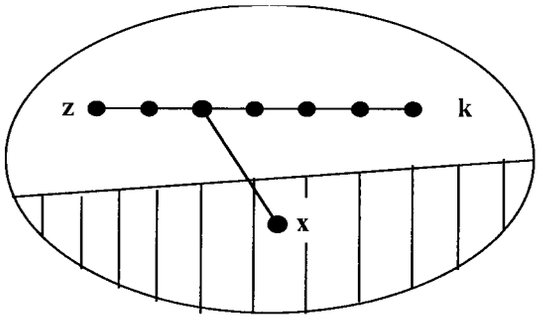
g) definíciu zakázaného sektora stavového priestoru (v obr. šrafovane),

h) definíciu dôsledkov vzniku stavu x,

i) definíciu kvantitatívnych charakteristík prechodu do stavu x,

j) definíciu návratu zo stavu x,

k) dekompozíciu oblasti stavového priestoru, v ktorej sú stavy x a osobitné charakteristiky pre každú časť tejto oblasti.



Obr. 2. Stavový priestor s poruchovými stavmi ***x***
Fig.2. The state space with fault states ***x***

U všetkých častí aparátu musí byť ponúkané riešenie úloh analýzy aj syntézy (V diagram). Požadovaná miera presnosti sa dosahuje iteráciou.

Riadenie, ktorého princíp je na Obr. 2. vyžaduje vždy určitú mieru nadbytočnosti informácie o stave systému. Touto časťou sa zaoberá informačný model riadenia. Príkladom vkladania nadbytočnosti je tvorba nadbytočného kanálového kódu pri garancii úrovne rizika narušenia integrity správy pre bezpečnú komunikáciu.

Pre zvládnutie poruchy a pre návrat systému zo stavu **x** do bezporuchovej oblasti stavového priestoru je potrebná vždy nejaká nadbytočnosť, ktorá umožní vytvorenie mechanizmu na zabránenie účinkov ohrození z vnútra, alebo z okolia riadeného systému. Mechanizmy na ochranu pred ohrozením sú konštruované obvykle na znalostnom princípe. V niektorých prípadoch (kanálová kódovacia teoréma) sa dá dokázať, že konštrukcia takého mechanizmu nie je „vypočítateľná" . Znalostný (expertný) princíp konštrukcie ochranných mechanizmov na redukciu rizika postupne prechádzal do oblasti inteligencie. Najprv s plným využitím inteligencie človeka (experta), neskôr do podpory riadenia expertnými systémami a nakoniec do umelej inteligencie.

Problém riadenia so zaručenou úrovňou rizika možno, aj keď nie celkom presne, zhrnúť do základnej teorémy:

Identifikácia poruchového stavu riadenia systému je možná len na základe využitia nadbytočnosti. Zvládnutie identifikovanej poruchy je možné len na základe uplatnenia pravidiel pre vkladanie nadbytočnosti.

Túto teorému treba dokázať, vymedziť jej platnosť a stanoviť smerovanie jej využitia pri redukcii rizík. Vkladanie nadbytočnosti môže mať jednoduchú podobu kanálového kódu, alebo jednoduchej zálohy funkcie, až po vytvorenie určitého stupňa inteligencie.

Podľa množstva a spôsobu vkladania nadbytočnosti je volený postup pre vytvorenie ochranných mechanizmov na redukciu, alebo potlačenie účinkov ohrození.

Typickou oblasťou, v ktorej sa požaduje riadenie s definovanou úrovňou rizika, sú dopravné systémy. Pre riadenie dopravného systému pomocou HW a SW prostriedkov súčasného technologického stupňa je vytvorenie určitého stupňa inteligencie nevyhnutné. V tomto úvodnom článku sa len poukazuje na potrebu inteligentných dopravných systémov. Relevantné prvky teoretického aparátu budú uvedené spoločne aj pre ostatné prípady riadenia.

2. INTELIGENCIA DOPRAVNÉHO SYSTÉMU

Inteligencia dopravného systému (TS) je základným východiskom pri spracovaní odpovedí na dve základné otázky, týkajúce sa rozhodnutí o koncepcii riešenia TS:

- aký je výkon TS
- aká je kvalita služby poskytovanej TS

Zvýšenie výkonu a kvality služieb dopravného systému nad určitú hranicu je možné len cez uplatnenie inteligencie v procesnej aj operatívnej úrovni riadenia. Predpokladom úspechu je podpora riadenia komponentmi, ktoré sú nevyhnutnou súčasťou inteligentného systému. Podpora riadenia dopravných systémov komponentmi informačných technológií je nevyhnutná, ak sa vyžaduje určitý stupeň inteligencie TS. Vývoj určitého stupňa inteligencie TS je determinovaný stratégiou (dopravnou politikou) štátu, kritickými faktormi úspešnosti stratégie, potrebami zákazníka (používateľa), okolím TS a jeho ekonomickou silou.

Dopravu možno z pohľadu vedy a výskumu považovať za súbor procesov, ktorý začína vývojom nových materiálov a technológií potrebných pre novú kvalitu dopravných prostriedkov a ich pohonov, novú konštrukciu dopravných ciest a končí vývojom integrovaných dopravných systémov.

Vo všetkých fázach životného cyklu TS je otázka jeho výkonu a kvality konfrontovaná s mierou efektívnosti.

Pre riešenie integrovanej témy je identifikovaný problém návrhu systémovej funkčnej, fyzickej a organizačnej architektúry inteligentného TS. Rozhodovanie o vlastnostiach architektúry inteligentného TS sa musí podriadiť cieľom stratégie (dopravnej politiky). Preto je návrh takej stratégie kľúčovým pre implementáciu inteligencie do TS.

Čiastkové úlohy treba riešiť na spoločnom základe, ktorý vychádza z faktu, že každý systém má dve základné charakteristiky (štruktúru a správanie).

Na opis obidvoch charakteristík treba zvoliť formálne opisné, výpočtové a modelovacie nástroje. Kým štruktúra systému je dôležitá najmä pre riešenie úloh analýzy, správanie je charakteristikou, využívanou pri syntéze a prevádzke systému.

Inteligentné dopravné systémy (ITS) majú okrem všeobecných systémových charakteristík ďalšie vlastnosti, ktorými ich možno podrobnejšie špecifikovať. Ide o základné atribúty inteligencie:

- schopnosť pamätať si,
- schopnosť učiť sa,
- schopnosť odvodzovať.

Tieto atribúty má ITS už pri svojom vzniku, alebo ich získava počas doby života. Pre jednotlivé atribúty treba postaviť elementy teoretického aparátu. Ide najmä o:

- systémovú architektúru ITS (funkčná, informačná, fyzická, komunikačná),
- konštrukciu ITS,
- inštaláciu ITS,
- základné úlohy pre prevádzku ITS počas celého životného cyklu
- manažment ITS,
- údržba ITS,
- prevádzka ITS.

Pre správanie sa ITS sú potrebné nástroje na opis:

- temporality,
- kauzality,
- dynamiky,
- bezpečnosti,
- analýzy rizík,
- mechanizmov na redukciu rizika.

Oddelené riešenie charakteristík a úloh ITS nerieši podstatnú časť identifikovaných problémov úplne. Efektívnosť integrovaného riešenia je evidentná pri narastaní podpory systému cez komponenty IT. Integrované riešenie uplatní inteligenciu, vloženú do TS viacnásobne. Aby sa získala pružnosť využitia inteligencie TS, treba vyvolať širokú škálu výskumných aktivít v oblasti IT, Informačnej teórie a Systémovej teórie. Závažným argumentom pre vyvolanie výskumných aktivít tejto témy je vysoký počet mŕtvych v cestnej doprave.

3. CIELE INTEGROVANÉHO PRÍSTUPU

Stanovenie cieľov je veľmi závislé od naliehavosti riešenia, doby implementácie a ďalších faktorov. Každý zámer vkladania inteligencie do riadenia dopravného systému by mal obsahovať najmä tieto ciele:

- Vypracovanie stratégie pre implementáciu ITS a využitie ich služieb s rešpektovaním používateľských potrieb
- Architektúra služieb ITS
- Definovanie potrebných elementov pre otvorený trh produktov inteligentných TS (ITS) v Európe
- Vytvorenie mostu medzi komunitou ITS a komunitou informačných technológií
- Zdôvodnenie alokácie základnej infraštruktúry pre naplnenie služieb ITS
- Podpora identifikácie nových oblastí výskumu a demonštrácia ich potrieb
- Spracovanie odporúčaní – podľa legislatívy európskych štátov – pre zvyšovanie kvality dopravy s ohľadom na bezpečnosť všetkých účastníkov
- Spracovanie odporúčaní pre dopravnú politiku jednotlivých štátov a pre medzinárodné dopravné inštitúcie v oblasti budovania ITS

Ide o hlavné ciele, potrebné na vloženie inteligencie do aktivít TS. Stupeň priority jednotlivých cieľov je závislý od druhu TS. Napríklad pre TS cestnej dopravy bude mať prioritu použitie inteligencie na zvýšenie bezpečnosti. Redukcia rizík v cestnej doprave má takmer vyčerpané extenzívne metódy, preto musia nové metódy využiť vloženú inteligenciu.

4. SPÔSOB DOSIAHNUTIA CIEĽOV

Naplnením cieľov zámeru vkladania inteligencie sa významne zmenia charakteristiky a parametre doterajších dopravných systémov. Samotné vyriešenie postavených cieľov však neznamená automatickú zmenu parametrov dopravného systému. To sa stane až po realizácii výsledkov. Na túto realizáciu sú potrebné kladné výstupy z jednotlivých úrovní tvorby rozhodnutí.

Riešenie akéhokoľvek systému v celom životnom cykle má štyri vzájomne prepojené sady rozhodnutí:

- politické,
- ekonomické,
- sociálne,
- technické.

Kým politické rozhodnutia majú najvyššiu váhu a odvíjajú sa od základnej stratégie (dopravnej politiky štátu), ich presnosť opisu systému je minimálna. Ide naozaj „len „ o stratégiu riešenia a prevádzky systému. Váha politického riešenia je najvyššia preto, že všetky ďalšie druhy riešení volia kritické faktory úspešnosti podriadené strategickým cieľom.

Ekonomické riešenie systému sa už zaoberá základnými charakteristikami systému, z ktorých má dominanciu ekonomická efektívnosť, návratnosť vloženej investície, voľné investičné prostriedky a niektoré ďalšie. Harmonogram ekonomických riešení systému je podriadený stratégii, určenej v úrovni politických riešení.

Sociálne riešenie systému berie do úvahy aj vplyvy systému na svoje okolie. Ide najmä o vplyv na zákazníka systému, ale nepriamo aj na riešenie sociálnych problémov okolia.

Technické riešenia sú podstatnou časťou náplne integrovaného splnenia cieľov. Tieto riešenia sú však prvým predpokladom na to, aby sa v ostatných troch úrovniach prijalo rozhodnutie o ich aplikácii.

Pri veľkej miere abstrakcie možno stanoviť smerovanie postupu na dosiahnutie cieľov takto. Stupeň inteligencie TS determinuje možnosti ochrany pred ohrozením dopravného procesu. ITS sa dokáže vyhnúť takým ohrozeniam, ktoré jeho inteligencia dokáže identifikovať a následne vyvolať akciu na zabránenie nežiadúcej udalosti (nehody). Treba však rešpektovať fakt, že vložená inteligencia zvyšuje náklady na TS a niekedy redukuje aj jeho priepustnosť.

5. PRÍSTUP K REALIZÁCII CIEĽOV

Vypracovaním **stratégie pre implementáciu ITS** bude k dispozícii prvý nástroj, ktorým sa dá posudzovať efektívnosť uspokojovania potrieb zákazníka dopravným systémom. Pri paramet-rizovanej stratégii sa dajú stanoviť kritické faktory úspešnosti a z nich odvodiť výkonové charakte-ristiky ITS (stupeň inteligencie, ekonomická efektívnosť, bezpečnosť, spoľahlivosť atď.).

Architektúra služieb ITS umožní objektívne zdôvodnenie alokácie služieb a najmä ich úrovne vo vzťahu k potrebám zákazníka a k efektívnosti vynaložených prostriedkov na rozvoj ekonomickej sily mesta, regiónu, štátu.

Definovanie elementov pre trh produktov ITS vytvorí pevné pravidlá kooperácie medzi odvetviami hospodárstva v potrebnom časovom intervale. Sem patria aj podklady pre marketingové štúdie ITS.

Most medzi komunitou ITS a komunitou IT významne zvýši efektívnosť prostriedkov, vložených do technického rozvoja obidvoch odvetví. Rovnako to platí aj pre podporu identifikácie nových oblastí výskumu.

Spracovanie odporúčaní pre dopravnú politiku štátu pripraví metodiku exaktného stanovenia smerov rozvoja jednotlivých časti dopravného systému.

Za podstatnú zmenu kvality dopravného systému po vyriešení cieľov treba považovať stupeň bezpečnosti dopravy pre jednotlivé subsystémy. Z analýzy rizík sú výsledky prenese-né do požiadaviek na stupeň inteligencie dop-ravného systému, ktorý je zárukou neprekročenia akceptovateľného rizika. Cieľom je umožnenie 4. stupňa bezpečnosti (SIL4) pre podstatnú časť dopravných procesov, v ktorých môže prichádzať k poškodeniu zdravia, alebo života. „Vedľajším" produktom zvýšenia bezpečnosti je profit v efektívnosti dopravného systému.

Všetky uvedené charakteristiky sú v strede záujmu odbornej verejnosti aj poskytovateľov dopravných služieb na celom svete. Splnením cieľov dôjde v podstatnej časti problémov k vyrov-naniu rozdielov v riešení inteligencie TS medzi krajinami (Kanada, Japonsko, Francúzsko, Nemec-ko) v oblasti koncepcie a architektúry ITS.

Vložená inteligencia dokáže meniť (k lep-šiemu) základné charakteristiky TS (štruktúra a správanie). Nové charakteristiky umožnia nové funkcionality TS a jeho účinnejšiu kooperáciu s okolím.

6. POTREBA A RELEVANCIA RIEŠENIA IDENTIFIKÁCIA RIZÍK

Úloha riadenia s pevným koncom je postavená tak, aby integrálnym kritériom optimality bola hodnota akceptovateľného rizika pri fixovaných hodnotách efektívnosti. Teoretické nástroje musia byť použiteľné pre výpočet rizika systémov riadenia, ktoré na zaručenie bezpečnosti používajú preventívne, alebo ochranné metódy. Model musí byť postavený tak, aby boli využiteľné dostupné nástroje na zložité výpočtové postupy. Výstupy modelovania sa musia dať porovnať s výsledkami doterajších metód, založených na skúse-nostnom princípe. Použiteľnosť výstupov modelu sa pred-pokladá pri úlohách analýzy aj syntézy. Kľúčovým problémom projektu je vypracovanie podkladov pre výpočet klasifikovaných porúch pri dynamickom riadení viacerých konjunkčných náhodných procesov s viacrozmerným rozdelením. Riešenie je súčasťou podpory prechodu systémov riadenia kritických procesov na nový technologický stupeň – inteligentné dopravné systémy.

Vloženie inteligencie do TS je problém, ktorý pokrýva celú škálu oblastí (riadenie kritických procesov, umelá inteligencia, pravidlá a kritéria rozhodovania, etc.). Mení sa pohľad na posudzovanie vlastností inteligentného objektu. V minulosti sa šikovný (smart) subsystém nie celkom oprávnene považoval za inteligentný. Pre jednotlivé druhy dopravy sa dá zjednotiť súbor kritérií na posudzovanie bezpečnosti, čo prinesie v budúcnosti zásahy do dopravnej politiky štátov. Politické riešenie stratégie TS má spätnú väzbu aj na technické riešenie.

Technicko-ekonomická stránka výsledkov riešenia má byť sledovaná aj z pohľadu plynulosti a bezpečnosti cestnej dopravy a ochrany životného prostredia.

7. INTEGRÁCIA

Vo všeobecnom inteligentom dopravnom systéme (ITS) možno identifikovať niekoľko samostatných systémov, ktoré sú schopné samostatne vykonávať čiastkové činnosti, alebo spolupracovať s inými systémami. Ide napríklad o subsystémy:

- inteligentný systém vedenia vozidla,

- inteligentný úsek,
- inteligentná križovatka,
- inteligentná garáž,
- inteligentný parkovací systém,
- inteligentný systém mestských komunikácií,
- inteligentný systém verejných komunikácií,
- inteligentný diaľničný systém,
- inteligentný železničný systém.

Tieto subsystémy kooperujú cez inteligentné komunikačné rozhranie a zároveň komunikujú s:

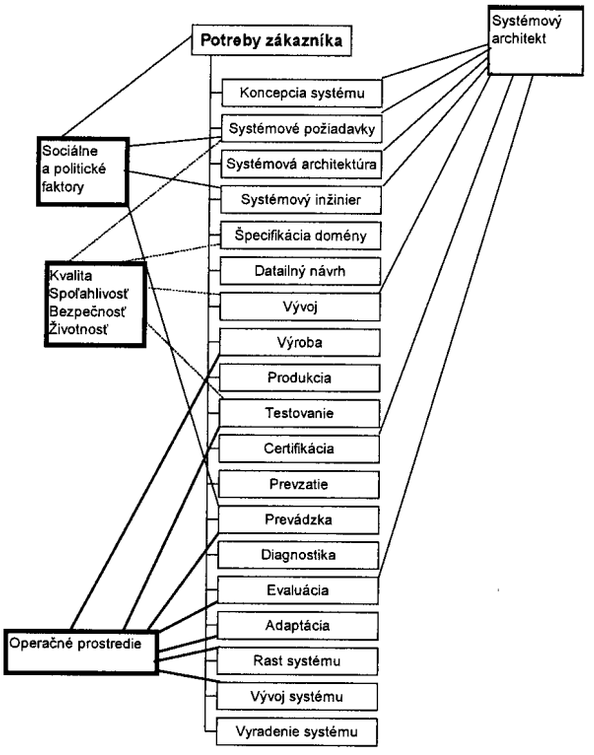
- platobným systémom
- záchranným systémom
- policajným systémom
- colným systémom
- navigačným systémom.

ITS je určite rozsiahlym systémom. Jeho správanie ani štruktúru nemožno opisovať v jednom stupni. Musí sa využiť princíp dekompozície sys-tému. Tým sa síce dá vysporiadať s rozsiahlosťou systému, ale komplikuje sa vyjadrenie temporality, dynamiky a kauzality systému. Situácia sa kom-plikuje spôsobom rozhodovania ITS. Toto vytvára široký priestor pre kooperáciu niekoľkých vedných aj technologických oblastí. Ide najmä o formálne metódy opisu systému a o metódy modelovania. Vedecká komunita má v riešení koncepcie ITS mnoho príležitostí dostať výsledky separátneho výskumu pod „jednu strechu" ITS. Na spoločnú koncepciu ITS nadväzuje kooperácia technológií a prevádzky rozsiahlych TS. Na tejto kooperácii sa podieľajú mnohí dodávatelia a mnohé profesie v prevádzke TS počas jeho celého životného cyklu.

8. MULTIDISCIPLINÁRNY PRÍSTUP

Príklad funkčnej architektúry inteligentného dopravného systému v celom jeho životnom cykle je na Obr.3.

ITS nemožno vytvoriť len rozvojom jednej disciplíny. Podiel jednotlivých disciplín na riešení krokov postupu v obrázku musí byť vyvážený. Koordinácia týchto disciplín je jedným z hlavných kritických faktorov úspešnosti celej stratégie rozvoja ITS.



Obr. 3. Príklad funkčnej architektúry ITS
Fig.3. An example of function ITS architecture

9. ZÁVER

Algoritmus riadenia systému obsahuje štyri základné operácie manipulácie s informáciou. Ide o získavanie, úschovu, prenos a transformáciu informácií. Pri všetkých týchto operáciách môže vzniknúť chyba. Chyby vedú k nesprávnemu vytvoreniu riadiacej veličiny (povelu na zmenu stavu), alebo k nesprávnej interpretácii riadiacej veličiny (prechod do nepríslušného stavu). Pre definovanie úrovne bezpečnosti treba tieto chyby klasifikovať a nájsť opatrenia na zaručenie akceptovateľného výskytu (pravdepodobnosti, alebo intenzity) nezistených, alebo neošetrených chýb. Chyby možno klasifikovať do tried:

a) tok porúch technických prostriedkov (vozidlá, dopravná cesta, zabezpečovacie zariadenia,...),

b) tok „porúch" v činnosti obsluhujúceho personálu,

c) pohyb vozidla v riadenom priestorovom úseku,

d) vonkajšie vplyvy (vis major, cudzie teleso na dopravnej ceste,...).

Riešenie tohto problému by bolo jednoduché, keby šlo o disjunkčné procesy. K tomuto zjednodušeniu sa uchyľovali doterajšie postupy pri analýze nehôd. V skutočnosti však ide o kojunkčné procesy, pre ktoré treba stanoviť marginálne, spoločné a podmienené rozdelenie pravdepodobnosti.

Na základe analýzy európskych štandardov pre bezpečnosť pri riadení kritických procesov treba vypracovať kritiku doterajších postupov výpočtu a hodnotenia rizík. Novým prvkom i v oblasti teórie riadenia bude vymedzenie presahu konjukčných

čiastkových náhodných procesov s viacrozmerným rozdelením. Na základe týchto výsledkov možno zostaviť model pre výpočet výsledného pôsobenia čiastkových procesov.

Výsledky modelovania čiastkových procesov sa dajú indukovať do ďalších spôsobov riadenia kritických procesov (okrem preventívnych, budú vzaté do úvahy aj ochranné opatrenia pre odvrátenie ohrozenia systému)

V aplikačnej fáze pôjde o vypracovanie súboru odporúčaní pre rutinné postupy stanovenia akceptovateľného rizika, vypracovanie odporúčaní pre rutinný postup stanovenia úrovne bezpečnosti zabezpečovacieho systému pre stanovenú mieru rizika a o rozširovanie dosiahnutých výsledkov .

Pri riešení problému redukcie rizika možno použiť doposiaľ vypracované postupy, ich kombinácie a niektoré nové prvky teoretického aparátu. Postup na dosiahnutie cieľov spočíva v cielenom vkladaní nadbytočnosti a možno ho zhrnúť do týchto krokov:

a) Špecifikácia funkcií dopravného procesu. Pre tento krok existujú dva základné postupy:

- pre dohodnuté funkcie sa vyberá štruktúra technických, personálnych a programových prostriedkov na základe skúseností z predošlých aplikácií. podrobne sa špecifikujú požadované
- funkcie procesu vo väzbe na riadiaci systém bez ohľadu na budúcu skladbu jeho komponentov.

b) Model štruktúry udalostí pre postavenú úlohu riadenia.

Pri definovaní modelu udalostnej štruktúry je kardinálnym krokom označenie udalostí. Treba zaviesť osobitné označenie, ktoré dáva dostatok informácií o úlohe udalosti v systéme a má požadované matematické vlastnosti.

c) Stanovenie hraníc konjuktivity čiastkových procesov.

V tomto bode sa použije aparát dostatočných štatistík a základné operácie teórie pravdepodobnosti. Z výsledkov tohoto bodu postupu možno priamo prejsť k stanoveniu podielu čiastkových procesov na celkovom riziku, ak sú stanovené chránené hodnoty riadeného procesu.

d) Mapovanie miery rizika do charakteristík zabezpečovacieho systému

e) Porovnanie výsledkov modelovania s dote-rajšími výsledkami analýzy nehôd

V pokračovaniach tohto článku budú pod-robne rozvedené jednotlivé časti teoretického apa-rátu, potrebné pre postavenie modelu riadenia dopravného systému s definovanou mierou rizika.

LITERATÚRA

[1] HENNESSY, M.: *Algebraic Theory of Processes*, The MIT Press, Cambridge, Massachusets, 1988.

[2] REITER, M. - KENNETH B. - VAN RENESSE R.: *A security architecture for fault-tolerant systems,* Technical Report TR93-1354, Department of Computer Science, Cornell University (June 1993). 29 pages.

[3] GONG, Li, SHACHAM N.: *Elements of trusted multicasting*, Proceedings of the IEEE International Conference on Network Protocols (Boston, Massachusetts, October 1994).

[4] STEINER, M. - TSUDIK, G., Waidner, M.: *Diffie-Hellman key distribution extended to group communication,* Proceedings of the 3rd ACM Conference on Computer and Communications Security (March 14–16, 1996). 7 pages.

[5] TOMAŠOV, P. - RÁSTOČNÝ, K. - ZAHRADNÍK, J.: *Apparatus for analysis and synthesis of system with defined level of safety.* In. TEMPT '97, 10-th International scientific conference. Sofia, 1997. pp 152-160.

Článok bol spracovaný za podpory grantovej úlohy VEGA 1/8182/01: Teoretické podklady pre výpočet akceptovateľného rizika v riadení dopravného procesu, najmä železničného a úlohy VEGA1/8261/01: Uplatnenie umelej inteligencie v riadení kritických procesov.