



**Společná
Laboratoř spolehlivosti systémů**

Fakulta dopravní ČVUT Praha

Konviktská 20, 11000 Praha 1
tel. 24221721/416 (fax), 417(sekr), 418, 413 (lab)
e-mail: mirko@fd.cvut.cz

Ústav informatiky AV ČR

18207 Praha 8, Pod vodárenskou věží 2
tel. 6606/2080, 821639 (fax)
e-mail: mirko@cs.cas.cz

Obecná hlediska spolehlivosti a bezpečnosti technických systémů

Výzkumná zpráva č. LSS 100/01

Autor: Doc. Ing. Mirko Novák, DrSc

Praha, červen 2001

Souhrn:

V této zprávě jsou charakterizovány hlavní (mě se jevící) problémy spolehlivosti a bezpečnosti technických, zejména dopravních systémů. Na příkladě systémů řízení dopravy v silničních tunelech pak prezentuji některá základní hlediska, která by při řešení otázek bezpečnosti a spolehlivosti složitějších a závažnějších systémů měla být brána v úvahu. Zejména by přitom měla být respektována okolnost, že většina takových systémů je heterogenní povahy, kde významnou roli hraje spolehlivost interakce mezi jednotlivými funkčními bloky, uvažovaný systém tvořícími a též spolehlivost interakce systému, resp. jeho jednotlivých komponent s lidským činitelem. V závěru této zprávy ukazují též některé přístupy k analýze spolehlivosti a bezpečnosti takových systémů.

Tato zpráva byla vypracována v souvislosti s řešením výzkumných grantů AV ČR č. S 1124002 „Analýza spolehlivosti rozsáhlých hybridních technických a biologických systémů“, MDS ČR č.803/110/105 „Analýza a řízení rizik v tunelech na pozemních komunikacích“ a výzkumného záměru MDS ČR č. VZ 02100024 „Automatické systémy v dopravě, diagnostika dopravních systémů a procesů“.

Obsah:

Souhrn.....	str. 2
1. Úvod.....	str. 2
2. Heterogenní systémy.....	str. 3
3. Interakce v heterogenních systémech.....	str. 4
4. Možnosti zvyšování spolehlivosti systémů.....	str. 13
5. Literatura.....	str. 15

1. Úvod

Spolehlivost a bezpečnost se stávají stále více dominantními kritérii při posuzování vlastností technických systémů, zejména pak, jestliže se jedná o systémy, které interagují s lidským činitelem. To platí, ať již se jedná o interakci s člověkem jako individuálním činitelem, či o interakci se skupinami lidí nebo posléze o interakci s životním prostředím lidské společnosti.

Při takovém posuzování nejde jenom o to, aby jistý systém splňoval na něj dané požadavky co do jeho výkonů, ale že jde též a zejména o to, aby tyto výkony byl schopen podávat po dostatečně dlouhou dobu (či v dostatečně velkém intervalu jiných nezávisle proměnných), a to bez poruch a bez odchylek od požadovaných hodnot o více než je dovolený limit – to jsou hlavní aspekty spolehlivosti.

Aspekt funkční bezpečnosti se pak týká především toho, aby ani činností uvažovaného systému, ani jeho selháním nedošlo k ohrožení člověka či lidské společnosti ani hodnot jimi užívaných.

Oba tyto aspekty spolu sice úzce souvisí, totožné však nejsou:

systémy nelze považovat za dostatečně bezpečné, nejsou-li též odpovídajícím způsobem spolehlivé, protože zejména u dopravních systémů může jejich funkční selhání vést ke značnému ohrožení bezpečnosti jednotlivce i společnosti.

To platí zejména o systémech pro zabezpečení dopravy.

Dopravní zabezpečovací systém, který by sice byl schopen podávat velmi pozoruhodné výkony, ale podával by je přitom nespolehlivě a v nedostatečně velkém intervalu nezávisle proměnných, by mohl být sice zajímavý, ale pro reálné aplikace by mohl být zčásti či dokonce zcela bezcenný. Případně by mohl být dokonce nebezpečný.

Nezbytnou podmínkou pro činnost každého reálného systému pak je, aby měl svůj specifický informační subsystém, který pro jeho potřebu zajišťuje nezbytný příjem, zpracování, uchovávání, předávání a využívání informací.

Existenci a řádnou funkci informačního subsystému můžeme proto považovat za nutnou (avšak nikoliv postačující) podmínku pro existenci a řádnou funkci všech reálných systémů.

2. Heterogenní systémy

Reálné dopravní systémy i systémy pro zabezpečení dopravy mají vždy heterogenní strukturu.

S hlediska struktury lze totiž systémy obecně klasifikovat na:

- systémy amorfní,
 - systémy homogenní
- a
- systémy heterogenní.

Amorfní systémy nemají žádnou výraznou vnitřní strukturu a nepředstavují pro tuto studii předmět hlubšího zájmu.

Homogenní i heterogenní systémy výraznou vnitřní strukturu mají. V ní lze specifikovat jednotlivé funkční bloky FB_i , více či méně specializované. Tyto bloky realizují jednotlivé dílčí systémové funkce F_i , z nichž je pak syntetizován soubor výsledných systémových funkcí F , charakterizující činnost celého uvažovaného systému.

U homogenních systémů jsou všechny dílčí funkční bloky identické, u heterogenních systémů tomu tak není.

Veškeré reálné systémy (kromě amorfních) se sestávají z vzájemného propojení jednotlivých funkčních bloků, kterých v jistém systému může být M (výjimku tvoří elementární systém, sestávající se pouze z jednoho funkčního bloku, $M=1$).

Jak pro analýzu, tak pro syntézu systémů složených z jednotlivých funkčních bloků FB_m jsou kardinálními otázkami zejména :

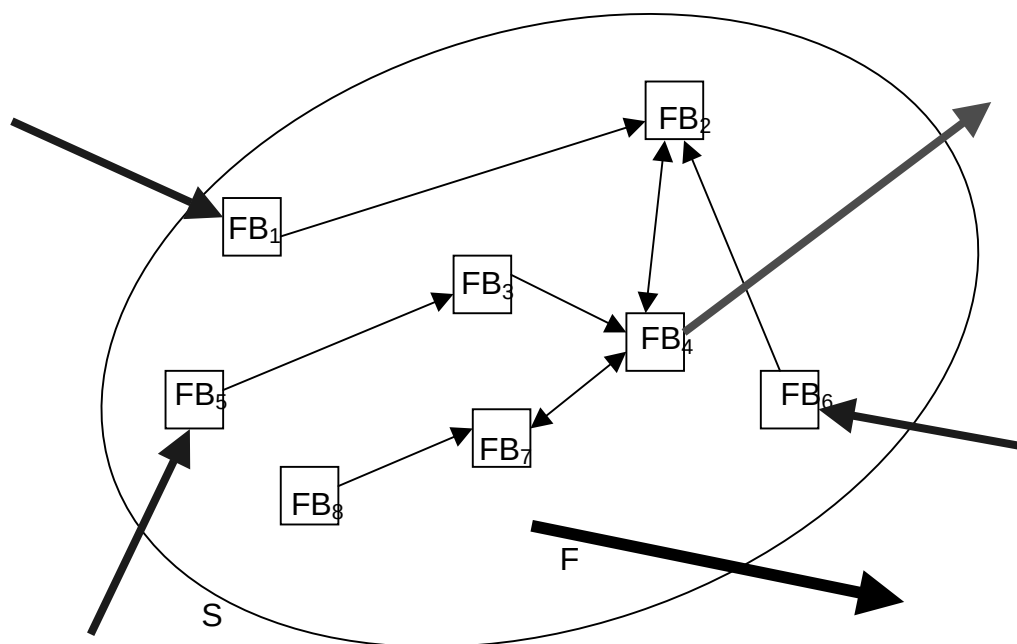
- Jak interagují jednotlivé FB mezi sebou v různých topologiích jejich uspořádání a propojení ve struktuře celého uvažovaného systému?
- Jak závisí systémové funkce F celého systému na dílčích systémových funkcích F_m jednotlivých FB ($m=1\dots M$)? Přitom musíme ovšem mít na zřeteli, že F i F_m mohou být celými soubory dílčích systémových funkcí, tedy

$$F = \{F_k\}_{k=1\dots K}, \quad F_m = \{F_{mk}\}_{k=1\dots K, m=1\dots M} \dots\dots\dots(1)$$

- Jaká je souvztažnost mezi funkční spolehlivostí jednotlivých FB a funkční spolehlivostí a bezpečností celého systému?

3. Interakce v heterogenních systémech

Mezi jednotlivými dílčími funkčními bloky dochází k vzájemné výměně informací, jak je schematicky naznačeno na obr. 1.



Obr. 1: Příklad systému S sestávajícího se z 8mi vzájemně interagujícími FB_i . Modré toky představují interakci se vnějším světem. Červená šipka označuje výstup informace pro vnější svět. Černá šipka představuje výsledný soubor systémových funkcí F realizovaných uvažovaným systémem.

Uvažujme systém skládající se z jistého počtu M funkčních bloků FB_m , $m=1\dots M$.

Každý z těchto funkčních bloků realizuje jistý dílčí soubor systémových funkcí F_m . Ve vzájemné souhře a interakci jednotlivých FB_m je z těchto dílčích systémových funkcí vytvářena výsledná systémová funkce F .

Aby však k takovéto souhře mohlo docházet, musí často mezi jednotlivými funkčními bloky probíhat vzájemná výměna informací, a to velmi koordinovaně.

To je tím závažnější, jestliže proces realizace výsledné systémové funkce probíhá v jisté časové dynamice. Vzájemně koordinovaně realizovaná výměna informací mezi jednotlivými funkčními bloky je pak jeho nutnou podmínkou.

Styk mezi jednotlivými FB_m zprostředkují rozhraní IF (interface, synapse). Pro činnost a vlastnosti celého systému mají kritický význam, protože na styku jednotlivých FB_m v systému působících dochází velmi často k potřebě překladu vzájemně předávané informace.

Jednotlivé FB_m mohou totiž své informace zpracovávat s rozličnými abecedami A_m i rozličnými gramatikami G_m . Příslušná rozhraní pak zajišťují potřebné překlady předávaných informací tak, aby přijímající funkční blok spolehlivě a bezpečně rozuměl informaci, kterou mu předává funkční blok vysílající.

Se zřetelem k sortimentu FB_m a rozhraní IF_m v systému působících můžeme rozlišovat heterogenní systémy:

- systémy s homogenními FB_m a rozdílnými IF_m ,
- systémy heterogenní s rozdílnými FB_m i IF_m .

V obou těchto případech mají rozhraní zásadní důležitost.

Funkce jakéhokoliv systému se vztahují k základním kategoriím hmoty (dále též jen H), energie (dále též jen E), a informace (dále též jen I), a k jejich vzájemným vztahům.

Vzhledem k problematice spolehlivosti a bezpečnosti nás pak zvláště zajímají vztahy činnosti systému ke kategorii informace, kterou zde budeme chápat ve smyslu Následující pracovní definice:

Informace I jsou taková data D, která příjemce je schopen využít ke splnění svých cílů nebo která vedou ke změně cílů jeho chování.

Takto chápaný pojem I je ovšem nutně subjektivní a je zřejmé, že z téže množiny dat D mohou různí příjemci vytěžit různá množství informace, resp. informace různé kvality.

Budeme-li se zabývat obecnými heterogenními systémy, složenými z jednotlivých, ať již stejných či rozličných FB_m , nahradíme ve výše uvedené pracovní definici pojem příjemce pojmem přijímajícího funkčního bloku – je však zřejmé, že adjektivum přijímající, resp vysílající FB se uplatní v souladu se způsobem přenosu informace I také mezi jednotlivými FB_m .

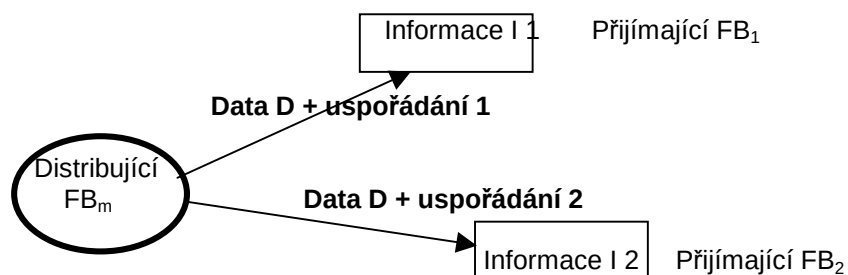
Informaci I je tedy v uvedeném pojetí třeba přisuzovat nejen kvantitativní, ale též kvalitativní charakteristiky (podobně jako je tomu i v případě kategorie energie E).

Bylo by dokonce možno připustit, že jistá data mohou být dvěma různými je přijímajícími FB interpretována jako zcela opačné informace a tedy že by mohlo dojít při jejich interakci též k dílčí či plné negaci informace.

Zabývejme se situací u FB_m vysílajícího data. Přitom může jít o případ skutečného *pouhého vysílání dat*, bez zřetele na to, jaké informace z nich přijímající FB_m vytěží nebo o případ, kdy ve vysílajícím FB_m jsou tato data *záměrně upravena*

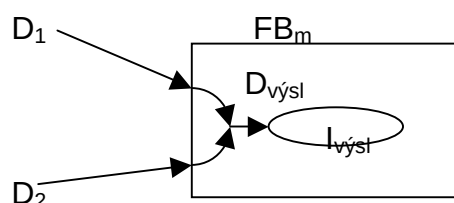
tak, aby z nich přijímající FB mohl vytěžit pouze jistou informaci. To může být jak v případě adresného, tak neadresného vysílání (obecná distribuce dat, broadcasting).

Obecně musíme připustit i případ, kdy do jistých obecně šířených dat D bude jejich distributor *vkládat záměrně* taková uspořádání, která jistou skupinu přijímajících FB_m povedou k vytěžení jiné informace než jakou z nich může vytěžit jiná skupina FB (viz obr.2).

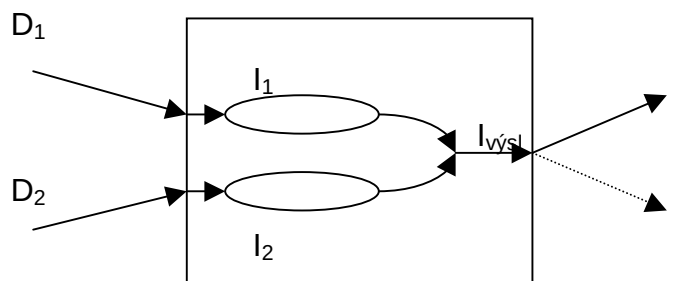


Obr.2. K distribuci informace.

Alternativou této situace je případ, kdy na tentýž přijímající FB mohou působit dva či více FB_m , vysílajících data. Pak dojde u téhož přijímajícího FB k interakci dvou toků dat, z nichž se těží informace. Může dojít k interakci již mezi toky dat (viz obr.3) ale též k interakci mezi informacemi, z nich vytěženými (viz obr.4).



Obr.3. K interakci dvou toků dat



Obr. 4. K interakci mezi informacemi, z dat vytěžených.

Protože jsme již učinili předpoklad, že informace nemá jen svou kvantitativní, ale též kvalitativní charakteristiku, je třeba se z tohoto hlediska zamyslet nad procesem interakce informací.

Ten nemusí být jen superpozicí, ale může být podstatně složitější povahy. Obecně může mít silně nelineární charakter. Lze též připustit negaci dílčích informací interakcí s informacemi jinými, vzájemné maskování informací či stimulování vzniku jisté informace interakcí s informací jinou. Některé nové informace mohou též být získány procesem vytěžování z dat (data-mining).

Kdybychom byli schopni přesněji informaci charakterizovat co do její kvantity i kvality, mohli bychom uvažovat o algebře operací, kterými mohou informace navzájem interagovat.

Jednotlivé FB_m se mohou stýkat buď po dvojicích či vícenásobně.

Je zřejmé, že spolehlivost funkce celého systému závisí nejen na spolehlivosti funkce jednotlivých dílčích FB_m , z nichž se skládá, ale též na spolehlivosti funkce rozhraní, tedy především na spolehlivosti překladů, uskutečňovaných na všech rozhraních, jejich prostřednictvím jednotlivé FB_m interagují.

Rozhraní mohou však kromě vlastního překladu uskutečňovat ještě jiné funkce, zejména paměťové, mohou zpožďovat přenos jistých informací o určitý časový interval a tím ovlivňovat souhru jednotlivých funkčních bloků v systému působících, mohou realizovat prahové funkce a může v nich též docházet ke kombinaci různých informací či vytěžování skrytých informací. Všechny tyto činnosti lze pak zahrnout do zobecněného pojmu překladu, který v takové interpretaci chápeme jako proces obecně nelineárního vzájemného převodu informace mezi interagujícími funkčními bloky. Tento proces ovšem může být realizován v jednotlivých uzlech systému rozličné časové dynamice.

Funkční vlastnosti celého uvažovaného systému i jednotlivých FB_m , ze kterých je složen, jsou vyjádřeny soubory systémových funkcí F_m . Ty závisí obecně

na struktuře systému St , resp. na vnitřní struktuře St_{Fbm} jednotlivých FB_m ,

na souboru systémových parametrů $X = \{x_i\}$, $i=1...N$ a

na vektoru nezávisle proměnných $P = \{p_j\}$, $j=1...J$.

Jednotlivé složky p_j vektoru nezávisle proměnných P mohou mít různý fyzikální význam, vždy však je v reálných případech mezi nimi zahrnut čas $p=t$, který probíhá nevratně bez možnosti našeho ovlivnění jeho průběhu.

Uvažujme nyní obecný dynamický systém, u něhož budeme brát v úvahu jeho chování za působení nezávisle proměnných.

Vydeme z toho, že spolehlivost celého systému $H(X,P)$ ^{*)} je interpretována jako pravděpodobnost, že celý soubor F jeho uvažovaných systémových funkcí F_k se v daných intervalech ΔP nezávisle proměnných P nebude odchylovat od požadovaných hodnot F_0 o více než dovolené odchylky systémových vlastností ΔF (přičemž intervaly ΔP i dovolené odchylky ΔF musíme chápat jako vzdálenosti ve případně vícerozměrných prostorech $\{P\}$, resp. $\{F\}$, měřené vhodnými metrikami).

Takto chápanou spolehlivost je možné též reprezentovat pravděpodobností, že pro dané ΔP nevybočí trajektorie $\Psi(P)$ - tzv. čára života (life curve) - vektoru

^{*)} V anglosaské literatuře je spolehlivost často označována symbolem R od reliability. Protože však zde tento symbol používáme pro označení oblasti (region) zvolil jsem pro symbol spolehlivosti písmeno H .

parametrů X uvažovaného systému z hranic tzv. oblasti přijatelnost R_A .

Ponecháme nyní stranou problematiku metod pro vyšetřování R_A a budeme předpokládat, že jsme, alespoň v jisté části prostoru X a s jistou neurčitostí schopni R_A stanovit.

Zjednodušíme dále naše úvahy tím, že budeme uvažovat pouze časově závislý dynamický systém, tj. případ $P = t$.

V obecné teorii spolehlivosti a bezpečnosti systémů je pak vyjadřováno tvrzení, že pro dostatečně velké t musí u reálného, tedy uzavřeného systému nakonec vždy každá trajektorie $\Psi(t)$ vybočit z hranic R_A . Mohou sice nastat případy, kdy časová závislost $x_i(t)$ některých parametrů systému probíhá tak, že po předchozím vybočení z hranic oblasti přijatelnosti R_A se na jistou dobu vektor X může vrátit dovnitř R_A , jestliže však $t \rightarrow \infty$, platí, že bez dostatečných dodávek hmoty H , energie E a informace I dodávaných do uvažovaného systému zvenčí se vektor X dovnitř R_A trvale vracet nemůže.

Abychom tedy dosáhli toho, že vektor $X(t)$ se bude pohybovat uvnitř R_A po neomezenou dobu, museli bychom mít k dispozici neomezené zdroje hmoty H , energie E a informací I , které ovšem může poskytnout pouze celý neomezený (otevřený) vesmír.

Toto tvrzení sice koresponduje s veškerými dosavadními zkušenostmi lidstva, jeho exaktní důkaz však není znám.

Průběh výsledné trajektorie $\Psi(t)$ vektoru $X(t)$, reprezentující vývoj celého systému je ovšem ovlivněn dílčími průběhy trajektorií $\Psi_m(t)$ jednotlivých FB_m . Ty nemusí být ovšem vždy navzájem shodné (a to ani u homogenních systémů) a mohou se od sebe lišit též časy $t_{m \text{ krit}}$, v nichž čáry života jednotlivých FB_m překročí hranice svých oblastí přijatelnosti. Jednotlivé časy $t_{m \text{ krit}}$ se mohou lišit i od času t_{krit} , v němž trajektorie $\Psi(t)$ celého systému překročí hranici R_A .

Budeme dále chápat životnost systému jako pravděpodobnost, že po jistou dobu t_p bude jeho čára života $\Psi(t)$ probíhat pouze uvnitř příslušné oblasti přijatelnosti R_A . Tuto životnost lze též vyjádřit pravděpodobnou dobou života (life-time) L_t .

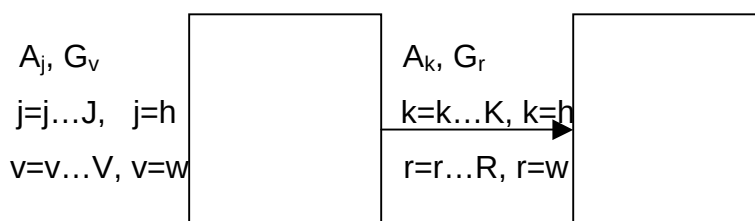
Skutečnost, že i v jistém homogenním systému mohou mít jednotlivé FB_m její tvořící různé hodnoty L_{tm} souvisí se známým přístupem k tzv. čerpání životnosti jednotlivých komponent složitého systému, který je často uplatňován u náročných zařízení (např. u energetických systémů a jaderných elektráren). Při takové analýze jsou stanoveny hodnoty L_{zm} nejvýznačnějších komponent a v průběhu provozu celého systému se pečlivě sleduje, jaká rezerva v hodnotách jednotlivých L_{tm} ještě zbývá tak, aby bylo zavčas možno provést nápravná opatření, tj. buď korekci parametrů příslušné komponenty, nebo pokud to není možné pak její výměnu.

V každém systému působí však kromě jistého množství FB_m ještě celá řada rozhraní. Tato rozhraní (interface, synapse) se podílejí na přenosu a překladu informací mezi jednotlivými FB_m tvořícími uvažovaný systém.

Jednotlivé FB_m působící v libovolném systému předávají své výstupní informace jiným s nimi spolupracujícím FB_m v jisté abecedě A_m a s jistou gramatikou G_m . Tyto FB_m , které informace od s nimi spolupracujících funkčních bloků přebírají, mohou však rozumět informacím buď pouze ve své vlastní abecedě a pouze se svou vlastní gramatikou.

Obecně mohou ovšem nastat případy, kdy některé FB_m jsou schopny vysílat informace v několika různých abecedách a s několika různými gramatikami, a naopak kdy některé FB_m mají podobné multijazykové schopnosti pro příjem.

Pro správnou funkci interakce mezi jednotlivými FB_m je tedy nutno, aby alespoň jedna dvojice abeced a gramatik, kterými disponují navzájem komunikující FB_m (viz obr. 5) si odpovídala, tj. aby příslušné FB_m byly schopny vzájemné komunikace, tj. aby si mohly rozumět.



Obr.5. K interakci mezi funkčními bloky

Pokud tomu tak není, je zapotřebí, aby informace byla na styku takových dvou či více vzájemné komunikace neschopných FB_m přeložena z jedné abecedy a gramatiky do druhé.

Nezbytný překlad, který je podmínkou úspěšné spolupráce je uskutečňován právě rozhraními. Spolehlivá, rychlá a efektivní překladatelská činnost rozhraní je proto pro funkci celého systému neméně důležitá, než funkce FB_m samých.

Každý překlad Tr_j , uskutečňovaný rozhraním je realizován s jistým časovým zpožděním (doba překladu) t_{tr} a s jistou nepřesností. V této nepřesnosti mohou být zahrnuty jednak chyby překladu $ErTr_j$ a jednak neúplnosti překladu $FzTr_j$.

Chyby překladu $ErTr_j$ představují nesprávně přeložené části původní informace.

S náročností překladu roste ve většině případů též doba, potřebná pro jeho provedení a tím se pochopitelně prodlužuje reakční čas RT celého systému. Tento reakční čas se skládá z úhrnu reakčních časů jednotlivých dílčích FB_m a reakčních časů příslušných rozhraní a to podél celé informační cesty, podél níž v systému probíhá příjem, zpracování a přenos informace. Čím je tato cesta delší a komplikovanější, tím je větší i RT . Hodnota RT je jedním z nejdůležitějších parametrů pro posuzování kvality systému. Systémy s příliš velkými hodnotami RT mají menší naději na úspěch ve srovnání se systémy, které sice mají shodné funkční vlastnosti, ale reagují rychleji.

Aby jistý systém mohl mít požadované funkční vlastnosti F , je třeba aby se na jejich vytváření podílel jistý počet dílčích FB_m . Syntéza celého souboru F pozůstává z určení informační cesty a jednotlivých v ní působících FB_m , realizujících dílčí systémové funkce F_m . Čím větší budou rozdíly mezi jednotlivými FB_m , tím větší budou pravděpodobně též rozdíly mezi jejich výstupními a vstupními abecedami a

gramatikami a tím náročnější bude i příslušný překlad. Doba jeho zpracování v rozhraní bude tedy pravděpodobně též delší.

Při uskutečňování překladu záleží nejen na tom, jaké jsou rozdíly mezi vstupní a výstupní abecedou, ale též na tom, po jakých úsecích bude příslušná informace překládána a předávána z výstupního FB_m na FB_m vstupní. Překlad po malých úsecích (až po bitech) může být rychlejší a jeho spolehlivost může být vyšší, potíže však mohou být se skladbou výsledné informace.

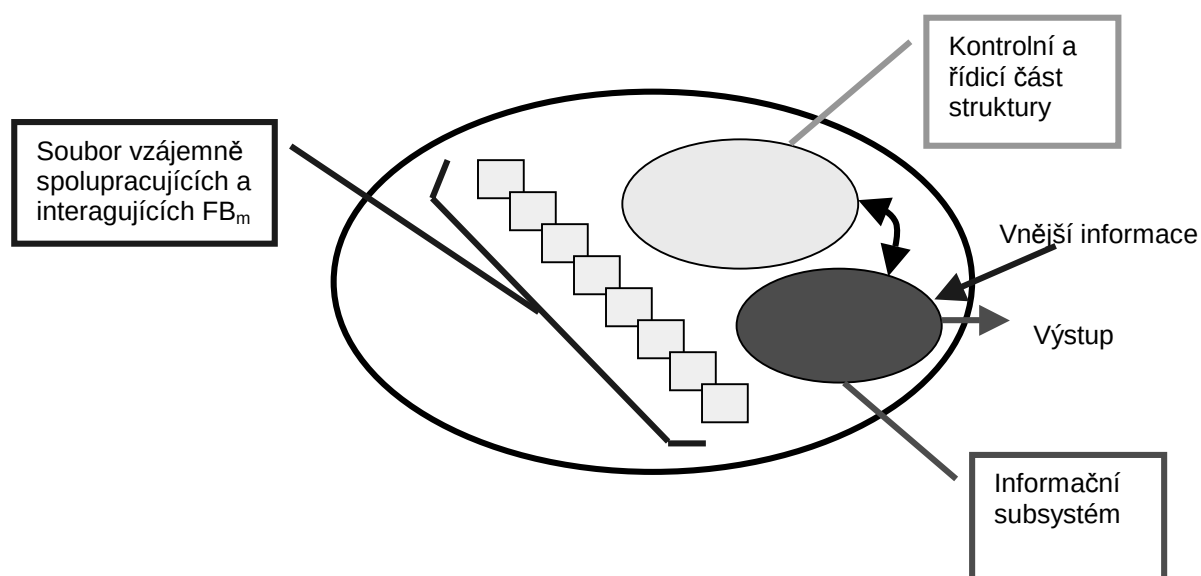
Lze soudit, že mezi těmito všemi hledisky existují jisté kompromisy, představující přiblížení se k optimu podle toho či onoho kritéria.

Výraznou předností informačních systémů, složených z vysokého počtu dílčích FB je značná spolehlivost $H(X,P)$ a s ní spojená odolnost proti poruchám. Ta je ovšem realizována nejen vyšší funkční spolehlivostí jednoduchých FB_m samých, ale jejich vzájemnou zastupitelností ve složitých, navzájem zálohovaných dílčích informačních cestách a možnostmi adaptivně měnit jejich propojení.

Je zřejmé, že při výrazně menším počtu použitých FB_m musí mít jakékoliv vyřazení dílčího FB_m na celkovou spolehlivost systému $H(X,P)$ mnohem větší negativní vliv.

U náročnějších systémů je do jejich struktury zařazena zvláštní kontrolní a řídicí část (viz obr. 6).

Ta zajišťuje nejen koordinaci činnosti jednotlivých dílčích funkčních bloků, ale i činnost jednotlivých rozhraní.



Obr. 6: Kontrolní a řídicí část a informační subsystém ve struktuře vyspělého systému

Informační subsystém a kontrolní a řídicí část struktury systému spolu musí navzájem těsně spolupracovat.

Mezi funkčních bloků systému existují četné přímé i zpětné vazby. Protože však mnohé z těchto funkčních bloků se uplatňují ve větším počtu paralelně, vzájemné vazby a interakce jimi realizované se projevují v celých svazcích a mezi jednotlivými vazbami v témže svazku často ještě působí příčné (laterální) vazební spoje. Jejich existence, účelnost uspořádání a spolehlivost funkce mají obecně kardinální vliv na spolehlivost a bezpečnost celého systému.

4. Možnosti zvyšování spolehlivosti systémů

Při analýze spolehlivosti a bezpečnosti jakéhokoliv systému je třeba respektovat několik hlavních přístupů. Mezi ně patří zejména:

a) celková analýza spolehlivosti a bezpečnosti systému

Všechny dílčí systémové funkce jednotlivých FB_m i funkce rozhraní jsou závislé jak na parametrech x_i příslušného funkčního bloku či rozhraní, tak na nezávisle proměnných.

Parametry samy se vlivem nezávisle proměnných též mění. Velmi nás tedy zajímají příslušné citlivosti

$$S^F_X = \{S^{Fk}_{xi}\}, \text{ resp.}$$

$$S^F_X = \{S^{Fm}_{xi}\}, \text{ resp.}$$

$$S^F_P = \{S^{Fk}_{pj}\}, \text{ resp.}$$

$$S^F_P = \{S^{Fm}_{pj}\}.$$

Jejich složky můžeme uspořádat do 4 matic citlivostí a jejich rozbořem nalézt takové dílčí funkční bloky a takové dílčí systémové funkce, které jsou změnou parametrů, resp. nezávisle proměnných ovlivněny nejvíce či naopak ty, které jsou vůči takovým změnám dostatečně vzdorné.

Lze se domnívat, že mezi komponentami těchto matic citlivostí mohou platit podobné vztahy, jaké byly již před drahnou dobou dokázány S.K. Mitrou pro lineární elektrické obvody (Mitrova věta o tzv. invarianci citlivostí – viz např. [8]).

Hodnoty citlivostí jsou pochopitelně závislé též na hodnotách systémových parametrů samých, tedy mění se podle toho, pro kterou hodnotu vektoru $X = \{x_i\}$ v N -rozměrném prostoru X je vyšetřujeme.

U některých systémů mohou existovat takové oblasti tohoto prostoru, v nichž jsou některé z těchto citlivostí tak veliké, že postačí i jen velmi malá změna hodnot x_i k tomu, aby celý systém výrazně změnil své vlastnosti a přešel od více či méně stabilního chování k chování chaotickému (to se může stát např. při náhlém přechodu od laminárního proudění či obtékání profilu a proudění či obtékání turbulentnímu). Vyšetření mezních přechodových stavů je proto přes svou značnou náročnost mimořádně závažné.

Nezbytnou součást analýzy spolehlivosti a bezpečnosti systému tvoří tzv. krizový management, tj. soubor doporučení a pravidel, jimiž se provozovatel a uživatelé systému musí řídit v případě mimořádných situací. Závažnost krizového managementu roste se závažností systému a jeho vypracování je obecně třeba věnovat zcela mimořádnou pozornost. Z historie katastrof různých systémů v posledním období jednoznačně vyplývá, že neexistence, nedokonalost či nedodržení krizového managementu má většinou fatální následky. Příkladů by bylo možno doložit desítky. Přitom je třeba si uvědomit, že příčiny mimořádných situací netkví obvykle jen v selhání funkce toho kterého dílčího funkčního bloku či rozhraní, byť sebedůležitějšího, ale v souběhu řady dílčích selhání. Obzvláště nebezpečné jsou z tohoto hlediska dlouhé řady posloupností činnosti dílčích funkčních bloků, u nichž se dílčí pravděpodobnosti selhání sečítají.

Východiskem krizového managementu je krizový scénář, založený na kritickém rozboru spolehlivosti a bezpečnosti celého uvažovaného systému. Podkladem k němu je nejen zmíněná

- analýza citlivostí, ale též
- rozbor možností dynamického vývoje čar života $\Psi_m(t)$ jednotlivých FB_m ,
- rozbor jejich časového souběhu,
- rozbor možností koordinace aktivit jednotlivých FB_m a provedení pečlivé
- stromové analýzy celkové pravděpodobnosti selhání systému.

Dále je velmi žádoucí, abychom alespoň pro nejdůležitější funkční bloky a rozhraní měli možnost uplatnit principy predikční diagnostiky a z ní vyplývající nástroje pro odhady pravděpodobností selhání jednotlivých uvažovaných bloků na dostatečně dlouhý predikční horizont, ale pokud je to možné i nástroje pro zavčasné korekce postupně či náhle nastávajících změn jednotlivých parametrů x_i .

Vytvoření krizového managementu nelze ovšem chápat pouze jako vypracování jisté příručky či souboru formulářů, ale jako systém, ve kterém je brán zřetel i na pravděpodobnou časovou dynamiku vývoje mimořádné situace a nezbytnou včasnou koordinovanost nápravných a záchranných operací. Zkušenosti z nedávných katastrof v alpských silničních tunelech ukazují, že právě nerespektování těchto dvou faktorů může významně zvýšit rozsah fatality následků.

5. Literatura

- [1]...Mac Donald S., Grebogi C., Ott E., Yorke J.A.: Fractal basin boundaries
Physica 17D, 1985, 125-183
- [2]...Yorke J.A.: Nonlinear Dynamics and Chaos, J. Wiley, Chichester, 1986
- [3]...semináře „Teorie informatiky“, vedené Prof. Ing. Dr. J. Vlčkem, DrSc, ČVUT
Praha, FD, 1999 až 2000
- [4]... Votruba Z.: podkladové materiály k semináři „Teorie informatiky“, ČVUT FD,
15.3.1999
- [5]... Brandejský T.: podkladové materiály k semináři „Teorie informatiky“, ČVUT FD,
30.3.1999
- [6]...Novák M.: Spolehlivost informačních procesů, výzkumná zpráva LSS FD ČVUT
č. LSS 69/66, Praha, 1999
- [7]...Novák M.: Spolehlivost interakce v heterogenních systémech, výzkumná zpráva
LSS FD ČVUT č. LSS 100/01, Praha, 2001