PROBLÉMY SÚVISIACE S POUŽÍVANÍM NIEKTORÝCH POJMOV PRI ANALÝZE BEZPORUCHOVOSTI SYSTÉMOV

PROBLEMS RELATED TO USE OF SOME TERMS IN SYSTEM RELIABILITY ANALYSIS

Nadežda Hanusová, Jiří Zahradník

Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina

Abstrakt Článok sa zaoberá problematikou uplatnenia pojmov z oblasti spoľahlivosti, definovaných v súčasnosti platnou normou STN IEC 50 (191): Medzinárodný elektrotechnický slovník, kap. 191: Spoľahlivosť a akosť služieb (1993), pri analýze spoľahlivosti technického systému. Cieľom tohoto článku je nájsť súvis medzi pojmami uvedenými v tejto norme a používanými pri analýze spoľahlivosti technických systémov, s pravidlami a postupmi používanými pri analýze systémov tak ako ich uvádza teória systémov. Východiskom je opis časti životného cyklu systému, týkajúcej sa jeho bezporuchovosti. Táto časť životného cyklu systému je opísaná pomocou stavového diagramu, ku ktorému sú nakoniec priradené vhodné termíny z oblasti bezporuchovosti.

Summary The paper deals with problems of using dependability terms, defined in actual standard STN IEC 50 (191): International electrotechnical dictionary, chap. 191: Dependability and quality of service (1993), in a technical systems dependability analysis. The goal of the paper is to find a relation between terms introduced in the mentioned standard and used in the technical systems dependability analysis and rules and practices used in a system analysis of the system theory. Description of a part of the system life cycle related to reliability is used as a starting point. The part of a system life cycle is described by the state diagram and reliability relevant therms are assigned.

1. ÚVOD

V mnohých publikáciách zaoberajúcich sa problematikou spoľahlivosti technických systémov sa používajú pojmy, ktorých význam je často chápaný odlišne, a to podľa subjektívneho názoru daného autora. Aj keď v súčasnosti platná norma STN IEC 50 (191): Medzinárodný elektrotechnický slovník, kap. 191: Spoľahlivosť a akosť služieb (1993) definuje pojmy z oblasti spoľahlivosti, treba vzhľadom na vývoj v oblasti počítačových riadiacich systémov a špeciálne v oblasti počítačových riadiacich systémov bezpečnostne kritických procesov, doplniť túto normu o ďalšie pojmy, ktoré by umožňovali precíznejšie opísať problematiku spoľahlivosti počítačových systémov. V článku budú použité aj iné definície, týkajúce sa tejto problematiky, ktoré sú preferované v niektorých zahraničných publikáciách.

2. VYMEDZENIE POJMOV

Pojem *systém* je všeobecný pojem, ktorý v technických disciplínach predstavuje spravidla určitý reálny objekt, ktorý je v norme [1] definovaný ako akákoľvek časť, súčasť, zariadenie, subsystém, funkčná jednotka, prístroj alebo systém, o ktorom možno uvažovať jednotlivo.

Z hľadiska teórie systémov neskúmame reálne objekty v celej ich komplexnosti, ale sledujeme len tie ich veličiny, ktoré sú rozhodujúce pre dosiahnutie zadaného cieľa. *Objekt* je potom tá časť objektívnej reality, ktorú skúmame a všetko ostatné je jeho okolím. Systém potom predstavuje určitú abstrakciu reálneho objektu a zobrazuje len tie jeho veličiny a vlastnosti, ktoré sú podstatné z hľadiska problému, ktorý máme na objekte riešiť. V rámci teórie systémov je dôležité určenie systému na danom objekte.

Definujeme si najskôr nasledujúce základné pojmy: *objekt*, *systémový objekt, systémové vlastnosti* a *systém*.

(Reálny) objekt je každý predmet, projekt, proces a problém objektívnej reality.

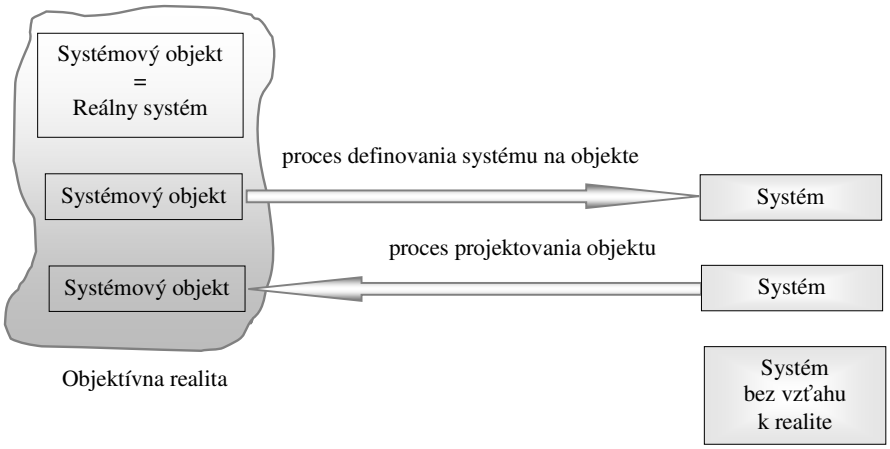
Systémový objekt je každý (reálny) objekt vykazujúci tzv. *systémové vlastnosti* a možno ho považovať za *reálny systém*.

Podľa [2] možno *systémové vlastnosti* zhrnúť nasledovne:

- systém je komplexom vzájomne spätých prvkov,
- systém vyjadruje zvláštnu jednotu s okolím,
- každý systém môže byť súčasne prvkom systému vyššieho rádu,
- každý prvok systému môže byť súčasne systémom nižšieho rádu.

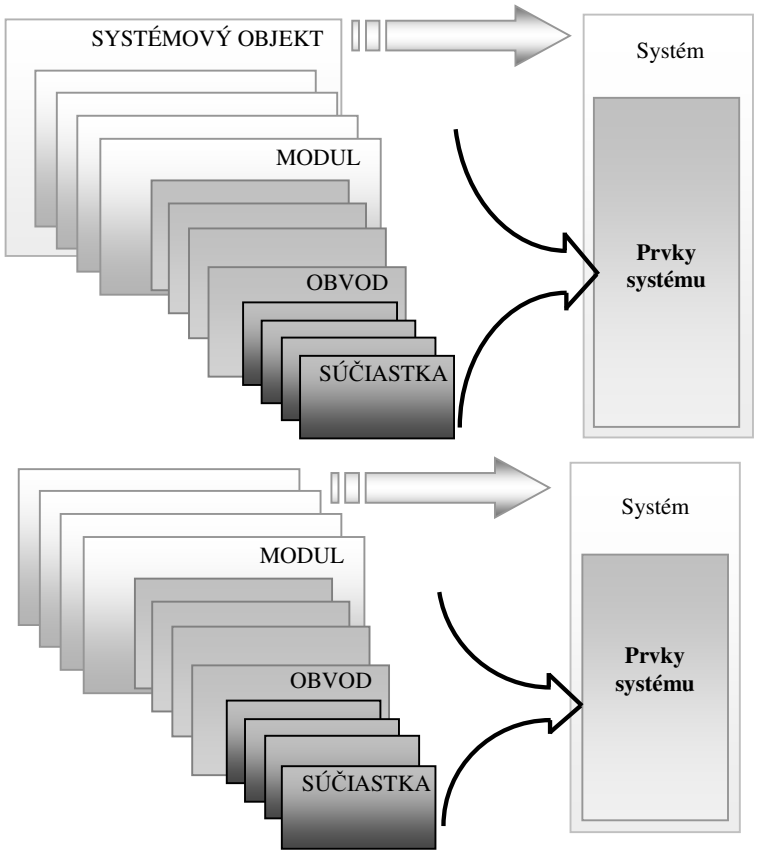
Prijmime teraz za správnu nasledujúcu definíciu systému. *Systém* je (obr. 1):

- jednoduchý reálny objekt (systémový) t.j. *(reálny) systém*, alebo
- abstraktná myšlienková konštrukcia, výroková konštrukcia, konštrukcia matematických výrazov zavádzaná na zložitom alebo rozľahlom reálnom objekte (systémovom) alebo jeho projekte t.j. *(abstraktný) systém*, alebo
- abstraktná myšlienková konštrukcia, výroková konštrukcia, konštrukcia matematických výrazov vytváraná bez priameho vzťahu k reálnemu objektu (systémovému) t.j. *(abstraktný) systém*.



Obr. 1. Vzťah medzi pojmami „objekt“ a „systém“.
Fig. 1. Relation between terms „an object“ and „a system“.

Na obr. 2 je zobrazené hierarchické usporiadanie objektu a k nemu zodpovedajúce priradenie jednotlivých hierarchických úrovní systému. Je naznačená aj podstata systémových vlastností (uvedené vyššie), podľa ktorej sa na ľubovoľný prvok systému (už definovaného na určitej hierarchickej úrovni) možno pozerať ako na systém nižšej hierarchickej úrovne.



Obr. 2. Definovanie systému na objekte a princíp zníženia rozlišovacej úrovne v systéme.
Fig. 2. System definition on an object and a decreasing principle of system identification level.

3. ŽIVOTNÝ CYKLUS TECHNICKÉHO SYSTÉMU A JEHO PRVKOV

Opíšeme teraz všeobecne časť životného cyklu objektu [6], a to od jeho návrhu a vývoja, cez výrobu, uvedenie do prevádzky až po vlastnú prevádzku. V jednotlivých fázach životného cyklu budeme sledovať príčiny, ktoré môžu viesť k poruche objektu počas jeho prevádzky. *Porucha* objektu je definovaná ako ukončenie jeho schopnosti plniť požadovanú funkciu [1]. Na danom objekte si definujeme systém, ktorého jadro homomorfie je volené s ohľadom na poruchovosť objektu, ktorú chceme analyzovať. Za týmto účelom môžeme rozlíšiť nasledujúce tri fázy životného cyklu systému:

1. Fáza: návrh, vývoj, projektovanie a výroba systému.

V dôsledku fyzikálnych vlastností materiálov, omylov pri špecifikácii systémových požiadaviek resp. v dôsledku neúplnej alebo nepresnej špecifikácie systémových požiadaviek a v dôsledku omylov pri návrhu, programovaní algoritmov funkcií, dimenzovaní súčiastok, výrobe a pod. existujú vo vnútri systému určité *nedostatky*, ktoré môžu spôsobiť zlyhanie požadovanej funkcie systému. Autori publikácií [3], [4], [5] označujú zhodne tento nedostatok vnútri v systéme termínom *fault*.

2. Fáza: prevádzka systému (analýza správania sa systému pri konkrétnych vstupoch)

Pri prevádzkovaní systému sa nedostatky *vložené* do systému v prvej fáze životného cyklu môžu aktivovať a v dôsledku toho vznikne v stavovom priestore systému *odchýlka* stavu niektorého prvku (resp. viacerých prvkov) systému od stavu zadaného špecifikáciou. Pre takúto odchýlku je v norme [1] a aj v už uvedených publikáciách [3], [4], [5] zhodne použitý pojem *chyba (error)*. Norma [1] definuje chybu nasledovne: *chyba* charakterizuje nesúlad medzi počítanou, pozorovanou alebo meranou hodnotou či parametrom a skutočnou, definovanou alebo teoreticky správnou hodnotou či parametrom.

3. Fáza: spracovanie odchýlky

Predpokladajme, že vzniknutú odchýlku v stavovom priestore systému systém zistí a vykoná jej *spracovanie* tak, aby sa nepreniesla na výstup systému a teda, aby nemala vplyv na proces, ktorý je daným systémom riadený. Týmto spracovaním môže byť napr. uplatnenie techniky *odolnosti proti nedostatkom vnútri systému (fault tolerance)*.

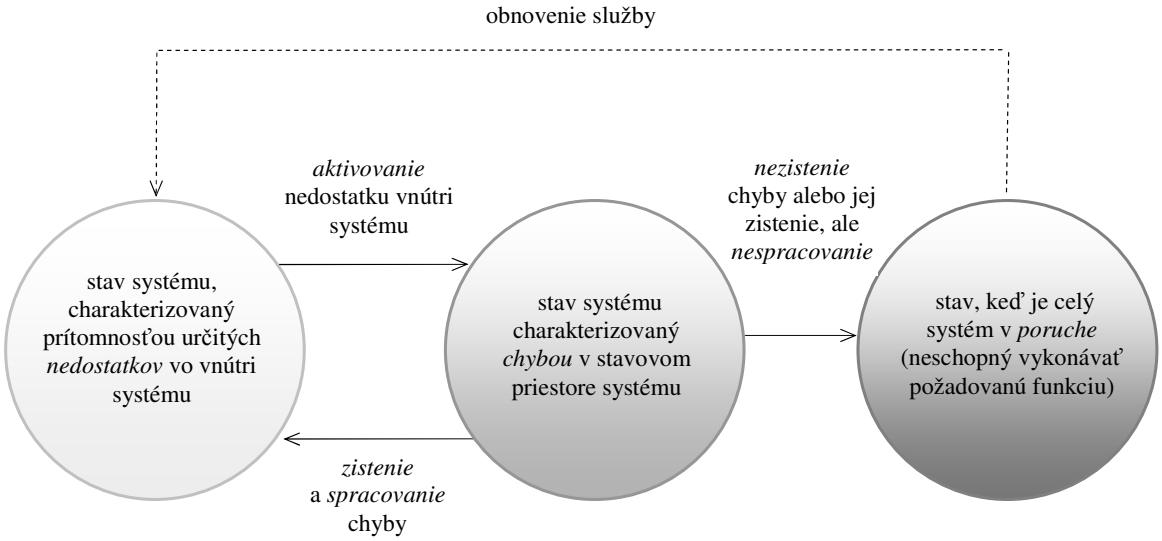
Ak ale táto odchýlka nie je zistená, alebo je zistená, ale nie je spracovaná, presunie sa na výstup systému a spôsobí ukončenie schopnosti systému plniť požadovanú funkciu. Takto je v norme [1] a aj spomínanej publikácii [4] definovaný pojem *porucha (failure)* s tým, že v norme [1] je použitý pojem objekt namiesto pojmu systém. V prípade, že sú prítomné aj „vhodné“ prevádzkové podmienky, môže dôjsť až k *nehode spôsobenej poruchou systému (failure – accident)*.

Nech na vstup systému pôsobí v danom okamihu a pri určitej predpokladanej hodnote stavového vektora vstupná veličina, ktorá má podľa špecifikácie požiadaviek vyvolať na výstupe systému konkrétnu výstupnú veličinu. Môžu nastať dva prípady, ktoré sú uvedené v tab. 1.

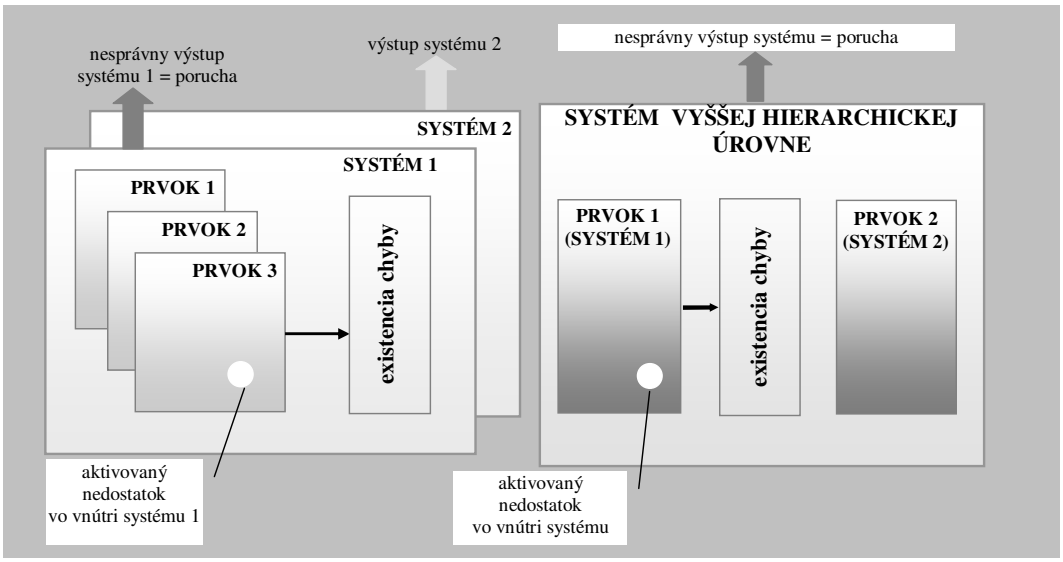
Na obr. 3 sú pomocou stavového diagramu systému zobrazené stavy uvedené v tab. 1. Každý zo stavov uvedených na obrázku vznikol následkom určitej zmeny, *javu*, ku ktorému v systéme došlo. Postupnosť týchto javov, aj s ich vzťahom ku konkrétnej časti systému, je pre dve rôzne rozlišovacie úrovne systému zobrazená na obr. 4 a obr. 5. Ak sa v niektorom z prvkov systému aktivuje nedostatok, ktorý v tomto prvku existuje, vznikne v stavovom priestore systému chyba. V prípade, že chyba nie je systémom zistená a spracovaná, spôsobí poruchu systému ako celku.

Tab. 1. Stavy systému zodpovedajúce danému výstupu systému.
Tab. 1. System states related to a given system output.

Výstup systému zodpovedá špecifikácii požiadaviek.	Systém je v stave, keď sú prítomné určité nedostatky vnútri systému, ale nebola zaznamenaná žiadna odchýlka v stavovom priestore.
	Systém je v stave s chybou (nedostatky vnútri systému sa *aktivovali*), bola zaznamenaná *odchýlka* v stavovom priestore, ktorá bola spracovaná.
Výstup systému nezodpovedá špecifikácii požiadaviek.	Systém je v stave s chybou (nedostatky vnútri systému sa *aktivovali*), bola zaznamenaná *odchýlka* v stavovom priestore, ktorá nebola spracovaná. Na výstup systému sa prenesie táto odchýlka a spôsobí ukončenie schopnosti systému plniť požadovanú funkciu, čo je definované už spomínaným pojmom *porucha (failure)*.



Obr. 3. Zobrazenie opísanej časti životného cyklu systému pomocou stavového diagramu systému.
Fig. 3. The part of a system life cycle state – space diagram.



Obr. 5. Znázornenie postupnosti: nedostatok (fault) – chyba (error) – porucha (failure) na určitej rozlišovacej úrovni systému.
Fig. 4. The fault – error – failure sequence representation of concrete system identification level.

Obr. 5. Znázornenie postupnosti: nedostatok (fault) – chyba (error) – porucha (failure) vo vzťahu k vyššej rozlišovacej úrovni systému.
Fig. 5. The fault – error – failure sequence representation in the higher system identification level relation.

V norme [1] sú definované pojmy *porucha* a *chyba*. Význam pojmu *chyba* je v tomto prípade jednoznačný. *Porucha* sa chápe aj ako porucha prvku a aj ako porucha systému. A tu by bolo vhodné tieto dva pojmy rozlíšiť. Z uvedeného vyplýva, že *porucha (failure)* môže byť spôsobená:

1. ***Nedostatkami, ktoré sú zavedené do systému ešte pred jeho uvedením do prevádzky a majú pôvod v ľudskej činnosti, napr.:***

- zlá, neúplná alebo nepresná špecifikácia systémových požiadaviek na činnosť systému,
- omyly pri programovaní, návrhu, projektovaní, konštrukcii, výrobe a montáži,
- nevhodná manipulácia,
- neúplná alebo nepresná dokumentácia systému,
- nepresnosti v určení prevádzkových podmienok, postupov obsluhy a údržby systému.

2. ***Nedostatkami, ktoré sú zavedené do systému ešte pred jeho uvedením do prevádzky a majú pôvod:***

- vo fyzikálnej podstate materiálu (starnutie alebo opotrebovanie),
- v neodolnosti systému voči rušivým vplyvom okolia systému (teplotné, elektromagnetické, mechanické, chemické a pod.).

To znamená, že problémom je absencia pojmu vhodného pre opis nedostatkov vo vnútri systému, ktoré, ak sa aktivujú, sú príčinou:

- porúch *prvkov* spôsobených ich starnutím alebo opotrebením,
- porúch *prvkov* z nesprávneho použitia,
- porúch *prvkov* spôsobených nesprávnym zaobchádzaním,
- porúch *prvkov* spôsobených poddimenzovaním,
- konštrukčných porúch *prvkov***,**
- výrobných porúch *prvkov*.

V publikáciách [3], [4], [5] používajú autori pre uvedené nedostatky v systéme pojem *fault*, ktorý možno preložiť ako *defekt*, *závada* a ktorý budeme používať aj my. Tu však dochádza ku kolízii s pojmom *poruchový stav (fault)*, ktorý je definovaný normou [1].

Tieto nedostatky sú po aktivácii príčinami porúch prvkov systému, ktoré môžu byť zároveň príčinami poruchy systému.

Softvér, ktorý je v súčasnosti súčasťou väčšiny riadiacich systémov, nemôže byť v poruche lebo sám o sebe nevykonáva žiadnu funkciu systému. Ale *závada*, resp. *defekt* v softvéri môže byť, po implementácii softvéru do počítača, príčinou jeho poruchy. Teda omyly pri vývoji softvéru môžu viesť k poruchovému stavu systému.

Nedostatkom normy [1] je skutočnosť, že neodlišuje poruchy prvkov systému od porúch systému ako celku. Ak je systém schopný plniť požadovanú funkciu v daných podmienkach a v danom časovom intervale, nachádza sa v bezporuchovom stave. V opačnom prípade je v poruchovom stave, ktorý je následkom poruchy systému. Pri pozorovaní vykonávania požadovanej funkcie systému je potrebné určiť na akej úrovni systému sa pozorovanie uskutoční. V prípade úrovne prvkov sa sleduje vykonávanie požadovanej funkcie ľubovoľného prvku systému. Výsledkom pozorovania je určenie, či sa prvok nachádza v poruchovom alebo bezporuchovom stave. V prípade úrovne systému ako celku sa sleduje vykonávanie požadovanej funkcie systému v súvislosti s poruchami jeho prvkov. Porucha ľubovoľného prvku systému spôsobuje v systéme chybu, ktorá môže, ale nemusí viesť k poruche systému. Z pohľadu systému ako celku je porucha ktoréhokoľvek jeho prvku dôsledkom aktivovanej závady v systéme. Aktivovaná závada predstavuje neschopnosť časti systému plniť požadovanú funkciu. Podmienkou aktivácie závady systému je existencia takejto *skrytej* závady v systéme, ktorá je vlastnosťou každého systému a má pôvod v procese návrhu a výroby systému. Aktivácia závady v systéme môže byť samovoľná (napr. proces starnutia prvkov, opotrebovávania v prevádzke) alebo vyvolaná vonkajšími činiteľmi v okolí systému (napr. obsluhou, údržbou, rušením).

Nakoniec uvedieme príklady ilustrujúce postupnosť javov: závada (defekt) – chyba – porucha:

1. ***Omyl pri programovaní algoritmov funkcií***

- je to *skrytá závada* softvéru (v dátach alebo inštrukciách),
- po spustení softvéru v prevádzke sa táto závada stáva za určitých podmienok aktívnou a produkuje *chybu* v stavovom priestore systému,
- ak chybné dáta postihnú poskytovanú službu, vzniká *porucha systému*.
- ak sa chybné dáta zistia a opravia ešte predtým, než opustia rozhranie systému, na výstup sa dostane správna hodnota a systém je v počiatočnom stave (stav so skrytou závadou).

2. ***Ovplyvnenie systému rušením***

- *skrytou závadou* v tomto prípade môže byť napr. nedokonalé tienenie hardvéru,
- po ovplyvnení vstupu rušením sa táto závada aktivuje a produkuje inú hodnotu na výstupe postihnutého prvku systému, čo je *chyba*,
- ak sa nesprávna vstupná hodnota vnútri systému spracuje a postihne rozhranie, dochádza k *poruche systému*,
- ak sa odchýlka vnútri stavového priestoru systému zistí a spracuje (napr. uplatnením techniky odolnosti proti závadám – fault tolerance), systém je v počiatočnom stave a k poruche nedochádza.

Uvedené tri javy: *závada – chyba – porucha* možno teda podľa vonkajších príznakov rozdeliť na:

- *závadu skrytú* (ešte neaktivovanú) a *závadu aktivovanú* (produkujúcu chybu),
- *chybu latentnú* (nezistenú) a *chybu detegovanú* (zistenú),
- *poruchu systému* (postihnutie služby poskytovanej systémom) a *poruchu systému prechádzajúcu na závadu* vo vyššej hierarchickej úrovni pozorovania

systému (ak systém s poruchou je prvkom systému na vyššej hierarchickej úrovni).

4. ZÁVER

Článok poukazuje na potrebu pojmového rozlíšenia javov, ktoré môžu byť v konečnom dôsledku príčinou zlyhania požadovanej funkcie systému. Pri úvahách sa vychádza zo systémových vlastností systémov, ktoré sú definované v teórii systémov. Pritom je veľmi dôležité na akej rozlišovacej úrovni systému sa daný problém rieši. Treba vždy rozlišovať medzi prvkami systému a samotným systémom. Poruchy prvkov systému ešte sami o sebe nemusia mať vplyv na proces, ktorý uvažovaný systém riadi. Riadený proces je ovplyvnený až funkciou, ktorú produkuje systém ako celok. V článku sú ďalej analyzované príčiny, ktoré môžu viesť k zlyhaniu požadovanej funkcie systému a sú navrhované upresňujúce pojmy na ich opis. Problém je hlavne v absencii pojmu všeobecne opisujúceho možné príčiny porúch prvkov v systéme, pre ktoré je v tomto článku používaný pojem závada alebo defekt systému. Pritom tieto závady (defekty) môžu, ale nemusia spôsobiť zlyhanie požadovanej funkcie systému, tzv. poruchu systému.

LITERATÚRA

[1] STN IEC 50 (191): Medzinárodný elektrotechnický slovník, kap. 191: Spoľahlivosť a akosť služieb, 1993

[2] Habr, J., Vepřek, J.: Systémová analýza a syntéza, SNTL Praha, 1986

[3] Rushby, J.: Formal Methods and the Certification of Critical Systems, 1993

[4] Thane, H.: Safe and Relible Computer Control Systems, Concepts and Methods, Stockholm, 1996

[5] Powell, D.: On Dependability, Intrusion Tolerance and the MAFTIA project, Toulouse, France, 2001

[6] Rástočný,K.; Tomovič, M.: Bezpečnosť a životný cyklus zabezpečovacieho zariadenia. Medzinárodná konferencia "Zabezpečovacia technika - súčasnosť a budúcnosť", 19. - 20. 9. 2002, Žilina, Slovenská republika, *ISBN 80-7135-061-3*