Spolehlivost elektronických systémů

Úvod do řízení spolehlivosti

studijní text frekventantů předmětu PV171/1

Obsah

1 Úvod do problematiky řízení spolehlivosti

S problémem spolehlivosti nejrůznějších přístrojů a zařízení se dostává do styku (a často též do konfliktu) téměř každý z nás ve svém denním životě. Uživatel většinou hodnotí spolehlivost podle toho, zda s ní je nebo není spokojen. Konstruktéři a výrobci jsou nuceni se spolehlivostí zabývat podstatně důkladněji, protože na jejich práci v převážné míře závisí, zda výrobek bude spolehlivý nebo ne. S pasivním přístupem ke spolehlivosti by se však ve skutečnosti neměl spokojovat ani uživatel, protože i on může svými znalostmi významně ovlivnit výslednou spolehlivost zařízení, které používá. Měl by proto být schopen především kvalifikovaně ohodnotit spolehlivost, umět se rozhodnout, jakou spolehlivost skutečně potřebuje, měl by vědět, jak jí dosáhne a také co za ni zaplatí.

Některé základní úvahy, použitelné jako východisko při studiu spolehlivosti číslicových systémů, budou uvedeny v tomto textu. Pro potřeby exaktního popisu zavedeme několik pojmů, na které se v dalším textu budeme odvolávat, a popíšeme jejich vzájemné vztahy. Z dnes již velmi rozsáhlé teorie spolehlivosti tím samozřejmě pokryjeme jen nepatrný zlomek. Pro podrobnější studium teorie spolehlivosti je třeba obrátit se na některou ze specializovaných publikací, jichž je ve světové i naší technické literatuře dostatek, viz např. [*Shooman*], [*Ross*], [*Arsenault*], [*Navabi*] nebo [*Lala*].

V průběhu rozpracování teorie spolehlivosti se postupně konstituovaly tři základní úlohy, jimiž se teorie spolehlivosti zabývá. Jedná se o následující disciplíny:

- zajišťování (měření) spolehlivosti,
- předvídání (predikce) spolehlivosti,
- řízení (zlepšování) spolehlivosti.

1.1 Definice spolehlivosti

Chceme-li mít možnost hodnotit a srovnávat spolehlivost systémů, musíme především definovat veličiny, v nich hodnotu spolehlivosti budeme udávat a v níž ji budeme měřit, protože spolehlivost jako taková není sama o sobě kvantifikovatelná i když ji téměř každý uživatel dokáže intuitivně popsat. Ve starší normě **ČSN 010102*** je spolehlivost charakterizována jako ***„obecná vlastnost objektu spočívající ve schopnosti plnit požadované funkce při zachování hodnot stanovených provozních ukazatelů v daných mezích a v čase podle stanovených technických podmínek“***.

Tato definice je doplněna několika vysvětlujícími poznámkami:

- spolehlivost je komplexní vlastnost, která může zahrnovat např. bezporuchovost, životnost, udržovatelnost a skladovatelnost, buď jednotlivě, nebo v kombinaci,
- technickými podmínkami se rozumí souhrn specifikací technických vlastností, předepsaných pro požadovanou funkci objektu, dále způsoby jeho provozu, skladování, přepravy, údržby a opravy,
- provozní ukazatele jsou ukazatele produktivity, rychlosti, spotřeby elektrické energie, paliva, apod.

Pro jednoznačnost diskuse by bylo vhodné upřesnit, co rozumíme pod pojmem ***objekt***. Je to zjevně velmi obecný pojem, jehož význam je možno chápat vždy podle toho, co právě zkoumáme. Do uvedené definice spolehlivosti lze za objekt dosadit libovolně malý nebo libovolně velký celek, který jsme schopni zkoumat současně. V číslicové technice to tedy může být součástka, obvod, funkční blok, jednotka, systém, apod.

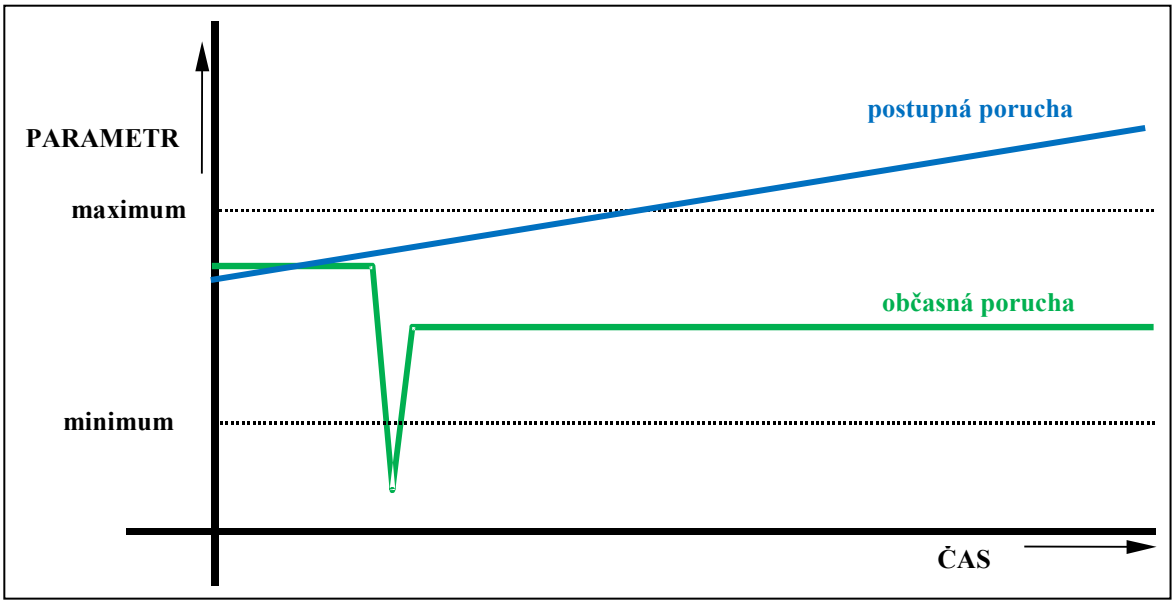
Z citované definice lze vyvodit několik závěrů použitelných při studiu možností kvantitativního vyjádření spolehlivosti. Jako „***komplexní vlastnost***“ (zahrnující několik různých hledisek) lze spolehlivost zřejmě stěží vyjádřit jednou číselnou hodnotou, která by nám umožnila uspořádat všechny objekty podle spolehlivosti. Přístup tvůrce normy je odlišný, namísto komplexní vlastnosti norma zavádí tzv. ukazatele spolehlivosti, což jsou veličiny, které lze jednotlivě vyhodnocovat. Ty jsou pak kvantitativním vyjádřením dílčích vlastností tvořících ve svém souhrnu spolehlivost.

Při studiu spolehlivosti se často budeme setkávat s pojmy ***závada, porucha, selhání*** a ***chyba***. I když je jejich smysl intuitivně zřejmý, bude vhodné uvést jejich definice, protože mají pro další výklad klíčový význam. Ve smyslu citované názvoslovné normy:

- ***závada*** (angl. *defect*) představuje konkrétní kaz v technickém vybavení (ang. *hardware*);
- ***porucha*** (angl. *fault*) je projevem závady. V simulačních programech slouží pro analýzu závad v elektronických obvodech. Je to jev bránící systému provádět požadovanou funkci (ISO 2382-14:1978);
- ***selhání*** (angl. failure) je projev závady, který způsobuje nesprávnou funkci systému, kterou nelze potlačit nebo znemožňuje obnovit správnou jeho správnou funkci. Je to jev spočívající v ukončení stavu provozuschopnosti objektu. Kritéria selhání jsou stanovována technickou dokumentací daného objektu (ČSN 01 0102-1979). V simulačních programech je selháním změna zamýšlené funkčnosti systému v důsledku existující poruchy;
- ***chyba*** (angl. *error*) – je způsobena závadou je definována jako jakýkoliv nesoulad mezi vypočtenou, pozorovanou nebo změřenou hodnotou na jedné straně a teoreticky správnou nebo očekávanou hodnotou na straně druhé (ČSN 36 9001/2 - 1987).

Poznámka:
porucha se projevuje chybou na výstupu systému.

Z uvedených dvou definic vyplývá, že chyba je obvykle důsledkem nějaké poruchy, avšak každá porucha se nemusí nutně projevit jako chyba (např. u latentních poruch, kdy se na realizaci výstupní proměnné porouchaná součástka-modul nepoužívá).



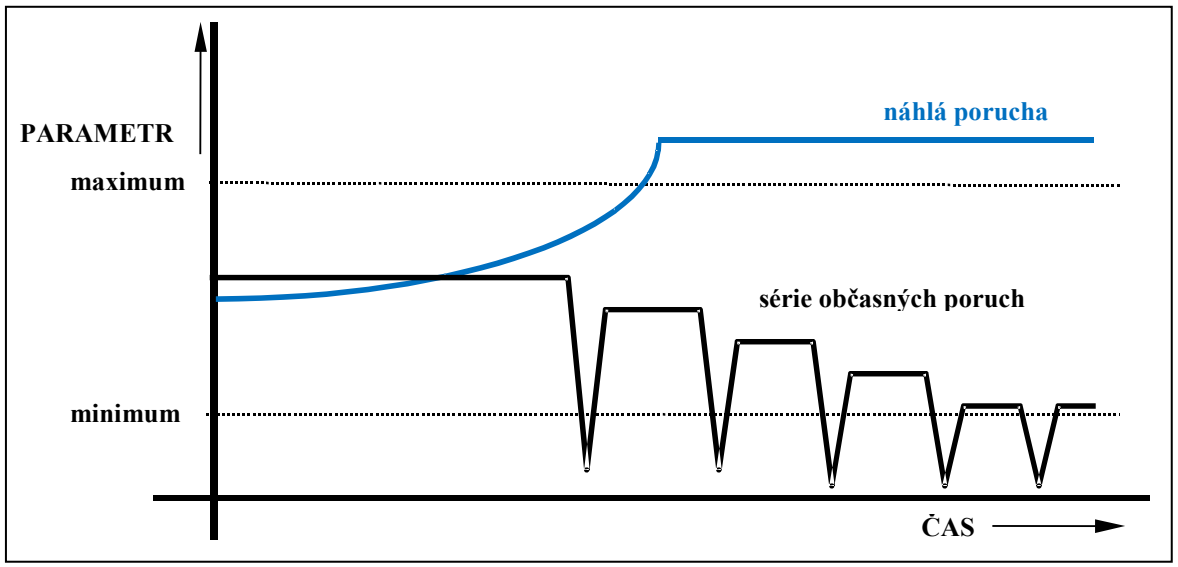
Obrázek 1.1: Základní typy poruch číslicových systémů

Technický stav elektronického zařízení se odráží ve výskytu poruch nejrůznějšího charakteru. Typologií poruch se zabývá norma a rozlišuje následující poruchy:

- latentní porucha,
- náhlá porucha,
- postupná porucha,
- občasná porucha,
- úplná porucha,
- částečná porucha,
- havarijní porucha (náhlá a úplná),
- degradační porucha (postupná a částečná).

Charakteristické vlastnosti některých typů poruch jsou schematicky zobrazeny na obrázcích - viz Obrázek 1.1 a Obrázek 1.2.

V zařízení bez poruchy nabývají parametry signálů přenášejících informaci hodnot, které se pohybují uvnitř oblastí omezených mezními, povolenými hodnotami. U číslicových systémů platí, že parametry signálů se uvnitř vymezených oblastí nenacházejí nepřetržitě, ale pouze v určitých, přesně definovaných okamžicích. Pro číslicové obvody jsou definovány statické a dynamické parametry. Na změny obou typů parametrů mají vliv fyzikální a chemické procesy probíhající v materiálech, z nichž jsou vytvořeny konstrukční prvky elektronického zařízení. Tyto procesy způsobují, že pracovní body konstrukčních prvků se přibližují k mezním hodnotám a tím se k mezním hodnotám posouvají parametry signálů přenášejících informaci. Takto se konstrukční prvky stávají citlivější na další fyzikální a chemické jevy, výsledkem čehož je dočasný a později trvalý posun některého parametru signálu nesoucího informaci mimo povolenou oblast - tedy vznik poruchy.



Obrázek 1.2: Základní typy poruch číslicových systémů

Vysoký počet poruch v elektronických systémech má dočasný charakter, jedná se o občasné poruchy, přičemž se četnost těchto poruch mění. Příčina těchto poruch spočívá ve fyzikálních jevech souvisejících se šířením elektrických impulsů po vedení a na fyzikálních vlastnostech vodičů sloužících k šíření těchto impulsů mezi jednotlivými obvody elektronického zařízení. Každý vodič elektrických signálů parazitně vyzařuje elektromagnetické záření do okolního prostoru, ale také přijímá elektromagnetické záření z okolního prostředí. Přeslechy a odrazy na

nepřizpůsobených vedeních se mohou navzájem sečítat a odečítat s užitečným signálem a takto ovlivňovat přenášenou informaci.

Velký počet různých typů poruch, které v číslicových systémech mohou nastat, vedl k vytvoření zjednodušené reprezentace poruch, k tzv. ***modelům poruch***. Nejběžnějším modelem jsou poruchy ***trvalé nula*** (t_0) a ***trvalá jednička*** (t_1), které symbolizují trvalou přítomnost konstantního napětí odpovídajícího jedné ze dvou logických úrovní. Tímto způsobem lze modelovat převážnou většinu fyzikálních poruch vznikajících v kontaktních (reléových) obvodech, pro něž byl původně vytvořen, a v polovodičových číslicových obvodech (především v obvodech typu TTL). Výjimku tvoří zkraty signálních vodičů, které je třeba modelovat jinak. Samostatný model vyžadují též poruchy ***trvale sepnuto*** a ***trvale přerušeno***, které jsou charakteristické pro obvody vyrobené technologií CMOS.

Při dalších úvahách budeme rozlišovat dva stavy objektu, a to ***poruchový*** (tj. stav, kdy porucha nastala) a ***bezporuchový*** (tj. stav kdy porucha nenastala). V nejjednodušším případě systém po výskytu poruchy setrvá v poruchovém stavu až do okamžiku, kdy je porucha opravena, nebo kdy je systém vyřazen z provozu. Takovou poruchu označujeme jako ***stálou***. V praxi se však často setkáváme s tím, že porucha zcela neočekávaně mizí a znovu se objevuje v okamžicích, které nikdo nedokáže předvídat. Takovou poruchu označujeme jako ***nestálou*** nebo ***občasnou***.

Pro výslednou spolehlivost objektu je nesmírně důležité, zda během jeho provozu provádíme obnovu bezporuchového stavu nebo ne. Podle toho budeme rozlišovat objekty ***obnovované*** a ***neobnovované***. Obnova je přitom chápána jako vlastní přechod z poruchového do bezporuchového stavu, zatímco činnost, která k tomu vedla, se označuje jako oprava. Tyto termíny odpovídají **ČSN 010102***, a proto je zde budeme používat, i když v praxi se častěji ve stejném významu používá označení opravovaný nebo neopravovaný objekt. Objekt může být neobnovovaný proto, že je neopravitelný (např. integrovaný obvod), nepřístupný (kosmické sondy, speciální vojenská zařízení, přístroje umístěné na odlehlých místech Země), nebo proto, že není opravován z organizačních důvodů (např. oprava není rentabilní). Tato hlediska hrají významnou roli zejména při specifikaci vlastností systémů odolných proti poruchám, a proto se k nim ještě vrátíme.

Se spolehlivostí velmi úzce souvisí i bezpečnost provozu systému. Obvykle bývá definována jako pravděpodobnost, že se na výstupu systému neobjeví *nedetekovaná chyba*, což nelze vyjádřit žádným spolehlivostním ukazatelem. Kromě vlastní pravděpodobnosti výskytu chyby tu totiž hraje významnou roli i pravděpodobnost detekce chyby. Zvýšené bezpečnosti systému se dosahuje použitím průběžných kontrol správnosti funkce systému. Metody kontroly lze rozdělit na:

- obvodové,
- programové,
- mikroprogramové,
- smíšené (hybridní, kdy se používají kombinace předchozích metod).

Nejběžnější obvodové kontroly pracují s pomocí:

- redundance (informační = bezpečnostní kódy, obvodová = zdvojování atd.),
- predikce následujícího stavu,
- kontrola časových sousledností.

Výstupem hlídačů průběžných kontrol lze ovlivnit činnost systému. Systém lze zastavit, lze modifikovat jeho činnost, rekonfigurovat používané prostředky a zdroje, degradovat výkonnost

nebo funkce systému, případně zajistit vhodným způsobem zotavení po chybě.

Pokud výstupem hlídačů těchto kódů ovlivníme činnost systému, můžeme zabránit škodlivým důsledkům, které by v řízené soustavě měla nesprávná činnost elektronického systému.

Aplikace, při nichž na správné činnosti systému závisejí velké materiální hodnoty, případně lidské životy, obvykle vyžadují vysokou bezpečnost i spolehlivost.

1.2 Metody řízení spolehlivosti

Každý uživatel přirozeně požaduje co nejvyšší spolehlivost zařízení, které používá. Požadavek zvyšování spolehlivosti přitom obvykle implicitně zahrnuje současné zlepšení všech ukazatelů spolehlivosti, které je však většinou nerealizovatelné nebo realizovatelné jen v omezené míře. Výhodné je, když se nám podaří snížit hodnotu *intenzity poruch* λ, protože tím automaticky zlepšíme hodnoty všech důležitých ukazatelů spolehlivosti. To má za následek zvýšení pravděpodobnost bezporuchového provozu, prodloužení střední doby bezporuchového provozu, zvýšení hodnoty součinitele pohotovosti, atd.). Takovýto zásah, který lze jednoznačně označit jako zvýšení spolehlivosti, je však nesmírně obtížný, protože metody snižování intenzity poruch jsou velmi složité a především nákladné.

Pro metody a opatření vedoucí ke snižování intenzity poruch se vžilo souhrnné označení ***předcházení poruchám*** (angl. *fault avoidance*). Použitelnost těchto metod je omezená, protože od jisté úrovně rostou náklady spojené s dalším snižováním intenzity poruch neúměrně rychle a také proto, že se vyskytují objektivní fyzikální překážky, jejichž překonání se vymyká našim možnostem, resp. znalostem.

V takové situaci je třeba hledat jiné možnosti zlepšování hodnot ukazatelů spolehlivosti. Jednou z nich je možnost vzít výskyt poruch v úvahu a respektovat ho při návrhu a realizaci systému. Smíříme se tedy s tím, že k poruchám součástek bude docházet i nadále, ale dosáhneme toho, že se tyto poruchy nebudou projevovat na chování systému, případně se budou projevovat jen minimálně. Tento způsob reakce na poruchy se nazývá ***odolnost proti poruchám*** nebo ***tolerance poruch*** (angl. *fault tolerance*) a systém, který je takové reakce schopen, je ***systém odolný proti poruchám*** (angl. *fault-tolerant system*). Při hodnocení spolehlivosti systému odolného proti poruchám pak musíme rozlišovat mezi poruchou součástky a poruchou systému, označovanou též jako *selhání systému* (angl. *failure*). Za poruchu systému považujeme pouze takovou poruchu jeho součástek, která způsobí nepřijatelnou změnu chování, takže je ve smyslu definice poruchy z ods. 1.1 ukončena schopnost systému jako celku plnit požadovanou funkci. Odpovídajícím způsobem pak musíme upravit i metodu výpočtu hodnot jednotlivých ukazatelů spolehlivosti (např. střední doba mezi poruchami bude měřena výlučně na základě poruch systému jako celku, apod.).

Společnou vlastností všech metod tolerance poruch je nerovnoměrnost jejich vlivu na jednotlivé ukazatele spolehlivosti. To znamená, že pro zlepšení hodnoty jednoho ukazatele máme k dispozici určité metody, které mohou hodnotu jiného ukazatele buď zlepšit jen v omezené míře, nebo ponechat beze změny, či dokonce zhoršit. Vhodná metoda se pak volí jako kompromis mezi požadavky kladenými na hodnoty různých ukazatelů spolehlivosti a je ovlivněna ještě dalšími omezujícími podmínkami, jako je cena, hmotnost, rozměry, spotřeba energie, apod. V takovém případě tedy nemůžeme zaručit zlepšení všech ukazatelů spolehlivosti současně, takže by nebylo správné mluvit zjednodušeně o zvyšování spolehlivosti. Budeme proto používat obecnější výraz řízení spolehlivosti.

1.2.1 Předcházení poruchám

Metody předcházení poruchám byly již teoreticky podrobně rozpracovány, avšak s jejich uplatněním v praxi stále nemůžeme být spokojeni. Je to způsobeno především překážkami organizační povahy, případně ekonomickými hledisky. Navíc stojí v cestě i zmíněné fyzikální překážky. Víme, že pro projekty, v nichž jsou na spolehlivost kladeny extrémní požadavky, jsou výrobci schopni zajistit – za příslušnou cenu – spolehlivostní ukazatele o několik řádů lepší, než je běžný standard. S takovou extrémní spolehlivostí však konstruktér nemůže při běžných projektech počítat. Přesto existuje řada metod, jak u sériově vyráběných součástek zaručit co nejvyšší *„rozumně“* dosažitelnou spolehlivost. Tyto metody nelze přehlížet jako překonané nebo dokonce nepotřebné, protože můžeme velmi snadno dokázat, že takto lze tolerovat určitý počet poruch. Nejprve tedy musíme využít všech dosažitelných prostředků předcházení poruchám, a pouze na zbývající poruchy uplatnit metody tolerance. S nejdůležitějšími metodami předcházení poruchám se proto musí seznámit každý odborník bez ohledu na to, jaké metody řízení spolehlivosti bude používat.

Poruchám lze předcházet při návrhu, výrobě i provozu systému. Při návrhu je třeba především volit spolehlivou součástkovou základnu a spolehlivou technologii. V obou případech musíme brát v úvahu podmínky, v nichž bude výsledný systém pracovat. Kromě toho je třeba volit optimální pracovní bod všech součástek z hlediska výkonu (nevyčerpávat povolené zatížení výstupů), tepelného režimu (zajistit dostatečné chlazení), napájení, odrušení, pracovní frekvence, apod.

Při výrobě hraje klíčovou roli vstupní kontrola součástek, polotovarů a použitých materiálů. Důležitost vstupní kontroly vyplývá z výsledků řady prováděných rozborů a statistických výzkumů. Např. firma DEC (později integrovaná do firmy COMPAQ) vyřazovala při vstupní kontrole 2,5 % všech součástek, které pocházely od subdodavatelů. Mezi převzatými součástkami pak zůstávalo jen 0,04 % vadných. Cenu, kterou za takto dokonalou vstupní kontrolu zaplatí uživatel, je možné chápat též jako cenu za zvyšování spolehlivosti. Sami výrobci se snaží zajišťovat spolehlivost především velkou technologickou kázní, sledovat průběžnými (mezioperačními) kontrolami. Výsledné výrobky se navíc podrobují tzv. spolehlivostním testům, při nichž se zkoušejí při zvýšené, případně snížené teplotě, při zvýšeném napětí, při vibracích, apod.

Z hlediska předcházení poruchám jsou velmi účinné různé teplotní cykly, protože při nich se projeví skryté poruchy, které by jinak mohly ovlivnit funkci výrobku až během jeho použití. Z hlediska průběhu intenzity poruch to znamená, že se snažíme podstatně zkrátit první úsek křivky (období časných poruch) a při montáži pak používat již jen součástky s konstantní intenzitou poruch. Při tom je však třeba podrobně znát fyzikální děje, které probíhají v testovaných součástkách, a pečlivě jim přizpůsobit teplotní režim. Neodborně a především nedbale prováděné teplotní cykly (např. bez možnosti přesně nastavovat a měřit pracovní teploty) mohou naopak snížit spolehlivost, protože způsobí vznik nových degradačních mechanismů, které se projeví až při použití součástky.

K významným metodám předcházení poruchám patří i zvyšování stupně integrace polovodičových součástek. Vývody pouzdra patří k nejporuchovějším částem integrovaných obvodů, takže snížením počtu pouzder ubývá nespolehlivých míst. Navíc odpadá i poruchové propojování plošnými spoji a zmenšuje se tepelné vyzařování (ubývá výstupních budičů).

Z hlediska provozu je pro předcházení poruchám nejdůležitější dodržování technických

podmínek. Mezi ně patří požadavky na:

- klimatické podmínky (teplota, vlhkost a prašnost vzduchu),
- intenzitu rušení (ze sítě i přímým vyzařováním ze zdrojů),
- stabilitu napájení, apod.

Navíc je třeba zajistit pravidelnou profylaxi a opravy v souhlase s předpisy výrobce. Vzhledem k tomu, že se na výpadcích systému významnou měrou podílí i vliv lidského činitele, je třeba omezit možnosti jeho chybných zásahů. Toho se dosahuje čitelným a srozumitelným označením ovládacích prvků, vytvořením kvalitní dokumentace a převedením komunikace člověka s počítačem do takové formy, která je člověku blízká a srozumitelná (přirozený jazyk, grafické symboly, apod.).

1.3 Odolnost proti poruchám

Systém se označuje jako odolný proti poruchám, jestliže je schopen správně vykonávat svou funkci i v přítomnosti poruch technického vybavení nebo chyb v programech. Protože však termín „správně vykonávat funkci“ lze chápat různě, je třeba upřesnit, kdy je funkce považována za správně vykonanou. Obvykle se vyžaduje splnění těchto tří podmínek:

- zpracování dat nebylo zastaveno ani zaměněno v důsledku poruchy,
- výsledek je správný,
- výsledek byl získán v předepsané době.

Jsou-li splněny pouze některé z uvedených tří požadavků (např. výsledek je správný, ale byl dodán opožděně), označuje se systém jako ***částečně odolný proti poruchám***. První požadavek, tedy zachování funkceschopnosti programu, se ovšem považuje za dominantní, takže musí být splněn i v systémech, které jsou odolné jen částečně.

Během práce na projektech systémů odolných proti poruchám, z nichž mnohé byly realizovány a vyzkoušeny v praxi, se vyvinula poměrně dobře propracovaná metodika návrhu založená na heuristických postupných aproximacích výsledku, takže jeho aplikace vyžaduje značnou míru zručnosti a zkušeností. Navíc nikdy nešlo předem rozhodnout, zda bude dosažen cíl, který byl zvolen. V současné době však tento postup představuje nejlepší metodu, která byla na základě dosavadních znalostí zformována.

Návrh systému odolného proti poruchám vychází obvykle z tzv. neodolného systému, tedy systému navrženého s minimálními prostředky, které splňují dané požadavky na funkci. Tento prvotní tvar systému se pak dále zdokonaluje postupnými obměnami a doplňky tak, aby se co nejvíce přiblížil ideálnímu stavu splňujícímu všechny požadavky na spolehlivost při dodržení omezujících podmínek.

Hlavní fáze, kterými návrh systému odolného proti poruchám prochází, jsou tyto:

- stanovení cílů,
- volba metod detekce poruch,
- návrh algoritmů zotavení po poruše,
- vyhodnocení odolnosti proti poruchám.

V první fázi je třeba vytvořit především jasně formulované ***zadání projektu***. Vzhledem k tomu, že žádný systém nemůže být odolný proti „všemu, co může selhat“, je třeba přesně specifikovat všechny situace, v nichž si systém má zachovat funkceschopnost. Prakticky to znamená sestavit co nejúplnější seznam poruch, které při provozu systému mohou nastat, a roztřídit je podle

pravděpodobnosti výskytu, případně podle toho, jak na ně systém má reagovat. Pokud v některých případech připustíme, aby jeho funkceschopnost byla omezená, musíme dostatečně přesně charakterizovat všechny přípustné změny, např. pokles výkonnosti, prodloužení doby reakce, omezení repertoáru funkcí, které systém dokáže vykonávat, apod.

Dále musíme stanovit mezní hodnoty ukazatelů spolehlivosti pro výsledný systém. Tyto hodnoty se často vztahují k určitým specifickým typům poruch (např. omezujeme střední dobu do poruchy opravitelné za provozu), nebo k jednotlivým dílčím funkcím systému. Proto je třeba hned na začátku projektu stanovit metodiku, podle níž se bude hodnotit dosažený stupeň odolnosti výsledného systému proti poruchám. K této otázce se podrobněji vrátíme při upřesnění čtvrté fáze popisované metody návrhu.

Systémy odolné poruchám zajišťují následující činnosti:

- detekci poruch,
- zotavení po poruše.

1.3.1 Detekce poruch

Detekce poruch má při zajišťování odolnosti klíčový význam, protože systém je schopen správně reagovat pouze na ty poruchy, o nichž je dostatečně přesně informován. Při volbě metod detekce poruch je třeba vzít v úvahu, jaké typy poruch se v systému mohou vyskytnout (při tom můžeme použít seznam sestavený během první fáze návrhu), jak rychle má systém na jednotlivé typy poruch reagovat, jaké prostředky jsou již v systému k dispozici, atd. Metodami a prostředky detekce poruch se zabývá diagnostika číslicových systémů, jíž byla věnována řada specializovaných publikací. Zde se proto omezíme jen na stručnou rekapitulaci nejdůležitějších poznatků.

Diagnostika, používaná v číslicových systémech odolných proti poruchám, můžeme mít jednu z těchto čtyř forem:

- spouštěcí diagnostika,
- periodická diagnostika,
- průběžná diagnostika,
- diagnostika redundantních částí.

Spouštěcí diagnostika je soubor diagnostických testů spouštěných automaticky při zapnutí napájecího napětí. Jejich úkolem je prověřit v co nejkratší době všechny důležité funkce systému a signalizovat případnou poruchu obsluze. Jsou to tedy pouze detekční testy, které navíc často nebývají úplné, především tehdy, když aplikace nedovoluje příliš odkládat okamžik zahájení provozu systému.

Periodická diagnostika se provádí v přestávkách mezi aplikačními programy. Po dobu testu tedy musí být výpočet na určitou dobu přerušen, aby systém mohl být podroben testu. Výsledkem takového testu je úplná informace o technickém stavu testované jednotky v okamžiku provedení testu. Není však zaručeno, že se tento stav nezmění ani během následujícího výpočtu až do okamžiku příštího testu. Proto je třeba volit periodicitu testů tak, aby pravděpodobnost vzniku poruchy mezi dvěma po sobě následujícími provedeními testů byla dostatečně malá.

Průběžná diagnostika představuje nepřetržitý zdroj informací o správnosti operací prováděných v systému a je v podstatě totožná se zabezpečením systému proti poruchám. Obvykle je

založena na *kontrole správnosti bezpečnostního kódu*. Hlavní výhodou průběžné diagnostiky realizované tímto způsobem je její časová nenáročnost (výpočet se nepřerušuje ani nezpomaluje) a velmi jednoduché řízení. Průběžná diagnostika však může být realizována i jinou formou kontroly správnosti výsledku, např. *kontrolním výpočtem* probíhajícím v jiném procesu, *opakovaným výpočtem* ve stejném procesu, jednoduchou kontrolou důležitých vlastností získaného výsledku (např. *porovnáním s mezními hodnotami*), apod.

Velmi oblíbeným prostředkem kontroly správné funkce číslicových systémů, zejména pokud jsou použity při řízení v reálném čase, je tzv. hlídací časovač (angl. *watchdog timer*), někdy nazývány také diagnostické hodiny. Je to v podstatě čítač, který v předem stanovených intervalech pravidelně přerušuje činnost procesoru a vyžaduje obsluhu (nulování nebo nastavení výchozí hodnoty). Jestliže procesor nezareaguje správně a v předepsaném čase, signalizuje hlídací časovač poruchu, případně přímo vyvolá zotavení po poruše.

Určitou nevýhodou průběžné diagnostiky je závislost rozsahu získané informace o technickém stavu objektu na řešeném problému, protože *průběžná diagnostika signalizuje jen takové poruchy, na které je navržena* (které byly vybrány jako pravděpodobné, že by mohly nepříznivě ovlivnit funkci).

Obvod pracující s bezpečnostně kódovanými informacemi, jejichž správnost se kontroluje hlídačem kódu, se nazývá samočinně kontrolovaný (*self - checking*). Z hlediska kvality diagnostiky je však účelné, aby obvod byl schopen indikovat správnost své funkce. Takový obvod se nazývá úplně *samočinně kontrolovaný* (*totally self - checking*, zkratka ***TSC***). Formálně se úplně samočinně kontrolovaný obvod definuje jako *samočinně testovaný* a současně *bezpečný proti poruchám*. Obvod je samočinně testovaný, jestliže vektory převedené na jeho vstupy během normálního provozu tvoří úplný diagnostický test. Bezpečný proti poruchám je obvod, v němž lze poruchu, která způsobí chybu výstupního signálu, zjistit na základě kontroly správnosti kódu výstupu.

Redundantní části se diagnostikují proto, že bez informací o technickém stavu záložních prvků bychom riskovali, že některý z těchto prvků bude nepoužitelný ve chvíli, kdy bychom na něj potřebovali přenést funkci. Záložní prvky jsou většinou vystaveny stejným podmínkám jako prvky provádějící vlastní řízení (i když většinou jsou bez zátěže nebo jejich pracovní zátěž je menší), takže u nich nemůžeme předpokládat nulovou intenzitu poruch.

1.3.2 Zotavení po poruše

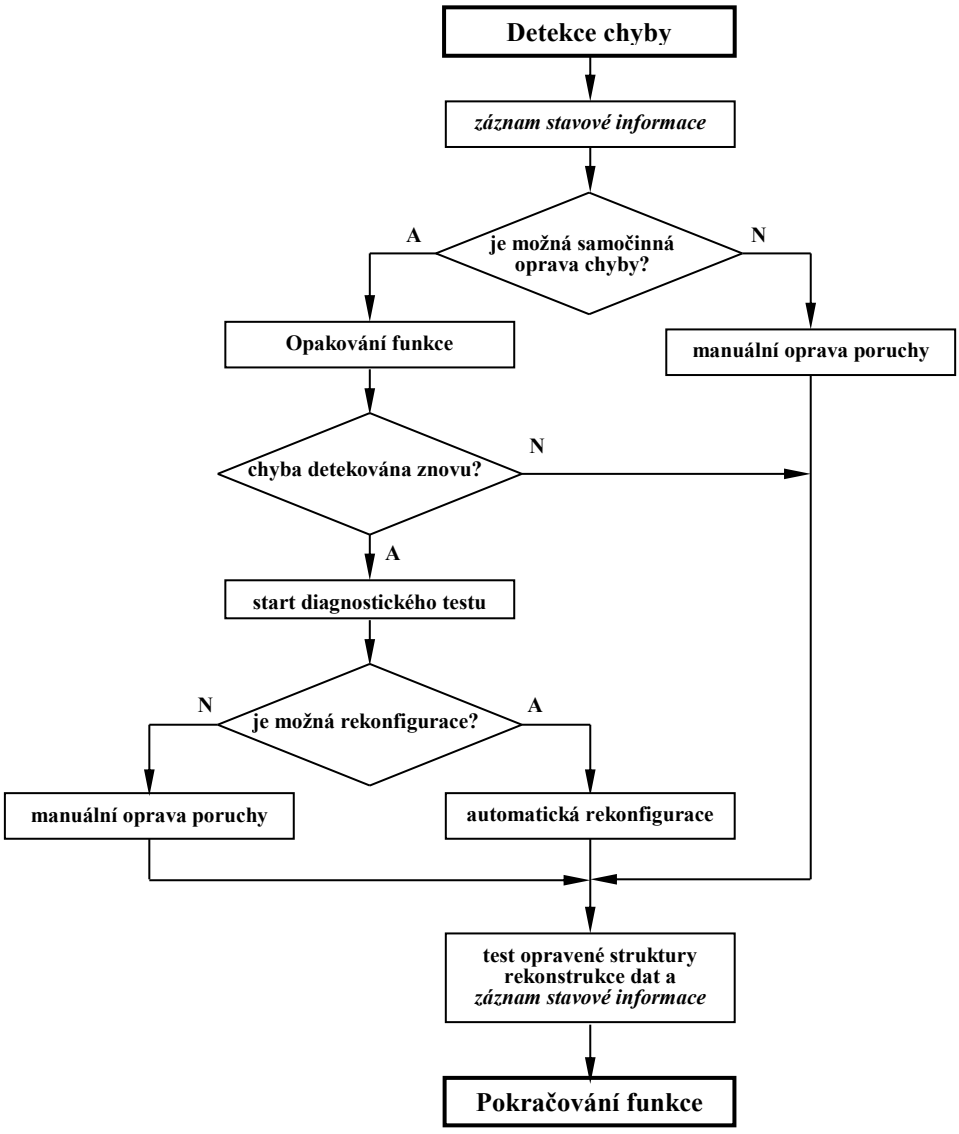
Zotavení po poruše zahrnuje všechny úkony, které je třeba provést od okamžiku zjištění poruchy do obnovení funkce systému. Zotavení je vlastně hlavním nástrojem odolnosti proti poruchám, a proto má určující význam pro kvalitu výsledného systému. Průběh zotavení po poruše určuje, jak bude systém reagovat na poruchu. Podle výsledků můžeme rozlišovat tři úrovně zotavení:

- zotavení do původní úrovně funkceschopnosti,
- zotavení do degradovaného stavu,
- bezpečné ukončení funkce.

Každá úroveň zotavení je v praxi užitečná. Záleží na úrovni technického a programového vybavení systému. Šíře technického a programového vybavení představuje zvýšené náklady na pořízení a provoz systému, a proto konkrétní konfigurace závisí na účelu použití systému a na požadavcích odběratele.

Obecný tvar vývojového diagramu zotavení po poruše je znázorněn níže - viz Obrázek 1.3. Pro úplnost je třeba připomenout, že k zotavovacím mechanismům v obecném slova smyslu patří i obvodové maskování chyby, i když při něm k detekci poruch nedochází. Tato nejdokonalejší, nejrychlejší, ale též nejnákladnější forma zotavení je výhodná tím, že porucha se neprojeví chybou na výstupu systému.

Vyhodnocení odolnosti proti poruchám je kontrolou, do jaké míry se nám podařilo splnit zadání. Protože s formulací požadavků na odolnost i s jejich ověřováním jsou zatím poměrně malé zkušenosti, je třeba dbát na to, aby při hodnocení byla použita stejná kritéria jako při formulaci zadání. Používají se analytické metody hodnocení, tj. výpočet, dále simulační metody a ověřování na funkčním vzoru. Kromě číselných hodnot vybraných ukazatelů spolehlivosti se hodnotí též některé další vlastnosti, které se spolehlivostními ukazateli souvisejí jen nepřímo (úspěšnost zotavení, pokrytí poruch, schopnost reakce na změněné pracovní podmínky, apod.). Používá-li systém též zotavení do degradovaného stavu, vyhodnocuje se i pravděpodobnost přechodu na různé úrovně výkonnosti.



Obrázek 1.3: Vývojový diagram zotavení po chybě

1.3.3 Oblasti využití systémů odolných proti poruchám

Odolnost proti poruchám byla donedávna výsadní vlastností systémů používaných v několika privilegovaných oborech, např. v kosmonautice, letectví nebo ve vojenské technice. S poklesem ceny, rozměrů a energetické náročnosti elektronických systémů však odolnost proti poruchám postupně proniká do řady dalších aplikačních oblastí, takže již zdaleka není ničím výjimečným. Za všechny příklady, dokumentující její potřebnost, uveďme alespoň jeden, který je velmi přesvědčivý.

Dne 22. listopadu 1985 utrpěla Bank of New York během půl druhé hodiny ztrátu 5 miliónů dolarů jen proto, že v jejím ústředním počítači se vyskytla porucha, které si nikdo nevšiml. Počítač totiž začal vyzvedávat peníze z konta u centrální banky a během uvedené doby si stačil „vypůjčit“ 32 miliardy dolarů. I když dlužná částka byla při nejbližší příležitosti vrácena, musela Bank of New York zaplatit za tuto neobvyklou výpůjčku úroky, které představovaly vzniklou ztrátu. Kdyby systém použitý ve zmíněné bance byl odolný proti poruchám, tak by k takovému omylu by s největší pravděpodobností nemohlo dojít.

Uvedený příklad, stejně jako mnoho podobných, které můžeme najít v tisku, dokazuje, jak je každodenní život je v současnosti závislý na komunikačních a výpočetních systémech. Z toho, jak velké škody může jejich případné selhání způsobit, lze odvodit, jak velkou částku se vyplatí investovat do zajištění jejich odolnosti proti poruchám. Při aplikacích v oblasti financí je takový výpočet poměrně jednoduchý, protože potenciální ztráty jsou přímo vyjádřeny v měnových jednotkách a lze je tedy velmi snadno srovnat s pořizovacími, případně udržovacími náklady na výpočetní techniku. Poměrně přehledné jsou i vztahy ve výrobní sféře a ve službách, protože i zde můžeme porovnávat měnové jednotky. Složitější situace ale nastává tam, kde je v sázce *zdraví, nebo politické důsledky*, apod. Zde jsme obvykle nuceni vzdát se přesných kalkulací, protože uvedené hodnoty lze těžko vyčíslit (i když pojišťovny mají sazebník i pro tyto kategorie). Klesající cena a snadná dostupnost systémů odolných proti poruchám však usnadňují rozhodování, protože díky jim lze tyto systémy použít i v případech, které by donedávna byly považovány za sporné.

Podle povahy řešeného problému lze úlohy vyžadující použití systémů odolných proti poruchám rozdělit do několika aplikačních oblastí. Mezi nejrozsáhlejší patří *řízení v reálném čase* a *zpracování transakcí ve spřaženém režimu*. Kromě toho existuje velké množství speciálních oblastí, pro které se většinou používají systémy odvozené z uvedených hlavních kategorií.

Řízení v reálném čase se využívá především ve výrobní sféře (při řízení technologických procesů), v dopravě (včetně kosmických letů), v lékařství, apod. Tyto aplikace kladou vysoké nároky na hodnotu pravděpodobnosti bezporuchového provozu, zatímco hodnoty ostatních ukazatelů spolehlivosti (včetně střední doby bezporuchového provozu) většinou nejsou považovány za kritické. Systémy používané pro tento typ aplikací se někdy zjednodušeně označují jako ***vysoce spolehlivé***.

Zpracování transakcí ve spřaženém režimu se využívá především v bankách, spořitelnách, pojišťovnách, na poštách, ve zdravotnické službě, při rezervaci místenek na nejrůznější dopravní prostředky a v mnoha dalších aplikacích vyžadujících styk s bázemi dat. Do této kategorie patří též systémy používané v telekomunikacích, zejména pro číslicové řízení telefonních ústředen. Většina těchto úloh vyžaduje především velkou pohotovost. Naproti tomu krátkodobý výpadek systému není považován za kritický, takže pro pravděpodobnost

bezporuchového provozu většinou nejsou vyžádány extrémní hodnoty. Systémy této kategorie se zjednodušeně nazývají ***vysoce pohotové***.

Další důležitou kategorii systémů odolných proti poruchám představují systémy, u nichž jsou kladeny značné nároky na hodnotu střední doby bezporuchového provozu. Patří sem například tzv. ***systémy s odloženou údržbou***, u nichž je pevně stanovena doba, během níž nelze provádět údržbu. Typickým reprezentantem této kategorie jsou palubní počítače letadel. Další speciální aplikační oblast představují systémy s dlouhou životností, u nichž se s údržbou nepočítá vůbec. Jsou to např. počítače pro nepilotované kosmické lety, nepřístupné pozemní nebo podmořské stanice, apod.

Závěrem je třeba zdůraznit, že uvedený výčet je provizorní, protože počet oblastí, v nichž se uplatňují systémy odolné proti poruchám, se neustále zvětšuje. Každý úspěch totiž vyvolává snahu vyzkoušet výhody odolnosti proti poruchám i v dalších oblastech, což je značně usnadňováno celkovým rozšířením výpočetní techniky.

Seznam obrázků