Návrh časově kritických systémů I: specifikace a verifikace

Josef Strnadel

Při návrhu systému může být požadováno, aby na vstupní podněty reagoval nejen správnou odezvou, ale aby navíc tuto odezvu poskytl včas, tj. v předem vymezeném časovém intervalu měřeném od vzniku podnětu. Při vývoji takovýchto systémů jsou velmi důležité zejména fáze jejich specifikace, verifikace a realizace v souladu s verifikovanou specifikací. V článku, prvním z připravené volné série čtyř příspěvků autora věnovaných problematice návrhu časově kritických systémů (systémů reálného času, systémů RT), jsou přehledově představeny první dvě z uvedených fází s ilustrací souvisejících pojmů na příkladech.

Časově kritické systémy se vyznačují především tím, že je u nich spolu s funkčně správnou odezvou na daný podnět požadováno také *včasné* poskytnutí této odezvy. Běžně jsou označovány jako *systémy pracující v reálném čase*, *systémy pracující s reálným časem* či *systémy pro řízení v reálném čase* – zkráceně také *systémy reálného času*, popř. *systémy RT*, v zahraniční literatuře *RTS* (*Real Time Systems*) [1]. Ačkoliv si to mnohdy neuvědomujeme, setkáváme se s nimi běžně v každodenním životě. Nacházejí totiž uplatnění v časově kritických úlohách vyskytujících se v mnoha oblastech lidské činnosti, počínaje jednoduchými řídicími systémy běžně používanými v domácnostech (např. mikrovlnné trouby, pračky, chladničky), přes systémy zabudované v komunikačních a multimediálních zařízeních (např. mobilní telefony, PDA, digitální fotoaparáty, kamery, přehrávače DVD, herní konzoly), dopravních prostředcích (např. automobily, letadla), lékařských přístrojích (např. přístroje pro monitorování životních funkcí člověka, přístroje pro dávkování léků) až po komplexní systémy řídicí průmyslová či armádní zařízení, dopravu apod. (např. systémy pro řízení výrobních linek, provozu v dopravních uzlech, zbrojní systémy či systémy řídicí provoz jaderného reaktoru atd.).

Okamžitá odezva nemusí být včasná

I ze shora uvedeného, zdaleka ne úplného výčtu oborů a úloh vyžadujících použití systémů RT lze vytušit, že požadavky na ně kladené se v konkrétních případech mohou výrazně lišit – a to nejen z hlediska časové kritičnosti, ale také např. bezpečnosti a provozuschopnosti. Navíc je velmi důležité si uvědomit, že význam pojmu *včas* velmi výrazně závisí na konkrétní úloze, a tudíž laicky očekávaná rovnost *odezva v reálném čase* = = *okamžitá odezva* obecně neplatí.

Odezva poskytnutá dříve, než je třeba, totiž může mít stejný dopad jako odezva poskytnutá pozdě či odezva žádná. Jistě však platí, že čím vážnější následky může mít nedodržení *časových mezí kladených na jednotlivé odezvy* (dále jen *mezí odezev*), tím větší požadavky musí být kladeny na daný systém RT. Pro ilustraci uveďme kontrast mezi následky vzniklými nedodržením mezí odezev v systému pro bezhotovostní úhradu platební kartou a v systému pro řízení železničního přejezdu.

V prvním případě povede nedodržení (způsobené např. přetížením bankovních serverů) k prodloužení doby potřebné k provedení platební transakce, popř. k úplnému zrušení transakce po vypršení časového limitu daného komunikačním protokolem mezi platebním terminálem a bankou. V takovém případě bude nutné celou bezhotovostní transakci opakovat, popř. v mezní situaci zaplatit v hotovosti. Tyto skutečnosti, např. spolu s nutností řešit vzniklou situaci tehdy, kdy kupující u sebe nemá potřebnou hotovost, mohou vést k narušení psychické rovnováhy zúčastněných osob, nutnosti vzdát se pracně vybraného nákupu, popř. stížnostem na kvalitu služeb. Tyto ani další související následky však zpravidla nelze označit za vážné.

Jinak tomu ovšem je v případě, kdy nejsou dodrženy odezvy v systému pro řízení železničního přejezdu. V takovém případě může systém reagovat v nesprávném čase např. na příjezd vlaku k přejezdu či odjezd vlaku z přejezdu opožděným či předčasným pohybem závor nebo aktivací světelného či zvukového výstražného zařízení. Následky tohoto nedodržení mohou být bezpochyby velmi vážné – újma na zdraví a psychice zúčastněných osob, úmrtí, velké škody na majetku a životním prostředí.

Klasifikace mezí odezev a systémů reálného času

Z uvedeného ilustrativního kontrastu mezi požadavky kladenými na systémy RT je dále patrné, že některé meze odezev v rámci systémů RT mohou být z hlediska časové kritičnosti naléhavější než jiné. Aby bylo možné tuto naléhavost určitým způsobem vyjádřit, musí být každá z mezí odezev již v ranných

Tab. 1. Typy mezí odezev systémů RT – klasifikace a charakteristika

Typ meze odezvy	Časová kritičnost typu meze	Charakteristika typu meze	Příklad
měkká (*soft*)	malá	meze odezev tohoto typu jsou optimální k dosažení uživatelem očekávané kvality služeb poskytovaných systémem RT; nedodržení mezí odezev, např. při přetížení systému v důsledku nadměrného počtu podnětů, zpravidla vede k dočasnému poklesu kvality služeb se zanedbatelnými dopady na okolí systému	mez pro přivolání výtahu po stisku tlačítka; mez reakce ve videohře
tvrdá (*hard*)	velká	každá mez odezev tohoto typu musí být bezpodmínečně dodržena; nedodržení jediné z nich vede k nevratným a trvalým následkům v okolí systému, neboť reakce v okolí systému nebyla provedena včas; pokusy o dodržení jakýchkoliv dalších mezí jsou nemožné nebo zbytečné, jelikož vlivem selhání podstatné vlastnosti systému již neexistuje způsob vedoucí ke zmírnění vzniklých následků	mez pro zasunutí regulačních tyčí do jaderného reaktoru po zjištění poruchy v chladicím okruhu
pevná (*firm*)	střední	meze odezev tohoto typu se typicky vyznačují předem danou tolerancí jejich nedodržení; překročení této tolerance může mít vážný dopad na okolí systému; ale – je-li tolerance navrhována s dostatečnou rezervou – systém může předvídat její potenciální překročení s předstihem dostačujícím ke včasnému spuštění zotavovacích mechanismů; při překročení tolerance a neschopnosti systému zotavit se ze vzniklé situace může být např. signalizována nutnost řešit vzniklou situaci prostředky mimo systém; následky nedodržení mezí tohoto typu jsou typicky vratné a mohou být dodatečně zmírněny či zcela odstraněny, neselžou-li záchranné mechanismy	mez pro ventilaci plic pacienta ležícího na jednotce intenzivní péče: tolerance 1 s, signalizace lékaři

etapách vývojového cyklu systému zařazena do jedné ze tří typových kategorií jako odezva *měkká*, *tvrdá* nebo *pevná* podle charakteristiky uvedené v *tab. 1*.

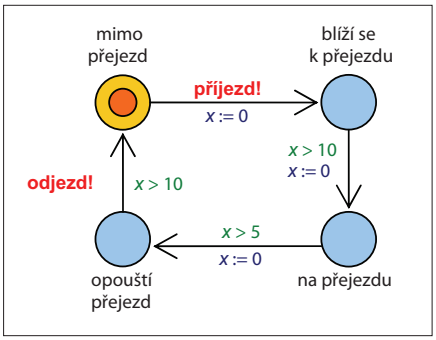
Podle uvedené klasifikace mohou být rozčleněny i systémy RT, přičemž typ systému RT je určen typem časově nejkritičtější meze zahrnuté ve vstupních požadavcích kladených na systém v jeho tzv. *specifikaci*. Zvláště tvrdé (*hard*) systémy RT musí být konstruovány tak, aby už způsobem jejich návrhu bylo možné vyloučit, že budou-li za běhu systému splněny požadavky dané jeho specifikací, mohou být překročeny některé z mezí odezev.

Specifikace

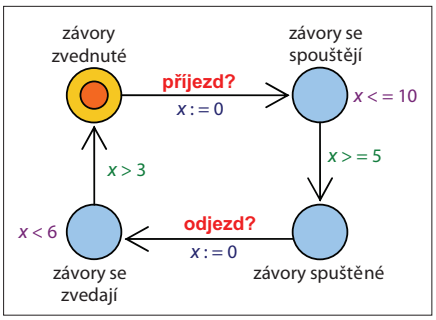
Prvotní specifikace systému RT je obvykle zapsána s použitím prostředků *přirozeného jazyka* (např. český, anglický). Tato forma zápisu bývá typicky používána při komunikaci se zadavatelem systému, jelikož je pro něj často nejsrozumitelnější a umožňuje mu plně se soustředit na detaily zadání. Avšak, zejména v souvislosti s návrhem složitějších systémů RT, je pouze tato (neformální) forma zápisu specifikace nevhodná, jelikož může vést k nejednoznačnostem, rozporům, komplikacím při ověřování vlastností systému či strojovém zpracování specifikace. Specifikace v přirozeném jazyce tedy bývá převedena na specifikaci formální, často zapsanou např. prostředky *logiky reálného času* (*Real-Time Logic* – RTL) [1], *časovaných automatů* (*Timed Automaton* – TA) [4], SMV (*Symbolic Model Verifier*, [5]) či grafického hierarchického popisu systémů, mezi které patří např. nástroje Modechart [1] nebo RT-Lotos [3]. Protože detailní popis prostředků formální specifikace značně překračuje rámec tohoto článku, ilustrujme tuto návrhovou etapu alespoň na jednoduchém systému RT *vlak-přejezd*, vytvořeném pro cvičení v rámci jednoho z předmětů vyučovaných na pracovišti autora [6]. Daný systém je specifikován přirozeným jazykem (v našem případě českým) takto: systém je tvořen jedním podsystémem typu *vlak* a jedním podsystémem typu *přejezd*,

- *specifikace vlaku*:
  - vlak blížící se k přejezdu vyšle přejezdu signál PŘÍJEZD,
  - vlak vjede na přejezd za více než 10 s po vyslání signálu PŘÍJEZD,
  - přes přejezd vlak jede déle než 5 s; poté přejezd opouští,
  - vlak vyšle přejezdu signál ODJEZD za více než 10 s od zahájení opouštění přejezdu,
- *specifikace přejezdu*:
  - závory přejezdu jsou zvednuté, dokud přejezd neobdrží signál PŘÍJEZD,
  - obdrží-li přejezd signál PŘÍJEZD, závory se začnou spouštět, což trvá od 5 do 10 s; po dokončení spouštění jsou závory spuštěné,
  - závory přejezdu jsou spuštěné, dokud přejezd neobdrží signál ODJEZD,
  - obdrží-li přejezd signál ODJEZD, závory se začnou zvedat, což trvá déle než 3 a méně než 6 s; po ukončení zvedání jsou závory zvednuté.

Na *obr. 1* a *obr. 2* jsou ukázány odpovídající specifikace vyjádřené s použitím časovaných automatů (TA). Podsystém (*vlak*, popř. *přejezd*) je reprezentován dvěma komunikujícími TA, jejichž kompozicí vznikne výsledný TA, přičemž oranžově obarvený stav je počáteční, červené značení hrany zakončené znakem *!*, popř. *?* znamená vyslání, popř. čekání na příjem signálu, *x* je lokální čas automatu, *x := 0* je příkaz nulování lokálního času, zeleně obarvená značení jsou podmínky proveditelnosti příslušné hrany (tzv. *stráže*) a purpurově obarvená značení stavů určují čas, do kterého může automat setrvat v daném stavu (tzv. *invarianty*).



Obr. 1. Specifikace vlaku prostředky TA



Obr. 2. Specifikace přejezdu pomocí TA

Vedle toho, že specifikace popisuje chování systému RT, je možné ji chápat jako souhrn předpokladů, které musí být splněny pro zajištění dané funkce systému. Mimo jiné to znamená, že při jejich nedodržení lze očekávat, že chování systému může vybočit z popisu daného specifikací.

Verifikace

V další etapě vývojového cyklu, během tzv. *verifikace*, je možné pomocí dotazů ověřit, zda při splnění souhrnu předpokladů bude systém vykazovat očekávané vlastnosti nebo naopak, že určité chování systému nemůže za daných okolností nikdy nastat. Lze se dotazovat na *živost* systému, *bezpečnost*, *dosažitelnost* stavů apod. V případě našeho jednoduchého systému je možné ověřovat např., zda systém *může uváznout* (dotaz 1), zda *vždy, když na přejezdu bude vlak, budou závory spuštěné* (dotaz 2), zda *se spuštěné závory poté vždy zvednou* (dotaz 3). Pro účely strojového zpracování je však vhodnější, podobně jako při tvorbě specifikace, zapisovat dotazy v některém z formálních jazyků – v *tab. 2* je uveden příklad zápisu dotazů 1 až 3 v jazyce logiky s časovým větvením (*Computational Tree Logic* – CTL).

Verifikační nástroj je schopen dotaz zapsaný uvedeným způsobem vyhodnotit a sdělit, zda dotazovaná vlastnost je či není splněna (v *tab. 2* zelený, popř. červený symbol vpravo od dotazu znamená, že dotazovaná vlastnost je, popř. není splněna). V případě, že vlastnost není splněna, jsou nástroje schopné poskytnout informace o tom, za jakých okolností může k nesplnění dojít – tzv. *protipříklad*. Tímto způsobem lze odhalit, zda mezi specifikací a ověřovanými vlastnostmi je či není rozpor, a popř. zahájit činnosti vedoucí k jeho odstranění – obvykle modifikací či doplněním specifikace. Po verifikaci tohoto jednoduchého systému je jisté, že systém (je-li navržen podle uvedené specifikace) nemůže uváznout (dotaz 1) a že vždy, když bude vlak na přejezdu, budou závory spuštěné (dotaz 2).

U dotazu na poslední vlastnost (dotaz 3) je však zřejmé, že tato splněna není. V tomto případě však rozpor představuje rys systému specifikovaného uvedeným způsobem, nikoliv chybu ve specifikaci. Tento rys vysvětlíme blíže. Představme si, že ihned po odeslání signálu PŘÍJEZD vlak zastaví, tj. zůstane ve stavu *blíží se k přejezdu*. Podle specifikace musí v tomto stavu setrvat alespoň 10 s. Ale – horní mez tohoto čekání není specifikována (stavu není přiřazen invariant), a proto přejezd může čekat na signál ODJEZD potřebný ke zvednutí závor spuštěných po přijetí signálu PŘÍJEZD neomezeně dlouho. V systému navrženém podle dané specifikace tedy může za jistých okolností nastat situace, že již spuštěné závory se nezvednou. Proto je vlastnost podle dotazu 3 nesplněna.

Tab. 2. Příklad zápisu verifikačních dotazů prostředky CTL

Dotaz na vlastnost systému zapsaný v přirozeném jazyce	Zápis dotazu v jazyce CTL	Výsledek ověření dotazu
Platí, že systém nikdy neuvázne?	*A [ ] not deadlock*	■
Platí, že vždy, když je vlak na přejezdu, jsou závory spuštěné?	*A [ ] (vlak.na_přejezdu imply přejezd.závory_spuštěné)*	■
Platí, že spuštěné závory se poté vždy zvednou?	*přejezd.závory_spuštěné --> přejezd.závory_zvednuté*	■

Příčin těchto okolností může být několik – např. problémy spojené s přenosem signálu ODJEZD, výpadek proudu na trati po odeslání signálu PŘÍJEZD, nouzové zastavení vlaku před přejezdem apod. Pro tvorbu specifikace a její následné ověření s použitím verifikačních dotazů je možné využít mnoho různých komerčních i volně dostupných nástrojů. Pro základní seznámení se s diskutovanými etapami vývojového cyklu systému RT lze doporučit volně dostupný nástroj Uppaal [4].

Realizace

Po ukončení etap specifikace a verifikace systému RT je možné zahájit fázi jeho realizace (implementace, resp. zavedení). Před jejím započetím je nutné rozhodnout, které části systému budou realizovány obvodově, které programově a jaké prostředky se použijí. Z hlediska časové kritičnosti existuje jediné kritérium: realizovaný systém musí být v souladu s verifikovanou specifikací. K hardwarovým základnám používaným při realizaci systémů RT patří zejména *mikrořadiče* (*Microcontroller Unit* – MCU) programované v jazycích asembler/C, *programovatelná hradlová pole* (*Field-Programmable Gate Array* – FPGA) s tvorbou aplikačních programů v jazycích VHDL/Verilog a *jednodesková PC*. Je-li specifikace systému jednoduchá, není nutné použít vrstvu odstiňující realizovaný systém RT od cílového hardwaru. V opačném případě je tato vrstva nezbytná a obvykle bývá realizována *operačním systémem reálného času* (*Real-Time Operating System* – RTOS), někdy také označovaným termínem *RT jádro*. Operačních systémů reálného času existuje velmi mnoho, od komerčních po volně použitelné, a výjimkou nejsou ani aplikačně specifické RTOS. Předtím, než je možné systém RT realizovat s použitím prostředků RTOS, je třeba převést specifikaci systému RT na tzv. *množinu úloh RT* a zvolit vhodný mechanismus jejich *plánování* (lze použít i označení *rozvrhování*, v tomto a souvisejících článcích se přidržíme označení „plánování" – *pozn. aut.*).

Problematice návrhu systémů RT při použití RTOS se bude podrobněji věnovat navazující článek, který vyjde v některém z dalších čísel tohoto časopisu. Do té doby lze doporučit k prohlédnutí alespoň zdroj základních informací z oblasti RTOS [2].

Poděkování

Článek vznikl za podpory výzkumného záměru MSM0021630528 – *Výzkum informačních technologií z hlediska bezpečnosti* (agentura CEZ MŠMT), projektu specifického výzkumu FIT-S-10-1 (VUT v Brně) a projektu GAČR č. 102/09/1668 – Zvyšování spolehlivosti a provozuschopnosti v obvodech SoC.

Literatura:

[1] CHENG, A. M. K.: *Real-Time Systems: Scheduling, Analysis, and Verification*. Wiley, 2002, 552 s., ISBN 0-471-18406-3.

[2] *eg3 „best of the web" for embedded systems* [online]. 2000 [cit. 2009-08-10]. Dokument dostupný z <http://www.eg3.com/rtos/>.

[3] *RT-LOTOS (Real-Time LOTOS) Project* [online]. 1995 [cit. 2009-08-03]. Dokument dostupný z <http://www.laas.fr/RT-LOTOS>.

[4] *UPPAAL home* [online]. 2006 [cit. 2009-08-24]. Dokument dostupný z <http://www.uppaal.com/>.

[5] *The SMV System* [online]. Model Checking Group at Carnegie Mellon University. 1998 [cit. 2009-08-28]. Dokument dostupný z <http://www-2.cs.cmu.edu/~modelcheck/smv.html>.

[6] SMRČKA, A.: *Uppaal – Železniční přejezd* [online]. 2007 [cit. 2010-03-25]. Dokument dostupný z <http://www.fit.vutbr.cz/~smrcka/fav/guide/train.html>.

Ing. Josef Strnadel, Ph.D.,
Fakulta informačních technologií,
Vysoké učení technické v Brně
(strnadel@fit.vutbr.cz)

krátké zprávy

▸ CAN/J1939 Product Guide 2010

Organizace CAN in Automation (CiA) vydala katalog s názvem *CAN/J1939 Product Guide 2010*, obsahující uspořádané informace o produktech pro obě příbuzné komunikační sběrnice, CAN a J1939. Katalog je dostupný na webové stránce CiA (www.can-cia.org) a popř. také na CD-ROM. Produkty a služby jsou v katalogu setříděny podle svého názvu, kategorie produktu a jména výrobce. V části J1939 jsou všechna zařízení v katalogu navíc zatříděna podle odvětví průmyslu, v nichž se používají. Informace o produktu obsahuje v obou částech katalogu vždy foto, popisující text a detaily kontaktního spojení. V obou verzích, webové i na CD-ROM, mohou uživatelé snadno přecházet mezi oběma částmi katalogu pouhým kliknutím na příslušné logo umístěné na každé jednotlivé stránce v obou částech. Katalog CAN/J1939 Product Guide 2010 na CD-ROM bude distribuován členům organizace CiA a na požádání i ostatním zájemcům poštou, a to zdarma (kontakt: headquarters@can-cia.org). K dispozici bude také na seminářích pořádaných organizací CiA a v jejích stáncích na výstavách a veletrzích.

[CiA, 14. září 2010.] *(sk)*