Spolehlivý a bezpečný provoz PLC s operačním systémem Linux

Jaké možnosti mají ti, kdo chtějí implementovat systémy PLC do prostředí operačního systému Linux, nastínil článek s názvem Kombinace softPLC a operačního systému Linux v Automě č. 6/2008 na str. 59. Tento příspěvek na něj navazuje a věnuje se otázkám spolehlivosti a bezpečnosti takového kombinovaného systému. Zmíněné otázky lze řešit oddělením systémových zdrojů za použití mikrojádra.

Prostorové rozdělení

Pro zajištění běhu hostujícího operačního systému (OS) musí mikrojádro poskytovat přístup k části systémového hardwaru, tedy k paměti a k registrům mapovaným pomocí paměti nebo portů. Mikrojádro umožňuje také přístup k přerušením a dále určuje mechanismus, který zajistí jednak distribuci zdrojů aplikačních programů, které běží na hostujícím OS, jednak rušení přístupu k těmto zdrojům. To vše je třeba udělat bez ztráty flexibility „portování“ různých operačních systémů (tj. upravení programů pro platformu, pro kterou původně nebyly určeny). Zároveň je třeba zajistit co nejsnazší přenos dalších operačních systémů či API. Pro zabezpečení nezávislosti hostujících systémů musí tyto zdroje přidělovat důvěryhodná báze kódu, zde tedy jádro. To každé přihrádce s operačním systémem určí sadu virtuálních adresních prostorů, které budou použity jako „kontejnery“ pro systémové zdroje. Použitím této metody se zamezí vzájemné střety přihrádek.

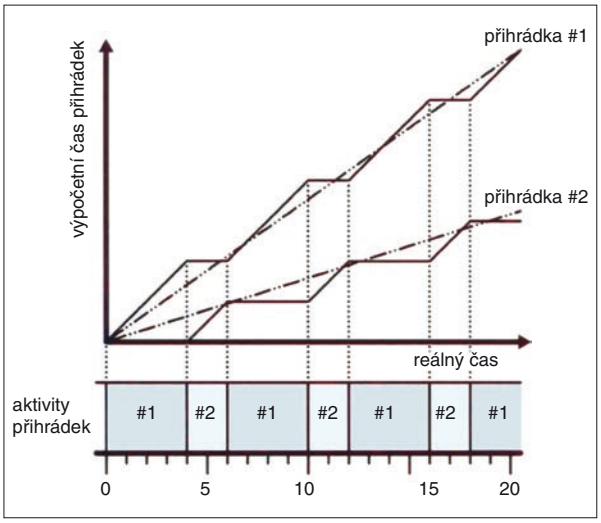
To však pokrývá pouze zdroje v uživatelském prostoru. Vlastní mikrojádro potřebuje paměť pro řízení zásobníků (*stack*), front, tabulek stránek (*page tables*) apod. Tyto zdroje je také třeba oddělit a zabránit tak nechtěnému spotřebovávání paměti.

Popisované prostorové rozdělení vychází z normy ARINC 653. Zdroje jsou rozděleny staticky podle fixní konfigurace. Norma velmi přísně předepisuje nastavení systému. Statická konfigurace je implementována na úrovni systémového softwaru, která mj. zajišťuje také komunikační služby, jako např. sdílenou paměť či oznamovací mechanismy mezi přihrádkami. Tím je umožněna i zabezpečená komunikace mezi hostujícími operačními systémy přes hranice přihrádek.

Časové rozdělení

Existuje mnoho systémů umožňujících prostorové rozdělení. Většina mikrojader však nebyla navržena pro práci v reálném čase a neumožňuje deterministicky přidělovat časové zdroje.

Cílem virtualizačního prostředí je dát každému hostujícímu operačnímu systému iluzi, že má k dispozici konstantní poměrnou část výkonu procesoru. To vede k lineární závislosti výpočetního času přiděleného každé individuální přihrádce, jak ukazuje čerchovaná čára v grafu na *obr. 1*. V praxi však může být práce procesoru přihrádkám rozdělena pouze v čase. To



Obr. 1. Výpočetní čas přihrádek a reálný čas

znamená, že každá přihrádka má pro své aktivity časový interval. Ideální lineární průběh výpočetního času je odhadnut ve funkci znázorněné v grafu (*obr. 1*) lomenými čarami. Kvalita takového odhadu se zlepšuje se zkracováním přidělovaných intervalů. To však vede k vyšší frekvenci přepínání úloh, a tím k nadměrnému časovému zatížení.

Programovatelné logické automaty (PLC) jsou striktně časově spouštěné systémy a okamžiky aktivace jsou u nich předem známy. Z toho vyplývá, že pro synchronizaci přepínání přihrádek musí být použit měnič s čistě časovou funkcí. V tomto bodě selhává většina existujících virtualizačních prostředí. Umožňují jednotlivým virtuálním počítačům (přihrádkám) vlastní přerušení, po kterém následuje přepnutí na další přihrádku. Tato metoda, jakkoliv se může zdát výhodná z pohledu využití procesorového času, znemožňuje předpovídat časy přepnutí. Pak není možné časově spouštěný systém PLC synchronizovat s přepínačem přihrádek.

Virtualizační koncept společnosti Sysgo je rozšířenou variantou normy ARINC 653. Kombinuje striktně časový plánovač s apriorním řízením. Systému Linux se dynamicky přiřadí každý časový úsek, který je sice přiřazen PLC, ale není jím využit. Toho je možné dosáhnout umístěním linuxu do tzv. přihrádky v pozadí, která je vždy ve spustitelném stavu s nižší prioritou než má PLC. Množství času, které může PLC spotřebovat, je omezeno intervalem, a tak i v případě, že by PLC (s vyšší prioritou než linux) spotřeboval veškerý čas procesoru, zbude i čas pro činnost linuxu. Tak tomu není např. u RTAI (*Real Time Application Interface*) nebo systému RTLinux.

Systém PLC vždy získá svůj podíl času CPU a zároveň je zaručeno minimální množství času pro linux. Systém Linux nemůže narušovat vykonávání aktivit PLC a PLC nezadržuje čas přidělený linuxu. V tomto případě si již kód PLC s kódem linuxu nemusí navzájem „důvěřovat“.

Problémy a vedlejší efekty

Izolace přihrádek je zcela závislá na adresních prostorech mikrojádra, které spravuje hardware MMU (*Memory Management Unit*). Pokud jsou připojena zařízení, která mohou přistupovat ke sběrnici přímo, a obejít tak MMU, celý spolehlivý systém se zhroutí. Řešením je omezit přístup k hardwaru na periodické dotazování (*polling*) nebo využívat paměti zvané frame buffer (určeny k dočasnému uložení vypočítaných snímků) a zrušit jakoukoliv schopnost řízení sběrnice zařízeními. Jinou možností je rozdělit ovladač na důvěryhodnou a nedůvěryhodnou část, a důvěryhodnou část (přistupující k hardwaru) implementovat mimo linuxové jádro na odděleném serveru.

Obě řešení znamenají komunikační zatížení. Nejnovější čipové sady a CPU již problém odstranily, neboť obsahují systém IOMMU, což je MMU pro vstupní a výstupní (I/O) zařízení s podobnou funkcí, jakou plní MMU pro procesor.

Jan Rollo, SYSGO, s. r. o.