

Řízení experimentálního vědeckého zařízení v kosmu (2)

Jiří Zděnek

1.2 Struktura řídicího počítače

V prvním přiblížení se řídicí počítač zařízení dělí na tři části (obr. 1), TC, CIC a TMC. O celkových úkolech jednotlivých částí již byla zmínka výše. Podrobnější členění řídicí elektroniky je na obr. 2. Řídicí počítač zařízení je postaven jako distribuovaný systém sestavený z nezávislých inteligentních jednotek, které samostatně vykonávají dílčí funkce. Jednotky jsou propojeny informační volnou vazbou (sériové komunikační kanály). Funkce dílčích jednotek je optimalizována tak, aby komunikace mezi nimi byla minimální. Celý řídicí počítač vytváří hierarchický systém se čtyřmi hladinami (obr. 2). Nejvyšší hladinu (master) tvoří CIC a technicky je realizován zodolněným přenosným počítačem platformy PC doplněným o stykovou jednotku sériové komunikace. V nejbližší nižší hladině je TMC a tři části technologického počítače TC. Ten se dělí na část, která řídí vlastní pec (označený CSK4) a na část TEGRA pro přesná měření teploty vzorků a mikrogravitace. V třetí a čtvrté hladině jsou pak části CSK4 (Ht, Dv, Tp, resp. Pt). Předmětem zkoumání v tomto příspěvku je část technologického počítače, označená CSK4. Ten sám osobě opět tvoří hierarchický systém o třech hladinách. V nejvyšší hladině je centrální kontroler (Cc), (master CSK4). Ve střední hladině jsou počítače řízení teplot v peci (Ht), řízení pohonů (Dv) a měření teploty pohyblivou sondou ve vzorcích (Tp). Nakonec v nejnižší hladině je počítač teplotní ochrany (Pt), dozorující proces topení v peci během experimentu a vybavený právem experiment zastavit při překročení povolených teplotních parametrů. Všechny akční členy i senzory daného dílčího počítače jsou obvodově připojeny pouze k němu, mezi jednotlivými dílčími počítači existuje propojení jen komunikačním (obousměrným) kanálem.

1.3 Architektura software

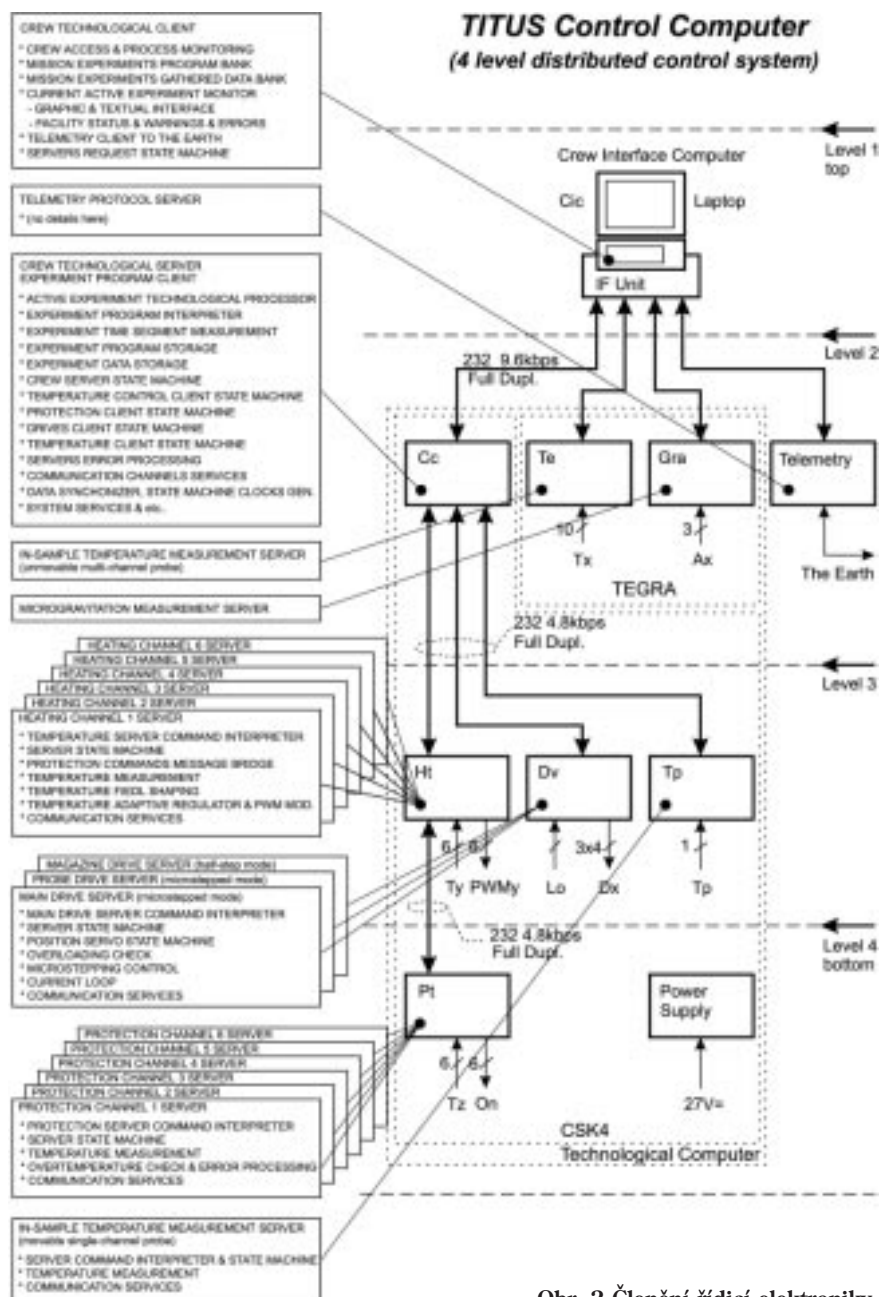
Z pohledu uživatele je každý dílčí počítač (uzel počítačové sítě) vybaven souborem příkazů technologického programovacího jazyka. CIC má programovací příkazy nejkomplexnější (grafické i textové), v každé další nižší hladině je soubor příkazů přizpůsoben vykonávané činnosti. Soubor příkazů každého uzlu je dále rozdělen na část pouze technologickou (používanou vyšší hladinou během zpracování vzorku) a část

ladící. Ta se používá při vývoji programů ve vyšší hladině, při kalibraci a postupném ožívání celého systému. Programové vybavení je postaveno na modelu klient/server, kdy klient požaduje určité služby a server je provádí, podává o výsledku své činnosti hlášení a předává zjištěná data. Podrobnější rozdělení celého systému na klienty a servery je na obr. 2. Všechny šest topných segmentů (kanálů) pece je řízeno z jednoho uzlu (Ht), programové vybavení

se však chová, jako by kanály byly zcela nezávislé. Totéž platí o řízení všech tří pohonů z uzlu Dv a monitorování pracovních teplot všech kanálů z uzlu Pt.

Vnitřní konstrukce programového vybavení ovlivňuje řada faktorů, a to především:

- Spolehlivost software a bezpečnost vykonávaných funkcí (bezpečnost posádky a stanice, extrémně vysoká cena při opravě chyb nalezených až na orbitální stanici).



Obr. 2 Členění řídicí elektroniky

- Možnost chybové analýzy při nestandardním chování software.
- Omezené zdroje (rychlost procesorů, velikost operační paměti i paměťových médií (pouze CIC používá magnetická záznamová média – HDD, jinde jsou FLASH disky).
- Omezený čas na vývoj zařízení, striktně limitovaný datem startu expedice.
- Omezené finanční i lidské zdroje.

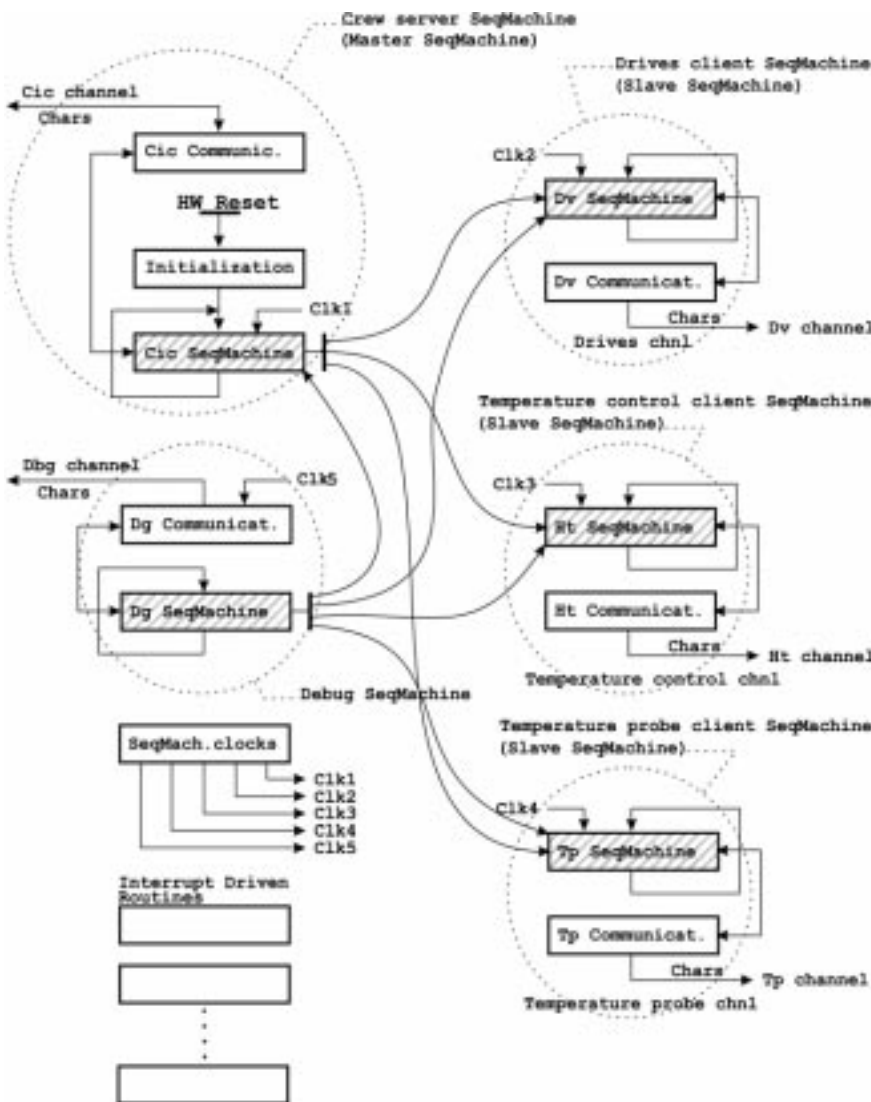
Při řešení programového vybavení pro CSK4 byly využity možnosti rozdělit vývoj tak, že systémový software (BIOS, nízkourovňové uživatelské služby – komunikační API apod.) je společný všem uzlům a aplikační software vznikl rozdělením, a to metodou jeden uzel/jeden programátor. Problémy vznikající prací více programátorů na vybavení jednoho uzlu tím byly vyloučeny. Toto členění umožnilo nepoužít plnohodnotný operační systém reálného času. Konečné systémové řešení programového vybavení vedlo na tabulkově řízený plánovač s exekutivou na pozadí (background-command level). Procesy jsou složeny ze staticky naplánovaných vláken (threads). Proces je spouštěn událostmi (je dynamicky plánován buď výstupem

z příkazového procesoru příslušného serveru, nebo časovým plánováním časovači). Prováděné vlákno nemůže být přerušeno (preempted) jiným procesem. Mezi jednotlivými vlákny procesu je přerušeno a spuštění vlákna jiného procesu možné. Plánovač a exekutiva umožňují používat pro různé skupiny procesů různé synchronizační hodiny. Časově kritické části programů jsou řešeny pod přerušením, mimo působnost plánovače s exekutivou. Výsledná architektura software tedy používá model coroutines-background/interrupts. Dílčí detaily architektury jsou v následujícím seznamu:

- vysokoúrovňové uživatelské příkazy,
- model klient/server,
- komunikace master/slave,
- komunikační dvojice cmd/status nebo cmd/response,
- komunikace pomocí zasílání zpráv,
- dvojí zabezpečení zpráv (kódem znaku a kontrolním součtem),
- jednotná konstrukce v různých jednotkách,
- minimalizovaný datový tok mezi jednotkami,
- smíšená konstrukce,

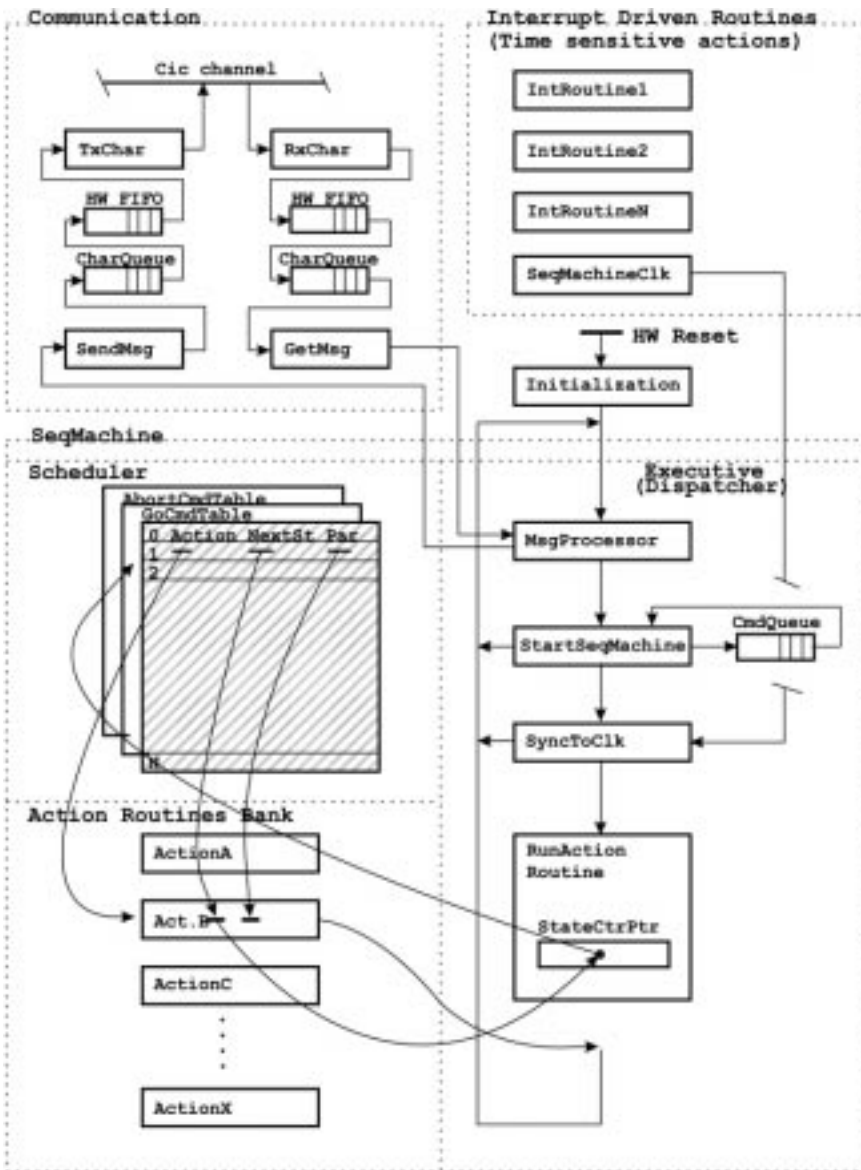
- pozadí/přerušeni,
- na pozadí coroutines (několik sekvencí strojů, každý s mnoha programy konečného automatu (FSA)),
- společný zásobník,
- spuštění FSA – žádosti klienta nebo časovači,
- procesy pod přerušením s pevnou prioritou,
- nepoužívá se plnohodnotný OS reálného času,
- kritické sekce s minimální dobou zákazu přerušeni,
- status dostupný klientovi v libovolném stavu programu,
- manažer přidělování paměti (RAM, FLASH-disk),
- fronty na kritických místech,
- přehledná konstrukce FSA, dokumentující zdrojové tabulky vláken,
- zabezpečení proti nahodilým hw chybám – dvojnásobný WDT,
- program ve FLASH disku, běh z RAM,
- programováno v „C“, výjimečně v assembleru.

Systémová konstrukce software uzlu Cc (centrálního kontroleru) je na obr. 3. Uzel Cc komunikuje čtyřmi pracovními kanály (směrem k CIC, Ht, Dv, Tp – viz obr. 2). Během ladění ve fázi návrhu programu a ověřování činnosti celého systému je k dispozici ještě další komunikační kanál (Dbg) pro připojení monitorujícího PC. Stavový automat Cic SeqMachine je spouštěn z výstupu příkazového procesoru po přijetí zprávy od klienta a taktován časovými značkami Clk1 z hodinového generátoru. Podle typu prováděné žádosti proces vykonávaný Dv SeqMachine aktivuje jeden nebo více automatů Dv SeqMachine, Ht SeqMachine, Tp SeqMachine. Ty pak řídí komunikaci na svém příslušném kanálu, hovoří se svým serverem, předávají nebo přebírají data a výsledky činnosti hlásí automatu Cic SeqMachine. Automaty na kanálech Ht, Dv, Tp mají své vlastní synchronizační hodiny. Všechny automaty nejsou jen čisté synchronní, za běhu některých vláken procesů by čekání na synchronizační značku bylo zbytečné. Pro tyto případy obsahuje program (tabulka) každého kroku automatu možnost zařadit nesynchronní krok (provede se ihned, jakmile vlákno získá zpět procesor, bez čekání na synchronizační značku). V době ladění je možné synchronizační značky (hodiny) stavových automatů zpomalit. Činnost systému je potom možné sledovat na PC připojeném k ladicímu kanálu přímo, bez použití záznamu post-mortem a off-line analýzy. Přijem a vysílání dílčích znaků zpráv ve všech kanálech i činnost generátoru synchronizačních značek probíhá pod přerušením (s pevnou prioritou jednotlivých zdrojů).



Obr.3 Vztahy mezi FSA centrálního kontroleru

Konstrukce každého jednotlivého stavového automatu FSA je zachycena na obr. 4. FSA je připojen na příslušný komunikační



Obr.4 Konstrukce FSA

kanál přes příkazový procesor (MsgProcessor). Služba GetMsg komunikačního kanálu zajišťuje postupný příjem jednotlivých znaků rámce zprávy sériovým kanálem, dekodování a ověření její neporušenosti a předání dat ze zprávy příkazovému procesoru. Služba SendMsg zajišťuje zakódování zprávy, opatří ji kontrolním součtem a postupně vyšle znaky celého rámce. Obě služby pracují pod přerušením mimo dosah plánovače-exekutivy procesů. Kritické sekce komunikace pozadí-přerušeni těchto služeb jsou ošetřeny semaforem (využívají atomické operace s pamětí a počítadlo stavu přijímacích a vysílacích front).

Příkazový procesor vyhodnotí přijatou zprávu a vybere odpovídající program (tabulku) žádaného procesu a spustí FSA. Každá programová tabulka pak určuje časový výběr předprogramovaných vláken procesů z banky vláken (Action Routines Bank). Vlákna procesu se postupně vykonávají synchronně (s možnými nesynchronními kroky) se synchronizačními značkami (hodinami) příslušného automatu až do ukončení procesu dle tabulky.

Exekutiva obsahuje též frontu (CmdQueue) na dekodované příkazy z příkazového procesoru, které zatím nebylo možné provést (spustit FSA), neboť předchozí proces zatím nebyl dokončen.

Literatura

(vybrané tituly)

[7] Zděnek, J.: Oven_1c – centrální kontroler – řídicí jednotka krystalizační pece. BBT/ DLR/ DARA/ ESA (TITUS). VZ AMITEK, Praha 1995.

[8] Gunther, M.- Kell, G. - Morgenstern, T. - Winkler, F.: High Resolution Temperature Measurement Technique for Materials Sciences Experiments in Space. IAF-94-J.2.234. In Proc. 45th Congress of International Astronautical Federation, Jerusalem 1994.

Pokračovanie v budúcom čísle.

Jiří Zděnek

**ČVUT Praha, Fakulta elektrotechnická
Katedra Elektrických pohonů a trakce
Technická 2, 166 27 Praha 6, ČR**

53