Űreszközök fedélzeti autonómiájának kialakítása a naprendszer távoli objektumainak kutatásához

BAKSA ATTILA tudományos munkatárs

Központi Fizikai Kutató Intézet RMKI, Űrtechnikai osztály
baksa@rmki.kfki.hu

Reviewed

Kulcsszavak: űrszonda, autonóm működés, hibatolerancia, többfeladatos valós idejű operációs rendszer

A naprendszer távoli objektumainak eredményes űrszondás kutatása magas fokú autonómiát követel meg az adott űreszköztől, ami a processzorok fejlődésének köszönhetően szoftver úton valósítható meg. Egy távoli égitest felszínén tevékenykedő űreszköz bonyolult feladatainak sokasága szükségessé teszi egy átfogó vezérlési modell kialakítását, amely megfelelő sebességgel képes kezelni a gyors környezeti eseményeket, mégis rugalmasságot biztosít egy hosszú távú küldetés változó igényei számára. Kidolgozott modellünket a Rosetta űrszondán alkalmaztuk, amely 2004. március 2-án sikeresen kilépett bolygónk gravitációs teréből.

Napjainkban indulnak olyan űreszközök, amelyek kihasználva a legújabb technológiai vívmányok adta lehetőségeket, távoli világok kutatását kezdik meg ebben az évtizedben. A legújabb fejlesztésű elektronikai eszközök, úgy mint alacsony fogyasztású, nagyteljesítményű processzorok, FPGA-k, magas hatásfokú napelem cellák és nagy energiasűrűségű akkumulátorok megjelenése lehetővé teszik olyan objektumok felszíni tanulmányozását, amelyek az éltető napenergiától és egyben Földünktől távol róják köreiket naprendszerünkben.

A problémák

A nagy távolságok elérése nemcsak az űreszközök hajtóműveit állítja komoly feladat elé, hanem a kommunikációt biztosító rádiórendszereket is, amelyek segítségével a kapcsolatot tarthatjuk égi küldöttünkkel. Amíg például a Mars bolygót kutató felszíni járművel, átlagosan húsz perc holtidővel tarthatja a kapcsolatot a földi operátor személyzet, addig a távolabbi objektumokat kutató szondák rádió válaszideje több óra is lehet. Amíg tehát egy földközeli űreszköz földi központú vezérlése elfogadható szabályozási holtidővel rendelkezik, addig az energiaszegény külső naprendszerben tevékenykedő eszköz nem hagyatkozhat a több órás késéssel érkező földi vezérlő jelekre.

Különös figyelemmel kell lennünk az űreszköz energia felhasználására, mert a naprendszer alacsony hőmérsékletű külső övezetében, jelenlegi elektronikus berendezéseinknek folyamatos fűtésre van szükségük, üzemképességük fenntartásához. Ez azt jelenti, hogy a szonda működtetése várakozó állapotban is rendkívül energia igényes. Adott esetben akár az is előfordulhat, hogy a szűkös energiaforrások következtében napokig tart annak az energiamennyiségnek az összegyűjtése, ami mindössze néhány óra üzemidőt biztosít a tudományos kutatások elvégzéséhez, hacsak nem használunk radioaktív energiaforrást.

Belátható tehát, hogy egyrészt nem pazarolhatjuk az energiát földi parancsokra való tétlen várakozásra, másrészt pedig elfogadhatatlan a váratlan események több órás késéssel történő megoldása, hiszen kritikus esetben ennyi idő alatt rendszerünk akár működésképtelenné is válhat.

Megoldás

Jelenleg egyetlen megoldást tudunk ezeknek problémáknak a megoldására. Növelnünk kell az űreszköz autonómiáját. Olyan intelligenciával rendelkező adaptív fedélzeti rendszert kell beépítenünk, amely:

- Folyamatosan biztosítja az előre megtervezett tudományos műveletek végrehajtását
- Rugalmasan alkalmazkodik az előre nem tervezhető időigényű folyamatokhoz
- Önállóan reagál a nem várt külső eseményekre és teljes megoldást ad vészhelyzetek kezelésére
- Fenntartja a rendszer energia egyensúlyát és gondoskodik az összegyűjtött tudományos adatok tárolásáról energiamentes állapotban is

Csak a fenti tulajdonságokkal rendelkező kutatóeszköztől várhatunk tudományos eredményekben gazdag és üzembiztos működést olyan távoli helyen, mint például egy üstökös felszíne.

A korábbi űrszondák, amelyeket égitestek felszínének kutatásához terveztek, nem rendelkeztek olyan mértékű intelligenciával, hogy távolabbi helyeken is hosszabb időre sikerrel bevethették volna őket. Nagyon nehéz volt több napos önálló feladatsor megvalósítása, mert hiányzott a váratlanul bekövetkező események megoldásához szükséges számítási teljesítmény. Napjainkban a mikroelektronika rohamos fejlődésével, olyan űrminősítésű, alacsony energiaigényű és nagyteljesítményű processzorok jelentek meg, amelyek lehetővé teszik nagymértékű autonómia szoftver úton történő

megvalósítását. Magas szintű mesterséges intelligencia algoritmusok beépítéséhez természetesen még ezek az erőforrások sem nyújtanak elegendő számítási kapacitást, de megfelelő absztrakcióval olyan összetett viselkedésformát sikerült kialakítanunk, amely a körülményeknek megfelelő válaszidővel képes a valósidejű események kezelésére és az űreszköz feladatainak hosszú távon történő irányítására.

Alapvető megfontolások

Autonóm fedélzeti szoftver logika kialakításánál kiemelten fontos a szoftver rendszer hibatoleranciájának mértéke. A szoftver modell tervezésénél ezért feltétlenül figyelembe kell venni a következő irányelveket:

- Biztonságos működés érdekében a mért környezeti értékek hihetőségi vizsgálatát el kell végezni (határérték vizsgálatok), hasonlóan szükséges a vezérelt változók érvényesítés előtti érték ellenőrzése.
- A belső modellnek érzékelnie kell a környezetében előforduló hibákat. A szoftver csak érvényes környezeti modellt használhat fel. Indulás alatt, leálláskor és átmeneti hibák esetében sem használhat érvénytelen adatokat.
- Minden elképzelhető eseményre léteznie kell állapot átmenetnek. Ez a feltétel a nagyszámú lehetséges esemény, illetve a teljes várható eseményrendszer alacsony jósolhatósági fokának következtében rendkívül nehezen teljesíthető a hagyományos modellekkel. Kidolgozott modellünk újszerűsége abban rejlik, hogy megoldást kínál az állapotátmenetek és állapotok későbbi, akár éles, üzem közbeni pontosítására.
- Minden állapot kezelésénél/vizsgálatánál időhatárokat kell alkalmazni (time-out) a feltétlen átmenetek elérésére.
- A kritikus, nem megszakítható állapotokban való futásidőt minimalizálni kell a reakcióidő alacsony szinten tartása érdekében.
- Ismétlődő akcióknak hurokban kell lenniük.
- Az esetleges hibás állapotot létrehozó téves parancsok veszélyét minimalizálni kell, ezért minden esetben teljes parancs dekódolást kell végezni.
- Nem létezhet a modellben teljes leállást létrehozó (csak ki/be kapcsolással feloldható) logikai útvonal.

A feladat

Részletesen tanulmányoztuk egy feltételezett távoli kisbolygó vagy üstökös felszínén leszálló kutatóegység központi számítógépével szemben támasztott lehetséges követelményrendszert, amely funkcionalitás szerint a következő csoportokra bontható:

- A célobjektum megközelítése és a leszállás folyamatának felügyelete vagy akár közvetlen vezérlése.
- A leszállóegység energia és hő egyensúlyának fenntartása.
- A tudományos műveletek irányítása.
- A tudományos adatok gyűjtése a fedélzeti műszerektől valamint az adatok átmeneti tárolása.
- Kapcsolattartás a Földdel vagy az esetleg közelben tartózkodó rádiójelek átjátszását biztosító úgynevezett orbiter egységgel, parancsfogadás és a tudományos adatok továbbítása.
- Hibatolerancia biztosítása, a beépített redundanciák kezelésével.

A különböző részterületeket átvizsgálva arra a következtetésre jutottunk, hogy az egyes területek egymással összefüggő hatást gyakorolnak a rendszerre. Ezért olyan központi logika kialakítása szükséges, mely kapcsolatot biztosít az egyes feladatkörök között. Egy olyan bonyolult központi logika, amely a fenti feladatok koordinálására képes nehezen írható körül, ezért szükséges a modell absztrakciója.

A modell

Absztrakciónk alapja, hogy különválasztottuk a rendszer statikus és dinamikus viselkedését, ami számos előnyt nyújt az űrszondákon alkalmazott korábbi megközelítésekkel szemben.

Ez a megoldás minimalizálja a szondához küldendő vezérlő információ mennyiségét, hiszen a statikus és dinamikus viselkedést leíró algoritmusok nagy számú kombinációját lehet létrehozni kis számú parancs segítségével. Ez azért fontos, mert a bolygóközi szondák esetében – a nagy távolság miatt – a parancs adatátvitel sebessége maximum 10-2000 kbit/mp, és ugyanakkor a kapcsolat is gyakran csak 10 percekre tartható fenn elfogadható jel/zaj viszony mellett. Fontosnak tartottuk továbbá, hogy a központi logika az űrszonda működésének bármelyik fázisában áttervezhető legyen, a tudományos küldetési tervek változásainak megfelelően.

Ezért mindkét modellt önálló alapegységek halmazára bontottuk tovább, amelyek elnevezése MSO (Mission Sequencing Object). Ezzel az absztrakció olyan alapkövéhez jutottunk, amelyek egyrészt lehetővé teszik az űrszondák földi parancsokon úgynevezett *telekommandokon* keresztüli adatfeltöltéséhez való igazodást, másrészt a földi küldetés tervezési csoport számára egy részleteiben áttekinthető leíró nyelvezetet biztosít ember és gép között.

Az alapegységek (MSO) kapcsolatát úgy alakítottuk ki, hogy azok egymástól függetlenül kezelhetők legyenek tervezési, transzport és üzemi fázisaik alatt egyaránt. Méretüket pedig úgy terveztük meg, hogy egy-egy MSO egyetlen telekommand formájában az űreszköz fedélzetére juttatható legyen. A leendő űreszköz fedélzeti szoftvere számára olyan adattárolási formát dolgoztunk ki, amely a magas hibatolerancia érdekében redundáns adattárolás mellett, hatékony helykihasználással biztosítja a szükséges MSO elemek gyors elérését.

A statikus modell

A statikus modell állítja elő a rendszer aktuális üzemi állapotát és alapegysége az SMSO (Static Mission Sequencing Object). Egy-egy SMSO a következő állapot paramétereket állítja elő:

- Az aktuális működési üzemmód egymásnak ellentmondó tulajdonságainak szabályozása:
  - működési sebesség,
  - hibatolerancia foka,
  - energiatakarékosság mértéke.
- Az űreszköz fedélzeti berendezéseinek és tudományos műszereinek aktuális állapota a küldetés fázisának megfelelően
- Az egyes berendezések szolgálati adatainak gyűjtésére vonatkozó paraméterek
- Adatmennyiség kvóták felállítása a fedélzeti adattároló kapacitás mindenkori optimális (hatékony) elosztása érdekében
- A fedélzeti berendezések működés közbeni jogainak korlátozása, a kritikus üzemi szekciók védelme érdekében
- Prioritási sorrend felállítása az üzemelő berendezések között a következő szempontok szerint:
  - energiaellátás,
  - adattárolási kapacitás,
  - kiszolgálási sebesség.

A dinamikus modell

A dinamikus modell a bekövetkező eseményekre adandó válaszokat, valamint a statikus modell állapotainak átmenetét írja le. Alapegysége az DMSO (Dynamic Mission Sequencing Object), amely a következő állapot átmeneti paramétereket állítja elő:

- Hivatkozás az aktuális rendszer állapotot leíró SMSO elemre
- A várt és váratlan események észlelését leíró tartalom
- Az eseményekre adandó közvetlen válaszok leírása, amelyek az esemény súlya szerint a következők lehetnek:
  - beavatkozó algoritmus,
  - hibaelhárító algoritmus,
  - hibakezelő algoritmus,
  - folyamat újraindító (recovery) algoritmus,
  - vész üzemmód algoritmus.
- Időzítések és timeout események leírása
- Kapcsolatok és elágazások leírása, amelyek aktivizálódhatnak egyrészt a küldetés terveinek megfelelően, másrészt a váratlan külső események hatására. A következő kapcsolatok és elágazás típusok létrehozására van lehetőség további DMSO-elemek felé:
  - láncolt kapcsolat,
  - szubrutin szintű elágazás,
  - ugrás szintű elágazás.

Megvalósítás

Modellünket a Német Űrrepülési Intézet, a DLR (Deutschen Zentrum für Luft- und Raumfahrt) felkérésére, az ESA (European Space Agency) üstökös kutató Rosetta űrszondájának fedélzetén alkalmaztuk, a Philae nevű leszállóegység fedélzeti számítógépének szoftver rendszerét fejlesztettük. Az elméleti modell sok paraméterét kellett a leszállóegységet irányító fedélzeti számítógép, úgynevezett CDMS (Command and Data Management Subsystem) fizikai adottságaihoz igazítani, de a modell logikai felépítését pontosan adaptálni tudtuk.

Modellünk rugalmasságára különösen szükség van a Philae fedélzetén, mivel a küldetés pontos tudományos menetrendje a rendkívül sok bizonytalansági tényező miatt még nem kidolgozott. Ennek ellenére a szoftver rendszer fejlesztése és tesztelése mégis jóval a kilövés előtt lezárulhatott. A leszálló egység végleges viselkedésének leírása és az előállított a MSO elemek fedélzetre töltése elvégezhető lesz a rádiórendszeren keresztül akkor is, amikor a Rosetta orbiter egysége már alaposan feltérképezte az üstökös magjának tulajdonságait. Modellünk nyújtotta lehetőségekkel reméljük, hogy a Philae leszállóegység sikeresen teljesíti majd a leszállás és a felszíni működés feladatait egy mindhárom tengelye körül bukfencező jéghegyen, amellyel új korszakot nyit majd az űrkutatás történetében.

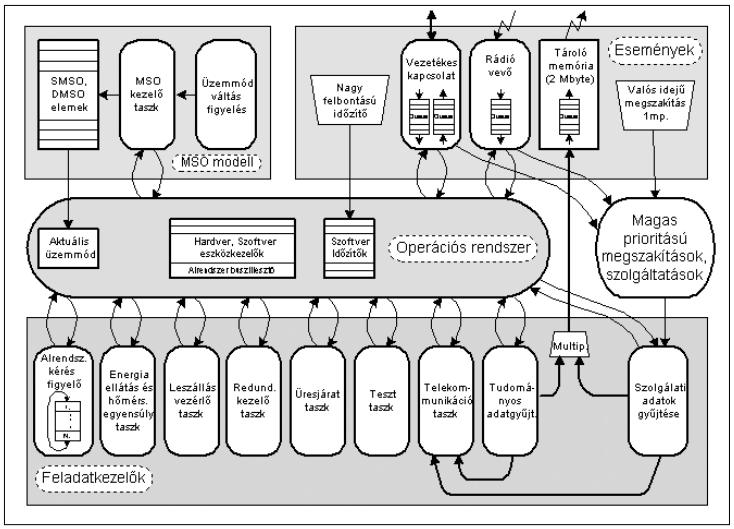
A megvalósítás környezete

A fedélzeti számítógéphez teljesen egyedi multitaszkos operációs rendszert fejlesztettünk ki, amelyre a számítógépben használt különleges processzor (Harris RTX 2010RH) miatt volt szükség. A leszállóegység feladatainak közvetlen vezérlését nyolc szintén egyedi fejlesztésű applikációs taszk végzi. A feladatok koordinálását és az applikációs taszkok algoritmusainak átfogó irányítását az itt ismertetett MSO alapú modell végzi. Az *1. ábra* az MSO modell és operációs rendszer illetve az applikációs taszkok kapcsolatát mutatja.

A fedélzeti számítógép hardver és szoftver elemeinek általános ismertetése megjelent a Magyar Elektronika folyóirat 2002. decemberi és 2003. januári számaiban.

A Rosetta-küldetés

Az ESA szervezésében futó Rosetta-küldetés az üstökösök kutatását tűzte ki célul. A Rosetta űrszonda a 67P/Churyumov-Gerasimenko üstököst közelíti meg és tudományos méréseket végez körülötte. Az űrszonda 2004. március 2-án sikeresen elhagyta Földünket egy Ariane 5 hordozó rakéta fedélzetén és megkezdte évtizedes utazását célja felé. Az üstökös megközelítése 2014 év elején várható, Földünktől 500 millió kilométer távolságban.



1.ábra
Az MSO modell és az operációs rendszer kapcsolata

Az üstökös részletes feltérképezése után 2014. novemberében a Philae nevű leszállóegység *(2. ábra)* különválik a keringő egységtől és leereszkedik az üstökös felszínére.

2.ábra
A Philae leszállóegység

Sikeres talajt érés után megkezdi kutatómunkáját, 10 tudományos műszerrel a fedélzetén. Berendezéseivel képes az üstökös anyagából mintát venni, azt mikroszkóp, spektrométer és gáz-analizátor segítségével vizsgálni, akusztikus- és radar-hullámokkal az üstökös belső szerkezetét tanulmányozni, mágneses és plazmafizikai vizsgálatokat végezni, valamint panoráma és sztereó kamerákkal fotókat készíteni és azokat a Földre továbbítani. Optimális viszonyok mellett a leszállóegység több hónapon keresztül folytathatja méréseit, lehetővé téve így számunkra, hogy nyomon követhessük a folyamatot, amikor egy üstökös „életre kel” naphoz közeledő pályaszakaszán.

Köszönetnyilvánítás

A Rosetta projektben való részvételünket a Magyar Űrkutatási Iroda segítette, amelyért ezúton szeretnénk köszönetünk nyilvánítani.

Irodalom

[1] Ron S. Kenett, Emanuel R. Baker:
Software Process Quality , New-York 1999.
[2] David P. Youll:
Making Software Developement Visible,
Chichester 1990.
[3] H. Dean Drake, Duane E. Wolting:
Reliability Theory Applied to Software Testing
Hewlett-Packard Jurnal, April 1987
[4] Gregory A. Krugel:
Project Management Using Software Reliability Growth Models
Hewlett-Packard Jurnal, June 1988.
[5] Gregory A. Krugel:
Validation and Further Application of Software Reliability Growth Models
Hewlett-Packard Jurnal, April 1989.
[6] Savio Chau, Abhijit Sengupta,
Tuan Tran, Ali Backhshi:
Ultra Long-life Spacecraft for
Long Duration Space Exploration Missions
Space Technology, Vol. 23, 2003.
[7] Baksa Attila, Balázs András, Pálos Zoltán,
Szalai Sándor, Várhalmi László:
A Rosetta Lander központi vezérlő és adatgyűjtő számítógépe
Magyar Elektronika, 2002. december
[8] Baksa Attila, Balázs András, Pálos Zoltán,
Spányi Péter, Szalai Sándor, Várhalmi László:
A Rosetta leszállóegység
fedélzeti szoftverrendszere
Magyar Elektronika, 2003. január-február