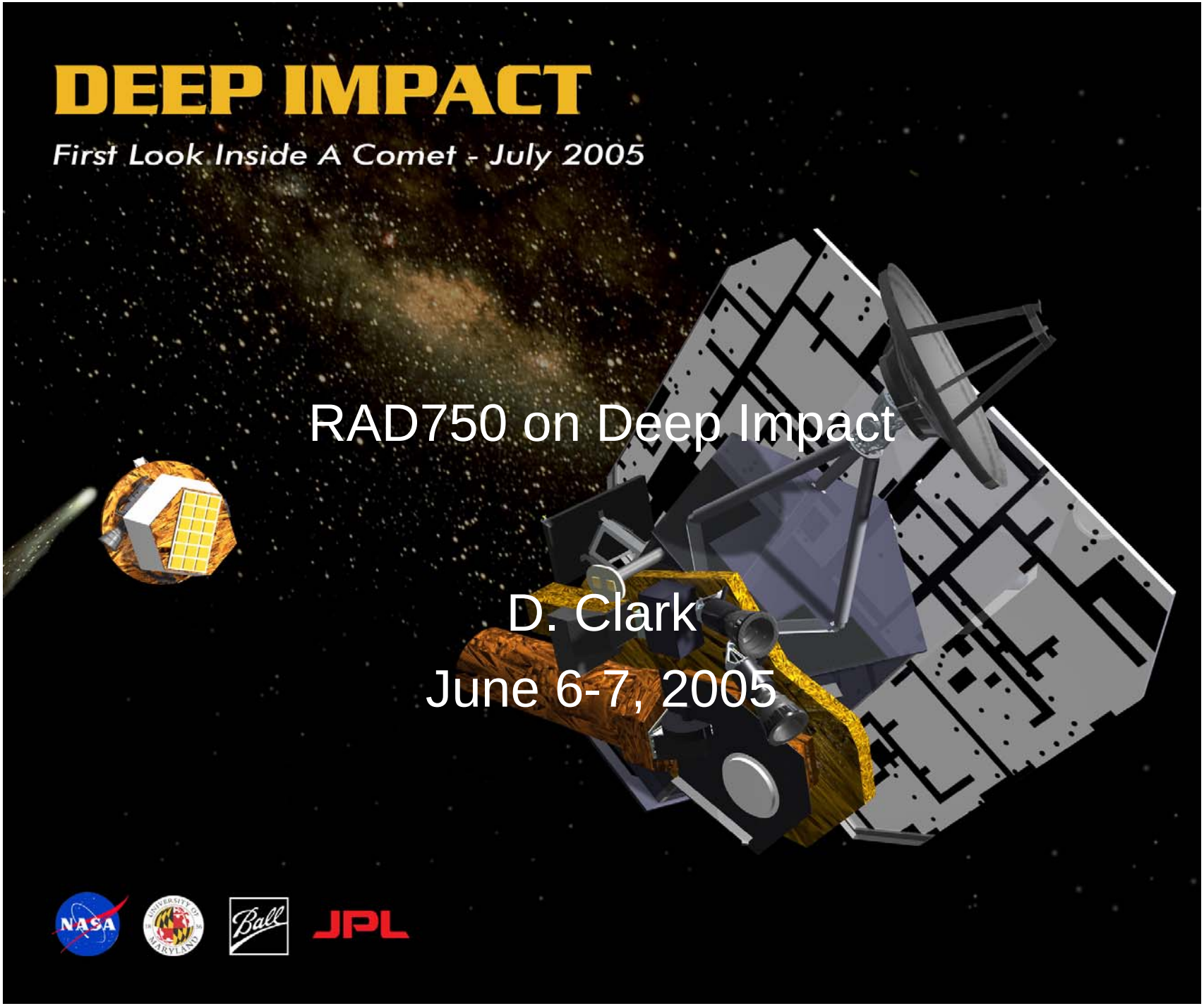
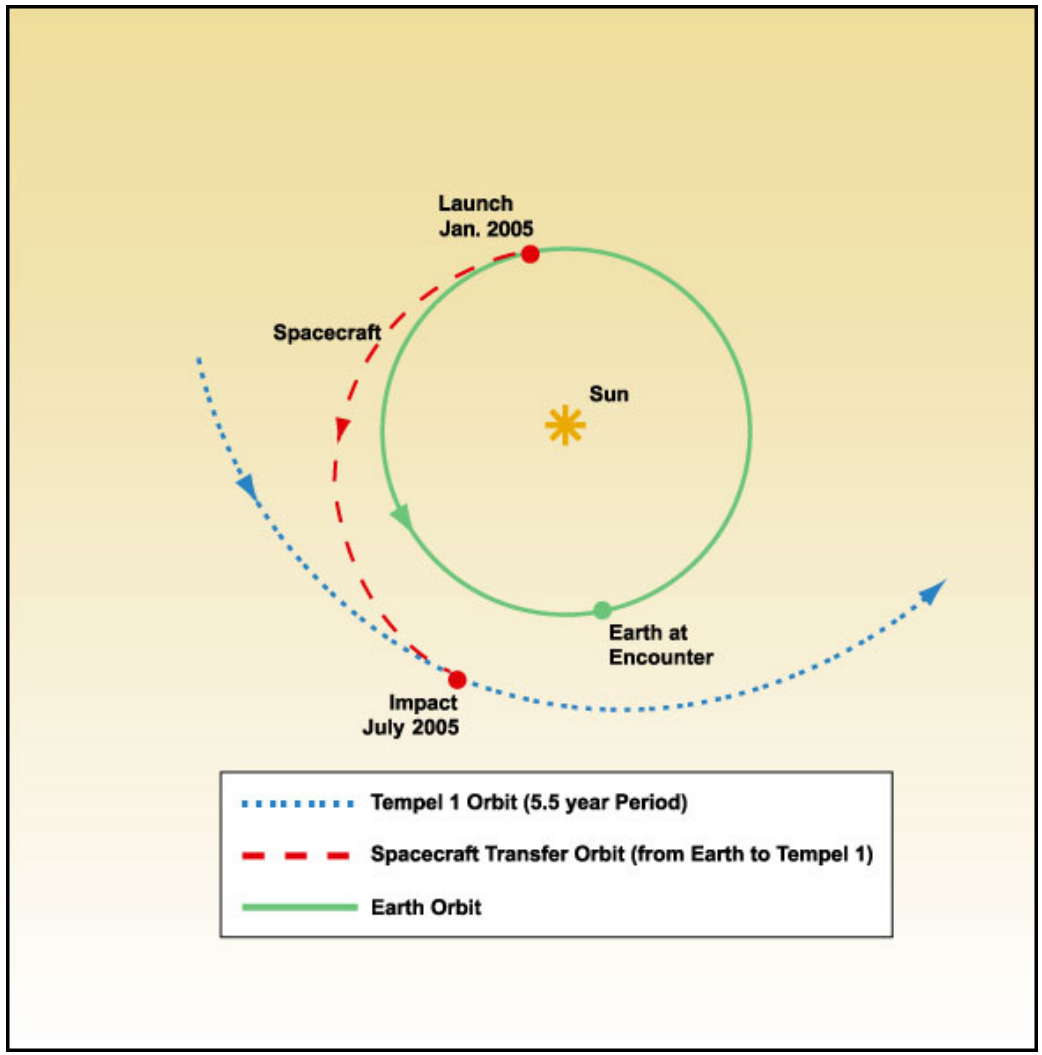

DEEP IMPACT
First Look Inside A Comet - July 2005
RAD750 on Deep Impact
D. Clark
June 6-7, 2005
NASA
Ball
JPL

Outline

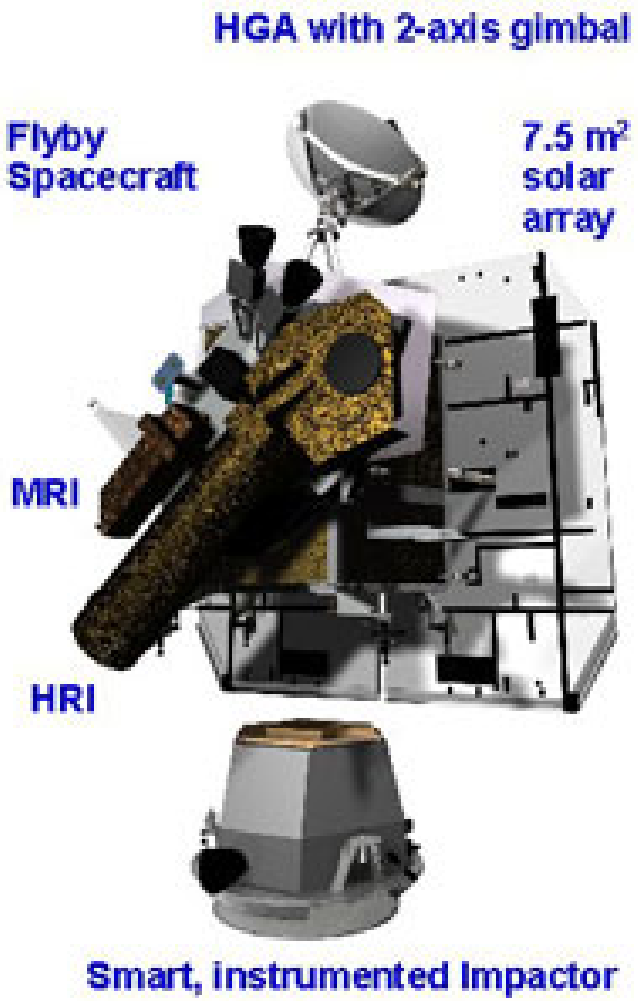
- Mission, spacecraft overview
- Mitigation strategies to address corruption of SDRAM and EEPROM
  - In-flight performance
- Selected development issues
  - EEPROM Corruption
  - RAD750 BIST failure
  - Power PCI Errata 15
  - Reset at power down
  - Mechanical issues
- Lessons Learned

Deep Impact Mission Overview

- University of Maryland, JPL, Ball Aerospace and Technologies, SwRI
- Launched: January 12, 2005
- Impact: July 4, 2005



Deep Impact Spacecraft



Use of RAD750 on Deep Impact

- RAD 750 is used in Spacecraft Computing Units (SCUs)
  - Built by Southwest Research Institute, under contract to Ball Aerospace and Technologies
  - RAD750 boards (3U base model) were built under JPL's X2000 contract and GFE'd to Ball.
  - Flight spare board shared with MRO project.
- Flyby Spacecraft
  - Two Identical Spacecraft Computing Units (SCU)
    - Configured as Prime and warm Backup
    - After an upset, first choice is to reboot the Prime, since it has better spacecraft state knowledge.
- Impactor Spacecraft
  - Single SCU
    - Original plan was for Impactor to be off for most of the mission to preserve life, but later decided that minimizing on/off cycles was more important.
      - So, Impactor has been on since shortly after launch when safing event turned it on.

SDRAM Corruption Mitigation Strategy

- Use built-in EDAC in Nibble Correct mode
- Map around bad SDRAM at bootup (see Nicolich, 2004)
  - Due to RAD750 Errata 1, required development of relocatable kernel
    - Errata 1: Operand errors when using page table to access cache
- Scrub SDRAM
  - Scrub performed with background utility with 20 minute period
  - Scrubbing mode: passive
  - Scrubbing must be aware of bad SDRAM locations found at bootup
  - No plans to turn off scrubbing during critical events
- After boot, “new” uncorrectable EDAC errors would force a reboot

In-Flight SDRAM Errors

	Errors detected during operation		Errors detected at startup	
SCU	Correctable (Note 1)	Non-correctable (Note 2)	Correctable, permanent (Note 3)	Non-correctable, permanent (Note 4)
Flyby A Launch + 120 days	176	0	0	(0)
Flyby B Launch + 121	203	0	0	(0)
Impactor Launch + 115	152	0	0	(0)

- Note 1: Corrected by EDAC during operation with no operational disruption. The fact that these counts are low relative to the number of 20 minute scrub cycles performed indicates that all of these errors were soft errors. Errors more frequent during solar flare.
- Note 2: These would have caused SCU to reboot. No reboots due to uncorrectable errors have occurred.
- Note 3: These would not be mapped out at startup, but if present, would have caused count of correctable errors detected during operation to be much higher.
- Note 4: These would be mapped out at startup. Data on number of non-correctable permanent errors is currently unavailable. No relocation of boot image from default location has occurred, and no correctable permanent errors have been observed, so it is likely that number of non-correctable permanent errors is zero for all SCUs.

EEPROM Corruption Mitigation Strategy

- Part type: Maxwell 28LV010RPFS-20 (Hitachi Die)
- EEPROM is single-bit EDAC-protected
- Project Management mandated:
  - Visibility into EEPROM health, including correctable errors
  - Ability to write and read EEPROM in flight (without reboot)
- Other measures
  - Minimize code footprint in EEPROM [see Nicolich, 2004]
  - Multiple copies of startup code in EEPROM to make in-flight modification of EEPROM contents easier if corruption were detected
- In-flight performance
  - Entire EEPROM is checked before flight software loads
    - Verifies integrity before planned reboot
    - Done several times on Flyby SCUs, twice on Impactor SCU
    - Checked by reading and looking for EDAC errors
    - No single or multi-bit errors seen

EEPROM Corruption During Development (on the ground)

- Error during update of SUROM on flight unit
  - Required removal of board and temporary addition of “EMC halt” haywire.
  - Mitigated via development of rigorous procedures for process of building EEPROM code images and installing them.
- Corruption during SW development
  - One incident occurred on non-flight board in laboratory setup
    - Did not occur during programming, but over the course of multiple power cycles over several days.
    - Lab setup did not assert MISC_POR_L until after 3.3 V rail dropped ~ 0.6 V.
      - BAE theory: noise on JTM_SRESETn could result in EEPROM memory accesses during power down.
    - Lab setup back-powered 3.3 V rail from 5 V on JTAG at power-up.
    - Attempts to duplicate problem with original setup were unsuccessful.
      - Problem was duplicated in “noisier” setups.

RAD750 BIST Problem

- Symptom: SCU took longer than expected to boot.
  - Original startup code called for restart of boot process upon RAD750 BIST failure.
  - Persistent BIST failures caused watchdog timer expiration followed by successful boot.
  - Occasional BIST failures were initially unnoticed
- BIST failure traced to sequence of events that allowed RAD750 to start execution of code prior to starting BIST.
- SUROM modified to freeze RAD750 before scanning in BIST instruction
  - Also ignore BIST failure.

Power PCI Errata 15

- Power PCI Errata 15: External DMA Device access to same cache line that CPU is accessing can cause Power PCI bridge to hang.
- Suspect that this was cause of unexpected resets in non-flight testbed with commercial network card
- Used CPCI bus analyzer to watch for resets
  - Bus traces examined after unexpected resets
  - Signature observed: NIC card apparently initiating a read of SFC SDRAM. Loop of termination by target, retry continued until expiration of system watchdog timer and reset.

Power up/down Reset Issues

- Without assertion of reset at power-down, EEPROM was considered to be in jeopardy.
  - Power-down reset was not specified in the documentation.
- This requirement for reset at power-down was missed until late in flight hardware fabrication cycle.
  - Asserting reset signal soon enough at power loss is a challenge
- SwRI and Ball added daughterboard with reset circuit to flight versions of power converter cards.

Mechanical Issues- Connectors

- CPCI connectors are fragile
  - Probing can damage sockets (on CPCI cards)
  - Backplane pins can easily be bent
  - At every mate/demate
    - Use magnifier to inspect sockets
    - Use flashlight to inspect backplane pins
- Avoid mate/demate of J7 as much as possible
  - Consider use of adapter cable, recommend removal before flight. (DI SCUs fly the adapter cable.)

Mechanical Issues- Qualification of Thermal Strap

- Qualification of the Base 3U RAD750 board was done by X2000 on EM version of the board, did not contain thermal strap.
- Problem with delamination of thermal strap observed by BAE on a board used on another program.
- Crack observed in bond layer on DI/MRO shared spare board. DI flight boards could not be removed from flight system for inspection
- Thermal strap was not needed for DI environment, but significant effort was expended to show that vibration of delaminated strap would not cause damage to RAD750 part or adjacent board, and that strap could not come loose.

Lessons Learned

- Programmatic
  - Good technical and programmatic relationships between BAE, JPL, Ball, and SwRI were key to working through issues.
  - Ensure hardware used in qualification program is representative of your flight hardware.
- System Engineering
  - Pay attention to system reset. Have architecture and circuits peer-reviewed early.
    - Assert MISC_POR_L at power up/down
- Software
  - Use EDAC and scrub SDRAM
  - Verify EEPROM and have ability to write it
- Handling/Test
  - Train board handlers in importance of CPCI connector inspection
  - Use CPCI bus analyzer where appropriate
  - Develop procedures for use of JTAG port and EEPROM update
- Considerations for future versions of RAD750 board
  - Give users an external means to halt EMC in case EEPROM corruption occurs during ground activities
    - Saves rework on the board, subsystem, and spacecraft
    - Not a substitute for careful EEPROM develop and loading procedures.
  - Design flight computer board with hardware inputs to select different startup images in EEPROM with off-board signal(s)
  - Select alternate image via low-level ground command (critical relay control) or external watchdog board. (i.e. bank or image select)