



# On-Orbit Anomaly Research: *Data Fragmentation*

NASA IV&V 2011 Annual Workshop  
September 13-15, 2011



# Introduction

---

- ▶ **Team Composition:**
  - ▶ Peter Medley (Technical Analysis)
  - ▶ Dan Solomon (Technical Analysis)
  - ▶ Sam Cilento (Technical Lead)
  - ▶ Dan Painter (Technical Analysis)
  - ▶ Koorosh Mirfakhraie (Technical Analysis)
  - ▶ Jennifer Neptune (Coordinator)



# Agenda

---

- ▶ Goals of Research
- ▶ Anomaly Description
- ▶ Background Information
- ▶ Factors Contributing to the Anomaly
- ▶ Science Data Storage
- ▶ Cause of Anomaly
- ▶ Anomaly Resolution
- ▶ Should/Could IV&V Have Caught This?
- ▶ Recommendations
- ▶ Conclusion
- ▶ Q&A



# Goals of Research

---

- ▶ Improve the NASA IV&V analysis and processes to help discover potential software-related faults, which have escaped IV&V analysis in the past, and identify ways to protect against them
- ▶ Provide value to current IV&V projects by communicating relevant lessons learned derived from anomalies on previous missions
- ▶ Provide the SW Engineering community with information to help develop more robust SW systems



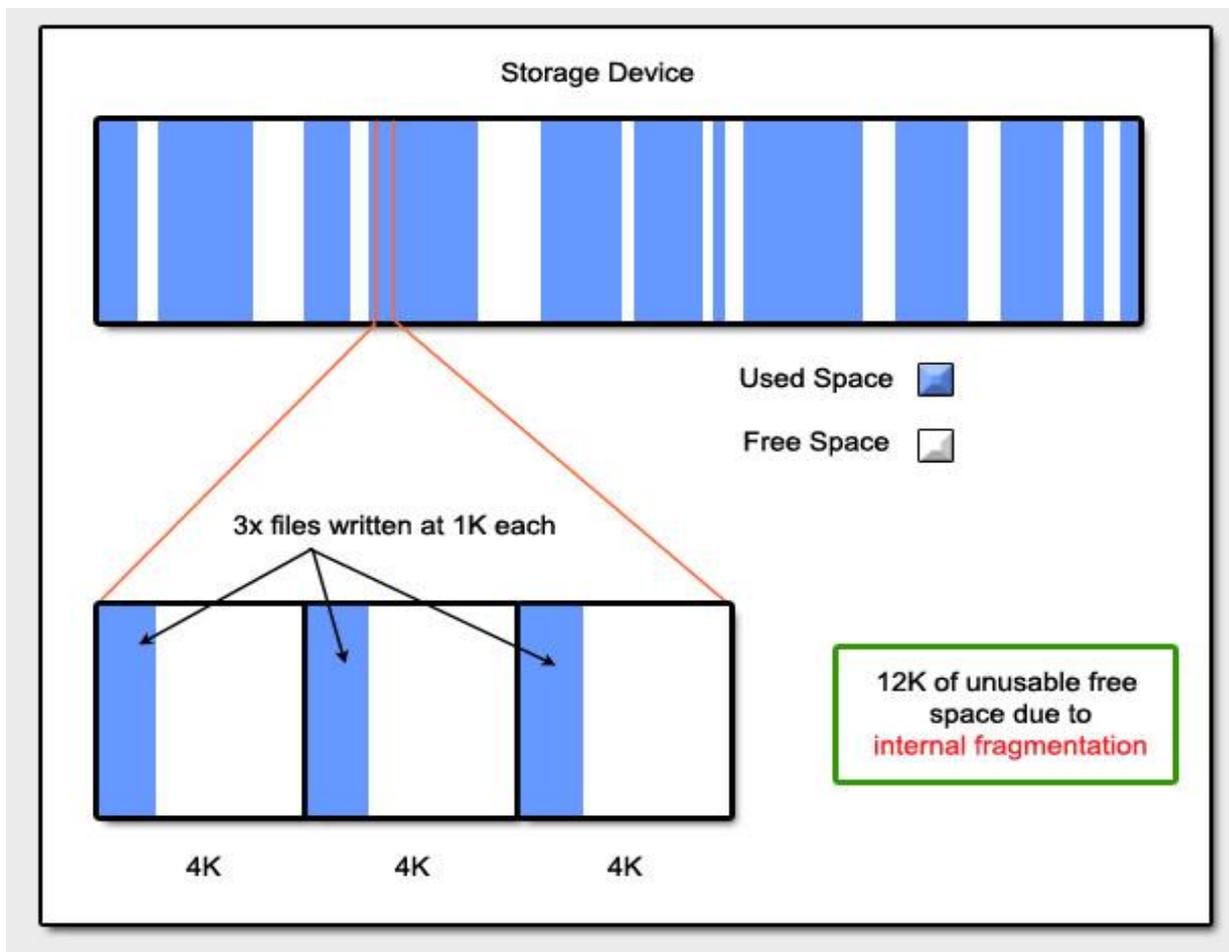
# Anomaly Description

---

- ▶ Impact: Science data lost; bus overflows
- ▶ Subsystem: Command and Data Handling (C&DH)
- ▶ Summary of Anomaly:
  - ▶ Write operations to store data on the recorder failed
  - ▶ Multiple buffers filled up and limits tripped
  - ▶ Science data lost
  
- ▶ Why we chose this anomaly:
  - ▶ Multiple occurrences were experienced on this mission
  - ▶ Similar anomalies were experienced on other missions

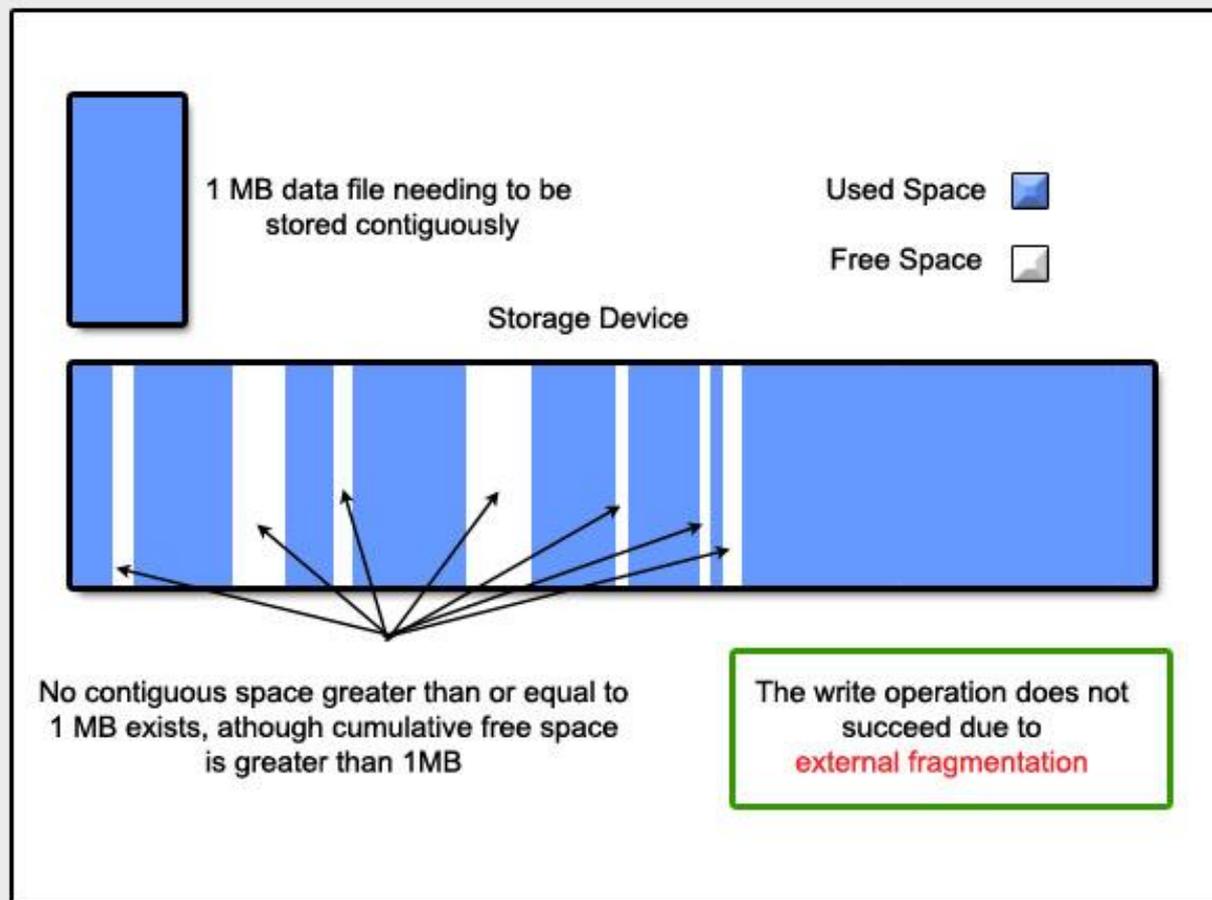
# Background Information

## ► Internal Fragmentation:



# Background Information (Cont'd)

## ▶ External fragmentation:





# Factors Contributing to the Anomaly

---

- ▶ The recorder was nearing full capacity and was heavily fragmented
- ▶ The spacecraft's recorder capacity was monitored and managed by Ground. However, the FSW function used to report free space to Ground did not account for external fragmentation
  - ▶ Ground couldn't see that fragmentation was becoming an issue

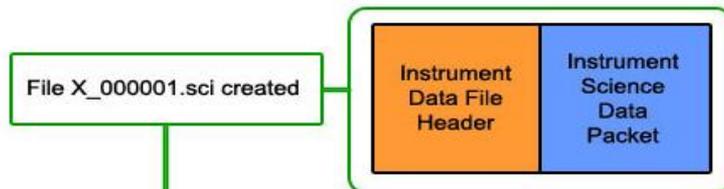


# Science Data Storage

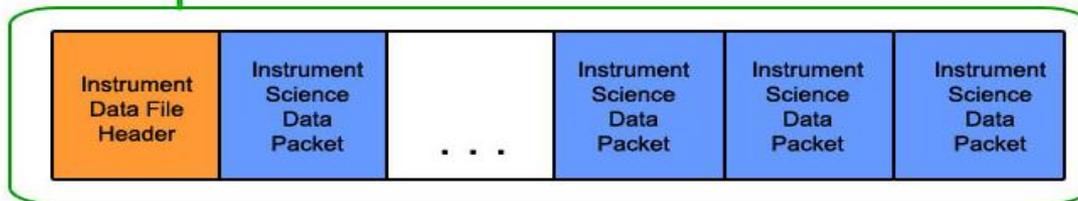
A packet of instrument science data is received



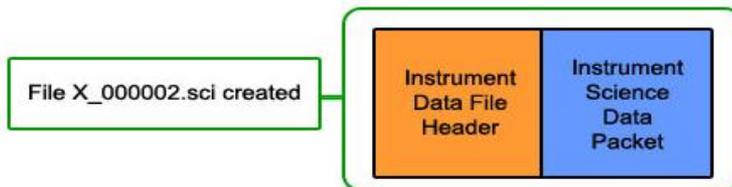
A science instrument data file is created



Additional science data packets received and stored contiguously until instrument science file max size reached or write failure



New science data file is created when next packet is received





# Cause of Anomaly

---

## ▶ Sequence of events:

- ▶ The instrument transmits data and FSW attempts to store it in a science data file
- ▶ Due to fragmentation and limited free space, each write operation causes the file system to search the entire partition for adequate contiguous free space
- ▶ With adequate space unavailable, a write-failure occurred
- ▶ Subsequent write requests also failed, causing:
  - ▶ A backup in processing tasks
  - ▶ A large number of event messages for SW bus overflow
  - ▶ Loss of science data



# Anomaly Resolution

---

- ▶ Original flight rule only said: “do not let partitions fill up”
- ▶ Flight rules were changed to forbid the SSR utilization to exceed 90% of its total capacity
- ▶ Solution was not 100% effective as the anomaly recurred



# Should/ Could Have IV&V caught this?

---

- ▶ Requirement does not say that the data file must be contiguous on the storage device:
  - ▶ “The Flight Software shall store the packets one right after the other, with no filler, into files, in CCSDS packet format.”
    - ▶ Ambiguous requirement?
- ▶ Code forces data file to be contiguous.
  - ▶ Missing requirement?
- ▶ Capacity utility checks for free space, NOT contiguous free space
  - ▶ Inconsistent code?
- ▶ Should we have caught it?
  - ▶ No reason to think the requirement was ambiguous.
- ▶ Could we have caught it?
  - ▶ Yes, if analyst had pursued ambiguity.
  - ▶ Yes, if IV&V pursued system/domain understanding of data storage



# Recommendations: Requirements Analysis

---

- ▶ Data fragmentation can adversely affect spacecraft operations. If not addressed adequately, data fragmentation may result in:
  - ▶ Loss of data
  - ▶ Latency issues in data handling
  - ▶ More severe issues
- ▶ In the case of managing fragmentation, the following elements and factors should be considered:
  - ▶ Distinction between types of data to be stored on a storage device
    - ▶ Housekeeping, engineering, science
  - ▶ Storage priority for various types of data
  - ▶ Data storage board configuration and partition allocation

# Recommendations (Cont'd): Requirements Analysis



- ▶ Data storage strategy with respect to the interaction of various types of data and the data storage boards/partitions, including aspects such as:
  - ▶ Preservation strategies for the protection of higher-priority stored data
    - ▶ Preserving housekeeping data over science data
    - ▶ Preserving new over old science data
  - ▶ Utilization plan for each partition
    - ▶ Schedule for partition utilization to avoid recorder overflow and system backpressure
    - ▶ Conditions causing flight software to change behavior in order to avoid recorder overflow and system backpressure
  - ▶ Size and storage methodology for types of data
    - ▶ What is the min/max size of a file for each instrument?
    - ▶ Does data within science files have to be stored contiguously?
      - If so, does FSW take account when checking for space?
    - ▶ How much space on the recorder is pre-allocated when a new science file is created?
  - ▶ Data-writing strategies for partition overflows
  - ▶ The ability to calculate the amount of “usable” free space on a

# Recommendations (Cont'd): Requirements Analysis

---



- ▶ Fault protection or other requirements which address the reality that a partition is rarely able to be 100% utilized
- ▶ Fault protection for subsystems supporting data storage and its ability to deal with the multiple consecutive write failures
- ▶ The absence of requirements, explicit or otherwise, addressing the elements and factors highlighted above, may warrant raising issues on missing requirements



# Recommendations (Cont'd)

---

## ▶ Design Analysis:

- ▶ A data storage design that relies heavily on ground, especially in addressing data storage strategies and fault protection, should particularly be scrutinized for its effectiveness and robustness

## ▶ Code Analysis:

- ▶ The source code needs to be inspected for the correct implementation of the following functionalities:
  - ▶ Identify functions used to calculate free space on a partition and ensure that the data returned by the functions is appropriate for their intended use.
    - For example, a function that returns the cumulative number of free blocks within a partition may not be useful in a system where data is required to be stored contiguously, especially if pre-allocation is utilized.
      - A cumulative free space of 100MB does not equate to a contiguous free space of 100MB
  - ▶ Executing strategies, such as overwriting existing data and denying a write request when there is not available space to store the requested data



# Recommendations (Cont'd)

---

## ▶ Test Analysis:

- ▶ Tests should not only trace to every relevant requirement but also cover the following conditions:
  - ▶ Storing data across multiple partitions
  - ▶ Writing data of different types and with various priorities
  - ▶ Storing data of both small and large sizes
  - ▶ Writing data to storage boards and partitions with a range of available storage spaces, from empty to full.
  - ▶ Operation of the spacecraft when the data recorder is heavily fragmented
  - ▶ Operation of the spacecraft when the data recorder is full



# Conclusion

---

- ▶ Data fragmentation is an issue that must be addressed
- ▶ Spacecraft design should specify a realistic data storage strategy consistent with storage requirements of the mission (Q1 analysis)
- ▶ Functions that calculate free space remaining on data storage device should be appropriate in respect to data storage strategy (Q1 analysis)
- ▶ Test scenarios should exert backpressure on the system HW (Q2 or Q3 analysis)



## Q & A

---

- ▶ Thank You!
- ▶ We have more anomaly examples to share. If interested, please send inquiries to [ivv-anomaly@lists.nasa.gov](mailto:ivv-anomaly@lists.nasa.gov)