Professional Development Short Course On:

Spacecraft QA Integration & Test

Instructor:

Eric Hoffman

ATI Course Schedule: http://www.ATIcourses.com/schedule.htm

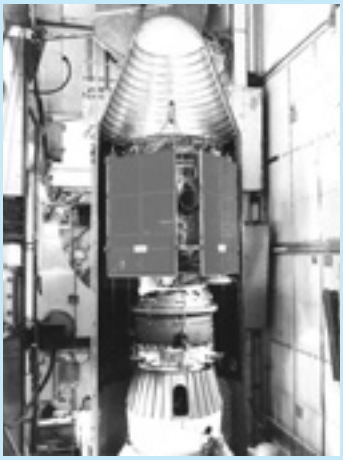
ATI's Spacecraft QA Integration & Test: http://www.aticourses.com/spacecraft_quality.htm

Applied Technology Institute (ATIcourses.com)

Stay Current In Your Field • Broaden Your Knowledge • Increase Productivity

349 Berkshire Drive • Riva, Maryland 21140
888-501-2100 • 410-956-8805
Website: www.ATIcourses.com • Email: ATI@ATIcourses.com

Spacecraft Quality Assurance, Integration & Testing



March 23-24, 2009
Beltsville, Maryland

June 10-11, 2009
Los Angeles, California

$990 (8:30am - 4:00pm)

"Register 3 or More & Receive $100[00] each Off The Course Tuition."

Summary

Quality assurance, reliability, and testing are critical elements in low-cost space missions. The selection of lower cost parts and the most effective use of redundancy require careful tradeoff analysis when designing new space missions. Designing for low cost and allowing some risk are new ways of doing business in today's cost-conscious environment. This course uses case studies and examples from recent space missions to pinpoint the key issues and tradeoffs in design, reviews, quality assurance, and testing of spacecraft. Lessons learned from past successes and failures are discussed and trends for future missions are highlighted.

Instructor

Eric Hoffman has 40 years of space experience, including 19 years as the Chief Engineer of the Johns Hopkins Applied Physics Laboratory Space Department, which has designed and built 64 spacecraft and nearly 200 instruments. His experience includes systems engineering, design integrity, performance assurance, and test standards. He has led many of APL's system and spacecraft conceptual designs and coauthored APL's quality assurance plans. He is an Associate Fellow of the AIAA and coauthor of Fundamentals of Space Systems.

What You Will Learn

- Why reliable design is so important and techniques for achieving it.
- Dealing with today's issues of parts availability, radiation hardness, software reliability, process control, and human error.
- Best practices for design reviews and configuration management.
- Modern, efficient integration and test practices.

Course Outline

1. Spacecraft Systems Reliability and Assessment. Quality, reliability, and confidence levels. Reliability block diagrams and proper use of reliability predictions. Redundancy pro's and con's. Environmental stresses and derating.

2. Quality Assurance and Component Selection. Screening and qualification testing. Accelerated testing. Using plastic parts (PEMs) reliably.

3. Radiation and Survivability. The space radiation environment. Total dose. Stopping power. MOS response. Annealing and super-recovery. Displacement damage.

4. Single Event Effects. Transient upset, latch-up, and burn-out. Critical charge. Testing for single event effects. Upset rates. Shielding and other mitigation techniques.

5. ISO 9000. Process control through ISO 9001 and AS9100.

6. Software Quality Assurance and Testing. The magnitude of the software QA problem. Characteristics of good software process. Software testing and when is it finished?

7. The Role of the I&T Engineer. Why I&T planning must be started early.

8. Integrating I&T into electrical, thermal, and mechanical designs. Coupling I&T to mission operations.

9. Ground Support Systems. Electrical and mechanical ground support equipment (GSE). I&T facilities. Clean rooms. Environmental test facilities.

10. Test Planning and Test Flow. Which tests are worthwhile? Which ones aren't? What is the right order to perform tests? Test Plans and other important documents.

11. Spacecraft Level Testing. Ground station compatibility testing and other special tests.

12. Launch Site Operations. Launch vehicle operations. Safety. Dress rehearsals. The Launch Readiness Review.

13. Human Error. What we can learn from the airline industry.

14. Case Studies. NEAR, Ariane 5, Mid-course Space Experiment (MSX).

Recent attendee comments ...

"Instructor demonstrated excellent knowledge of topics."

"Material was presented clearly and thoroughly. An incredible depth of expertise for our questions."

Applied Technology Institute (ATIcourses.com)

Stay Current In Your Field • Broaden Your Knowledge • Increase Productivity

349 Berkshire Drive • Riva, Maryland 21140
888-501-2100 • 410-956-8805
Website: www.ATIcourses.com • Email: ATI@ATIcourses.com

www.ATIcourses.com

Boost Your Skills with On-Site Courses Tailored to Your Needs

349 Berkshire Drive
Riva, Maryland 21140
Telephone 1-888-501-2100 / (410) 965-8805
Fax (410) 956-5785
Email: ATI@ATIcourses.com

The Applied Technology Institute specializes in training programs for technical professionals. Our courses keep you current in the state-of-the-art technology that is essential to keep your company on the cutting edge in today's highly competitive marketplace. Since 1984, ATI has earned the trust of training departments nationwide, and has presented on-site training at the major Navy, Air Force and NASA centers, and for a large number of contractors. Our training increases effectiveness and productivity. Learn from the proven best.

For a Free On-Site Quote Visit Us At: http://www.ATIcourses.com/free_onsite_quote.asp

For Our Current Public Course Schedule Go To: http://www.ATIcourses.com/schedule.htm

High Reliability: Lessons from NASA

1. Apply effective design principles, including extensive and meticulous design reviews.

2. Control and screen all parts and processes.

3. Thoroughly inspect and test.

Why Do Spacecraft Fail?

Independent studies and surveys have found that the causes of spacecraft failure are, in order of importance:

1. Poor design
2. Misjudged environments
3. Software
4. Human error (particularly mission ops)
5. Interconnects
6. Mechanically deployed systems
7. Piece part failure

Note that parts screening addresses only the 5th or 7th most prominent cause.

Refs: H. Hecht and M. Hecht, Reliability Prediction for Spacecraft. RADC-TR-85-229, 1985

R. Fleeter, *The Logic of Microspace* (Kluwer and Microcosm, 2000)

Performance Assurance Philosophies Are Changing

	Old	New
Risk	Risk Avoidance	Risk Management
Parts	Class S or B preferred	Learning to work with BCP and PEMs
Parts Testing	100% inspection	Selective test/re-test
Fabrication	NHB5300.4	BCP, ISO 9000, and AS9100
Software	Software “artistes”	Disciplined software engineers
System Test	Layered, multiple retest	Testing larger assemblies at once
Redundancy	Part and box level	Box and spacecraft level
PAE Philosophy	Outside the team; policeman	Inside the team; facilitator
Big Worry	Parts, interconnects	Software, interconnects, human error

Risk Management In A Nutshell

Risk = probability of occurrence x consequence if it occurs

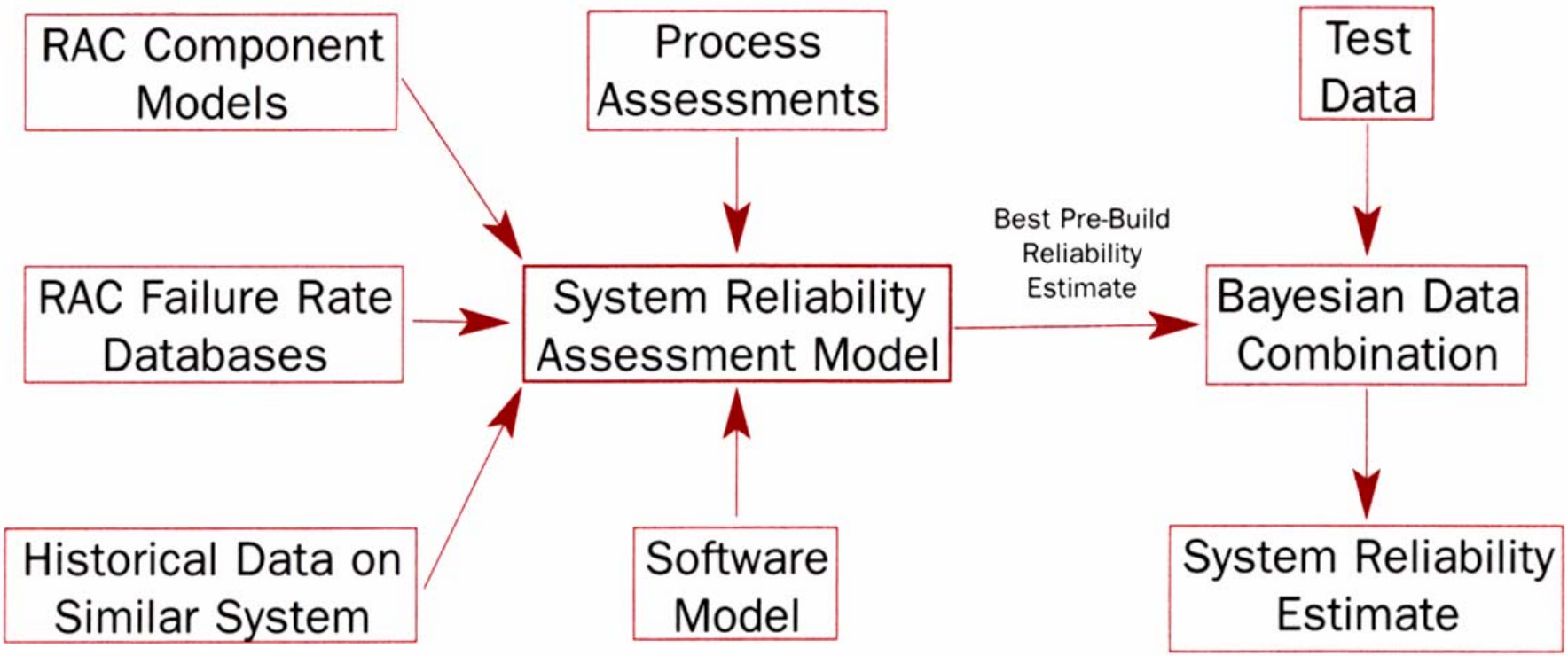
Risk management asks "What could possibly go wrong?"

Once you know this, ask such things as …

- "What is the probability of the bad thing happening?"
- "How much will it affect the project?"
- "What would we do if it happened?"
- "How can we reduce the adverse affects?"
- "How can we prevent it?"

Simply assuming that everything will work is a *worst practice*. Avoid it. Bad things happen on all aerospace projects … anticipate them.

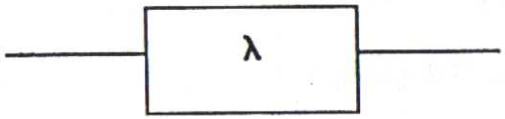
after D. Phillips, *The Software Project Manager's Handbook*, IEEE 1998



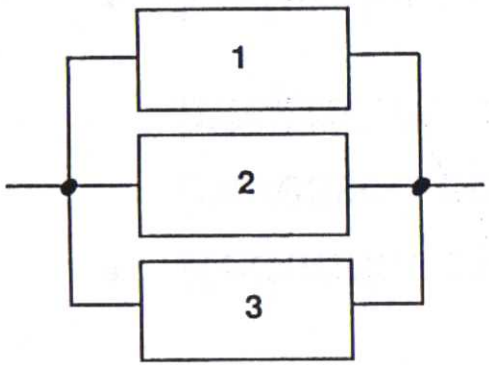
The Journal of the Reliability Analysis Center

download DEMO version of PRISM from RAC web site at http://rac.iitri.org/PRISM

Redundancy

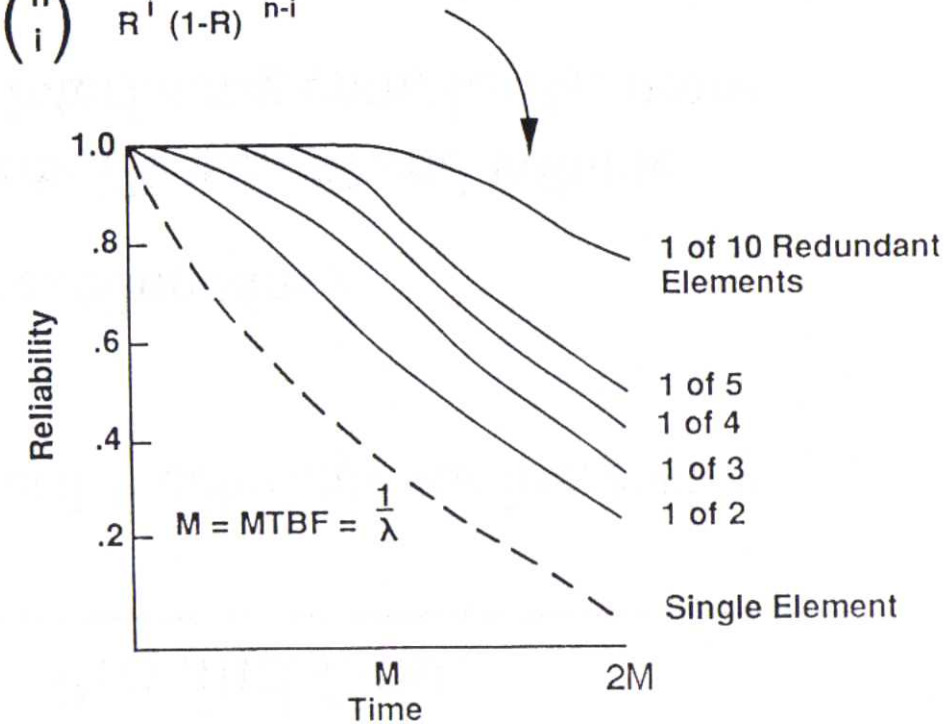


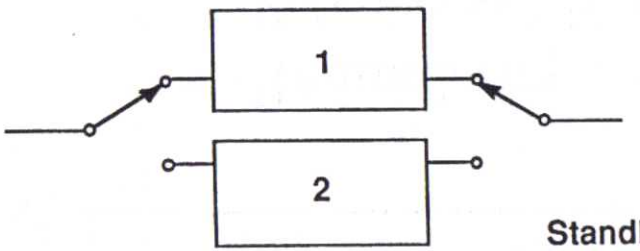
non-redundant $R(t) = e^{-\lambda t}$



r-out-of-n (active) redundancy

$$R_{sys} = \sum_{i=r}^{n} \binom{n}{i} R^{i} (1-R)^{n-i}$$





Standby Redundancy

Design Review Principles

- Determine what must be reviewed
  - new designs?
  - “heritage” designs?
  - purchased subsystems?
  - software, firmware?
  - test equipment, ground support equipment?
- Establish hierarchy of reviews
- Make sure design and requirements are stable
- Schedule the reviews for maximum effectiveness
- Design a realistic agenda

...cont’d

Design Review Presenters

- Help reviewers understand the design
  - adopt a pedagogic attitude
  - show requirements
  - present appropriate level of detail
  - show concern items, possible solutions

- Watch the clock!

  - Anticipate questions - include answers in presentation
  - Avoid long debates with reviewers
    - action item
    - splinter meeting
  - Learn the projection equipment
- Serve as ad hoc reviewer
- Accept comments objectively, non-defensively

Configuration Management: What It Includes

- Design Specs
- Purchase Specs
- Interface Control Documents
- Design Reviews
- Drafting Standards
  - content and format
  - checking
  - release
  - changes
- Change Control and Incorporation
- Change Control Board
- Software Problem Reports
- S/W Unit Development Folders
- Drawing Numbers, Serial Numbers
- Fabrication Controls
  - processes
  - fabrication control cards
  - workmanship standards
- Parts and material traceability
- Non-conformances
- Deviations and Waivers
- Material Review Board
- Configuration Accounting
- Test plans, procedures, data sheets
- Configuration audits
  - functional
  - physical
- As-built Documentation

ISO 9000

- ISO 9000:2000 is a series of three worldwide standards that define the elements and structure of QA systems.
- ISO 9000 registers a quality *system*. It emphasizes *management* and *process* (unlike, for example, QML, which certifies a hi-rel *product* - or - NASA NHB-5300.4, which *inspects in* quality)
- ISO 9001, the standard most applicable to spacecraft development, covers 8 specific areas (but in only 16 pages!).
- ISO 9000 requires you to:
  - demonstrate top management commitment
  - identify your processes
  - document them
  - scrupulously follow them
  - continually improve them
- But ISO 9000 does *not* guarantee high quality product.

SAE AS9100

- Quality system requirements for suppliers to the aerospace industry, issued Aug 2001. Originally AS 9000 (1997), expanded to address international requirements, now approved by Asian and European aerospace companies as well.
- Approximately 80 additional requirements plus 18 amplifications of ISO 9001.
- Intent is to achieve significant quality improvements and cost reductions by placing requirement for conformance on aerospace parts and process suppliers.
- Principal document: *Quality Systems - Aerospace - Model For Quality Assurance In Design, Development, Production, Installation And Servicing*
- Why do companies want AS9100? Market Pressure … many organizations decide to implement and register to AS9100 to assure customers that the company has a good Quality Management System (QMS) in place. Such companies typically meet customer expectations better than those without an effective QMS. Many aerospace organizations now require their suppliers to have AS9100.

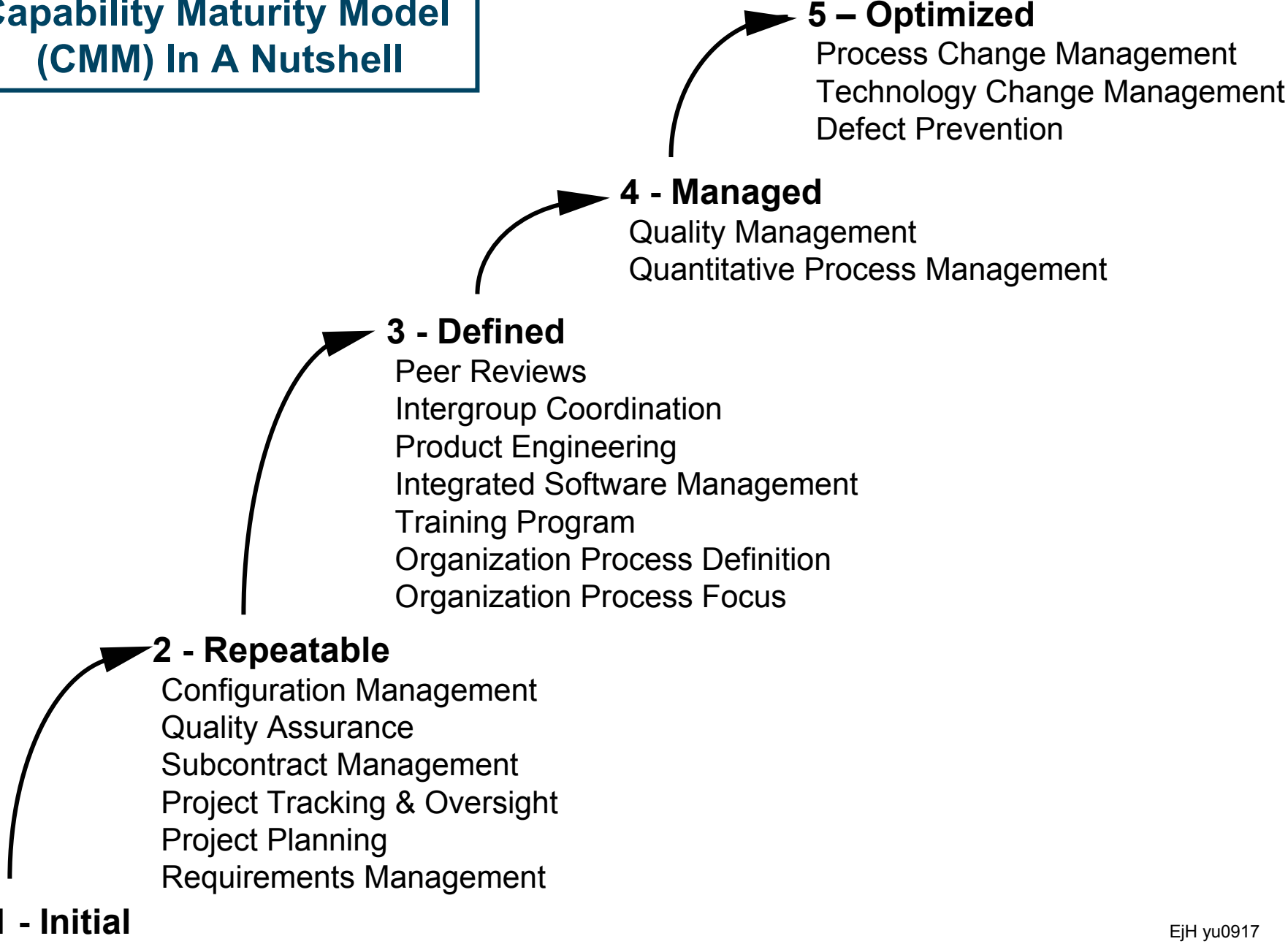
Software Quality Assurance

Software has become increasingly important to overall reliability.

But flight software is difficult to create because …

- It's often one-of-a-kind.
- It's usually multi-tasked, realtime, interrupt driven.
- Extreme reliability is required.
- It must be remotely reconfigurable and maintainable.
- It's often designed while flight hardware & MOps are still in flux.
  - interface definitions may occur late
  - ConOps may arrive late
  - schedules are tightly coupled
- The flight h/w and development tools greatly lag ground-based.
- Competitive bidding can interfere with optimizing requirements.

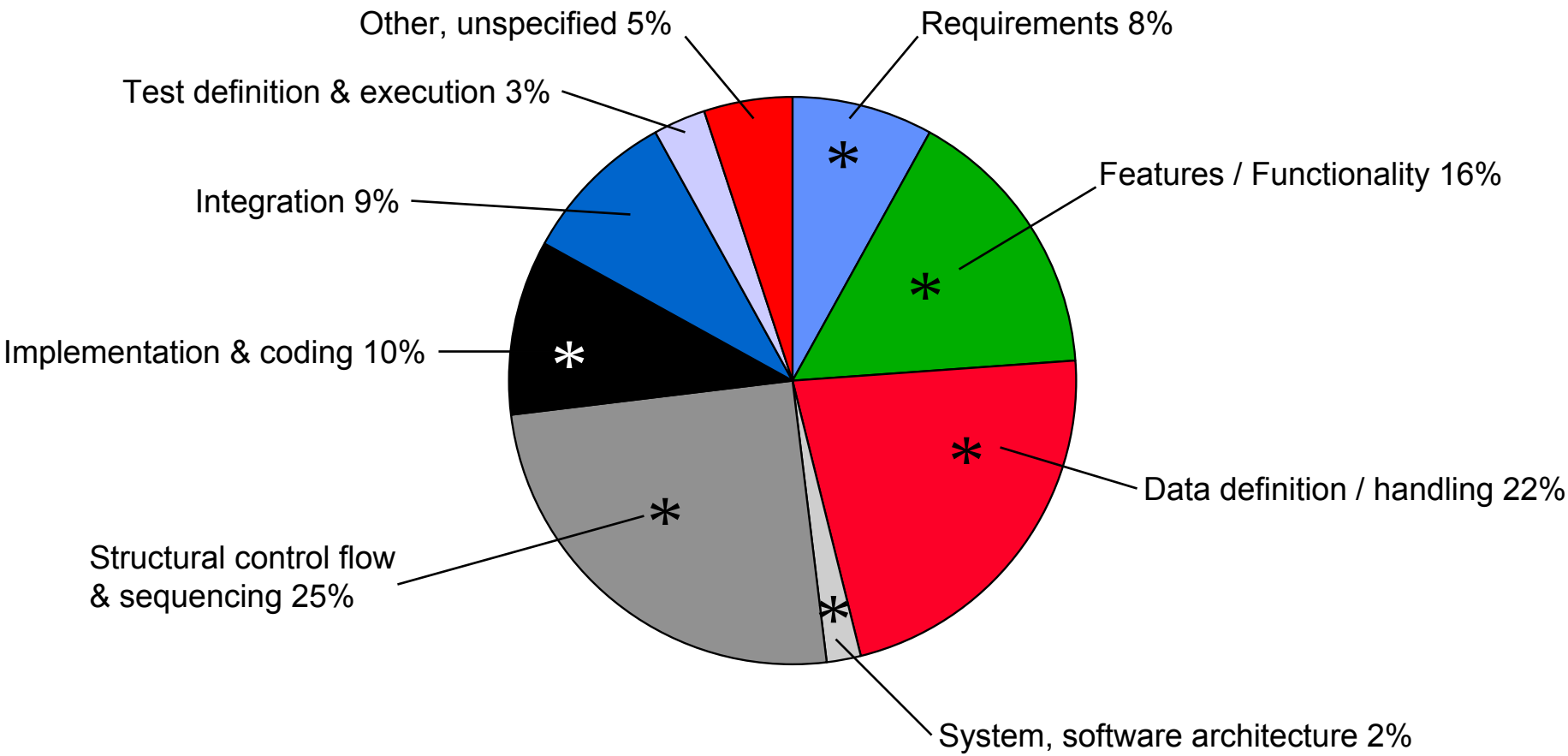
Capability Maturity Model (CMM) In A Nutshell



EjH yu0917

Early Software Reviews Pay Off!

Errors found in 6,877,000 source lines of debugged code (including comments) on 28 projects. (* = detectable by review)



Ref: *Software Engineering: A Holistic View,"* Bruce Blum, Oxford Press, 1992

Code Walkthrough / Fagan Inspection

- A very formalized, intense form of code walkthrough is called a “software inspection.”
- Requires a study period of the requirements, design, and code *prior* to the actual review.
- Some or all of the following players:

  presenter (lead reader, usually the designer/programmer)
  moderator (coordinator, chairman)
  recorder (scribe, secretary)
  1-2 other technical reviewers
  * maintenance oracle
  * standards bearer
  * user representative
  * system liaison (system engineer)

  * = optional

  - Performed module by module, after first good, clean compilation

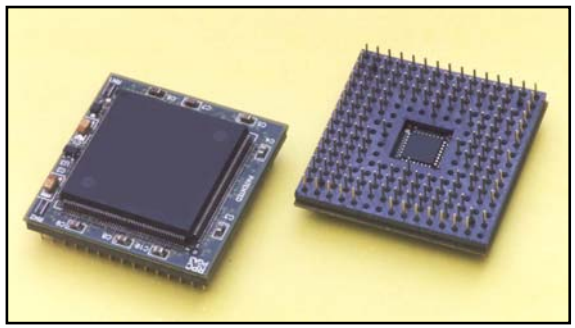
- Can be highly effective

Ref: Fagan, M., “Design and Code Inspection,” *IEEE Trans. Software Engng*, July 1986

Field-Programmable Gate Arrays

(courtesy R. C. Moore, APL)

A field-programmable gate array (FPGA) is an integrated array of logic elements in which the logic network can be programmed into the device after its manufacture. Most FPGAs for space flight are programmed once and retain their programming permanently. FPGAs for space flight have built-in single-event upset (SEU) protection.



Vendor	FPGA Family	Gate length	Number of gates	Number of user I/O pins	Propagation delay, clock rate	Total ionizing dose (TID) immunity	Single-event latch-up LET threshold	Bit error rate (errors / bit-day)
Atmel	AT40K	0.35µm	50k	240	18 ns / 60 MHz	200k rad(Si)	> 70 MeVcm^2/mg	10^{-9}
Actel	RTAX-S	0.15µm	250k	684	10 ns / 100 MHz	200k rad(Si)	>120 MeVcm^2/mg	10^{-10}
Aeroflex	UT6325	0.25µm	320k	365	12 ns / 80 MHz	300k rad(Si)	>120 MeVcm^2/mg	10^{-9}
Actel	RTAX4000S	---	500k	840	---	300k rad(Si)	104 MeVcm^2/mg	10^{-10}
Xilinx	Virtex-II	0.13µm	25k	624	10 ns / 100 MHz	200k rad(Si)	>125 MeVcm^2/mg*	10^{-8}

EjH yn0529
RCM

Software Testing

Defect Testing

Design tests that will cause the system to perform incorrectly, and thereby expose a defect.

Interface tests - use knowledge of functional specification, structure, and implementation to design tests that will exercise each object and message type in the system.

Never permit defect testing to replace static verification (e.g., code walkthroughs, formal methods).

Testing Methods

White Box - Based on detailed knowledge of design
(Ex: programmer testing her own module)

Black Box - Based on functional requirements (spec) only
(Ex: a Red Team conducting a test)

How Well Are We Doing?
Error Seeding

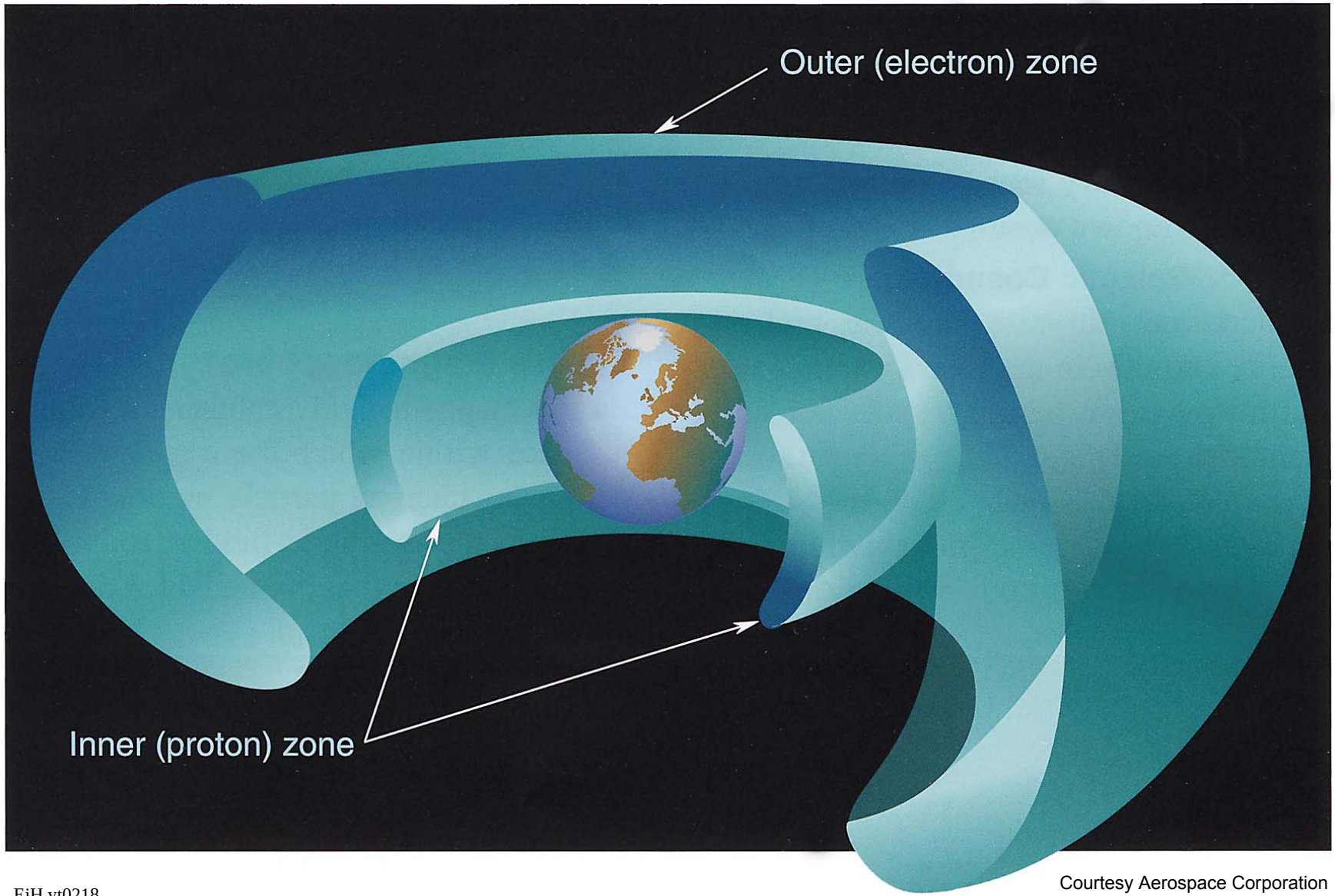
Error Seeding is the process of adding known faults intentionally in a program to:

-- monitor the rate of detection and removal

-- estimate the number of faults remaining in the program.

Don’t forget to *remove* the test faults! (Red Tag items)

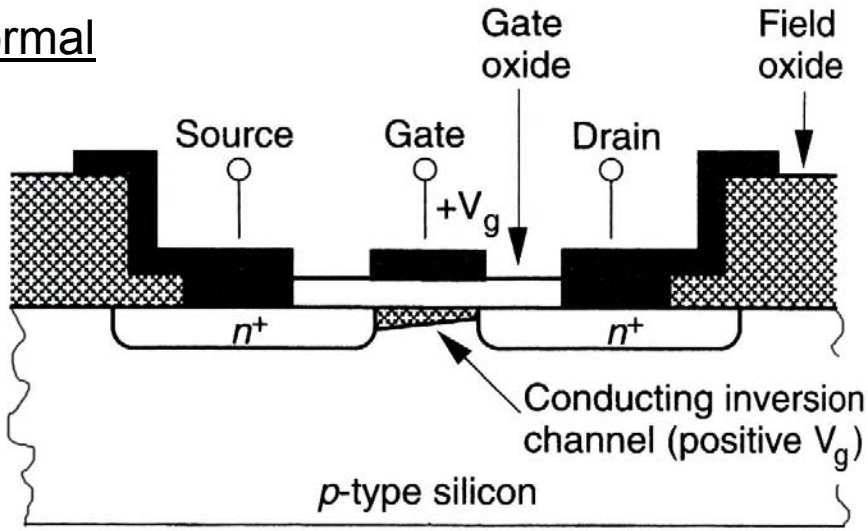
Earth's Van Allen Radiation Belts



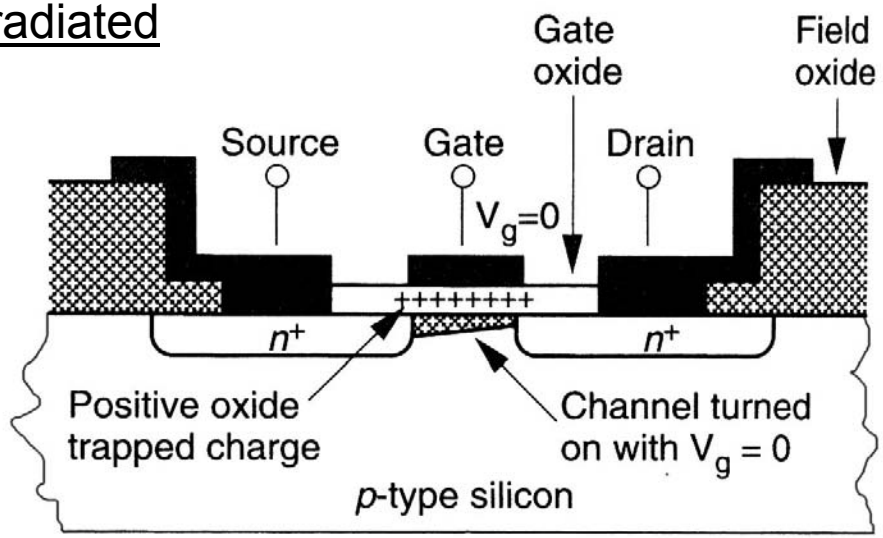
Courtesy Aerospace Corporation

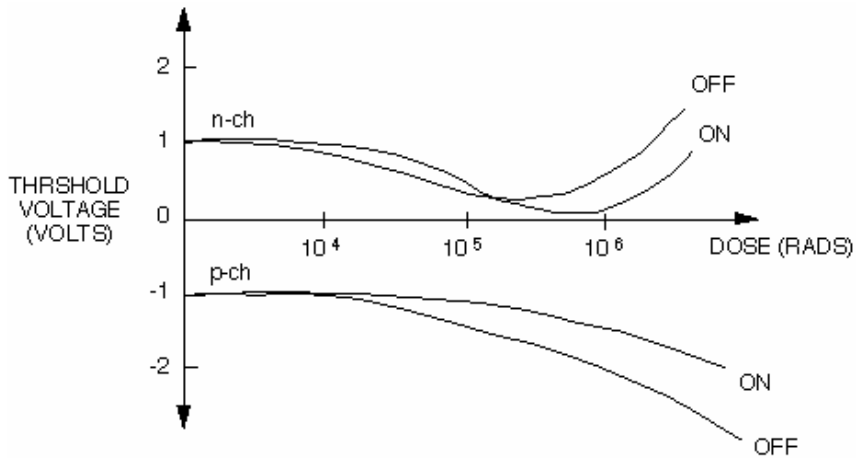
Total Dose Effects
Trapped charge in n-channel MOSFET

normal



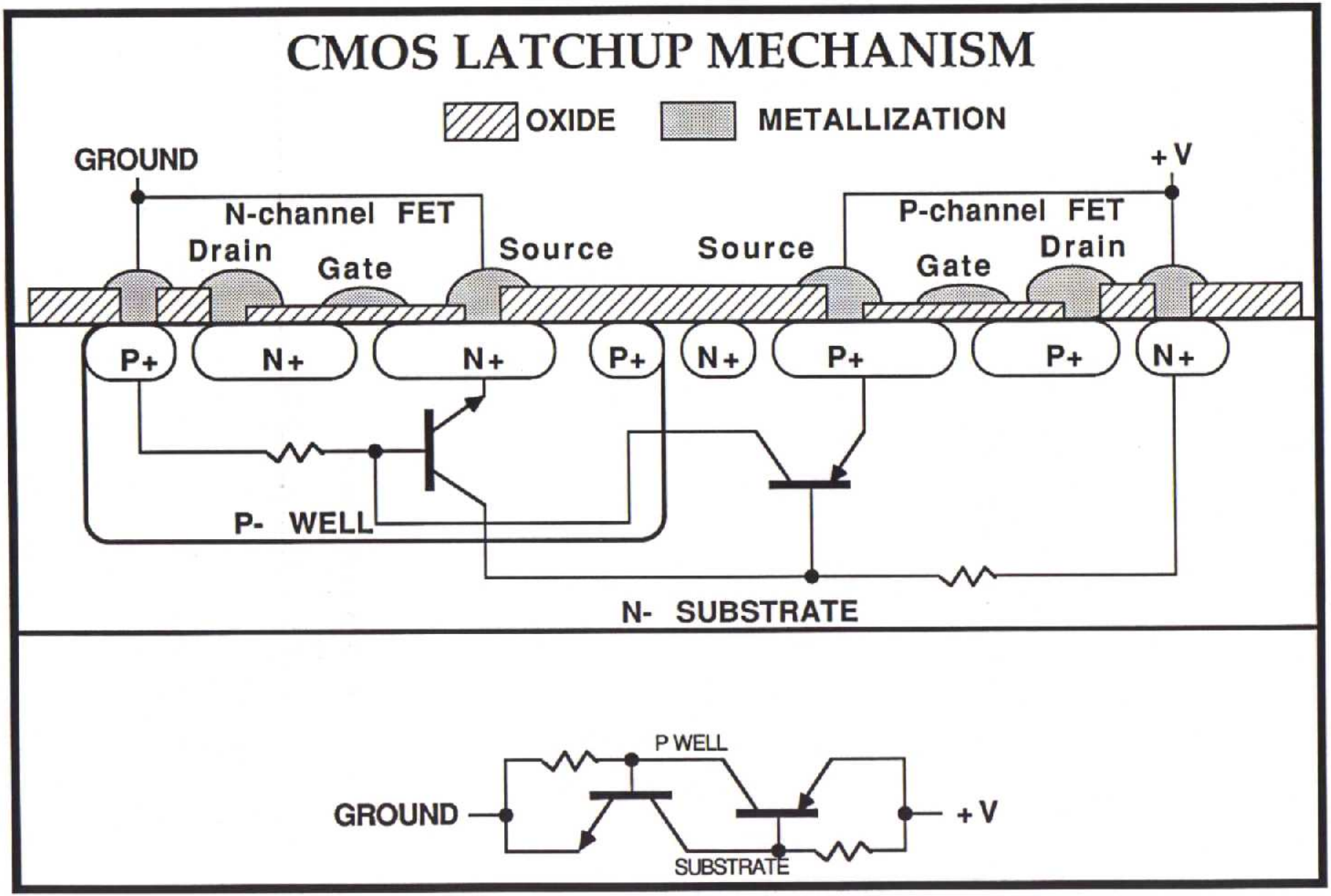
irradiated





NASA ASIC Guide: Assuring ASICS for Space

CMOS LATCHUP MECHANISM



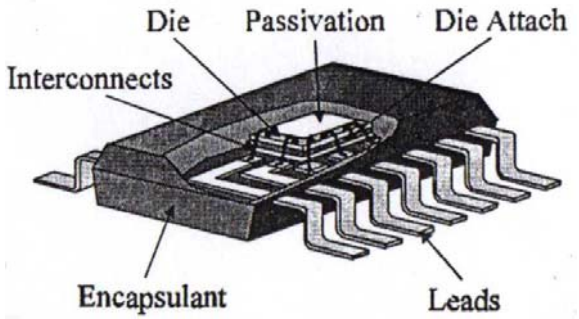
Acceleration Factors (Example)

- Test: 1000 cycles with $\Delta T_{test} = 125^o - (-55^o) = 180^o$ C
- Space application with $\Delta T_{app} = 55^o - (-30^o) = 85^o$ C with relative humidity assumed equal and the difference of relatively short dwell times at the upper temperatures ignored

$$AF = (180 / 85)^4 = 20$$

- The 1000 cycle temperature cycle test simulates 20,000 cycles in space – e.g., for a 90-110 minute low earth orbit, this test represents 3.4-4.2 years. Mission time simulated is even greater for deep space missions with a minimum of planetary shadowing and controlled sun angles
- Similarly, 1000 hours at 85º C and 85% RH simulates 70,000 hours or about 8 years of ground storage at 55º C and 40% RH using factors two and three.

What About Plastic Parts?



- Flight integrated circuits (ICs) have traditionally been required to be *hermetic*; plastic-encapsulated microcircuits (PEMs) were forbidden.
- Hi-rel, hermetic, military and space grade parts have declined to less than 1% of the total IC market (from 67% in 1965).
- Fortunately, PEM processes and our understanding of the physics of failure have improved greatly.
- The best of today's PEMs can be used for flight, *provided proper qualification, screening, storage, design, and fabrication processes are implemented.*
- Storage discipline - from the time the part is manufactured until it arrives on orbit - is especially critical.
- *Proper* use of PEMs can sometimes *increase* reliability.

Ref: "Reliable Application of Plastic Encapsulated Microcircuits for Small Satellites," W. Ash and E. Hoffman, Proc. 8th Annual Conf. on Small Sats., August 1994

It all begins with ...

... the **VERIFICATION MATRIX**

Show-- by one of 4 methods-- that every requirement is met.

Test. *Example:* "The transmitter output power shall exceed +34 dBm." Tests for requirements verification should be performed at the highest possible level of assembly.

Demonstration. *Example:* "The spacecraft shall demonstrate electro-magnetic self-compatibility." Often used when requirements contain phrases such as "shall support" or "shall not preclude" because of difficulty of proving that these requirements are met under all reasonable circumstances.

Analysis. *Example:* "For slews up to 110º, the slew rate shall be at least 0.5º/sec." Also used for requirements verified "by similarity" to previous designs. Analysis should be validated wherever possible by correlation to test data.

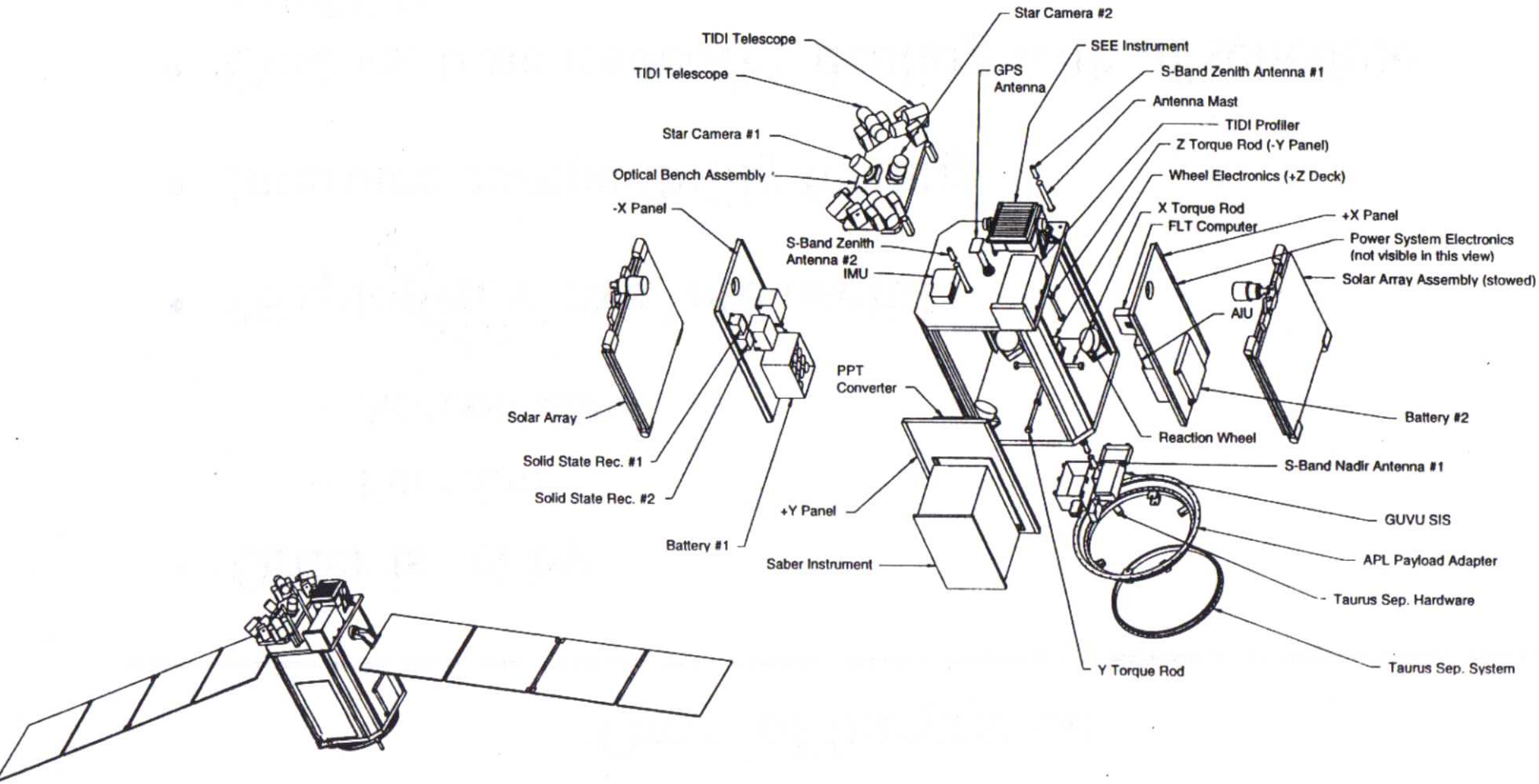
Inspection. *Example:* "The G&C application software shall be coded in C++."

In addition to indicating the verification method, the verification matrix must provide traceability to the (configuration managed) test procedures or analyses used to verify the requirement.

TIMED

Thermosphere • Ionosphere • Mesosphere • Energetics and Dynamics

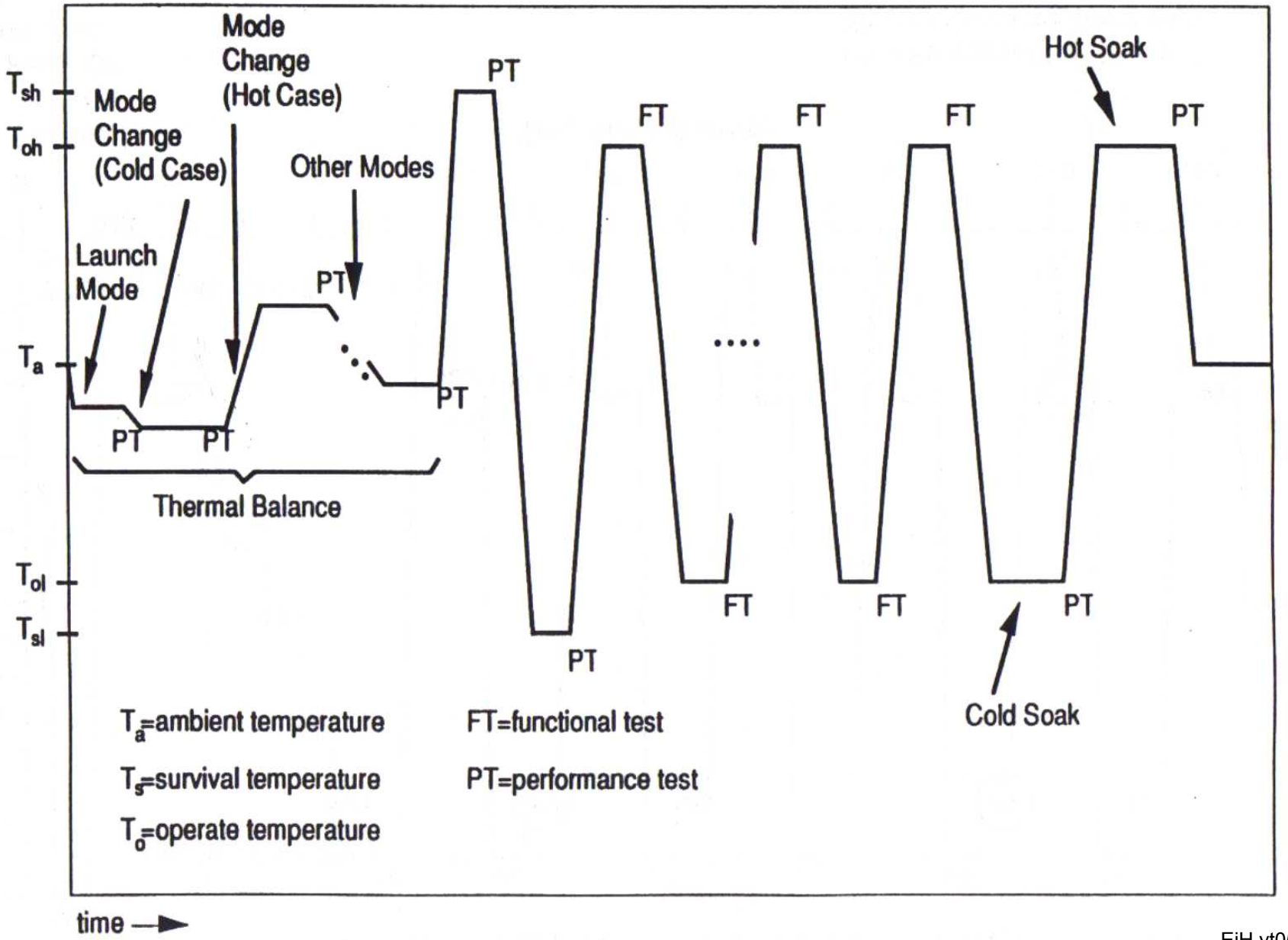
Exploded View



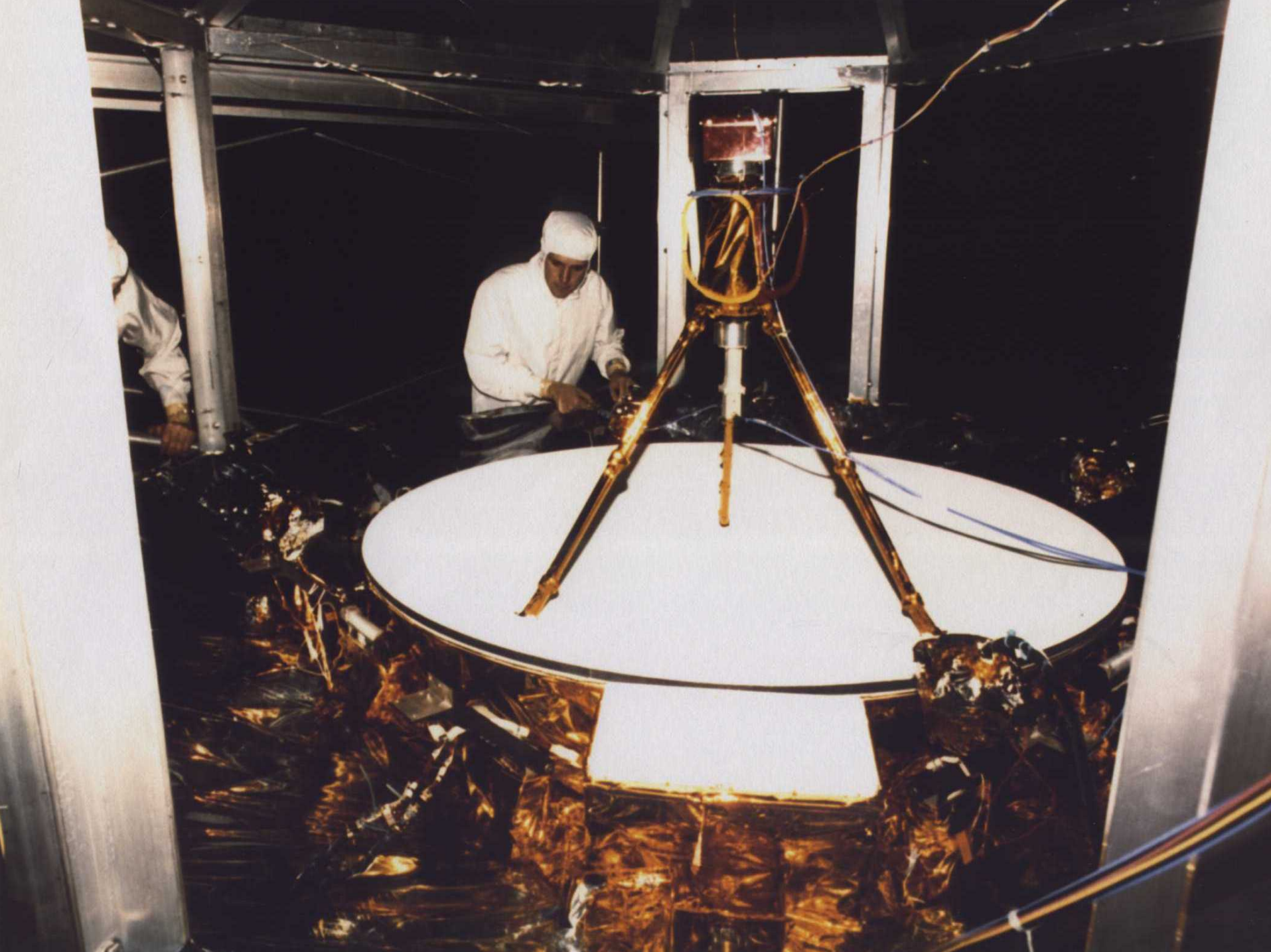
EjH gs1028

Courtesy: G. Cameron, AP

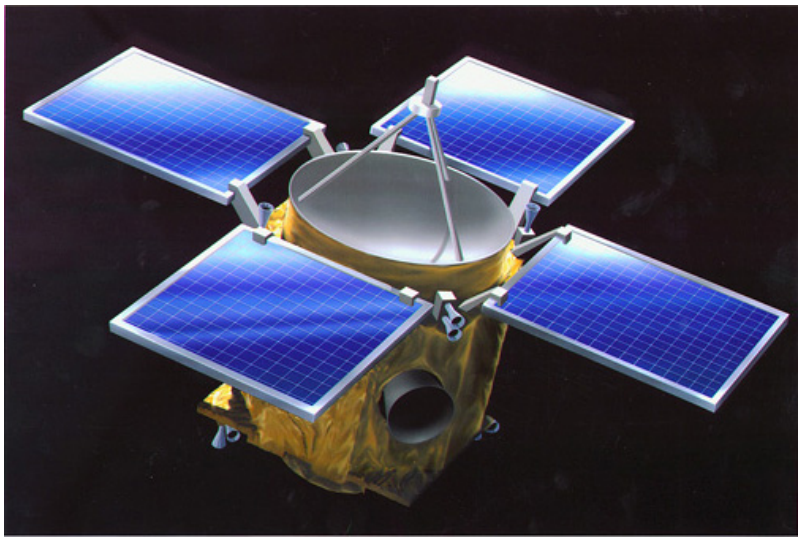
Spacecraft Thermal Vacuum Profile



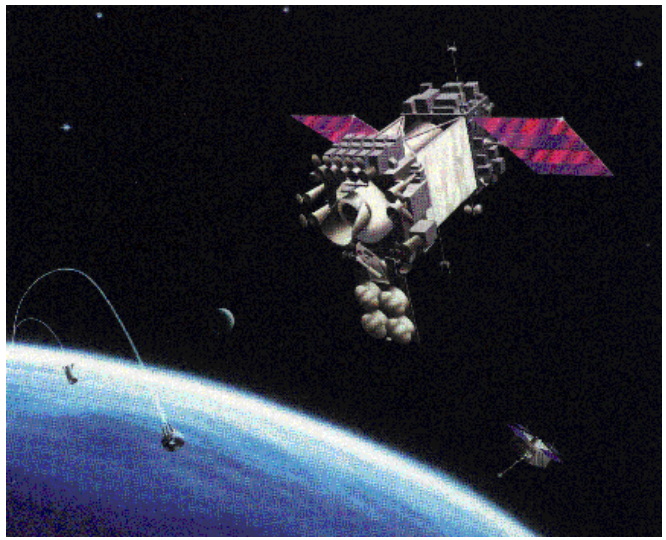
EjH yt0504



Case Studies



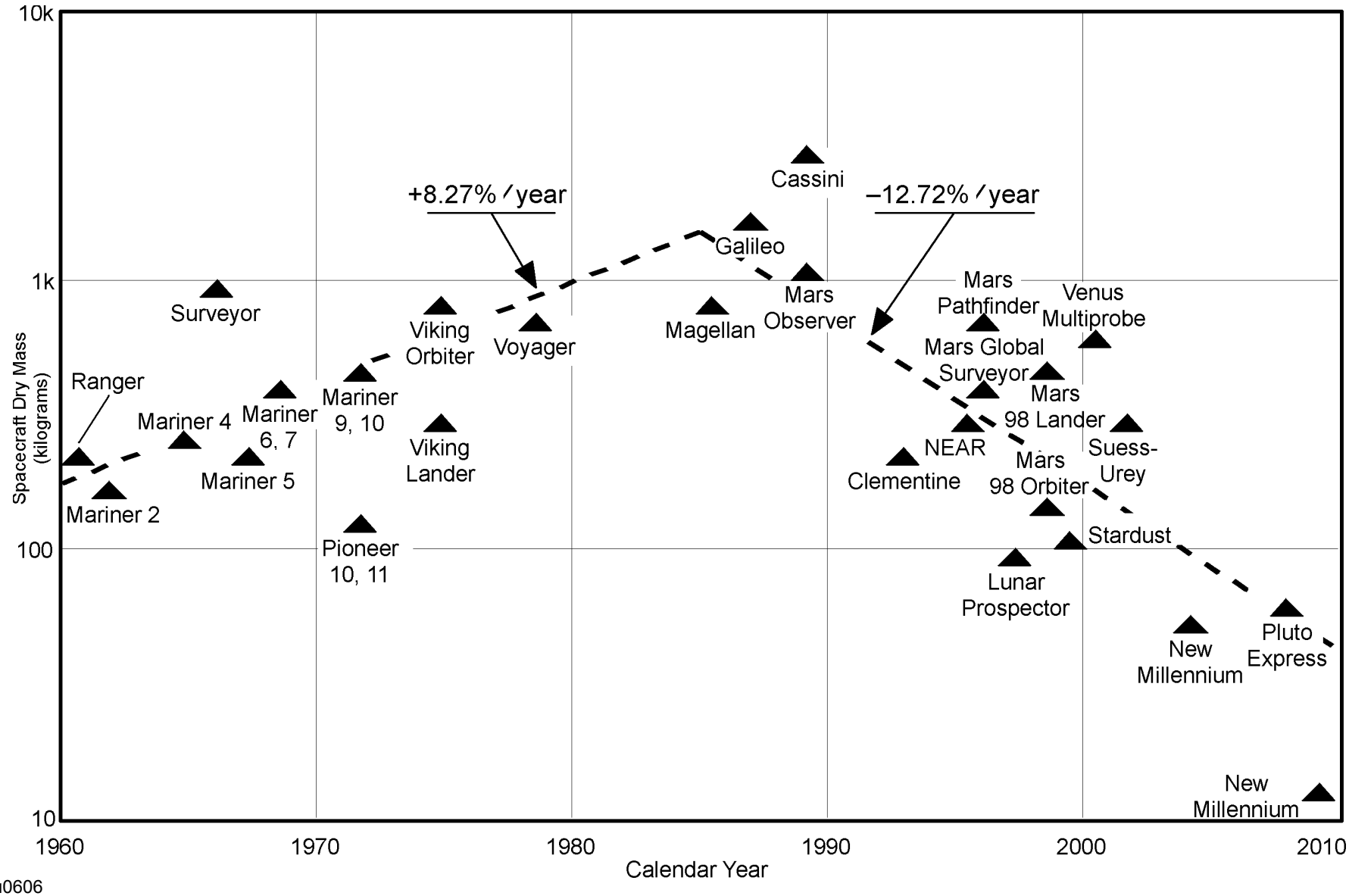
NEAR



MSX

Copyright © 2009 Eric J. Hoffman

Spacecraft Dry Mass vs. Calendar Year for Planetary Missions

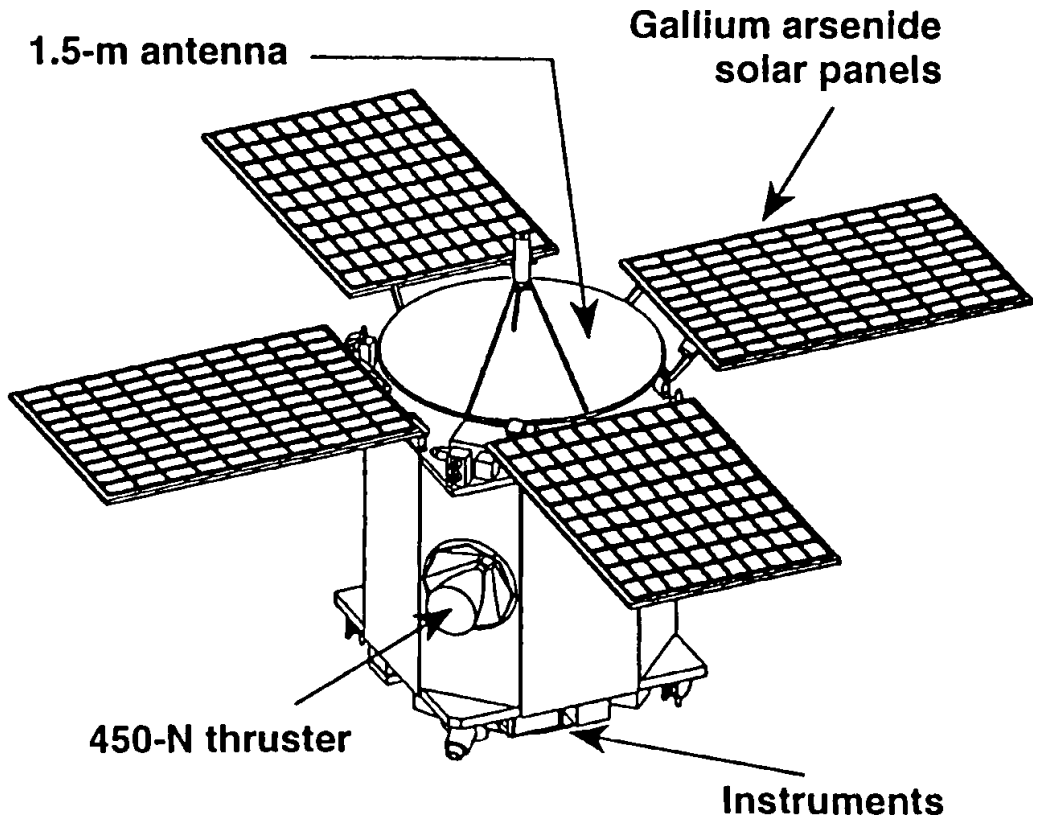


EjHyu0606
RCM.gsvp

NEAR Spacecraft Summary

- Three-axis stabilized
- Total weight: 800 kg
  - Propellants: 320 kg
  - Experiments: 60 kg
- Dual-mode propulsion system
  - Bipropellant (N_2H_4/N_2O_4)
  - Monopropellant (N_2H_4)
  - ΔV capability: 1450 m/sec
- Solar array power @ 1.00 AU: 1800 watts
- Data rate @ Eros rendezvous
  [Earth distance: 2.63 AU]
  - 34-meter DSN antenna: 4.4 kbps
  - 70-meter DSN antenna: 17.7 kbps
- Two solid-state recorders: 1.7 x 10^9 bits

  1.7 Gb ≈ 212 MB



EjH xu0629

MSX Mission

Midcourse Space Experiment

- BMDO-sponsored mission to demonstrate a variety of multispectral imaging technologies for identifying and tracking ballistic missiles during flight.
- Observe Earth and its limb and search for signatures of experimental missile launches across the ultraviolet, visible, and infrared parts of the spectrum.
- Spacecraft contamination experiment
- Space-Based Visible experiment (MIT Lincoln Lab)
- Design requirement: 4 years (goal: 5 years), 18 months IR cryogen
- Launched April 1996 from VAFB
- Over 12 years of continuous operation. Spacecraft decommissioned June 2008.

Instrument Section of MSX

EjH xu0629

Applied Technology Institute (ATIcourses.com)
Stay Current In Your Field • Broaden Your Knowledge • Increase Productivity
349 Berkshire Drive • Riva, Maryland 21140
888-501-2100 • 410-956-8805
Website: www.ATIcourses.com • Email: ATI@ATIcourses.com

You have enjoyed ATI's preview of

Spacecraft QA Integration & Test

Please post your comments and questions to our blog:

http://www.aticourses.com/wordpress-2.7/weblog1/

Sign-up for ATI's monthly Course Schedule Updates :

http://www.aticourses.com/email_signup_page.html