CS 335 — Software Development

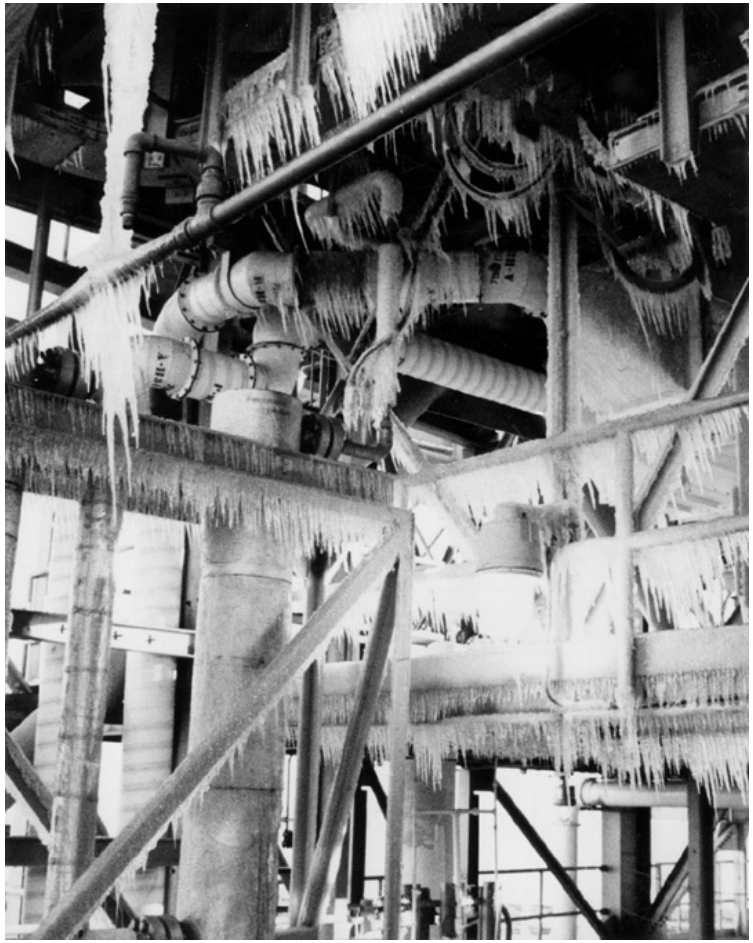
Problems in Engineering (Space Lecture)

Jan 13, 2010

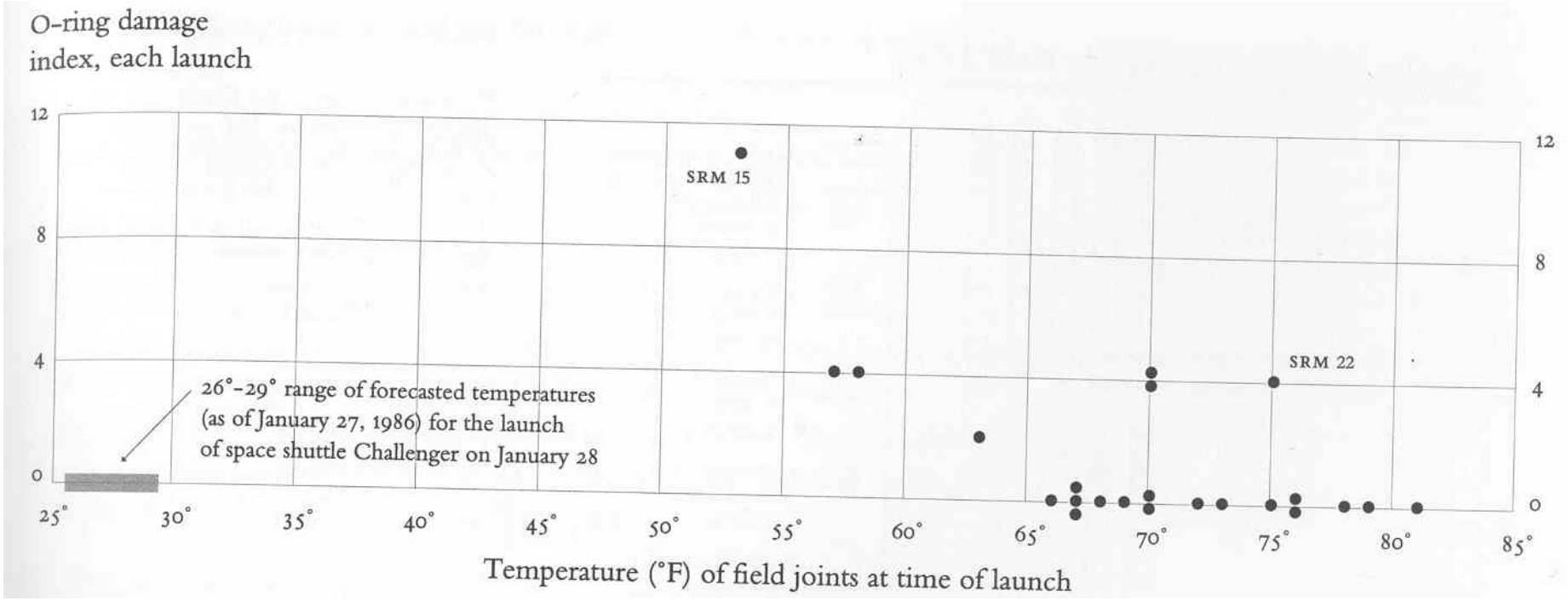
Lockheed Martin Corporation employs a Level 5 software group that puts together the shuttle software.
. . . Because we cannot afford to have deaths in the space program, the cost and effort are worth it. The cost amounts to making each subroutine a career-long research project.

Richard Gabriel, "Mob Software: The Erotic Life of Code"

AP; retreived from
http://news.bbc.co.uk/1/shared/spl/hi/pop_ups/06/sci_nat_1986_challenger_disaster/html/1.stm



Retreived from http://grin.hq.nasa.gov/index.html



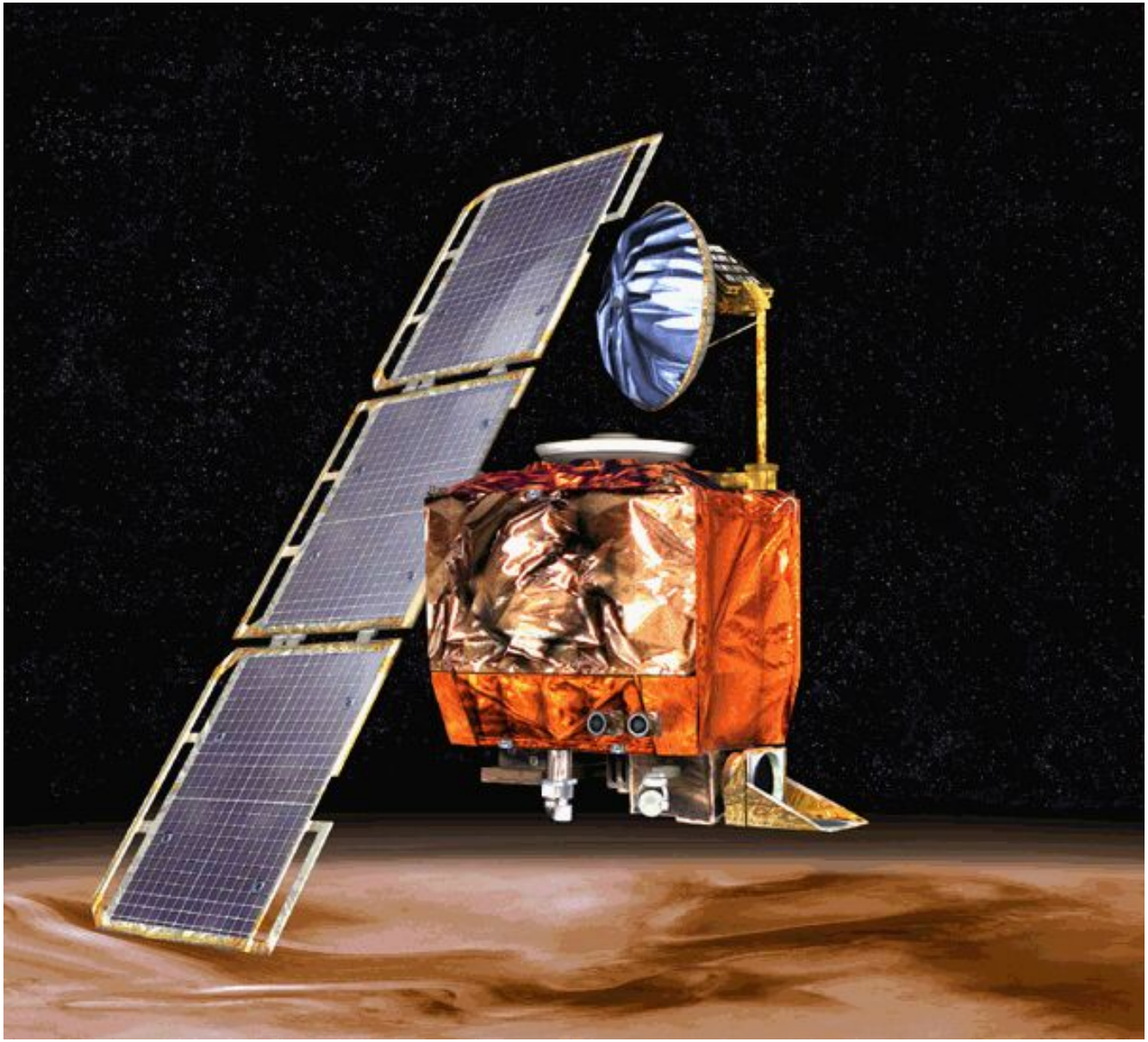
Edward Tufte, *Visual Explanations*, pg 45.

Review of Test Data Indicates Conservatism for Tile Penetration

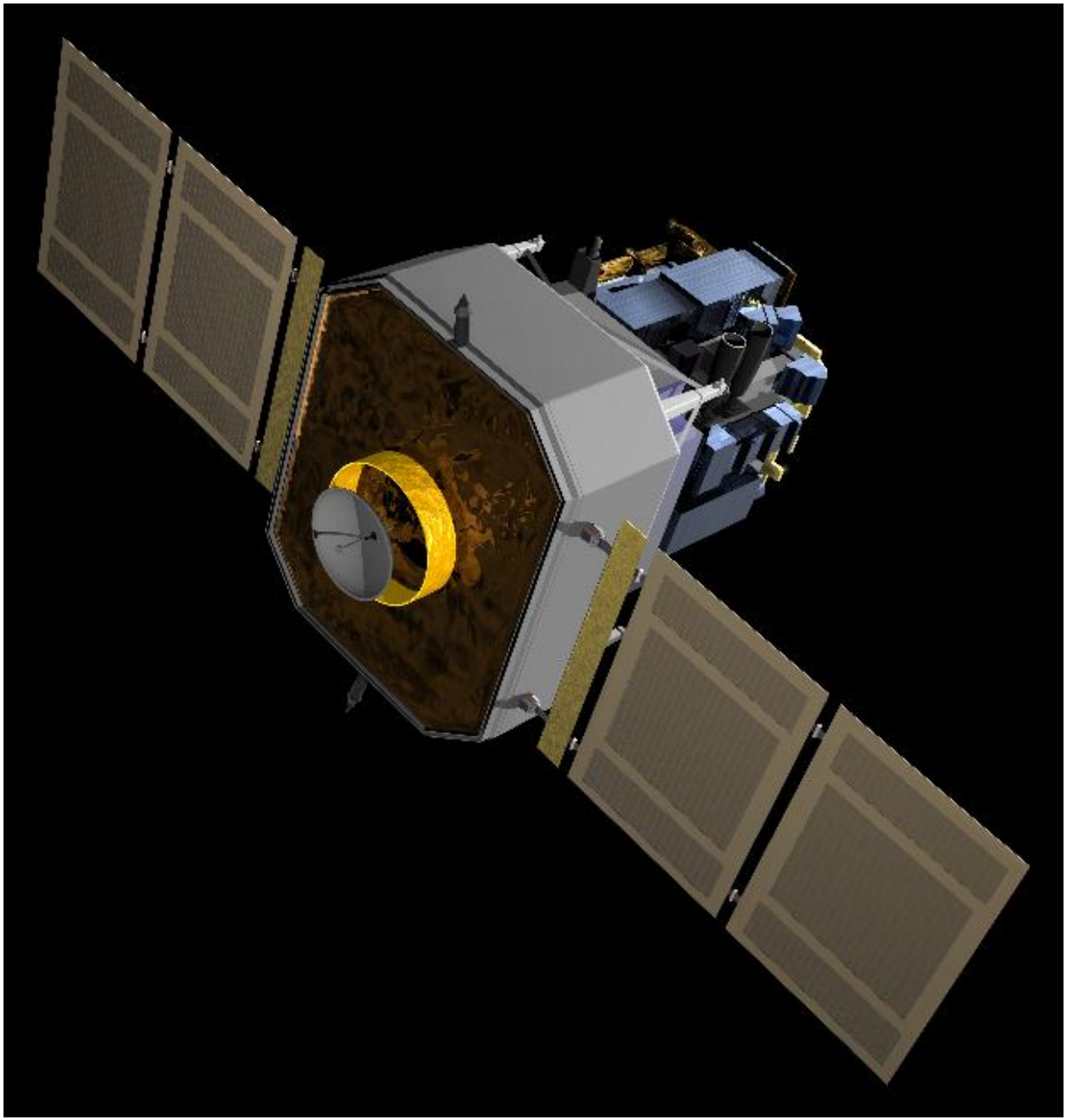
- **The existing SOFI on tile test data used to create Crater was reviewed along with STS-87 Southwest Research data**
  - **Crater overpredicted penetration of tile coating significantly**
    - **Initial penetration to described by normal velocity**
      - Varies with volume/mass of projectile (e.g., 200ft/sec for 3cu. In)
    - **Significant energy is required for the softer SOFI particle to penetrate the relatively hard tile coating**
      - Test results do show that it is possible at sufficient mass and velocity
    - **Conversely, once tile is penetrated SOFI can cause significant damage**
      - Minor variations in total energy (above penetration level) can cause significant tile damage
  - **Flight condition is significantly outside of test database**
    - **Volume of ramp is 1920cu in vs 3 cu in for test**

From "Orbiter Assessment of STS-107 Bipod Insultation Ramp Impact", retrieved from http://www.nasa.gov/columbia/foia/index.html

http://www.esa.int/SPECIALS/Launchers_Access_to_Space/ASEVLU0TCNC_1.html



http://en.wikipedia.org/wiki/Mars_Climate_Orbiter



http://soho.esac.esa.int/gallery/Spacecraft/SOHOLower2.html

JPL's 10 rules

1. Control flow must be simple. No goto statements or *recursion* allowed.
2. All loops must have a fixed upper-bound on the number of iterations.
3. No dynamic memory allocation (after initialization).
4. No function may be longer than a single sheet of paper.
5. Minimum of two assertions per function.
6. Declarations at the smallest possible level of scope
7. All return values must be checked by the calling function.
8. Preprocessor-use is restricted.
9. No more than one level of dereference is allowed.
10. All code is compiled from day 1 with no warnings.

G Holzman, "The Power of 10: Rules for Developing Safety-Critical Code." *IEEE Computer*, June 2006

Other references

Information on communication problems in the space shuttle missions from
Edward Tufte, *Visual Explanations*, Graphics Press, 1997.
Edward Tufte, *Beautiful Evidence*, Graphics Press, 2006.

Information on the software failures of various spacecraft accidents from
Nancy Leveson, "The Role of Software in Spacecraft Accidents", AIAA Journal of Spacecraft and Rockets, July 2004.