Illustrative Risks to the Public in the Use of Computer Systems and Related Technology

Peter G. Neumann, Computer Science Laboratory,
SRI International, Menlo Park CA 94025-3493

Risks cases as of **15 January 2001,** Copyright 2001, Peter G. Neumann, SRI International EL243, Menlo Park CA 94025-3493 (e-mail Neumann@csl.sri.com; http://www.CSL.sri.com/neumann/http://www.CSL.sri.com/neumann/; telephone 1-650-859-2375; fax 1-650-859-2844): Editor, ACM SIGSOFT Software Engineering Notes, 1976–93, Assoc.Ed., 1994–; Chairman, ACM Committee on Computers and Public Policy (CCPP); Moderator of the Risks Forum (comp.risks); cofounder with Lauren Weinstein of People For Internet Responsibility (http://www.pfir.orghttp://www.pfir.org, announced in RISKS-20.65). See also Lauren's Privacy Forum Digest (http://www.vortex.comhttp://www.vortex.com), partially sponsored by the ACM CCPP.

This list summarizes items that have appeared in the Internet Risks Forum Digest (RISKS) – which I moderate (comp.risks newsgroup) – and/or published ACM SIGSOFT Software Engineering Notes (SEN). In this collection of mostly one-liner summaries, (R i j) denotes RISKS volume i issue j; (S vol no:page) denotes an issue of SEN, where there has been one volume per year, with vol 25 being the year 2000; page numbers are given primarily only from 1993 on; (SAC vol no) indicates an item in the quarterly SIGSAC Security and Control Review, where vol 16 is 1998, which was the final volume. The SEN material prior to 1995 is summarized in my Computer-Related Risks book (see below). Later material is gradually being brought on-line, as noted below.

Some incidents are well documented, while others need further study. A few are of questionable authenticity, and are noted as such ("bogus???"). Please send me corrections and new cases, along with suitable references. This list is updated at least quarterly and is browsable on-line (`ftp://ftp.CSL.sri.com/neumann/illustrative.html` courtesy of Otfried Cheong's Hyperlatex), also printable in a two-column 8-point format (illustrative.pdfillustrative.pdf and illustrative.psillustrative.ps). [Incidentally, Hyperlatex is wonderful Free Software: (http://www.cs.ust.hk/˜otfried/Hyperlatex/http://www.cs.ust.hk/˜otfried/Hyperlatex/, and after September 2000: http://www.cs.uul.nl/˜otfried/Hyperlatexhttp://www.cs.uul.nl/˜otfried/Hyperlatex).]

```
SEN regular issues, by year, volume&number
..1976,vol 1: #1 = May; #2 = Oct
  ==================================
..year 1977 78 79 80 81 82 83 84 85
  volume  2  3  4  5  6  7  8  9 10
  ---------------------------------
  Jan    #1  1  1  1  1  1  1  1  1
  Apr    #3  2  2  2  2  2  2  2  2
  Jul    #4  3  3  3  3  3  3  4  3
  Oct    #5  4  4  4  5  4  5  5  5
  ==================================
..year 1986 87 88 89 90 91 92 93 94
  volume 11 12 13 14 15 16 17 18 19
  ---------------------------------
  Jan    #1  1  1  1  1  1  1  1  1
  Apr    #2  2  2  2  2  2  2  2  2
  Jul    #3  3  3  5  3  3  3  3  3
  Oct    #5  5  4  6  5  4  4  4  4
  ==================================
..1995,vol20: #1=Jan; 2=Apr; 3=Jul; 5=Dec
..1996,vol21: #1=Jan; 2=Mar; 4=Jul; 5=Sep
..1997,vol22: #1=Jan; 2=Mar; 4=Jul; 5=Sep
..1998,vol23: #1=Jan; 3=May; 4=Jul; 5=Sep
..1999,vol24: #1=Jan; 3=May; 4=Jul; 5=Dec
..2000,vol25: #1=Jan; 2=Mar; 3=May; 4=Jul
..2001,vol26: #1=Jan; 2=Mar;
```

Read the Risks Forum as comp.risks if you can, or send e-mail to risks-request@csl.sri.com for a subscription, single text line "subscribe" (append desired address only if not your From: address), or "info" for info. Send contributions to risks@CSL.sri.com. Archives are available from `ftp://ftp.sri.com/risks` or by "ftp ftp.sri.com", "login anonymous", "cd risks" (which gets the "dir" for the current volume, and "cd i" then gets you into the subdirectory for any preceding volume i = 1 to 19). A mirror at Newcastle http://catless.ncl.ac.uk/Risks/http://catless.ncl.ac.uk/Risks/ is maintained by Lindsay Marshall, and includes a nice search facility. Specific issues can be read directly as `http://catless.ncl.ac.uk/Risks/I.J.html` [where I=volume#, J=issue#]. An Australian mirror is at http://the.wiretapped.net/security/textfiles/risks-digest/http://the.wiretapped.net/security/textfiles/risks-digest/. "Inside Risks" distills some of the discussion into a monthly inside-back-cover column in the *Communications of the ACM.* The list columns to date is given at the end of this list.

My book (Peter G. Neumann, *Computer-Related Risks,* Addison-Wesley (ISBN 0-201-55805-X) and ACM Press (ACM Order 704943), 1995) summarizes many of these cases and provides additional analysis. (A few errata for the first three printings are on my Web page, noted above.) Most of the (S vol no) items listed below for i < 20 are discussed in the book; more recent items generally include the relevant on-line (R i j) references. If you cannot find the book in a bookstore, it is on amazon.com, or call A-W within the U.S. at 1-800-822-6339 – or if you are outside of the U.S., 1-617-944-3770 and ask for International Orders. The book is now also available in Japanese (ISBN 4-89471-141-9). Instead of trying to produce a second edition in the face of a massive influx of new RISKS cases, the fourth printing of the book gives the URL for the Addison-Wesley Web site (http:www.awl.com/cseng/titles/ISBN-0-201-55805-X/http:www.awl.com/cseng/titles/ISBN-0-201-55805-X/), which includes the first chapter of the book and an extended preface. That Web site and my own contain more material that would otherwise have gone into the second edition. See http://www.csl.sri.com/neumann/risks-new.htmlhttp://www.csl.sri.com/neumann/risks-new.html for new material and http://www.csl.sri.com/neumann/cal.htmlhttp://www.csl.sri.com/neumann/cal.html for an excerpted summary of Y2K and related calendar-clock problems.

Henry Petroski (among others) has noted that we rarely learn from our successes, and must learn more from our failures. The collection of cases cited here provides rich opportunities for reflection that could help us to avoid similar problems in the future. Unfortunately, it also demonstrates that the same types of mistakes tend to recur.

SEN and RISKS also consider approaches for developing better computer systems, e.g., safer, more reliable, more secure. There are many approaches to developing sound systems; none is guaranteed. Whereas the emphasis in the following list is on problems rather than on would-be solutions, the pervasive nature of the problems suggests that techniques for the effective development and operation of computer-related systems are frequently ignored. Worse yet, even ideal systems can result in serious risks, through unanticipated technological problems or human foibles. We include here primarily cases that have been publically reported, although we know of various additional cases whose existence for one reason or another has not seen the light of day. A few successes are also included, although the failures seem to predominate. We are always interested in hearing more about successes. Although I receive occasional complaints about the preponderance of failures in RISKS, there appear to be very few real successes. Perhaps not enough folks are heeding some of the advice that you can gather from RISKS and that are distilled in *Computer-Related Risks.*

Descriptor Symbols

The following descriptor symbols characterize each entry.

! = Loss of life/lives; * = Potentially life-critical or safety problem
V = Overall system or subsystem sur**ViV**ability problems (with respect to diVerse adVersities, including attacks *and* malfunctions). Startlingly many cases fit this category; many V-unflagged cases also represent failures to continue performing properly, or delays, or other cases of misuse that could have led to much more serious survivability problems.
$ = Loss of resources, primarily financial
S = **S**ecurity/integrity/misuse problem; P = **P**rivacy/rights abuse or concern
H = Intentional **H**uman misuse (e.g., user-administrator-operator-penetrator)
h = Accidental **H**uman misuse or other inadvertence
I = **I**nsider; O = **O**utsider; A = Inadequate **A**uthentication or **A**ccess controls
d = System **D**evelopment problems
e = Improper **E**volution/maintenance/upgrade. (H,h,i,f,d,e involve human foibles.)
r = Problems with **R**equirements for system or operation (including the overall system concept)
f = **F**laws (or **F**eatures in design, or hardware/software implementation
i = Mis**I**nterpretation/confusion/human errors at a man-system **I**nterface

m = Hardware **M**alfunction attributable to system deficiencies, the physical environment, acts of God, etc.
M = **M**alfunction specifically due to electronic or other interference
+ = Beneficial; - = problematic with none of the above categories
@ = This item is also listed in another category

Items Listed by Categories

Recent Items (yet to be merged in)

Vm PGN's Univ. Maryland survivable systems course beset with survivability problems (S 25 1:)
fm California government agencies' computers fail, cars impounded; Pac*Bell blamed (R 20 62)
Vfm Software disaster leaves new Australian submarine unfit; wide range of pervasive hardware/software failures reported (R 20 48)
*fh Cancelling errors, serendipity in avoiding risks, and Kepler: note by Henry Baker (R 20 48,51)
Vm Weather-predicting Cray C90 supercomputer lost in fire, weather predictions reduced (R 20 62)
Vm Netcom file-server hardware outage loses half of the e-mail customers, depending on first letter of name (R 20 49)
m Airport security check powers up computer (R 20 55)
f MIT system weather command gives "Temp: 2147483647 F (2147483647 C)"; yes, that's $2^{31} - 1$ (R 20 51-52); *USA Today* weather page: high of 577 F (R 20 58)
? NOAA radio +61 degrees F, wind-chill -64 (R 20 57)
f/m/h? Date failure on weather.com: 28 Apr not 16 Sep (R 20 58)
$fh Dispute over membership software used by German SPD (R 20 41)
$f Reliability of NT in embedded applications (R 20 41)
f Microsoft Word footnote problems irks federal appeals court: Word does not count words correctly (R 20 52)
fe IE2 cannot read www.microsoft.com for upgrade (R 20 55)
if More anomalies in Microsoft driving directions (R 20 62-63)
? Risks of "self-destructing e-mail" from Disappearing Inc. (R 20 62)
h,h Linux banned after Samba misconfigation blocks NT authentication (R 20 61)
rh Vending machine default phone number 000 (Australian emergency number) yields hundreds of false alarms (R 20 47)
f Kangaroo helicopter responses mess up Australian virtual-reality simulators (R 20 47,76)
hf Can you trust AT&T Wireless PCS text messaging? (no) (R 20 52-53)
f Risks of financial planning engines with bogus results (R 20 48)
h EverQuest is the "digital version of crack" (R 20 52)
rd More on California's software woes: welfare system problems (R 20 53)
h (but blamed on computer) Argos retail offered Sony Nicam TV for 3£ instead of 300£ (R 20 57)
f E*Trade Market Watch shows Dow Jones average at $1, down $10936.88 (R 20 56)
Vmfm Power coming back on causes UPS to lose power (R 20 55)
+/-?? Programming competency and the use of FORTH (R 20 49-53)
$f Toyota smog-warning computer suit (R 20 48)
fh CNN report on Gary Shandling lawsuit names him as "Changeling"; spelling corrected? (R 20 47)
h White House admits over one year of VP's e-mail lost forever (S 25 4:8, R 20 91)
f Software fault stops 76,000 customers receiving phone calls (S 25 4:8, R 20 87)
h UCITA, the Uniform Computer Information Transactions Act (Schneier, S 25 4:8 and R 20 87, and Simons in August 2000 *CACM* Inside Risks)
f Microsoft Explorapedia Nature: earth rotates in wrong direction (R 20 87)
+ Patent office revamps Web patent reviews (R 20 87)
h- 50 million U.S. adults at risk for Internet illiteracy (R 21 08-09; S 26 1:18)
(f/m/h?) Computer-related sewage release into Massachusetts Bay (R 21 08; S 26 1:18)
fid Not-so-smart weapons in Kosovo (R 21 01; S 26 1:18)
de Satellite system outage hits Associated Press (R 21 04; S 26 1:18)
m/f/h? Root servers used by Network Solutions failed (R 21 03; S 26 1:18-19)
$dh $35M San Mateo CAlifornia health system upgrade is a downer; receivables backlog over $40M; blame scattered (R 20 98)
$d WA King County blew $38 million on canceled payroll system (R 21 01; S 26 1:19)
eh Northeastern University admits 25% too many students (600 extra) after DB upgrade loses potential applicants (R 21 01; S 26 1:20)
f CSX crew spots problem signal, averts collision; insulation problem? (R 21 04; S 26 1:20)
e Upgrade to Guildford Station (Surrey, UK) software disables hundreds of train tickets for automated gates (R 20 94: S 26 1:20)
fi DC Metro can't label rerouted holiday trains on 4 Jul 2000: confusion (R 20 95; S 26 1:20)
m Computer crash caused loss of scheduled cab pickups (R 20 98; S 26 1:20)
m Sliced fiber-optic cable in Lancaster PA disrupts local and long-distance phone service NY to MD (R 20 93; S 26 1:20-21); another outage in Massachusetts (R 20 97)
m Heavy rains take out State Department phone service for 2 hours, backup batteries out because of earlier fire (R 20 93; S 26 1:21)
$mh Drop of welding material causes fire that affected 27 cables, telephone service for 25,000 (R 20 93; S 26 1:21)
m Remote line break leaves San Juan Puerto Rican without power (R 21 04; S 26 1:21)
- Booming computer firms are running out of power (R 20 98)
- Russian troops override power shutoff for unpaid bill affecting missile base (R 21 05; S 26 1:21)
!h Illinois man dies after utility cuts power for arrears (R 20 95; S 26 1:21)
f New Pentium III chip recalled (R 21 04; S 26 1:21-22)
*h F-117 stealth fighter in near-miss with UAL jet (R 21 04; S 26 1:22)
*SHA Fake air controllers alert in UK (R 21 04; S 26 1:22)
f/m? Collapse of UK air-traffic control computer (R 20 93-94); known bugs reduced from 500 to 200 (R 21 01)
def U.S. west-coast ATC woes 19 Oct (hundreds of flights affected) and 23 Oct 2000 (loss of flight plans for Northern CA and Western NV) (R 21 09; S 26 1:22)
mf FADEC computers cause uncommanded shutdowns of aircraft engines in flight; linked to power transistor (R 21 05; S 26 1:22)
m Total primary/secondary power outage at Sydney Airport leaves 20 planes circling (R 20 94; S 26 1:22-23)
m/f? Sydney Airport's new $43M baggage system fails for second time in five days (R 21 02; S 26 1:23)
h Oregon lottery coincidence reported by Infobeat caused by computer crash: winning numbers published before they were drawn by editor mistakenly using Virginia numbers after a crash! (R 20 94)
ef DB upgrade causes crash of Italian online stock trading (R 20 95)
f Fox network misprograms time on US VCRs for a year (R 20 95)
fh Army Automated Time and Attendance Production System (ATAAPS) loss of data for 10 days (R 20 97)
f Computerized air-conditioning bugs chill employees (R 21 05; S 26 1:26)
- ISP whacks game fan with $24,000 bandwidth fine (R 21 08; S 26 1:26)
e Memorial Society software upgrade loses some life-time members (R 21 08; S 26 1:26)
!!(f/h?) Russian nuclear sub explosion (missile test awry) kills crew of over 100 in Barents Sea, 13 Oct 2000. Also, *Izvestia* reported over 507 sub crew members had died previously. (R 21 01)
*f Sydney train system traps man's leg (R 21 01)
f New UK Millennium Bridge closed after one day, alarming instability despite extensive simulation; resonant frequencies at walking speeds! (R 20 93,95)
+/- People For Internet Responsibility (PFIR) Statement on Internet Policies, Regulations, and Control (http://www.pfir.org/statements/policies) (R 20 96)
S Navy to use Windows 2000 on aircraft carriers (R 20 95)
f Microsoft Windows Update Corporate Web site "features more than 1,000 system updates and drivers for the Windows 2000 platform"!!! (R 21 04)
f Y2K-leapyear hangover: CDMA GTE wireless date 31 Jun 00 (R 20 92)
+/- Stephen King's not scared of trusting online readers (R 20 98)
END of yet-to-be-merged recent material ...

Space

..... **Manned/Womanned [Peopled?] Space Exploration:**
!!$$Vrfh Shuttle Challenger explosion, 7 killed. [Removed booster sensors might have permitted early computer detection of leak?] [28Jan1986] (S 11 2) [Probably not? See Paul Ceruzzi, Beyond the Limits – Computers Enter the Space Age, MIT Press, 1989, Appendix.]
* Mercury astronauts forced into manual reentry? (S 8 3)
$f STS-1 1st Space Shuttle Columbia backup launch-computer synch problem. See Jack Garman, "The bug heard 'round the world" (S 6 5:3-10) Oct. 1981.
*f STS-2 shuttle simulation: bug found in jettisoning an SRB (S 8 3)
*f STS-2 shuttle operational simulation: tight loop upon cancellation of an attempted abort; required manual override (S 7 1)
*Vf STS-6 shuttle bugs in live Dual Mission software precluded aborts (S 11 1)
*m STS-9 Columbia return delayed by multiple computer malfunctions (S 9 1)
*f STS-16 Discovery landing gear – correlated faults (S 10 3)
*if STS-18 Discovery positioned upside down; mirror to reflect laser beam from

Mona Kea aimed upward (+10,023 miles), not downward (... feet) (S 10 3)

*$ STS-20 Two-day delay of Discovery launch: backup computer outage (NY Times 26 Aug 1985); Syncom 4 satellite failure as well (S 10 5)

$f SRS-36 Atlantis launch delayed [25Feb1990]; "bad software" in backup tracking computer system, but no details given. (S 15 2)

h Shuttle Discovery shutdown procedure for two computers reversed (S 16 1)

*hife STS-24 Columbia near-disaster, liquid oxygen drained mistakenly just before launch, computer output misread (S 11 5)

*f Columbia orbiter suddenly rotates, due to telemetry noise (S 15 3)

$m Columbia delayed by computer, interface, sensors; then navigation (S 16 3)

$f Shuttle Endeavour computer miscomputes rendezvous with Intelsat satellite; nearly identical values interpreted as identical; those SW problems force spec changes (AviatWkSpT 29May/8Jun1992, S 17 3 duplic S 17 4)

* Shuttle computer problems, 1981–1985; 700 computer/avionics anomalies logged; landing gear problems in STS-6 and -13; multiple computer crashes in STS-9, cutting in backup system would have been fatal; thermocouple failure in STS-19 near disaster (S 14 2)

m Atlantis spacecraft computer problem fixed in space (S 14 5)

$f Untested for change, SW delays shuttle launch; 3-min on-line fix (S 15 3)

$(m/f?)V Shuttle Atlantis launch scrubbed: "faulty engine computer" (S 16 4)

$*V Columbia launch scrubbed at T-3sec 22Mar93, leaky valve (S 18 3:A14)

$*V STS-56 Discovery launch scrubbed at T-11sec 5Apr93, main propulsion system high-point bleed valve open-indicator went to *off,* closed-indicator did not switch to *on*. Indicator problem? program error? (S 18 3:A14)

h Discovery SRB recovered with missing pair of pliers (S 18 3:A14)

fm Channel blocked, Discovery exhausts storage for ozone data (S 18 3:A14)

H Experimental Space Shuttle e-mail address divulged, bombarded (S 16 4)

m Woodpeckers delay shuttle launch (S 20 5:8)

*m Docking problem aboard Soviet space station Mir (S 15 5)

m Mir Space Station computer problems add to difficulties; main computer failed during docking attempt, 19 Aug 1997 (R 19 31,32), with detailed analysis by Dennis Newkirk (R 19 33)

m Mir computer failure affects steering; replacement computer fails to load (end of May 1998, just before Discovery launch) (R 19 78)

*$d GAO reports on NASA Space Station: increased safety risks, costs (S 17 4)

* Risks of junk in space much greater than previously thought (S 17 4)

*f$ Potential software nightmare for International Space Station, with considerable discussion (R 19 49-51)

..... **Satellites, Probes, Others:**

$f Hubble Space Telescope problems, soaring costs, missed deadlines, reduced goals, etc. (S 15 2); sensors misdirected because of wrong sign on precession in star data; antenna # 2 limited by misplaced cable, #1 limited because software had only one limit stop, same for both (S 15 3) No system test. 1mm error in monitor program of mirror polisher (S 15 5) See M.M. Waldrop, Science 249, 17Aug1990, pp.735-736.

Vf/m Hubble Space Telescope antenna swing causes shutdown (S 17 1)

fh More Hubble SW: misloaded ephemeris table, bad macro (S 18 1:24)

$fhV $150M Intelsat 6 comm satellite failed; booster wiring error, payload in wrong bay; miscommun. between electricians and programmers (S 15 3)

$mV Canadian TeleSat Aniks die: solar coronal hole electron flux (S 19 2:3) Anik E-2 control restored, but with shorter life ($203M asset) (S 20 2:11)

fmV SOHO Mission Interruption Preliminary Status and Background Report documents apparently unconnected multiple failures that caused the satellite to lose control (R 19 87)

fhV Final report on the Solar and Heliospheric Observatory (SOHO) spacecraft failure: software flaw and improper command (R 19 90); mis-identification of a faulty gyroscope, staffing problems, inadequate training, ambitious schedule, unreviewed procedure changes, etc. (R 19 90, 94); contact finally reestablished. (S 24 1:31)

hm 5 printers off-line or jammed, Voyager 1 data lost over weekend (S 15 5)

f Voyager 2 software faults at launch, 20 Aug 1977 (S 14 6)

V$ Titan 34D, Nike Orion, Delta-178 failures follow Challenger (S 11 3)

V$* Titan 4 rocket test-stand SRB explosion; simulation missed failure mode (S 16 4)

V(m/f?) Final Titan 4A launch explodes with Vortex satellite; total cost over $1B, Aug 1998 (S 24 1:32, R 19 91)

mV Titan 4B leaves missile warning satellite in useless orbit (R 20 36)

Vm/f? Titan 4B with Milstar communications satellite separates four hours early, resulting in a useless low orbit, 30 Apr 1999 (S 24 4:26, R 19 36)

Vhm$ 6 successive Theater High-Altitude Area Defense (THAAD) failures, including three typos; then a “success” (R 20 43,45); Titan 4B failure (R 20 39) blamed on shifted decimal point in upper-stage software (R 20 45)

Vf,f Delta III launch ends after 71 seconds due to software flaw; two weeks later, Delta III leaves Loral Orion comm satellite in useless low orbit 4 May 1999 (R 20 38)

Vmfh Centaur/Milstar upper-stage failure due to attitude-control system software (R 20 49); roll-rate filter constant .1 factor (-0.1992476, not -1.992476) (R 20 57,59)

Vm$ Private imaging satellite Ikonos 1 disappears 8 minutes after launch (S 24 4:26, R 20 36); loss blamed on an electrical problem that prevented the aerodynamic payload cover from coming off. Subsequent Ikonos launched successfully (R 20 60):

f Terra spacecraft navigation software problems (S 25 3:18, R 20 78)

V$(m?f?) Two satellite failures (R 21 19, S 26 2:)

Vm/f? Russian rocket blows 12 Globalstar satellites (S 24 1:32, R 19 95)

V$(f?m?) Computer blamed for Russian rocket crash (R 21 18, S 26 2:)

h Boeing space station tanks accidentally taken to Huntsville dump (R 20 83)

Vh Space Station endangered by NASA flight controllers’ blunder in maneuvering around space junk; predicted distance also way off (R 20 46-47)

SH Space Station Problem Reporting Database hacked (R 20 47-48)

$Vmf Space Station risks (R 21 14, S 26 2:)

V$ehf Canaveral Rocket lost; wrong key hit in loading guidance SW (S 16 4)

df NASA finds problems in EOSDIS Earth Observing System (EOS) spacecraft flight operations software development, expected to delay launch (R 19 67)

m+ Apollo 11 lunar module, pen used to replace circuit breaker (S 18 3:A14)

Vr* Lightning hits Apollo 12. "Major system upsets, minor damage". See article by Uman and Krider, Science 27 Oct 1989, pp. 457-464. (S 15 1)

V$m Lightning changed Atlas-Centaur program (51 sec). $160M lost (S 12 3, 15 1)

@V*$m Lightning hits launch pad, launches 3 missiles at Wallops Island (S 12 3)

V$f Mariner 1 Venus probe: HW fault plus programmer missed superscript bar in ‘R dot bar sub n’. See Paul Ceruzzi, Beyond the Limits – Flight Enters the Computer Age, Smithsonian, 1989, Appendix (S 14 5). (Earlier reports had suggested DO I=1.10 bug (see next item) or a garbled minus sign (or hyphen.) (S 8 5, 11 5, S 13 1)

$f Project Mercury had a FORTRAN syntax error such as DO I=1.10 (not 1,10). The comma/period interchange was detected in software used in earlier suborbital missions, and would have been more serious in subsequent orbital and moon flights. Noted by Fred Webb. (S 15 1)

*f Gemini V 100mi landing err, prog ignored orbital motion around sun (S 9 1)

V$f Atlas-Agena software missing hyphen; $18.5M rocket destroyed (S 10 5)

@VSH Lauffenberger convicted of logic bombing GD’s Atlas rocket DB (S 17 1)

Vm Navy Atlas rocket places satellite in worthless orbit (S 18 3:A14)

V$f Aries with $1.5M payload lost: wrong resistor in guidance system; (S 11 5)

V*f TDRS relay satellite locked on wrong target (S 10 3)

Vm AT&T Telstar 401 satellite failure (S 22 4:26, R 18 76)

Vm Ariane 5 test problems: motor failures, nitrogen leak (S 20 5:9, R 18 27,28)

V$f New Ariane 5 failure (S 21 5:15); More on Ariane 5: conversion from 64-bit floating to 16-bit signed caused Operand Error (R 18 27-29,45,47); Note: Matra made software for Ariane5 and Taipei subway system (S 21 5:15); Incidentally, Robert L. Baber, Univ. Witwatersrand, Johannesburg, suggests you browse http://www.cs.wits.ac.za/ bob/ariane5.htm – showing how a simple correctness proof could have avoided this problem. (R 18 89-91)

*Mm Cosmic rays hit TDRS, Challenger comm halved for 14hrs [8Oct1984](S 10 1)

$Mr Sunspot activity: 1979 Skylab satellite dragged out of orbit (S 13 4)

hM 1989 pulsar discovery now attributed to TV camera interference (S 16 3)

V$hfe Soviet Phobos I Mars probe lost (Sep 1988): faulty SW update (S 13 4); cost to USSR 300M rubles (Aviation Week, 13 Feb 89); disorientation broke radio link, discharged solar batteries before reacquisition. [*Science,* 16Sep1988] More on Phobos 1 and 2 computer failures (S 14 6)

V$? Soviets lose contact with Phobos II Mars probe. Automatic reorientation of antenna back toward earth failed. (S 14 2)

V$f 1971 Soviet Mars orbiter failed after "unforgivable" SW bug; new info (S 16 3)

f Assessment of predictions on the Russian Mars Probe crash site (S 22 2:22)

V$fm 1993 Mars Observer lost entering Mars orbit (S 18 4:11; R 14 87,89; 15 01); loss blamed on fuel line leak (Washington Post, 10 Jan 1994)

f What really happened on Mars Rover Pathfinder? David Wilner on VxWorks system resets and preemptive priority scheduling, and Glenn Reeves – first-hand commentary must be read (R 19 49,50,53,54) and further discussion of priority inversion (R 19 50,53,54,56)

V$fm Mars Climate Orbiter lost, dipped too close to Mars due to English/Metric confusion; Mars Polar Lander reprogrammed to report back directly on 3 Dec 1999 (R 20 59-62); Mars Lander then lost entirely on landing attempt, search abandoned after a month. Crash finally blamed on software shutting engines off prematurely (R 20 84,86)

$f/h? NASA HESSI shake test 10 times too strong, damaging spacecraft (S 25 3:15, R 20 86)

$f Sea Launch rocket drops satellite into Pacific Ocean (S 25 3:15, R 20 84,86); single line of code allowed launch with second-stage valve open, causing helium leak (R 20 97)

Vfm$ Electronics startup transient opened telescope cover prematurely, destroying

Wide Field Infrared Explorer (WIRE) spacecraft (R 20 47-48)

V$m $1.4B Galileo antenna jammed, en route to Jupiter (S 18 4:11)

V$m Landsat 6 vanishes; space junk tracked by mistake (S 19 1:10)

V$f Magellan space software problems: serious design flaw fixed (S 14 5) Nonatomic setting of scheduled and active flags interrupted. See H.S.F. Cooper, Jr., The Evening Star: Venus Observed, Farrar Straus Giroux, 1993. Discussion in J.M. Rushby, SRI-CSL-95-01.

$m Magellan spacecraft manual guidance overcomes faulty computer chip (S 15 2)

V*h Soyuz Spacecraft reentry failed, based on wrong descent program, (orbiting module had been jettisoned, precluding redocking) (S 13 4)

V$fe Viking had a misaligned antenna due to a faulty code patch (S 9 5)

*f Ozone hole over South Pole observed, rejected by SW for 8 years (S 11 5)

? Global-warming data confusion (R 19 91-92)

@Vfm Channel blocked, Discovery runs out of storage for ozone data (S 18 3:A14)

* Continuing trend toward expert systems in NASA (S 14 2)

f SW bug on TOPEX/Poseidon spacecraft "roll momentum wheel saturated" alarm aborted maneuver. It was recoverable, however. (S 18 1:24)

Defense

V!hhh U.S. F-15s take out U.S. Black Hawks over Iraq in Friendly Fire; 26 killed, attributed to coincidence of many human errors. (Other cases of friendly fire included 24% of those killed in the Gulf War.) (S 19 3:4) According to a seemingly reliable private correspondent who has read through at least 62 volumes of investigation reports, the public was seriously misled on this situation and there was a considerable cover-up. For now, contact me if you want further background.

!!$rhi Iran Air 655 Airbus shot down by USS Vincennes' missiles (290 dead); Human error plus confusing and incomplete Aegis interface (S 13 4); Commentary on Tom Wicker article on Vincennes and SDI (S 13 4); Aegis user interface changes recommended; altitude, IFF problems (S 14 1); Analysis implicates Aegis displays and crew (Aerospace America, Apr 1989); Discussion of further intrinsic limitations (Matt Jaffe, S 14 5, R 8 74); USS Sides Cmdr David Carlson questions attack on Iranian jet (S 14 6)

!!$rfe Iraqi Scud hit Dhahran barracks (28 dead, 98 wounded); not detected by Patriot defenses; clock drifted .36 sec. in 4-day continuous siege, due to SW flaw, preventing real-time tracking. Spec called for aircraft speeds, not mach 6, only 14-hour continuous performance, not 100. Patched SW arrived via air 1 day later (S 16 3; AWST 10Jun91 p.25-26); Shutdown and reboot might have averted Scud disaster (S 16 4) Patriot missiles misled by 'accidental' decoys; T.A. Postol report (S 17 2); summary of clock drift, etc. GAO/IMTEC-92-26, February 1992 (S 17 2); reprisals against Postol for his whistleblowing (R 13 32, S 17 2); Army downgrades success to about 10% rather than 80% (R 13 37, S 17 2, 17 3) GAO report documents clock problem in detail (S 17 3) 24-bit and 48-bit representations of .1 used interchangeably (S 18 1:25)

*f Patriot system fails again (S 25 3:18, R 20 85)

*f Software snafu slowed critical data during Iraq raid (S 24 3:25, R 20 23)

!!V$h? Sheffield sunk during Falklands war, 20 killed. Call to London hindered antimissile defenses on same frequency? [AP 16May1986](R 2 53, S 11 3) An "official" version disputes this conclusion – see "The Royal Navy and the Falkland Islands" by David Brown, written at the request of the Royal Navy. Page 159 of that report discusses another problem with the Sea Wolf system, occurring several days later.

!V$ British Falklands helicopter downed by British missile. 4 dead (S 12 1)

!!V$f USS Liberty: 3 independent warning messages to withdraw were all lost; 34 killed, more wounded. Intelligence implications as well. (S 11 5)

!Vhfi? Stark unpreparedness against Iraqi Exocets blamed on officers, not technology, but technology was too dangerous to use automatically (S 12 3); Captain blamed deficient radar equipment; official report says radar detected missiles, misidentified them. (S 13 1)

Vrf$ USS Yorktown Aegis missile cruiser dead in water for 2.75 hours after unchecked divide by zero in application on Windows NT Smart Ship technology (S 24 1:31, R 19 88-94); letter to *Scientific American*: it was an explicit decision to "stimulate" [sic] machinery casualties? (S 24 4:26, R 20 37)

$hfe Navy software problems in upgrading software on battle cruisers USS Hue City and USS Vicksburg (S 23 5:25, R 19 86-87)

*Vf 5th Bell V22 Osprey crash: assembly error reversed polarity in gyro (S 16 4); Bell V-22 Osprey - correct sensor outvoted (S 17 1)

!V$(f?m?h?) Another Osprey crash (R 21 14, S 26 2:)

*H Fraudulent test SW in Phalanx anti-missile system, Standard missile (S 13 4)

Hhf West German flies Helsinki-Moscow through Soviet Air Defense (S 12 3)

Hhf Soviet Air Defense penetrated again by amateur pilot (S 15 5)

$h Russian missile-site power outage due to unpaid utility bill? (S 20 1:17)

**f Returning space junk detected as missiles. Daniel Ford, The Button, p.85

** WWMCCS false alarms triggered scrams 3-6 Jun 1980 (S 5 3, Ford pp 78-84)

** DSP East satellite sensors overloaded by Siberian gas-field fire (Daniel Ford p 62); Ford summarized (S 10 3)

**f BMEWS at Thule detected rising moon as incoming missiles [5Oct1960] (S 8 3). See E.C. Berkeley, The Computer Revolution, pp. 175-177, 1962.

** SAC/NORAD: 50 false alerts in 1979 (S 5 3), incl. a simulated attack whose outputs accidentally triggered a live scramble [9Nov1979] (S 5 3)

*** Serious false 2200-missile-alert incident 3 Jun 1980 described by Stansfield Turner, mentioning thousands of other false alarms (S 23 1:12, R 19 43)

*fmh Russian early-warning system close to retaliatory strike: Norwegian weather rocket mistaken for American Trident (R 19 85)

m Report from Kommersant Vlast on Serbukov-15 base false detection of ICBMs en route to Moscow on 25 Sep 1983; human intervention stopped retaliation; system allegedly misbehaved due to radiation (R 19 97)

*$VfM Libyan bomb raid accidental damage by "smart bomb" (S 11 3) F-111 downed by defense-jamming electromagnetic interference (S 14 2) More on U.S. radio self-interference in 1986 Libyan attack (S 15 3)

* Iraq using British Stonefish smart mines, with "sensitive" SW (S 15 5)

*SP Britain bugged radio equipment sold to Iraq (S 16 4)

*SP Trojan horse implants in DoD weapons (S 16 4)

*SP Trojan horse inserted in locally netted printer sold to Iraq? (S 17 2)

*Vm Arabian heat causing problems with US weapons computers (S 15 5)

*V$m Lightning hits launch pad, launches 3 missiles at Wallops Island (S 12 3)

* Frigate George Philip fired missile in opposite direction (S 8 5)

*h? Unarmed Soviet missile crashed in Finland. Wrong flight path? (S 10 2)

*Vf 1st Tomahawk cruise missile failure: program erased [8Dec1986] (S 11 2)

*Vm 2nd Tomahawk failure; bit dropped by HW triggered abort (S 11 5, 12 1)

f/m? CALCM cruise missile software bugs revisited (S 22 2:22)

hi Accidental launch of live Canadian Navy missile: color-code mixup (S 22 1:18)

*$rf Program, model flaws implicated in Trident 2 failures (S 14 6)

*VrmM RF interference caused Black Hawk helicopter hydraulic failure (S 13 1); More on Black Hawk EMP problems and claimed backwards pin (R 17 39,42)

*VSM RF interference forces RAF to abandon ILS in poor weather (R 21 17)

*f Sgt York (DIVAD) radar/anti-aircraft gun – software problems (S 11 5)

$f Software flaw in submarine-launched ballistic missile system (S 10 5)

V$f AEGIS failures on 6 of 17 targets attributed to software (S 11 5)

Vf WWMCCS computers' comm reboot failed by blocked multiple logins (S 11 5)

$ WWMCCS modernization difficulties (S 15 1)

*$f Gulf War DSN 20-30% call completion persists 3 mos. until SW patch (S 17 4)

$f Armored Combat Earthmover 18,000 hr tests missed serious problems (S 11 5)

$rfi Stinger missile too heavy to carry, noxious to user (S 11 5)

**V$$Sr Strategic Defense Initiative – debate over feasibility (S 10 5); Pentagon says SDI complexity comparable to nuclear reactors (Newsweek, S 17 3) See *Way Out There in the Blue: Reagan, Star Wars, and the End of the Cold War,* Frances FitzGerald, Simon & Schuster, 2000 for a fine retrospective analysis.

$d SDI costs, budget issues, risks discussed (S 17 4)

$ StarWars satellite 2nd stage photo missed – unremoved lens cap (S 14 2)

f StarWars FireFly laser-radar accelerometer wired backwards (S 19 2:2)

$* 1.7M resistors recalled. Used in F-15, Patriot, radar, comm aircr. (S 16 3)

$hd DoD criticized for software development problems (S 13 1)

* US Navy radar jammers certified despite software errors, failed tests (S 17 3)

$ USAF software contractors score poorly on selections (S 14 1)

$d ADATS tank-based anti-copter missile system development problems, $5B overrun, unreliability, ... (S 16 1)

$d British air defense system ICCS SW causes ten-year delay (S 15 5)

*Sf US Army Maneuver Control System vulnerable to software sabotage (S 15 5)

$d US-supplied Saudi Peace Shield air defense software problems (S 15 5)

$d Serious software problems in UK Trident nuclear warhead control (S 15 5)

*m Russian nuclear warheads armed by computer malfunction (R 19 14)

*h Outdated codes made US missiles useless until annual inspection (S 14 5)

S Classified data in wrong systems at Rocky Flats nuclear weapons plant (S 16 4)

SPh Classified disks lost by Naval commanders on London train (R 17 54)

hi? Listing of US Navy safety problems in two-week period (S 15 1)

Vm Rain shuts down Army computers; lightning effects and prevention (S 15 1)

* Role of e-mail, Internet, FAX in defeating 1991 Soviet coup attempt (S 16 4); (S) power surges used to fry faxes and computers in countermeasure (S 16 4)

* Russian auto-response missile system still in place in Oct 1993 (S 19 1:10)

!! Analysis of U.S. peacetime submarine accidents http://freeweb.pdq.net/gstitz/Peace.htmhttp://freeweb.pdq.net/gstitz/Peace.htm

Military Aviation

!!V$f Handley Page Victor tailplane broke, crew lost. 3 independent test methods, 3 independent flaws, masking flutter problem (S 11 2-12, correction S 11 3)
!Vf Harrier ejection-seat parachute system accidentally deployed, blew through the canopy, but without ejecting the seat and pilot, who was killed (S 13 3)
f Harrier targets police radar gun; fortunately not armed! (S 21 4:14)
*V(h/m?) Japanese pilot accidentally ejected into the Pacific (S 19 4:12)
*V$h Sea Harrier 1 accidentally bombs its own carrier, Ark Royal (S 17 3) 5 injured. Auto aim-off SW blamed for the Ark Royal bombing (S 18 1:23)
*V$f SAAB JAS 39 Gripen crash caused by flight control software (S 14 2, 14 5)
*V$fmhi 2nd JAS 39 Gripen crash 8Aug1993 blamed on pilot/technology (S 18 4:11); interface difficulties, complicated analysis (S 19 1:12)
*V$rf Software problems in B-1B terrain-following radar, flight-control; electronic countermeasures (stealth) jam plane's own signals (S 12 2)
*V$h B-1B swept wing punctures gas tank on the ground; blamed on low lubricant; problem found in 70 of 80 B-1Bs inspected (S 14 2)! No computer sensors?
$fd Stealth development problems including SW miscalculation in wiring (S 15 1)
$f UHB demonstrator flight aborted by software error at 12,000 feet (S 12 3)
*V$fh F-22 prototype crash first blamed on computer SW, then on pilot (S 17 3)
*V$f F-18 crash due to missing exception cond. Pilot OK (S 6 2, more SEN 11 2)
*Vhi F-18 missile thrust while clamped, plane lost 20,000 feet (S 8 5)
*f F-16 simulation: plane flipped over whenever it crossed equator (S 5 2)
*f F-16 simulation: upside-down, deadlock over left vs. right roll (S 9 5)
$Vhi F-16 landing gear raised while plane on runway; bomb problems (S 11 5)
*Vfh Unstallable F-16 stalls; novice pilot found unprotected maneuver (S 14 2)
$d USAF ECM systems: software 2 years late for F-16 and F-111 (S 15 5)
*hif Accidental shootdown of one Japanese F-15 by another (R 17 65, R 18 18); controversy continues (R 18 41,57)
*V$f? F-14 off aircraft carrier into North Sea; due to software? (S 8 3)
*V$f F-14 lost to uncontrollable spin, traced to tactical software (S 9 5)
Vf YF-23 fly-by-wire prototype attempted tail corrections while taxiing. Same problem on first X-29. (AFTI/F-16 had weight-on-wheels switch.) (S 16 3)
AFTI/F-16 DFCS redundancy management: ref to J.Rushby SRI-CSL-91-3 (S 16 3)
+- Historical review of X-15 and BOMARC reliability experiences (S 17 3)
$ Systems late, over budget (what's new?); C-17/B-1/STC/NORAD/ASJP (S 15 1)
V*$fd C-17 SW/HW problems documented in GAO report; 19 on-board computers, 80 microprocessors, six programming languages; complexity misassessed GAO: "The C-17 is a good example of how *not* to approach software development when procuring a major weapons system." (S 17 3) Chairman John F. McDonnell's reply (S 17 4)
f C-130 testbed uncovers 25-yr-old divide-by-zero bug in X-31 SW (S 16 3)
*Vmf X-31 crash, 19 Jan 1995 (R 17 45,46,47,60,62; 60=Pete Mellor)
V(f?) Unplanned 360-degree roll of NASA's X-38 in test (R 21 10)
*VM US missile-warning radar triggers accidental explosions in friendly aircraft; radar must be turned off when planes land! (S 14 2)
* AF PAVE PAWS radar can trigger ejection seats, fire extinguishers (S 15 1)
!$h 1988 RAF Tornados collided, killing 4; flying on same cassette! (S 15 3)
V$ef DarkStar unmanned aerial vehicle (UAV) crash from software change, cost $39M (S 22 1:17-18)
mM? Air Force bombs Georgia – stray electromagnetic interference? (S 14 5)
*hme, etc. Navigation, GPS, and risks of flying (R 19 73,75,77); Implications of the U.S. Navy no longer teaching celestial navigation (R 19 75,77-79,81-82)

Commercial Aviation

..... Commercial flight incidents
!!$V(hi?) Korean Airlines KAL 007 shot down killing 269 [1Sept1983]; autopilot on HDG 246 rather than INERTIAL NAV? (NYReview 25 Apr 85; SEN 9 1, 10 3, 12 1) or espionage mission? (R.W. Johnson, "Shootdown") Further information from Soviets, residual questions (S 16 3); Zuyev reports Arctic gales had knocked out key Soviet radars; Oberg believed Sakhalin air defense forces were "trigger-happy" following earlier US Navy aircraft overflight incursions [Reuters 2Jan1993]; Analysis of recent articles on KAL 007 (Ladkin, R 18 44)
!!Vfe Korean Airlines KAL 901 accident in Guam, killing 225 of 254; worldwide b