

ACT
EUROPE

Ada Core
Technologies, Inc.

The Blue Screen of Death

atures

AC965 On to gate 28
ME202 On to gate 2
AC947 On to gate 28
AG980 On to gate 7

AC967 On to gate 18

L5002 On to L-Range
AL111 On to L-Range
B1098 On to open gate 9

AC977 On to L-Range

ere baggage unattended 11

A fatal exception 80 has occurred at 0040100000 in VED 00000000. The current application will be terminated.

- Press any key to continue the current application.
- Press any key to restart your computer. You will have your command window in all applications.

Press any key to continue

http://libre.act-europe.fr

© ACT Europe under the GNU Free Documentation License



Software Dependability


- **Dependability ≠ usability**
 - A word processor, for example, must be usable, not necessarily dependable!

Dimensions of Dependability

- Availability**
Ability of the system to deliver service when requested
- Reliability**
Ability of the system to deliver correct results
- Safety**
Ability of the system to operate w/o catastrophic failure
- Security**
Ability of the system to protect itself against intrusions

Measurement methods:


- Measured with defect rates** (Availability, Reliability)
- Expressed in terms of integrity levels** (Safety, Security)



Warning about Defect Rates

Is a defect rate of 0.1% acceptable? It depends...

- **1 document/year lost while word-processing**
 - Great ☺
- **2 accidents/month at the International Airport in London**
 - ☹ ☹
- **22,000 checks/hour drawn from the wrong account in the US**
 - ☹ ☹ ☹



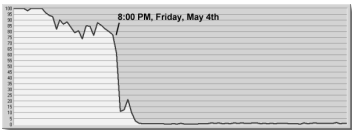
Software defect rates must be analyzed in the context of the application domain

<http://libre-act-europe.fr>

© ACT Europe under the GNU Free Documentation License

Software Failures: Availability

- **Denial-of-service attacks**
 - Example: attack against GRC.com
 - Attacked by 195 Windows 2000 servers running insecure versions of Microsoft's IIS web server. IIS was the apparent point of hacker entry into the system



The graph displays a line plot on a grid. The vertical axis (y-axis) is labeled from 1 to 100 in increments of 5. The horizontal axis (x-axis) represents time. A specific point on the x-axis is marked with a vertical line and labeled "8:00 PM, Friday, May 4th". Before this point, the line fluctuates between approximately 70 and 90. At 8:00 PM, the line drops sharply to a level near 10 and remains relatively flat with minor fluctuations thereafter.

<http://libre.act-europe.fr>

©ACT Europe under the GMI License Documentation License

11

Software Failures: Reliability

- **January 15, 1990: 9 hour nation-wide telecom shutdown**
 - 1 month earlier ATT updated its software in 114 switching stations
 - Cause: 1 misplaced "break" statement in a C program
- **January 2001: 230,000 units new Internet-enabled mobile phone recalled**
 - Users reported that their phones were freezing after accessing certain Web sites, and when they were powered back on, all stored information (addresses, e-mails, bookmarks, memos) had been lost
- **Matracom 6500 PABX (telephone switch)**
 - Random phone messages are garbled
 - Long phone calls are cut
- **Windows 95/98/ME/2000**
 - February 1997: propulsion system of the USS Yorktown ship failed
 - Cause: Windows NT 4.0 crashed
 - Personal experience: Installed an HP scanner on a SONY VAIQ with Windows 2000. Now I cannot enter suspend mode and when I try the screen disappears until powered-off (with loss of work ☹)


<http://libre.cit-europe.fr> ©ACT Europe under the GNU Free Documentation License.



Software Failures: Safety

- **1986: Therac 25 radiation machine kills patients**
 - Cause: poor testing of the software
- **June 4, 1996: maiden flight of Ariane 5 failed: rocket destroyed**
 - Cause: Code from Ariane 4 guidance system reused in Ariane 5 but not tested
- **2000: Deadly accident in French highway**
 - Cause: Software malfunction in car braking system. Car manufacturer acknowledges responsibility


<http://libre.act-europe.fr> © ACT Europe under the GNU Free Documentation License 13



Software Failures: Security

- **November 2, 1988 Internet Worm**
 - A self-replicating program was released upon the Internet
 - This program (a worm) invaded VAX and Sun computers running versions of Berkeley UNIX, and used their resources to attack still more computers.
 - Within hours this program had spread across the U.S., infecting thousands of computers and making many of them unusable due to the burden of its activity.
 - Cause: undetected buffer overflow in C routine `gets()`
- **Many more interesting virus stories (especially on Windows ...)**

<http://libre.act-europe.fr> © ACT Europe under the GNU Free Documentation License 14



1 in 3 Software Projects Doesn't Even Get There!

- **US Internal Revenue Service Modernization**
 - \$4 Billion, dropped in early 1997
- **FBI Fingerprint system**
 - \$500 million, dropped
- **Bell Atlantic 411**
 - November 1996, outage, backed out of upgrade

<http://libre.act-europe.fr> © ACT Europe under the GNU Free Documentation License 15