Ariane 5 (1996 explosion)

Presenter: Arash Kamyab

Outline

- Introduction
- Technical Issues
- Summary of events
- Stake-holders
- Ethical Issues
- Social Ramification of Disaster
- Comparing with other Engineering disciplines
- Conclusion

Introduction

- An American and Russian dominated industry
- Boosting the technical advancements
- U.S Space industry worth $60 billion in year 1999
- Handful of nations can afford such an industry
- European Effort : Formation of European Space Agency (ESA)
- ESA is the proud maker of the Ariane Rocket series

Technical Background of faulty component

- Ariane 5's Purpose: delivering satellite to space
- Improved version of Ariane 4
- Control system of Ariane 5 composed of:
  - An inertial reference system (SRI)
  - An On-Board Computer (OBC)
- SRI of Ariane 5 same as one in Ariane 4

Summary of Events

- Morning of June 4th 1996
- Rocket exploded around 40 seconds after lift-off
- Inquiry board set to discuss the failure
- Failure due to SRI software exception
- Exception caused due to a data conversion
- SRI failed about 31 seconds after lift-off (Same SRI worked perfectly in Ariane 4)

Consequences

- ESA spent $8 billion developing this rocket
- They flaunted Ariane 5 as a new era in Satellite delivery technology
- ESA's reputation was jeopardized
- Loss of market share and revenue
- ESA lost the European faith in the program
- Nobody was found liable for the damage
- European public left with no one to blame but faulty software

Causes of failure identified

- “Complete loss of guidance and altitude information (30 seconds after lift-off)” [2]
- “This loss of information was due to specification and design errors (in SRI software)” [2]
- Adequate analysis and testing could have detected the potential failure [2]
- Causes of failure were direct result of faulty design, review and testing

Stake-holders

- European space Agency (ESA)
- Centre National d'Etudes Spatiales (CNES)
- Governments funding the project
- 53 European shareholders
- European taxpayers
- Designers

Stake-holders

- Requirements engineers
- Test Engineers
- Project managers
- Reviewers
- The software engineering profession

Ethical Issues

- Some ethical standards engineer should obey by:
  - Engineers shall expose risks openly to supervisors
  - Engineers shall participate in a lifelong learning process regarding the practice of their profession
  - Engineers shall ensure that their products meet the highest professional standards possible.

Were engineers at fault?

- Were there engineering methods developed at the time that could have been used in order to prevent the disaster?
- The answer is yes, yes and for a long time
- Many areas of software development were lacking in the development of SRI software
  - Design
  - Documentation
  - Testing
  - Review

- Individuals involved in developing the SRI did break the code of ethics by engaging in erroneous software engineering practice
- Is software really needed?
  - Easier to maintain
  - Generally cheaper
  - Remote accessibility
  - Software does not wear

Was ESA at fault?

- ESA could have pursued the guilty parties and consequently punish them (More ethical approach)
- This would have caused
  - Loss of client
  - Waning of public trust in the program
  - Costly for ESA (but only in the short run)

- Why is it less costly in the long run?
  - The software error could be prevented if the faulty members were persecuted
- Why is it more ethical?
  - Not pursuing the guilty parties was a set back for the software industry as a whole
  - Could have been a warning: You can be held liable for the software you create

Social ramification of disaster

- Negative social implications:
  - No particular individual or group of individuals were identified as the cause of failure
  - Software can not be error free!?
- Software engineering would have to adapt to society's need for error free products, like other engineering disciplines have done before it

Comparing with conventional engineering disciplines

- Like other disciplines Software engineering has its disposal methods for proper creation of software
- The designers of Ariane 5 did not use that knowledge
- Engineers would have been held responsible if the error was made in electrical or mechanical sections
- Engineers in other disciplines had the power to inform different organizations of faulty engineering practices at ESA

Conclusion

- Engineers at ESA did break the following ethical engineering codes:
  - Did not expose risks associated with not fully testing and reviewing the software
  - Did not keep up with advancements in their field
  - Did not insure that the product was of the highest quality possible
- ESA broke the code of ethics by not holding anybody responsible

Conclusion

- The Ariane 5 disaster was a wake up call for the software engineering community
- Proper actions should be taken to ensure such a failure does not occur again
- True software engineers will carry the torch into an era where software will be error free

Questions and Comments

Referances

[1] NSPA publication No. 1102 as revised January 1987

[2] ARIANE 5 Flight 501 Failure, Reported by the Inquiry Board

http://www.esrin.esa.it/htdocs/tidc/Press/Press96/ariane5rep.html, Paris, 1996 July 19.

[3] D. G. Johnson, *Ethical Issues in Engineering,* Prentice Hall, New Jersey, 1991.

[4] http://www.esa.int/export/esaCP/GGGZM2D3KCC_index_0.html, European Space Agency.

[5] D. L. Parnas, J. van Schouwen, P. S. Kwan Shu, *Evaluation of Safety-Critical Software*, Communications of the ACM, 1990.

[6] Design by Contract: The Lessons of Ariane, J Jezequel, Jan 1997 IEEE.

[7] [13] www.cnn.com/WORLD/9606/o4/rocket.explode/, CNN.

[8] Dr. R. Baber, *The Ariane 5 Explosion as seen by a software engineer,* Johannesburg, 1997. http://www.cas.mcmaster.ca/~baber/TechnicalReports/Ariane5/Ariane5.htm

[9] http://nssdc.gsfcnasa.gov/planetary/lunar/lunartimeline.html, NASA (Lunar Exploration Timeline).