Case Studies:

Allpool on toodud näited võimalikest tehnoloogiatest, süsteemidest ja õnnetustest/intsidentidest, mida võiks Case Study's käsitleda. Osade teemade kohta olen välja toonud ka mõned viited, kust **alustada**. Kuid kindlasti otsige **täiendavat informatsiooni** (Google on siinkohal suurimaks abiks). **Miinimumnõue on vähemalt viie** (interneti lehekülgede korral) **või kolme** (teaduslike artiklite korral) **erineva allika kasutamine!**

Täiendavad allikad, kust otsida informatsiooni (teaduslikke artikleid):

- Citeseer: http://citeseer.ist.psu.edu/
- ACM Digital Library: http://portal.acm.org/dl.cfm
- IEEEXplore: http://ieeexplore.ieee.org/ (kõik konverentsid ja ajakirjad, mille nimes IEEE)
- SpringerLink: http://www.springerlink.de/

Viimased kolm andmebaasi (ACM, IEEE ja Springer) on kättesaadavad vaid TTÜ võrgust. Väljastpoolt TTÜ võrku saab neid kasutada läbi TTÜ portaali: https://portal.ttu.ee/

Lisaks:

- Accident Databases: http://www.ntnu.no/ross/info/data.php#Accident
- Safety Critical Systems Virtual Library: http://www.afm.sbu.ac.uk/safety
- ACM Risks Forum: http://www.csl.sri.com/risks.html

NB! Enne konkreetsel teemal kirjutama hakkamist saatke teema mulle kooskõlastamiseks: gerje@pld.ttu.ee. Igale teemale vaid üks autor!

Parimad tööd saavad võimaluse ilmuda ajakirjas A&A (http://www.ttu.ee/aa/). Ajakirja **ei kvalifitseeru** alljärgnevad teemad (kuna ilmusid eelmisel aastal): Therac-25, CAN - Controller Area Network, Triple-Triple Redundant 777 Primary Flight Computer, Sõltumatute ketaste liiasmassiiv (RAID), Londoni kiirabi automaatse edastussüsteemi läbikukkumine 1992. aastal.

Näiteid tehnoloogiatest, mille kohta võiks teha kirjanduse ülevaate:

- Vigade avastamise tehnikad:
  - Signatures
    - Nahmsuk Oh, P. P. Shirvani, and E. J. McCluskey, "Control-Flow Checking by Software Signatures", IEEE Trans. on Reliability, 51(2), 111-122, 2002.
    - Jien-Chung Lo et al., "An SFS Berger Check Prediction ALU and Its Application to Self-Checking Processor Designs", IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, 11(4), 525-540, 1992.
  - Watchdogs
    - A. Benso et al., "A Watchdog Processor to Detect Data and Control Flow Errors", Proc. 9th IEEE On-Line Testing Symp., 144 - 148, 2003.
    - G. Miremadi and J. Torin, "Evaluating Processor-Behaviour and Three Error-Detection Mechanisms Using Physical Fault-Injection", IEEE Trans. on Reliability, 44(3), 441-454, 1995.

    - Assertions
        - O. Goloubeva et al., “Soft-error Detection Using Control Flow Assertions”, Proc. 18th IEEE Intl. Symp. on Defect and Fault Tolerance in VLSI Systems, 581-588, 2003.
        - P. Peti, R. Obermaisser, and H. Kopetz, “Out-of-Norm Assertions”, Proc. 11th IEEE Real-Time and Embedded Technology and Applications Symp., 209-223, 2005.
    - Duplication
        - Nahmsuk Oh, P. P. Shirvani, and E. J. McCluskey, “Error Detection by Duplicated Instructions in Super-Scalar Processors”, IEEE Trans. on Reliability, 51(1), 63-75, 2002.
        - Nahmsuk Oh and E. J. McCluskey, “Error Detection by Selective Procedure Call Duplication for Low Energy Consumption”, IEEE Trans. on Reliability, 51(4), 392-402, 2002.
        - M. A. Gomaa and T. N. Vijaykumar, “Opportunistic Transient-Fault Detection”, IEEE Micro, 26(1), 92-99, 2006.
    - Memory protection codes
        - L. Penzo, D. Sciuto, and C. Silvano, “Construction Techniques for Systematic SEC-DED Codes with Single Byte Error Detection and Partial Correction Capability for Computer Memory Systems”, IEEE Trans. on Information Theory, 41(2), 584-591, 1995.
        - P. P. Shirvani, N. R. Saxena, and E. J. McCluskey, “Software-Implemented EDAC Protection against SEUs”, IEEE Trans. on Reliability, 49(3), 273-284, 2000.
    - Current monitoring
        - Y. Tsiatouhas et al., “Concurrent Detection of Soft Errors Based on Current Monitoring”, Proc. Seventh Intl. On-Line Testing Workshop, 106-110, 2001.
- Veakindluse tehnikad
    - Re-execution
        - N. Kandasamy, J. P. Hayes, and B. T. Murray, “Transparent Recovery from Intermittent Faults in Time-Triggered Distributed Systems”, IEEE Trans. on Computers, 52(2), 113-125, 2003.
    - Rollback recovery
        - S. Punnekkat and A. Burns, “Analysis of Checkpointing for Schedulability of Real-Time Systems”, Proc. Fourth Intl. Workshop on Real-Time Computing Systems and Applications, 198-205, 1997.
        - Ying Zhang and K. Chakrabarty, “A Unified Approach for Fault Tolerance and Dynamic Power Management in Fixed-Priority Real-Time Embedded Systems”, IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, 25(1), 111-125, 2006.
    - Active and passive replication
        - Y. Xie et al., “Reliability-Aware Co-synthesis for Embedded Systems”, Proc. 15th IEEE Intl. Conf. on Application-Specific Systems, Architectures and Processors, 41-50, 2004.
        - KapDae Ahn, Jong Kim, and SungJe Hong, “Fault-Tolerant Real-Time Scheduling Using Passive Replicas”, Proc. Pacific Rim Intl. Symp. on Fault-Tolerant Systems, 98-103, 1997.
    - Transparency

- N. Kandasamy, J. P. Hayes, and B. T. Murray, “Transparent Recovery from Intermittent Faults in Time-Triggered Distributed Systems”, IEEE Trans. on Computers, 52(2), 113-125, 2003.

Näiteid süsteemidest/lahendustest, mida võiks analüüsida:

- MARS süsteem
  - H. Kopetz et al., “Distributed Fault-Tolerant Real-Time Systems: The MARS Approach”, IEEE Micro, 9(1), 25-40, 1989.
  - H. Kopetz et al., “Tolerating Transient Faults in MARS”, Proc. 20th Intl. Symp. on Fault-Tolerant Computing, 466-473, 1990.
- Time-Trigered Protokollid (TTP) või arhitektuurid
  - H. Kopetz and G. Grunsteidl, “TTP - A Time-Triggered Protocol for Fault-Tolerant Real-Time Systems”, Proc. 23rd Intl. Symp. on Fault-Tolerant Computing, 524-533, 1993.
  - H. Kopetz and G. Bauer, “The Time-Triggered Architecture”, Proc. of the IEEE, 91(1), 112-126, 2003.
- Triple-Triple Redundant 777 Primary Flight Computer
  - Triple-Triple Redundant 777 Primary Flight Computer, Y.C. Yeh, 1996 IEEE Aerospace Applications Conference, pg 293-307, 1996. http://www.cs.uidaho.edu/%7Ekrings/CS449/Papers/Yeh1996-777.pdf
  - Uzuncaova, E., Ayala, M. A., *" Boeing-777 Flight Control System: A Software Safety Analysis"*, Naval Postgraduate School, December 2001. http://www.geocities.com/euzuncaova/docs/Analysis_of_Boeing777_FCS_Report.pdf

- Redundancy Management Technique for Space Shuttle Computers
  - Redundancy Management Technique for Space Shuttle Computers, by Sklaroff, J., R., IBM Journal on Research and Development, Vol. 20, No. 1, pp. 20-28, January 1976. http://www.cs.uidaho.edu/%7Ekrings/CS449/Papers/Sklaroff1976-SpaceShuttle.pdf
  - Space Shuttle Computers and Avionics: http://klabs.org/DEI/Processor/shuttle/
  - U.S. Space Shuttle/Modular Redundancy: http://www.plotnick.com/wtchow/papers/Shuttle/

- Redundant Arrays of Inexpensive Disks (RAID)
  - A Case for Redundant Arrays of Inexpensive Disks (RAID), by D.A. Patterson (Google)
  - RAID: High-Performance, Reliable Secondary Storage, Peter M. Chen, Edward Lee, Garth Gibson, Randy Katz, and David Patterson, ACM Computing Surveys, 1994. (CiteSeer)

- CAN (Controller Area Network) protocol
  - Bosch. CAN overview (incl. literature and links): http://www.can.bosch.com/
  - http://www.algonet.se/~staffann/developer/CAN.htm
  - Schill, Overview of the CAN Protocol, *Embedded Systems Programming*, September 1997.

    - Fredriksson, "CAN for critical embedded automotive networks," *IEEE Micro*, July 2002.
    - Ferreira, J.; Pedreiras, P.; Almeida, L.; Fonseca, J.A., "The FTT-CAN protocol for flexibility in safety-critical systems," *IEEE Micro*, July 2002.

- Airbus fly-by-wire süsteemid
    - Pascal Traverse, Dependability of Digital Computers on Board Airplanes, Dependable Computing for Critical Applications, Volume 4, A. Avizienis, J.C. Laprie, editors, 1991, pp. 134 – 152.
    - Dominique Briere and Pascal Traverse, AIRBUS A320/A330/A340 Electrical Flight Controls: A Family of Fault-Tolerant Systems, Digest of Papers FTCS-23: The Twenty-Third International Symposium on Fault-Tolerant Computing, June 1993, pp. 616 - 623.
    - Pascal Traverse, Isabelle Lacaze, Jean Souyris: Airbus fly-by-wire - A total approach to dependability. IFIP Congress Topical Sessions 2004: 191-212
    - Pascal Traverse, Isabelle Lacaze, Jean Souyris: A Process Toward Total Dependability - Airbus Fly-by-Wire Paradigm. EDCC 2005: 1

- ...

Näiteid õnnetustest/intsidendidest/probleemidest, mida analüüsida:

- F/A-22 Raptor Software
    - http://en.wikipedia.org/wiki/F/A-22_Raptor
    - http://www.pogo.org/p/defense/do-040301-fa22.html
    - F/A-22 Raptor Software Soars In Hard Tests: http://swig.stanford.edu/~candea/teaching/cs444a-fall-2003/readings/loeb-raptor.html

- Ariane V
    - Ariane 5 Failure Resources: http://www.niwotridge.com/Resources/DomainLinks/Ariane5Failure.htm
    - Failure Report: http://klabs.org/reports.htm#Ariane
    - Annotated Report: http://www.cafm.sbu.ac.uk/cs/people/jpb/teaching/ethics/ariane5anot.html
    - Additional Analysis by Eiffel Software: http://archive.eiffel.com/doc/manuals/technology/contract/ariane/page.html

- Erinevad NASA probleemid (Väga palju erinevaid teemasid: Patriot, Marsi süsteemid, etc. Kuid valige selline, kus põhiline probleem oleks seotud arvutite, elektroonika vms.)
    - http://klabs.org/reports.htm#failure_reports
    - http://mars.jpl.nasa.gov/msp98/lander/
    - http://mars.jpl.nasa.gov/msp98/orbiter/

- Therac 25
    - Loendamatu arv ressursse. Kasuta Google'it. Üht-teist on ka aine koduleheküljel.

- Londoni kiirabisüsteemi uuendamise läbikukkumine:
  - http://www.lond.ambulance.freeuk.com/cad.html
  - http://www.comp.lancs.ac.uk/computing/resources/IanS/SE7/CaseStudies/LondonAmbulance/index.html
  - http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html

- Cambridge'i ülikooli raamatupidamissüsteem CAPSA
  - http://news.bbc.co.uk/1/hi/education/1634558.stm
  - http://www.admin.cam.ac.uk/reporter/2001-02/weekly/5861/

- BMW 745i software defect
  - http://www.cs.unc.edu/%7Edorianm/academics/comp290test/bmw745bug.html

- eBay 21 tunnine seisak (1999)
  - http://internetweek.cmp.com/lead/lead061799.htm
  - http://www.salon.com/tech/log/1999/06/11/ebay/index.html

- Denver baggage handling system
- USS Yorktown (1998)
- London Stock Exchange's Taurus süsteemi läbikukkumine (1993)
- ...