Professional Development Topic 4: Dependence and Change

Prof Nick Taylor
Department of Computer Science
Heriot-Watt University

Content

- Technology and Society
  - Bi-directional influences
- Computer-related Risks
  - Safety Critical Systems
  - Millennium Bug

Technology & Society

- There are two cause-effect relationships to be aware of –
  - Technological developments affect society at large, *directly and indirectly* –
    - Work
    - Recreation
    - Domestic Life
    - Welfare Services
    - Law Enforcement
  - Outside factors affect the *direction and speed of technological developments* –
    - Commercial
    - Political
    - Cultural
    - Economic

Technology => Society

The Motor Car

- Facilitates personal travel over greater distances
  - More places and people visited
  - Domiciles further away from work
  - Re-location around the country more acceptable - movement of workforce
- Saves time
  - More efficient use of work time
  - More leisure time
- Pollution
- Safety

Technology => Society

The Telephone

- Instant communication over any distance
  - Became essential for any workplace
  - Facilitated communication with friends and relatives
- Replacing the letter
- Fax
- Computer networking
- E-mail replacing the telephone?

Technology => Society

The Television

- Entertainment
  - Perhaps THE most popular form of entertainment
- Up to the minute news
  - Live coverage of major events
- Viewers exposed to variety of
  - Cultures
  - Arts
  - Sports
  - Science
  - Views

Technology => Society

Computer Technology

- Two key elements -
  - *Information*
    - Storage
    - Processing
    - Communication
  - *Control*
    - Reliable
    - Repeatable
    - Adaptive

Technology => Society

Information

- Became essential in any workplace
- New forms of entertainment
- Reduced need to physically go to places
  - Shopping from home, home banking, etc.
  - For how much longer will we have to visit our GPs with minor ailments?
- Criminal records, etc.

Technology => Society

Control

- Automated manufacturing
- Washing machines and other timesaving devices
- Toys, MP3 players, Mobile phones
- Life-saving machines in hospitals
- Speed cameras, etc.

Society => Technology

Commercial Interests

- **Gas Refrigerator**
  - Hardly any mechanical parts
  - Silent
  - Gas was more prevalent (it had been around longer)
  - Supported by (in USA)
    - Servel
    - SORCO

LOST

- **Electric Refrigerator**
  - A compressor and a motor
  - Very noisy initially (and still hums!)
  - Electric services were limited
  - Supported by (in USA)
    - General Electric
    - General Motors
    - Westinghouse

WON

Society => Technology

Political Desires

Record/Playback Machine Tools

- Relatively cheap
- Skilled metal-worker needed
- Support bought out

LOST

Numerically Controlled Machine Tools

- Very expensive
- Skilled metal-worker not expected to be needed (McCarthyite concerns about reliability of union labour)
- Supported by USAF (who actually paid for installation of machines in subcontractors factories)

WON

Society => Technology

Cultural Attitudes

- The AR-15 and M-16 Rifles
  - AR-15 was
    - most reliable
    - lethal

    infantry rifle ever invented
  - M-16 was
    - developed from AR-15
    - useless!
- US Army ordnance bureaucracy made three modifications to the AR-15 (conservatism) –
  - Added manual bolt closure
    - Unnecessary extra weight
  - Increased twist of barrel
    - Greater accuracy but less lethal
  - Changed the gunpowder
    - 1000 rounds/minute and it jammed

Society => Technology

Economic Factors

- Spending power can drive technology in particular directions
- Military spending has been very influential in the way computer technology has developed
- Manufacturing/Commercial needs also direct the form of computer development
- Medical developments invariably follow behind rather than leading technology

Society => Technology

Computer Industry

- Intel and Motorola
  - Intel 8086 versus Motorola 68000
- IBM and Apple
  - IBM PC versus Apple Macintosh
- Microsoft
  - MS Office versus Lotus 1-2-3
  - MS Windows versus Apple Mac OS
  - MS Windows versus GNU/Linux
  - MS Internet Explorer versus Netscape
  - MS .NET versus Sun Java Enterprise
- Proprietary versus Free Software
- Client/Server versus Peer-to-Peer

Society => Technology

High Definition Optical Disc War

- HD-DVD versus Blu-Ray Disc
  - Blue laser based storage
  - Same compression schemes
  - Players will be backwards compatible
- HD-DVD
  - Can use current DVD manufacturing process
  - Capacity 15GB or 30GB on dual layer
  - Supported by
    - DVD Forum, Toshiba, NEC
    - Paramount, Universal, Warner
- Blu-Ray Disc
  - Needs expensive new manufacturing process
  - Capacity 25GB or 50GB on dual layer
  - Supported by
    - Blu-Ray Disc Association which includes everybody except Toshiba & NEC
    - Disney, Sony Playstation

Society => Technology

Afterword

- In January 2008 Warner Bros decided to cease releasing films on HD-DVD
- In February 2008 Toshiba abandoned production of HD-DVD equipment
- Victory for Blu-Ray Disc ?
- Meanwhile …
- Holographic Versatile Disc
  - Just launched
  - Capacity 200GB!

Computer-related Risks

- Safety Critical Systems
  - Hazard analysis
  - Notorious failures
- Dependence
  - Black Monday
    - 19th October 1987 automated share selling on Wall Street led to a stock market crash there and here
  - Y2K
    - 1st January 2000 was a problem date with enormous potential for widespread havoc (2038!)
- Privacy
  - Surveillance
    - ePOS, CCTV, mobile phones
  - Databases
    - Data, data, data, …
  - Social Networking
    - Privacy policies?

Safety Critical Systems

- Hazard analysis
  - Hazard severity
  - Hazard likelihood
  - Risk analysis
- Notorious failures
  - Therac-25
  - Ariane 5
  - Chinook Mk 2

Hazard analysis

- Hazard identification
- Hazard classification
  - Severity
    - US Department of Defense's 4 severities
    - Catastrophic, Critical, Marginal, Negligible
  - Likelihood
    - Levenson's 6 likelihoods
    - Frequent, Probable, Occasional, Remote, Improbable, Physically Impossible
- Hazard decomposition
  - To identify circumstances in which it might arise
- Risk analysis
  - To balance cost and delivery time against safety using severity and likelihood factors

Notorious failures

- Therac-25
- Ariane 5
- Chinook Mk 2

Therac-25

- The Therac-25 was a new version of a radiation therapy machine with more software control
  - Between June 1985 and January 1987 overdoses of radiation were given to six people
  - Three of them died
- Causes
  - Poor safety design - lack of safety interlocks
  - Software errors - insufficient testing and debugging
  - Inadequate reporting and investigation of accidents
  - Overconfidence

Ariane 5

- In June 1996, 40 seconds after initiation of its flight sequence, at an altitude of about 3700m, the Ariane 5 rocket veered off its flight path, broke up and exploded
- The cause was an internal variable related to the horizontal velocity exceeding the maximum value that a 16-bit integer could hold
- This software was, in fact, unnecessary for Ariane 5 but necessary in its predecessor, Ariane 4
- It had been retained in the inertial reference system of Ariane 5 for reasons of commonality

Chinook Mark 2

- In June 1994 a Chinook helicopter transporting 25 top Northern Ireland security experts crashed on the Mull of Kintyre killing all on board
  - For the next 15 years the Ministry of Defence (MoD) insisted that the pilots, Flt Lts Jonathan Tapper and Richard Cook, were responsible and guilty of gross negligence
- In 2009 an internal MoD document claiming serious concerns and warnings over the engine control computer system (FADEC) came to light
  - 21 Category 1 and 153 Category 2 anomalies had been revealed by the report
  - "The density of deficiencies is so high that the software is unintelligible… Pilot's control of the engine(s) through FADEC cannot be assured."
- The report had been written 9 months prior to the crash

Y2K - A Post Mortem

- What was/were the problem(s)?
  - 2 digit year format (00 and overflow)
  - Leap year (29.2.2000 & 366 days)
  - Sentinels (9.9.99 error condition)
- Why all the fuss?
  - Personal Computers, Embedded systems, Safety critical systems
  - Dependence and inter-dependence
- What were the fixes?
  - Date expansion, Windowing
- What were the consequences?
  - Cost of non-compliance, Cost of compliance
- What was learnt?

Y2K - The Problem(s)

- 2 digit year format
  - Time periods in excess of 99 years not computable
    - Not new - see PC “century byte”
  - Ambiguity of century
  - Incorrect sorting of dates by year
  - Year calculations not *modulo* 100
  - Year overflow on incrementing 99
- Leap year
  - 29.2.2000 not permitted
  - Days of week wrong after 29.2.2000
  - 2000 expected to have 365 days
- Sentinels
  - 9.9.99 used as error/test condition

Y2K - The Concerns

- Personal Computers
  - Century code hardwired to “19”
  - Roll-over in BIOS missing/broken
  - Date validation code broken
- Embedded systems
  - Field instrumentation & controllers
    - Sensors, transmitters, drives, valves
  - Process control systems
    - PLCs, custom chips, drivers
  - Plant management systems
- Safety critical systems
  - Safeguarding systems
- Dependence and inter-dependence
  - Business Continuity
    - Supply chains
  - Liabilities & compliance statements

Y2K - The Fixes

- Date expansion
  - Change to 4 digit years
    - Finding the dates
    - Package limitations (formats)
    - Interface limitations (EDI links)
    - Less efficient data entry
- Windowing
  - Choose a 2 digit year and assume all earlier 2 digit years are 21st century and all later ones are 20th
    - E.g. choose 50, then 49 means 2049 and 51 means 1951
  - Windows span only 100 years
  - Performance degradations
    - More processing required
  - Multiple windows
    - Systems with different chosen years

Y2K - Consequences of Non-Compliance

- Incidents during Y2K testing
  - Simulation of roll-over at International Federation of Airline Controllers sent all screens blank
  - 4 million gallons of raw sewage dumped onto a Los Angeles street
  - Robot assembly line crashed at GM factory and security system prevented staff from leaving
- Incidents after millennium
  - Nuclear plant failures in Japan, Spain, USA
  - Healthcare failures in Brazil, Norway, Sweden, UK
  - Power distribution failures in Honduras, South Korea

Y2K - Consequences of Compliance

- Cost of fixes (estimates)
  - Worldwide £300,000 million
    - **US** **£60,000 million**
      - Government £5,000 million
      - Command Centre £30 million
    - **UK** **£20,000 million**
      - Government £430 million
    - **Italy** **£500 million**
      - Billboards £1.5 million
- Side effects
  - Inventory management
    - Software - ROM, OS, Applications
    - Hardware - CPU, Cards, Networking
  - Legacy software
    - Skill shortages - COBOL, Packages
    - Long overdue revisions
  - Business environment awareness

Y2K - Learning Outcomes

- Computer professionals
  - Life expectancy of software
    - Considerably longer than realised
    - Need for skills thought to be outdated
  - Inventory management
    - Importance to enterprises
    - Need for methodologies and tools
- Computer users
  - IT dependence
    - Broader and deeper than realised
    - IT cannot be left solely to the boffins
    - Need to transfer much decision making from IT departments to Board level
  - Hostages to fortune
    - Need to be considerably more critical of and better informed about IT solutions and practices

Y2K - The Verdict

- Take your pick …
  - The fact that the Y2K problem arose demonstrates that the computer profession is immature and its practices are unsound
  - The computer profession's reaction to the Y2K problem was a double success story -

    i). Success in raising awareness of the problem and persuading enterprises to invest in fixing it

    ii). Success in fixing the problem
  - The computer profession refused to accept any liability for the problem, provoked widespread hysteria and then exploited the fear it had generated for financial gain

2038 - Unix

- What is the problem?
  - Unix and the C language use a 32 bit signed integer to hold the time/date
  - This variable counts seconds from 00:00:00 GMT on 01.01.1970
  - It will roll over to a negative number at 03:14:07 GMT on 19.01.2038
- Why so little fuss?
  - By 2038 it is expected that all versions of Unix will be using a 64 bit integer for the time/date
  - Unix could well be obsolete by 2038
  - The C language will probably be obsolete long before 2038
  - Libraries for the C language will have been updated to use a 64 bit variable by then anyway

2038 is a problem NOW

- Try writing and running a C program which counts through the critical time on a Unix operating system and see what happens
- Any software that needs to project into the future will hit the problem before 2038
  - What will your age be in 2039?
- Legacy software has a habit of hanging on, and on, and on ...
- Embedded systems could be using old versions of operating systems and software without anybody realising it