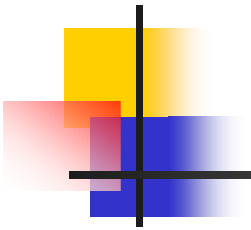
Bureaucracy, Safety and Software:
A potentially lethal cocktail

Les Hatton

CISM, Kingston University
L.Hatton@kingston.ac.uk

Version 1.1: 03/Feb/2010

Overview

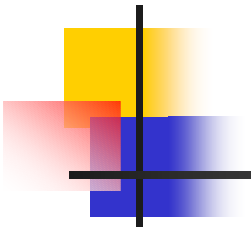


- The role of evidence
- The bureaucratic urge
- The impact on software systems

The evidence matrix

Level of evidence	Example area	Source of threat
Irrefutable	Engineering	Generally immune – hard to resist the laws of physics
Considerable	Medicine	Media, Political
None -> Little	Software systems	Media, Political, managerial/economic

Overview



- The role of evidence
- The bureaucratic urge
- The impact on software systems

The bureaucratic urge

- Blind tinkering and proliferation of documentation
- “Something must be done” – panic and proportion, sometimes with opposing evidence
- Risk assessment – a frightening new weapon in the battle against common sense

Blind tinkering

- Aug 2008: Maritime and Coastguard Agency discipline boat crew for saving teenage swimmer by using a recently repaired boat awaiting a seaworthiness certificate. (The MCA locked the boat away pending enquiries to avoid “any future moral dilemma”.)
- Nov 2008: Maritime and Coastguard Agency ban the use of flares in sea rescues because they could cause ‘considerable injury’. Rescue teams have been told to use ‘safer’ alternatives like torches. No incidents had been reported.

Proliferation of documentation

- Concerns in AA about the number of road signs, (up to 16 per junction).
- Need for dual Welsh / English signs in Wales doubling all signs
- ... leading to the following on a road entrance:

  “Nid wyf yn y swyddfa ar hyn o bryd. Anfonwch unrhyw waith i’w gyfielthu”
- Until it was politely pointed out that this says

  “I am not in the office at the moment. Send any work to be translated.”

Panic and proportion – failures of numeracy

- Battle of the River Plate
- Swine flu
- MMR and autism
- CRB and the Independent Safeguarding Authority

The Battle of the River Plate

- The earliest significant battle of World War II in December 1939. Very highly publicised, total casualties 109.

- Meanwhile at home, ‘experts’ from the Air Ministry had decided millions would die in air raids leading to a total black-out in hours of darkness. This caused 3,000 civilian deaths by accident in Sept – Nov 1939, more than armed forces fatalities in the same period.

Swine flu – millions will die

- Massive over-reaction, stoked by a rapacious media
- 10x diagnosis rate in the UK because of remote diagnosis – knee infections and in some cases meningitis were treated as swine flu.
- Significant side-effects from Tamiflu in children and ultimately the anti-flu vaccination in adults

MMR and autism

- Massive over-reaction based on a single highly flawed study, also stoked by a rapacious media
- Measles epidemic as a direct result
- Significant concerns about growth in Mumps outbreaks

CRB and the ISA, (Independent Safeguarding Authority)

- Even more massive over-reaction based on the Ian Huntley case
- Failure in police communication but politicians had to be soon to be doing something
- ISA includes whistle-blowing and intends to vet 12 million adults for paedophile behaviour
- False positive rate currently 3%. Backlog so large that blanket passes being given, (including to Ian Huntley)
- Experiments now show adults will not stop to help a child in distress

The wonderful world of Risk Assessment

If R is the Risk, F the Frequency and C the Consequence:

R = F x C

So unlikely catastrophic events have a similar risk to very frequent but unimportant events.

Mathematicians always seek to quantify risk.

Problems of measurement - A genius's view of risk

"The risk of the end of the universe is definitely less than 1 in 10^5."

Risk factor from the Large Hadron Collider, CERN.

"If a guy tells me that the probability of failure is 1 in 10^5, I know he's full of crap."

Richard P. Feynmann, Nobel Laureate commenting on the NASA Challenger disaster.

Detecting risk assessors in the wild

http://www.flickr.com/photos/fraserspeirs/4090224, student canteen at Brunel University

Doing risk assessments so you don't get asked again

- Step 1: Insist on using R = F x C in your assessment. This will panic Human Resources.

  (People go into Human Resources to avoid nasty things like multiplication.)

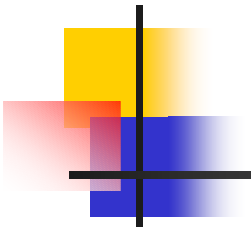
- Step 2: Put "end of universe" as risk number 1

  (Rationale: R = F x C. Since the end of the universe has an infinite consequence C, then no matter how small the frequency F, the Risk is also infinite)

- Step 3: Ignore all other risks as insignificant

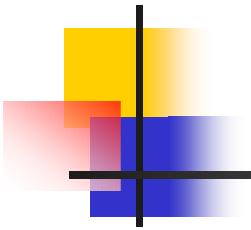
- Step 4: Wait for call from Human Resources

Overview



- The role of evidence
- The bureaucratic urge
- The impact on software systems

Proliferation of documentation



- Start (!) your safety library with MIL-STD-882C, MIL-STD-882B 300 Series Tasks, SAE ARP4754, ARP4761, IEC 61508, SAE ARP5580, MIL-STD-1629A, DEF STAN 00-56, NRC Fault Tree handbook, ...
- A nice little earner. They run from tens to hundreds of dollars each.
- Growth: Take languages, ISO C90, **190** pages, C99, **400** pages, ISO C++99, **808** pages and in the blue corner, the heavyweight ISO C++2009, **1728** pages.
- Cloning: The same rules move between standards. (e.g. no goto in language standards, even though there is no evidence).

Human interface standards

9126

9241

13407

13406

61997

18529

14598

10741

10075

18021

18019

14915

11581

18789

14754

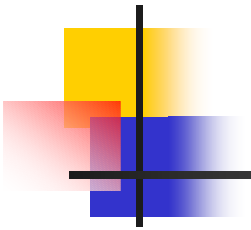
15910

16982

16071

20282

Safety-related software systems



Safety-related software systems are at risk.

We still have little empirical evidence to stave off mindless bureaucratic standardisation and as a consequence, standards proliferate like weeds.

However blind bureaucracy comes with a terrible price in such systems …

The Nimrod explosion, Afghanistan 2006

Daily Mail, 29/Oct/2009

- MOD Head of Air: “Complete failure to do his job in relation to the Nimrod Safety Case”
- MOD Safety Manager “Most of the time he was clearly out of his depth”
- BAE Systems Chief Airworthiness Engineer “Pushed through too quickly because he was too ambitious and assumed it was safe anyway”
- BAE Flight Systems and Avionics manager “Significant responsibility for poor planning, poor management and poor execution of project”
- QINETIQ Task manager of Safety Case project “agreeing on behalf of Qinetiq to sign off project without seeing or reading the reports”
- QINETIQ Technical Assurance Manager for Nimrod Safety Management “Guilty of allowing the manifestly inappropriate BAE reports to be approved”

Note the extensive safety bureaucracy and titles

An example – Nimrod explosion, Afghanistan 2006

"The Nimrod Safety Case was a lamentable job from start to finish. It was riddled with errors, it missed key dangers, its production is a story of incompetence, complacency and cynicism."

Charles Haddon-Cave QC

References

Loads of stuff on Wikipedia:-

http://www.wikipedia.org/

My writing site:-

http://www.leshatton.org/