

# Bureaucracy, Safety and Software: a potentially lethal cocktail

Les Hatton  
CISM, University of Kingston\*

September 15, 2009

## Abstract

This position paper identifies a potential problem with the evolution of software controlled safety critical systems. It observes that the rapid growth of bureaucracy in society rapidly spills over into rules for behaviour. Whether the need for the rules comes first or there is simple anticipation of the need for a rule by a bureaucrat is unclear in many cases. Many such rules lead to draconian restrictions and often make the existing situation worse due to the presence of unintended consequences as will be shown with a number of examples.

In science and engineering, the effects of such bureaucracy are generally mitigated because the rules naturally devolve from the exercise of the scientific method whereby evidence leads to policy and lasting benefit. In the absence of the scientific method, (which is usually the case in software systems development), policy flourishes like weeds without the constraints of reality. In software controlled systems, any consequent unintended side-effects could be lethal.

\$Date: 2009/09/10 16:12:07 \$

## 1 Overview

Complex systems often exhibit unintended behaviour as a result of well-intentioned change. Some examples follow under a number of general headings.

### 1.1 Division of responsibility

Dividing safety amongst separate bodies is known to be problematic. China's response to the melamine scandal that sickened over 53,000 infants who drank toxic milk formula in 2007-2008 is a perfect example. As Lelyveld [20] points out, the WHO specifically criticised China's division of responsibility for the part it played in this sad incident. In particular, China has separate ministries for health, agriculture, and commerce, as well as the State Food and Drug Administration (SFDA), the State Administration of Industry and Commerce (SAIC),

---

\*L.Hatton@kingston.ac.uk

and the General Administration of Quality Supervision, Inspection and Quarantine (GAQSIQ). Poor communication amongst such a diverse set of agencies is inevitable. This has considerable relevance to the corresponding position for safety-related software development as will be discussed further below.

The Chinese government has responded in the classic bureaucratic tradition by drafting new laws intended to prevent this happening again. Regrettably the new law is decidedly underwhelming. First the draft law bans all substances even those known to be unharmed unless they have been officially approved as additives. Second, the draft law only

”asks the departments, especially those at the grassroots level, to improve communication, cooperate closely with each other and faithfully fulfill their legal responsibilities,”

However, this does nothing to solve one of the major problems, which is conflict of interest. As one commentator in this article noted about the departments intended to carry out these directives,

”They have an incentive to keep the local economy growing and vibrant. But on the other hand, at the ministry level, they’re supposed to be taking care of food safety.”

In other words, it is a classic bureaucratic fix whereby a law is made which may well make things worse, (it is impossible to say), whereas one of the real problems is completely ignored.

## 1.2 Naming confusion

There is of course a related problem to confusion over responsibility with no clear division of authority, that of nomenclature. A perfect example of this occurs with the naming of drugs. Since Celebrex (generic name celecoxib) made its debut in January 1999, there have been 53 reports of errors due to name confusion, [11].

The confusion arises because there are two other similarly-named drugs, Cerebyx and Celexa, with very different application.

- Celebrex (celecoxib) is the new COX-2 selective inhibitor used for the treatment of arthritis.
- Cerebyx (fosphenytoin) is an intravenous drug used to treat epilepsy
- Celexa (citalopram) is a medication used to treat depression and symptoms of fibromyalgia

The similarity among the names has caused confusion and mistakes, but no serious injuries or fatalities at the time of reporting in the reference. In 10 of the 53 reported cases, the patient actually received the wrong drug. In 19 of the cases, the wrong drug was prescribed but the error was caught before the patient was dispensed the wrong drug. In the remaining 24 cases, doctors and pharmacists reported the name Celebrex to be confusing. The reported number

of errors is the most the Food and Drug Administration (FDA) had ever received for any drug that had only been available to consumers for 4 months and it is typically only around 5% of all cases which get reported anyway. In this case, drug marketing and wider implications of naming are not controlled by the same authority, although the FDA does indeed have an Office of Postmarketing to attempt to address this.

### **1.3 Interference based on well-intentioned meddling**

Well-intentioned meddling is normally the result of an inadequate grasp of number and specifically, probability. This is exceedingly widespread and essentially disables a large section of the population from making rational life decisions, [23]. In essence, somebody or possibly a group of people get a collective bee in their bonnet that something is important and then do something about it without any attempt to assess objectively whether it is important or not. Some examples follow.

#### **1.3.1 HM Coastguard bans flares**

This extraordinary piece of meddling occurred in November 2008 when the MCA (Maritime Coastguard Agency), a U.K. government organisation which co-ordinates search and rescue missions decided to stop HM Coastguard from using flares after discovering that they hadn't been used much recently. This is in spite of an MCA spokesman admitting that he was unaware of any incidents in which coastguard personnel had been injured using flares, and that the few times they had been used, they were apparently successful in saving lives which might not have been saved if the ban had been in place earlier. The suggestion by the way is that torches are used instead. Anybody who has been at sea in a boat at night will probably share the following quoted ([5]) view from a crewman:-

“This is the most stupid, ignorant thing I've heard of. Flares have been used for a century and, until now, have been a vital bit of kit.”

I could easily suggest a corollary to this to be erected next to a lifebelt.

“Do not use if the ship is sinking. You may drop it on your toe causing injury.”

As a warm-up to this piece of bureaucracy, the MCA had two months earlier disciplined a coastguard crew after they saved a girl with an inshore boat which was alleged to be structurally unsound, [21]. The boat had been repaired out of the crew's own funds because of the slow response of the MCA and was awaiting inspection, (also by the MCA). As a result of this incident, the boat was then locked up to prevent the crew having a “moral dilemma” in future. You really couldn't make this kind of thing up.

#### **1.3.2 Yellowstone National Park**

Yellowstone National Park is a wonderful example of sustained well-intentioned meddling based on things which taken individually might sound reasonable, as

described so eloquently by Michael Crichton, [8]. This quotation paints the background well.

“What, then, happened in Yellowstone? I would argue, people thought they understood the system. They thought they understood how nature worked. And they were wrong.”

They were not only wrong, they were lamentably and persistently wrong. Yellowstone National Park was set up in 1872 as the first formal nature reserve in the world. (Note that I am paraphrasing here - Michael Crichton’s version is far more eloquent). In 1903 President Theodore Roosevelt visited it for a dedication ceremony and noted with pleasure the abundant wild life - a thousand antelope, plentiful cougar, mountain sheep, deer, coyote, and many thousands of elk. Yet only 30 years later, the park service acknowledged that “white-tailed deer, cougar, lynx, wolf, and possibly wolverine and fisher are gone from the Yellowstone.” What they didn’t say was that they had actually caused this by well-intentioned muddled interference roughly as follows.

- In the 1890s, it was believed off no evidence that elk were becoming extinct, and so these animals were fed and encouraged. Over the next few years the numbers of elk in the park exploded.
- 1914- Antelope and deer began to decline, overgrazing changed the flora, aspen and willows were being eaten heavily and did not regenerate. In an effort to stem the loss of animals, the park rangers began to kill predators, which they did without public knowledge. They eliminated the wolf and cougar and were well on their way to getting rid of the coyote when the public realised and there was a national scandal. Independent studies showed that it was the elk explosion and the resultant over-grazing which were the problem. This was denied.
- Aspen disappeared because of the over-grazing taking the beaver with them. Without beaver there was no water management.
- By 1930, the small predators had disappeared. Those not finished by the park service needed a diet of beaver and other small animals and they had gone.

The whole charade continued in a similar vein into the 1980s until a devastating fire occurred by which time it had become abundantly obvious that when it comes to managing 2.2 million acres of wilderness, nobody since the Indians has had the faintest idea how to do it. (The Indians had regular controlled fires and otherwise left the park alone.)

The essential feature of all this was the problem of trying to manage a highly complex interconnected system by locally linear small changes, but more of this particular hallucination later.

### **1.3.3 CRB and the Independent Safeguarding Authority**

The CRB is the Criminal Records Bureau in the UK. It is a Home Office Agency and was set up in March 2002 with the laudable goal of vetting those working

with children and young people. It checks for criminal convictions and cautions but more insidiously an *enhanced check* also examines any other *relevant and proportionate* information held by the police, whatever that means. It was set up originally with the excellent intention to protect children from paedophiles and rapidly expanded to cover 1.5 million adults largely driven by the failure to stop Ian Huntley being given a job as a school caretaker in Soham, with tragic consequences. (It turns out that this was simply a failure in police communications but again the bureaucratic response is taking unintended directions [16].)

From 2010, (it has been delayed twice), this is being supplemented by the Independent Safeguarding Authority (ISA), a new agency intended to greatly increase the reach of the CRB. The ISA will use the *enhanced checks* to check *anybody* having any access to children however remote. This even includes spectators taking photographs at sports competitions, officials, coaches, drivers and so on and includes the whole of the voluntary sector.

The bottom line for this is that by 2015, a staggering 11 million people are planned to be in the register. In other words, the UK is intending to screen about one third of its adult population for anti-paedophile tests, an example of a disproportionate response which simply beggars belief.

So what are the unintended consequences here ? By far the worst is that the public at large will no longer help a child in distress for fear of being considered a paedophile. Beckford in [3] describes an ITV program which set up 2 child actors in apparent distress in a shopping mall, observed by hidden cameras. 1,817 people walked past them but only 5 offered to help and even those who stopped to help all admitted they had been worried their actions would be seen as suspicious.

In addition to this worrying trend, sadly, the UK Government has a dismal record of looking after its sensitive data. Even the best database management systems make mistakes, and in 2008 as reported in [16], some 1570 people were wrongly accused of criminal behaviour (False Positive) or not identified as having criminal records (False Negative), up from 690 the previous year. Even worse, most of these were towards the end of the year, (almost 1000 in December 2008 alone). The appeals procedure is of course bureaucratic with only 90% being cleared up in 21 days, during which time a great deal of anguish was created, due to the extreme sensitivity of the subject area. When the system is operating at its full level, this is likely to wrongly accuse around 5000 people a year, with a bad month being around 2000, assuming of course that it doesn't become overloaded and the error rate grows correspondingly.

A likely consequence of this as can be seen from the ITV experiment, will be that volunteers simply stop volunteering and that children will not benefit from their skills and time. Many sports in the UK depend entirely on the voluntary sector to function at all. If these sports suffer as a result, the children suffer directly. This does not appear to have been considered.

Last but not least, another unintended consequence of this is caused by the incompetence and oversight of the agencies themselves in soliciting data. As of the time of writing (early September 2009), the ISA web-site was still encouraging people to submit potentially highly sensitive whistle-blowing information by e-mail, in spite of it being completely insecure and some six weeks after I warned them of this.

#### **1.3.4 Black-outs and the Battle of the River Plate**

The great Black-out in Britain at the start of the Second World War is a classic example of wildly inaccurate expert advice, over-reaction and bureaucratic meddling. It was argued by experts from the Air Ministry, (see episode 2 of [17] for example), that 'millions' of people would die in air attacks. To prevent this, all the lights would be extinguished during the hours of darkness so that such attacks could not take place. This black-out came into force on the 1st September 1939, two days before the outbreak of the war. It was absolute (even a lit cigarette was considered a breach) and any breaches were harshly punished with big fines or court appearances.

The side-effect was that road traffic and other accidents such as drowning skyrocketed. Between September and November, there were 3,000 deaths. Some attempts to ameliorate this horrific toll were made. Torches were allowed from mid-September 1939 onwards but they had to be pointed down and covered with tissue, rendering them almost useless. From November 3rd, the black-out was shortened by one hour but it remained in place until September 1944 with many more casualties.

To put this into context, in the Battle of the River Plate, the first major sea battle of the Second World War and very widely published, the German pocket battleship Admiral Graf Spee fought a bloody battle with three Allied cruisers, the Achilles, Ajax and Exeter over 3 days in December 1939. The total casualties in this engagement, German and British were 109. Indeed for the first 3 months of the Second World War, more civilians were killed in the UK through black-out accidents than service personnel died on active service.

This observation is echoed by Michael Crichton, [8], who when intending to write a novel about Chernobyl and its reported 15,000-30,000 deaths with estimates of 500,000 more delayed deaths, discovered that the real figures were 56 dead and around 4,000 delayed deaths. Nobody wishes to undervalue this tragedy but the meal the media make of everything for its own ends can seriously distort the policy which then follows.

This is echoed yet again in the current scares about swine flu. The UK is reporting far more cases than other comparable population centres causing considerable panic, again amply swollen by media intervention. As of the time of writing it is unclear why, but a major contributing factor appears to be the practice of attempting to diagnose it over the phone to avoid spreading it. Unfortunately, there are significant concerns over this practice, [7]. An unintended consequence is that people have been given the anti-viral drug Tamiflu without

actually having flu, including patients with a knee infection and even tonsillitis. This drug has caused unpleasant side-effects in a significant number of patients and would be ineffective for potentially serious conditions such as meningitis which has similar symptoms. The drug was also dished out to young people in whom it caused significant side-effects.

In the absence of good, reliable data, media driven distortion will always prevail. Even when there is good reliable data, media driven distortion may still prevail if there is a good enough story as will be seen shortly.

### 1.3.5 Documentation proliferation and information overload

Although it is impossible to quantify its effect on safety yet, the gradual proliferation in road signs may be causing problems of information overload for drivers, [1], with some junctions having more than 16 signs. This sometimes has a humorous side as [19] notes about a major road sign displayed in Swansea. The English version said that this was a residential area and there was no entry for heavy goods vehicles. The Welsh translation was in a different league altogether. It read:

“Nid wyf yn y swyddfa ar hyn o bryd. Anfonwch unrhyw waith i’w gyfielthu”

A little while passed before someone had the nerve to point out that this gnomish message meant:

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

## 1.4 Interference based on political meddling and/or selectionism

Even when there is considerable scientific evidence available, the nature of political will coupled with a generally out of control and digitally lubricated media with its own agenda and needs can lead to important evidence being ignored with outrageous selectionism to give a highly distorted result.

### 1.4.1 Seat belt and other road safety legislation

Adams in [2] gives convincing arguments from detailed empirical studies that a number of road safety initiatives do not in fact reduce the total number of accidents. In fact for certain kinds of legislation, (for example mandatory safety belt legislation), he argues that the total number of injuries has gone up due to the phenomenon of *risk compensation*. In short, drivers when given safety aids, just drive faster. The effect is to transfer some of the risk to other more vulnerable road users, such as cyclists and pedestrians.

### 1.4.2 MMR and autism

This woeful piece of appalling science stoked up by a rapacious media is a perfect example of selectionism at its worst. It is described in detail by [12]. Little more need be said here apart from the fact that the media in essence

selected one particular discredited study which claimed a relationship between MMR and autism. In spite of all continuing evidence to the contrary, this has led to a significant percentage of children failing to be vaccinated against Measles, Mumps and Rubella, each a particularly nasty disease. As a consequence, there is now a measles epidemic, [24] for which the media can collectively claim the majority of the responsibility.

### 1.4.3 Risk assessment

In consort with the generally declining public awareness of number, there has been a rapid growth to the point of obsession with Risk assessments and Risk registers. Whilst thinking about risk has some value, assigning a level of risk is rather more difficult. Indeed, according to [2], risk is when you don't really know what will happen but you do know the odds. Uncertainty is when you don't know either. Most of the attempts at risk assessment I have seen are in fact uncertainty assessments and are usually devoid of any numeracy.

As a public service, here is how to do risk assessments so you don't get asked again.

1. Write the risk equation at the top,  $R = F \times C$  (Risk is Frequency times Consequence). This will immediately panic Human Resources as people join Human Resources to avoid nasty things like multiplication.
2. Write the principle risk as "End of Universe", for which F is very tiny according to the Large Hadron Collider website (the end of the universe is one of the risks), but not zero. Since the Consequence is infinite, then the Risk is infinite.
3. Include no other risks as they are finite and therefore compared with the end of the universe, can be neglected.
4. Forward to Human Resources. They will say something like, "You are not taking this seriously" to which you can answer, "I take the end of the universe very seriously". At this point, they will give up.

## 2 Safety standards and software development

So what has all the above to do with software development in safety-critical environments ?

### 2.1 Software development as a measurement free zone

The first thing I will note is that software development is a highly vulnerable activity in the sense that it is unusually prone to well-intentioned meddling because there has been insufficient attention paid to laying down a measurement basis from which to make reasoned conclusions about the reliability and potential safety of any system of which software plays a part. Indeed, one of the reasons why there are so many software project failures is the generally abysmal understanding of what it takes to build a successful software system, [22]. There is a touching but misguided belief in some quarters that this is because engineers

need more management skills. Unfortunately, the reverse is true. Managers need more engineering skills to be able to assess what is happening as their latest software project crashes silently around their ears.

It has long been known that software development inhabits a measurement-free zone. Walter Tichy made this point more than ten years ago in an excellent review [25]. As far as I can see, little has changed. We have even more technologies but experimental verification of them using the tried and trusty scientific method has simply not kept up.

As we have seen from the numerous examples above, bureaucracy and poor advice proliferates in areas devoid of the scientific method. Even when there is good quality data available, it can be seen that the media in pursuit of manufacturing a good story or some kind of political agenda can distort the evidence to lead to false conclusions. If there is almost no data to begin with, there is simply nothing with which to fight it.

## 2.2 Proliferation of software standards

I have just been sent a safety flier exhorting me to 'Start Your Safety Library' with

- MIL-STD-882C
- MIL-STD-882B 300 Series Tasks
- SAE ARP4754, ARP4761
- IEC 61508
- SAE ARP5580
- MIL-STD-1629A (it continues to be used)
- DEF STAN 00-56
- NRC Fault Tree Handbook

Note the use of the word 'Start' here. I don't know how much more I am intended to acquire but this is one of the reasons that I refuse to work on safety-related systems any more, (the other being that it is a legal minefield with lawyers just waiting for a juicy test case and no wonder given that we don't even know what constitutes best practice, [13]).

The first and most important lesson to be learnt is that software standards are a nice little earner. The general idea is to get together a team of willing volunteers to produce some sort of draft document for nothing. Then their free contributions are exploited, it is publicised as much as possible, and released at a handsome price with a set of copyright conditions which will make you wince. Having been released, nothing ever happens again and the standard rapidly becomes obsolete if it wasn't already when it was first released. I have sat on such committees *pro bono publico* and will not do so again.

A perfect example of this is the safety standard IEC 61508. This is a mighty tome of 7 parts, matched only by its mighty price. Since I couldn't get hold of it any other way, I actually bought a copy of part 3, which purports to be about software, solely for the purposes of writing this paper. I regret it deeply. It cost 193 Swiss Francs and for that I got the same standard twice, once in English and once in French, 50 pages of each and not updated since 1998. It comes with an alarming set of conditions which apparently even forbid me from backing it up. I have backed it up to protect my investment and challenge them to sue me. I will enlarge upon this standard shortly but in my view it is so vague that it is almost completely useless.

There are others. DO-178B comes in at 162.50 US dollars and ISO 26262-1 at 66 Swiss Francs. The MISRA-C standard is 40 UK pounds and its C++ twin is 45 UK pounds at the time of writing although you can download them more cheaply.

The one thing that all of these standards have in common is that they are primarily based on guesswork. They give lots of little tidbits of advice which sounds sort of reasonable but much of it is either out of date, never supported in the first place, maddeningly ill-defined or shamelessly imported from some other standard, [14]. For example table A.3 of IEC 61508-3 tells us that a certificated translator is highly recommended at SIL 2-4 but only recommended at SIL 1, <sup>1</sup>. SIL 1 has safety implications so why wouldn't it be highly recommended that the program translator, compiler or whatever had some form of quality control ? As it happens, and far more seriously, it doesn't really matter anyway because you can't get one any more - the certification of compilers disappeared in April 2000 without apparently a murmur from the software safety community.

We are also told that a suitable programming language is highly recommended at all SILs. This begs the question as to how we determine which language is suitable. What does suitable even mean ? There aren't any guidelines on what such a language might look like or how you would choose it although much of the technology it specifically mentions has disappeared anyway. What I think it really means is that the contributors to this document couldn't agree on anything, because choice of programming language is a) emotive and b) highly subjective, so they simply pass the buck on to the user. Of course the practical problems of finding engineers who are sufficiently fluent in a particular language are not considered, neither are there any references to enable further research.

How about testing ? In Table A.5, we are told that Dynamic Analysis and Testing is recommended at SIL 1 but highly recommended at SIL 2-4. With respect, this is just mumbo-jumbo. It is word-spinning with no quantifiable merit whatsoever.

There is of course a long history of inscrutability about belief systems and their rules. Take the following two quotations for example.

---

<sup>1</sup>A SIL is a System Integrity Level

These ye may eat of all that are in the waters: whatsoever hath fins and scales may ye eat; and whatsoever hath not fins and scales ye shall not eat; it is unclean unto you. Deuteronomy 14, v. 9-10.

This sensible advice probably reflected the fact that its harder to keep shellfish fresh but this does not exactly shine through the wording and the original justification is lost. Modern people who strictly adhere to these rules will continue to apply this in spite of massive advances in food handling hygiene and the fact that the people who wrote this very likely thought the earth was flat.

Star Alchemy, or Sealing of the Five Senses. This unifies the five shen, the five streams of personal consciousness that operate through our senses, with the five forces of the collective Stellar Self. The body of our stellar mind can be viewed in the four quadrants of fixed stars in the night sky, originally symbolized by heraldic animals (Black Turtle, Red Phoenix, Green Dragon, White Tiger). 5th formula of inner alchemy, The Seven Dao Alchemy Formulas of the Immortal Self, <sup>2</sup>

Is this supposed to mean anything ? It certainly doesn't to me. I don't have a collective Stellar Self, have only one stream of personal consciousness as far as I am aware unless I am missing out, the stars aren't fixed and their names differ both with culture and time. For example, I have always thought of the Red Phoenix more as a Concussed Lobster. No doubt, its supporters would consider me a callow scientist but I'm sure those supporters would be equally happy to have access to MRI scanners if necessary, neglecting the fact that they are a natural development of the scientific method, the antithesis of their own sphere.

So is IEC 61508 really the cutting edge of safety-related software standards ? Well, it isn't going to change unless another group of public-spirited individuals volunteers. Instead we will have other standards. A glance through the IEC, ISO and RTSA web-sites reveals that there is certainly no shortage of standards to adopt. Which ones do we choose ? It probably doesn't matter anyway. If I showed my copy of IEC 61508 to my students (which I am specifically forbidden to do by its terms and conditions in the best traditions of intellectual dissemination), I doubt if they would even agree on what the words meant.

Of course, what these standards really fall down on is that the individual engineers have to be competent. The activity known as Dynamic Analysis and Testing can cover almost anything from one useless test to an expensive, concerted, highly sophisticated but ultimately unsuccessful attempt to break the system somehow by people who really know what they are doing. The whole thing has been de-humanised into a box-ticking process as if engineer quality was a given. In my view, we would be far better off giving engineers a copy of Fred Brook's Mythical Man Month, [18] and breaking fingers for lapses of concentration. Only kidding.

---

<sup>2</sup>[http://www.healingtaousa.com/tao\\_alchemy\\_formulas.html](http://www.healingtaousa.com/tao_alchemy_formulas.html), accessed 6th August, 2009

### 2.2.1 The Human Interface

If anything, this is even worse with an astonishing array of standards, ISO or ISO/IEC 9126 (various parts), 9241 (various parts), 20282, 10741 (various parts), 11581, 11064, 13406, 14915, 14754, 61997, 18021, 18789, 18019, 15910, 13407, 14598, 16982, 18529, 10075 (various parts), 16071 and there may be more, [4], but I was beginning to lose consciousness in my search.

In spite of all this energy, the quality of human computer interfaces in many devices, safety and non safety-related, remains appalling. A perfect example is afforded by the McDonnell Douglas MD-11, which in spite of an obvious enormous amount of money spent on its avionics software, attracted this comment from its test pilot:-

“The airplane [computer system] manuals were written as though by creatures from another planet.”

He noted this after being presented with the wonderfully inscrutable “Button push ignored” by the Flight Management system, [9].

I list a few more examples of this kind of thing in [15]. There is no shortage.

### 2.3 Growth of software standards

Another important thing to note about software standards is that they must always grow. Shrinkage is considered unthinkable. Most ISO language standards grow substantially in size at each standards cycle until they collapse into obscurity rather like stars which exceed the Chandrasekhar limit and collapse into a white dwarf. For example the ISO C standard increased from 190 pages in ISO C 9899:1990 to around 400 pages in ISO C 9899:1999. This is a natural implication of the fact that it is much easier under ISO rules to introduce new things that might work than to take out old things that don't work, (on the principle of maintaining *backwards compatibility*, a supremely broken concept in engineering systems). Eventually language standards evolve into mind-bogglingly complex documents which defeat any individual's understanding. The ISO C++ standard is a good case in point, weighing in at over 800 pages in its 1999 incarnation and with so much undefined behaviour (implicit and explicit) that it is very difficult indeed to reason about many language constructs, let alone the intended functionality of the program of which they form a part.

### 2.4 Naming confusion

Naming is historically a rich source of confusion in software development. I have recently received notification of a seminar entitled “Providing Confidence in Safety Judgements”. This is organised by the IET / BCS ISA Working Group and advertises that it will describe an “ISA Code of Practice” and an “ISA Competence Framework”. I presume that ISA means Independent Software Assessment although I don't actually know and the flier does not say. This is what Google reported as of 01-Sep-2009:-

- Google(ISA Code of Practice): A Code of Practice to minimise Infectious Salmon Anaemia.

- Google(ISA Competence Framework): Reveals various competency frameworks none of which have ISA in them.
- Google(ISA): The Independent Safeguarding Authority. A U.K. government site created to help prevent unsuitable people from working with children and vulnerable adults, (of which we have already seen much above).

Perhaps this example would be considered slightly unfair, but the existence of other authorities associated with safety but nothing to do with software assurance and with much greater search engine impact, (arguably the only arbiter of success in modern times), is not going to be helpful.

## 2.5 The role of gravitas, governance, stakeholder-speak and other distractions

And so we come to the Tower of Babel. Management speak is full of nonsensical, ephemeral jargon. Because software development has no really well-agreed vocabulary, (even the definitions of fault and failure differ in some standards), management can intrude with its own peculiar rapidly evolving double-speak, introducing words like gravitas, governance and stakeholders into the jargon of software projects as if this had the slightest effect on how a system actually functions, or how it should be built. Using such jargon, people who really have no idea what is going on can give the illusion of control.

## 3 Conclusions - what is to be done ?

I am conscious of the fact that this short paper is critical but there are things which can be done if the will is there.

Perhaps the most urgent item for computer scientists to attend to is to lay down a representation independent measurement framework of quantifiable quality so that we actually know which techniques work, why and by how much. In spite of efforts to provide a forum for this by journals such as the Journal of Empirical Software Engineering, much remains to be done in the face of the seemingly endless supply of new paradigms, techniques and languages. Only by providing such a framework can the benefits of bureaucracy be gained without the well-intentioned meddling and arbitrary complexity which otherwise tends to emerge.

The standardisation process is broken. Standards need to be open source to facilitate easy updating in a highly volatile profession, and of unlimited free access. Proprietary file formats have caused enough misery without compounding it with proprietary standards. The current situation whereby standards are heavily protected, expensive and frequently outdated before they even appear is unhelpful to say the least and it is possible that Wikipedia and its like may play a substantial future role. NASA also has always been an excellent role model here providing free access to lots of useful documents and data, for example, [10]. However, on a cautionary note, open source standards without measurement constraint will simply produce free words.

Finally, the belief that defined process leads automatically to good product needs to be tempered. Much of what we do in successful software development, safety-related or otherwise, requires considerable analytic skills and it has always been true that good products are built by good engineers. Yet we face real challenges in the training and supply of such engineers with continuing and in some cases worsening shortages of trained engineers in the USA, Europe and Australasia as exemplified by these quotations:-

“It was perceived that student handling of mathematics had declined significantly and continues to decline. The perceived decline is steeper with home students and should be addressed via Government policy at pre-University level.”, [6].

“Analysis of public maths exam papers taken by 16-year-olds between 1951 and 2006 shows standards have declined markedly, the report for Reform argues.”

“India and China are producing four million graduates every year. The single largest area of graduate growth is mathematics, science and engineering.”

“A third of graduates in China are engineers - here [the UK] it's just 8%. Between 1994 and 2004, more than 30% of the physics departments in Britain disappeared.”

These latter three were all culled from <http://news.bbc.co.uk/1/hi/education/7431840.stm> on 7th Sept 2009.

That our shortages are balanced by growth in India and China will comfort only the most ardent of outsourcers and unless all of the above factors are resolved, there is a real danger that bureaucratic focus will overwhelm our systems development.

## References

- [1] The AA. Uk road sign survey, January 2009. Public Affairs : AA/Populus - too many road signs - The AA.
- [2] J. Adams. *Risk*. UCL Press, 1995. ISBN 1-85728-068-7.
- [3] Martin Beckford. Esther Rantzen: Fear of paedophiles is harming children, October 2008. <http://www.telegraph.co.uk/news/newsttopics/celebritynews/3122417/Esther-Rantzen-Fear-of-paedophiles-is-harming-children.html>.
- [4] N. Bevan. International standards for HCI and usability, April 2006. [http://www.usabilitynet.org/tools/r\\_international.htm](http://www.usabilitynet.org/tools/r_international.htm).

- [5] N. Britten. Coastguards banned from using flares over health and safety fears, November 2008. <http://www.telegraph.co.uk/news/uknews/3372215/Coastguards-banned-from-using-flares-over-health-and-safety-fears.html>.
- [6] W. Browne, D. Gregory, A. Phillips, and M. Unwin. Declining mathematical standards among science and engineering undergraduates: fact or fallacy? *Web*, September 2004. <http://www.nottingham.ac.uk/pesl/browse/faculty/cross/declinin208/>, accessed 07-Sep-2009.
- [7] D. Campbell. GPs fear swine flu misdiagnosis, August 2009. <http://www.guardian.co.uk/world/2009/aug/05/gps-fear-swine-flu-misdiagnosis>.
- [8] M. Crichton. Complexity theory and environmental management, November 2005. <http://www.michaelcrichton.net/speech-complexity.html>.
- [9] R.S. Drury. Flying the MD-11: One pilot's perspective. *Airways, a global view of commercial flight*, pages p.39–49, 1997.
- [10] Daniel L. Dvorak. NASA study on flight software complexity, March 2009. [http://oceexternal.nasa.gov/OCE\\_LIB/pdf/1021608main\\_FSWC\\_Final\\_Report.pdf](http://oceexternal.nasa.gov/OCE_LIB/pdf/1021608main_FSWC_Final_Report.pdf).
- [11] Carol Eustice and Richard Eustice. Celebrex causes concern: Name confusion plagues celebrex / celebrex tied to 10 deaths; gi bleeding, April 1999 (updated 1 Aug 2008). <http://arthritis.about.com/od/celebrex/a/causesconcern.htm>.
- [12] B. Goldacre. *Bad Science*. Fourth Estate, 2008. ISBN 0-00724-019-8.
- [13] L. Hatton. Towards a consistent legal framework for understanding software systems behaviour, June 1999. LLM thesis, Strathclyde Law School.
- [14] L. Hatton. Safer language subsets: an overview and a case history, MISRA C. *Information and Software Technology*, 46:465–472, 2004.
- [15] L. Hatton. The chimera of software quality. *IEEE Computer*, 40(8):101–103, 2007.
- [16] Christopher Hope. Hundreds wrongly branded criminals by agency, August 2009. London Daily Telegraph, 4th Aug, including editorial.
- [17] Jeremy Isaacs. The world at war, 1973. Thames Television, [http://en.wikipedia.org/wiki/The\\_World\\_At\\_War](http://en.wikipedia.org/wiki/The_World_At_War).
- [18] F.P. Brooks Jr. *The Mythical Man Month*. Addison-Wesley, 1975. ISBN 0-201-00650-2.
- [19] B. Johnson. Health and safety fears are making Britain a safe place for extremely stupid people, July 2009. <http://www.telegraph.co.uk/comment/columnists/borisjohnson/5754533/Health-and-safety-fears-are-making-Britain-a-safe-place-for-extremely-stupid-people.html>.

- [20] Michael Lelyveld. China's bureaucracy stymies food safety, November 2008. [http://www.rfa.org/english/energy\\_watch/food-safety-11042008154540.html](http://www.rfa.org/english/energy_watch/food-safety-11042008154540.html).
- [21] Daily Mail. Lifeboat banned by health and safety... three hours after saving drowning schoolgirl, August 2008. <http://www.dailymail.co.uk/news/article-1045170/Lifeboat-banned-health-safety-hours-saving-drowning-schoolgirl.html>.
- [22] Royal Academy of Engineering. The challenge of complex IT projects, 2004. Royal Academy of Engineering report, London, ISBN 1-903496-15-2.
- [23] John Allen Paulos. *Innumeracy: Mathematical Illiteracy and Its Consequences*. Hill and Wang, 2001. ISBN 0809058405.
- [24] R. Smith. Measles epidemic feared after 'unprecedented rise' in cases, January 2009. <http://www.telegraph.co.uk/health/healthnews/4208552/Measles-epidemic-feared-after-unprecedented-rise-in-cases.html>.
- [25] W.F. Tichy. Should computer scientists experiment more ? *IEEE Computer*, 31(5):32–40, May 1998.