

# Safety Standards Are Evil



(Maybe...)

*N.B. Deliberately pessimistic and provocative and not necessarily the views of the author*

# What are standards good for?

Perhaps they define an approach that guarantees a system is safe

If you follow the standard you'll be  
OK



# This is clearly **not** the case

There isn't any science behind most safety standards

*“It is astonishing – and a poor reflection on our technical community – that there is still no agreement, in the community that depends on the IEC 61508 standard, about what can be claimed about a system’s achieved dependability from the fact of its having been built using...a particular SIL.”*

*Bev Littlewood*



It is unclear why following the standard should lead to a safe system – Even the authors often don't seem to know

Where is the rationale?

# Standards are generally not applied in practice before issue

- So no empirical evaluation is carried out
- The potential for errors or inadequacies is high



*Would you be willing to try out the bungee rope to check if the design standard was effective?*

# “They at least capture agreed best practice in industry though”

Help people who don't have experience to know what to do...

Really? Have you ever attended a safety standards meeting?



# Standards Creation Process



- Often the loudest (most assertive) voice will get the most influence
- Everyone has their own ideas (and thinks they know best)  
Even though they're not necessarily experts!
- Messy compromise will often result

Motivation for many people on standards committees representing companies could be to have the bar set as low as possible so it doesn't cost too much

*“I don't mind what the outcome of the standard revision is as long as I don't have to change what I'm doing”*

# There *is* no agreement on what is best practice

If there were a consensus then we'd only  
need one standard

But there are multiple standards for all  
aspects of safety

Surely they can't *all* be right!



Even if they did represent best practice, the process of issuing is often so slow that they are out of date by the time of issue

Technology is moving much faster than the standards are



# But it's better to have something than nothing...right?

Well actually they are potentially very dangerous

- People may believe if they tick the boxes of the standard they'll be OK



- Encourages people to disengage their brain
  - Without standards people would have to think for themselves about why their system is safe (or not)

# Money

- Most standards cannot be viewed without paying a fee (IEC 61508 is \$2743)
- There is obviously a cost associated with producing the standard
- But such large costs affect:
  - Availability for review
  - Adoption by developers



# So what can we have instead?

Surely we can't just have a free-for-all?

Total anarchy

We need to have some way of judging if a system is acceptably safe



Accidents are very rare

So we must be doing something right

Standards must be playing a role in this

Maybe it's time to take a step  
back

Just because it has always been  
done that way doesn't mean it  
can't be changed

# Embracing Standards

Philippa Conmy

(actual opinions may vary...)

# *Process Consensus*

- **Collect industry, academic and expert consensus on techniques**
  - **My time on DO-297 showed broad range of participants**
  - **Broad range of knowledge and skills**
  - **Had to reach agreement that was both practical and acceptable**
  - **100s of years of theoretical and practical experience brought together**
  - **Regulators involved – independent observers**

# *Process - Ability to plan and predict effort*

- **Software development is expensive**
  - Very hard to anticipate time needed to build requirements
  - Let alone how to assess and analyse the product
  - With (process) standards can plan and cost techniques required in advance
- **Basis for sub-contracting**
  - Sets minimum baseline that must at least be achieved by contractors and system developers
  - Can't get away with short cuts

# Goal /Product based Standards

- **Based on assessment of the what the system actually does**
  - **Can concentrate on meeting functional and non-functional requirements**
  - **Traceability of evidence to requirements**
- **Requires the engineer to use their brain!**
  - **Within defined framework**
  - **Must think about safety goals**
  - **Concepts such as ALARP**
  - **What parts of the system are most important**
- **Allows use of process based standards as means to provide evidence**
  - **Best of both worlds**

## *Both - assess what's been done*

- **How do we assess the acceptability of system or software?**
  - **Standards describe a broad range of techniques**
  - **Acceptability criteria given**
  - **Understand safety and severity**
  - **Works for regulators too**
- **Evidence can be re-used (in theory)**

# *Both - Continuous Improvement*

- **Standards set a benchmark from which we can improve**
  - **Experience from applying standards builds up our knowledge**
    - ◆ **Both of techniques and the system/software we are building**
    - ◆ **Making an engineer look at a system in a different way can be very valuable**
  - **Learn from good and bad parts of them**
  - **Update the techniques and data**
    - ◆ **(okay this is a bit in theory too!)**

# *Both - We'd create them anyway*

- **Every software company has standards**
  - **Presentation, syntax, and testing**
  - **Allows communication and maintenance at very least**
- **Collecting all ideas together means less chance of incompatibilities**
  - **Need common language and understanding of basic concepts**



**A (MUDDY) MIDDLE GROUND  
OR  
THE GRAND, POOR EXPERIMENT**

# There Are Standards And *Standards*

- All standards include goals and prescriptions
  - DO-178B requires MC/DC coverage but does not constrain how this is achieved
  - DO-178B allows alternate means of compliance
  - DefStan 00-56 constrains safety process, mandates a hazard log, etc.
  - CAP 670 SW01 gives multiple 'regulatory goals'
  - It's a matter of degree, really
    - Can combine approaches: DO-17843\*

\* Thomas Jefferson was born 13 April 1743...

# Prescriptions Are Imperfect

- Rationale for belief that compliance yields safety would have to:
  - Hold for all applicable systems (even the oddest corner cases)
  - Be strong enough for the most critical systems
  - Account for the possibility of mis-compliance (compliance with text but not intent)
- Ha ha ha

# Goals Are Also Imperfect

- Regulator-developer dialogue used to improve solutions ... against pressure to accept
- Inspectors must assess solutions, but do they know the state of the possible in all fields?!?
- Developers must bring in 'good rocks'
  - Might Standard Rocks be better on average?
  - Can we force familiarity tools/techniques?

# . . . And So Is The Science

- How well do established techniques work?
  - Do you trust the probabilities from PFTA? Why?
  - How complete are guided enumerations?
- How well do they work in combination?
  - What reliability is established by MC/DC unit testing (given the other verification evidence)?
  - Do developers err less frequently when they know the argument behind what they do?
  - No calculus for confidence

# Given The Blinkers . . .

- Standards give us a common language
  - What do you mean by “software HAZOP”?
    - Is a technique standard different? Could cite compliance with a technique standard in a goal-oriented safety case...
  - I have no idea what “secure enough” means, but I know what is in Common Criteria EAL5

# Better Living Through Rx

- Prescriptions remind us to “think of that”
  - FDA guidance for infusion pumps gives hazard list
    - Probably best used as a check after the fact . . .
  - Are your tools qualified?
  - Do you have a configuration management plan?
- Of course, so could patterns . . .

# More Prescription Benefits

- Expectations clearer
  - Easier to budget time for MC/DC testing than for generating a compelling argument (and evidence)
- Role in education
  - Ignorance of MC/DC if not for DO-178B?
- Moving target defined
  - Expectations advance with technology; the text of a prescription (eventually, maybe) changes with it

Apologies to John Knight for cribbing this material from *A Standard for Standards?*

# A Standard (Unproven) Recipe

- Even if a standard's rationale is imperfect, it may be better than ad hoc rationales
  - After all, it was produced by expert consensus
    - Pay no attention to the man behind the curtain!
- Standards are the basis of a grand (but poor) experiment:
  - We make loads of people comply to various standards (without any randomisation, of course) . . .
  - . . . then find out which systems fail
  - . . . then (hopefully) fix the prescription