Undependable dependability claims, and the regulators' plight

Lorenzo Strigini

Centre for Software Reliability – City St George's, University of London, U.K.

reporting work with Peter Bishop, Andrey Povyakalo

CSR Building confidence in a computerised world

www.csr.city.ac.uk

A brief update on *inevitable doubt*

in previous episodes:

we have been looking at what {regulators, insurers, users} should make of the fact that

*intensive, expensive analyses supporting claims of accidents being as improbable as required to authorise operation... are so often **wrong**:*

- [...]
- so as to drive sensible decisions
- ...

NB this is *not* about human wickedness, ...

sophistry, tawdry compromises, regulatory capture...

these may well occur ***but***

even the best analyses by the best people cannot give *100% confidence* in a claimed probability of accident being less than 10^{-n} per {mission, hour, whatever}

certainly this applies to real analyses by real people

General approach

... most probability-literate people would accept a statement of the form

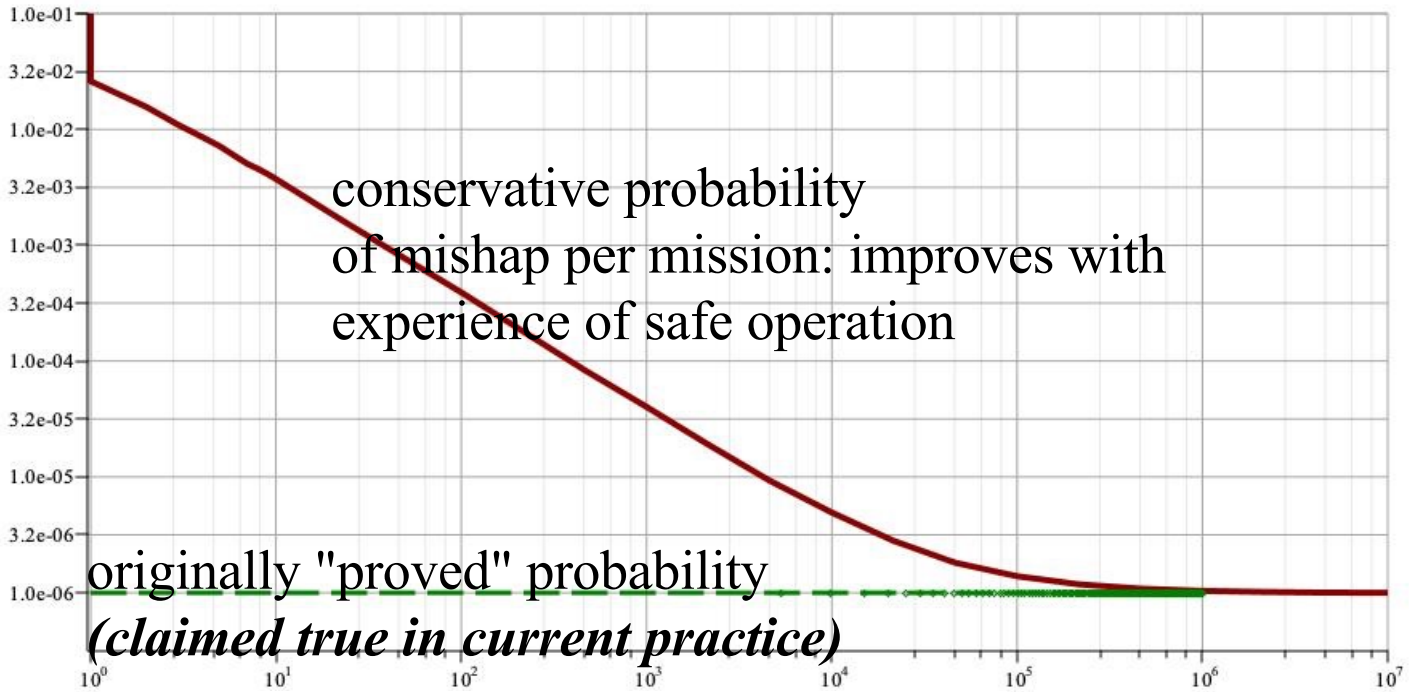
- *if 90% of new, properly certified airliner models have a probability of accident per flight $\leq 10^{-7}$,*
- *but 10% prove much worse, with 10^{-2}/flight,*
- *then if you take a flight in a new, freshly certified airliner, without any extra knowledge, you are accepting a risk bounded by :*

$$90\% * 10^{-7} + 10\% * 10^{-2} \approx 10^{-3}$$

but ... safe, surprise-free operation under strict monitoring will rightly reassure us about safety of a system type

Hence....

the upper bound you should really believe looks like:



maths in [Bishop et al, IEEETSE 2011]

We may not be very happy with that

... but some more probabilistic nitpicking may help:

- safety analysis often contains unused bits that would generate "backup claims"
- like "even if my primary claim of 10^{-7} were wrong, I could claim 10^{-4}, based on facts x, y and z"
- but if the 10^{-7} were correct with 100% probability, all this other knowledge would be superfluous!
- Yet regulators are happy to see this "superfluous" material
- and they are right! Why?
- we have general results for the case you can state a set of alternative claims for a bound on probability of accidents

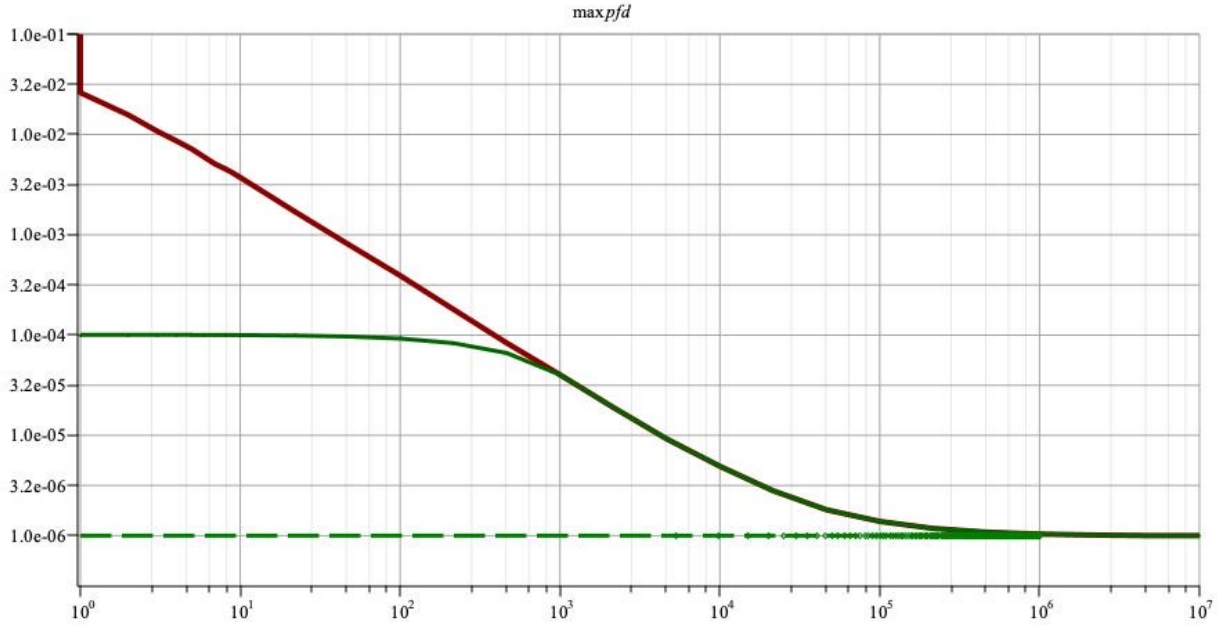
$$0 \leq q_1 \leq q_2 .... < 1$$

typically with increasing confidence that they are correct

$$p_1 < p_2 <... < 1$$

Effect of these "backup" arguments

suppose you have just one... High confidence that *even if* your main claim were wrong, still you know an alternative upper bound that is <1



amount of surprise-free operation

This limits initial risk (after a while, it stops helping)

Thank you for your attention...

Questions, comments?

To learn more, to give us your critique:

- Talk over coffee
- Do Email us
- Come to SASSUR at SafeComp 2025
- Ask us for the paper
  - theorem proofs,
  - future report on analysis of Airworthiness Directives

A brief update on *inevitable doubt*

or how stating formal probabilistic arguments for a dependability claim can show

that some claim made is outlandish

and yet a similar claim could possibly be proved right

usually at the cost of making the claim more modest

and digging up some actual evidence that the formalised argument shows to be needed

e.g. in the 1980s Bev Littlewood started asking "Airbus sales talk says FBW is a safe option, 10^{-9} probability of catastrophic failure per flight... how exactly did you turn that *requirement* into a *claimed fact*?

For highly critical computer applications we have...

sensible regimes, demanding

- *before* such a system is allowed into operation
- a demonstration that harm from its operation is unlikely enough

and we have remarkably safe operation in many areas

(e.g. scheduled civilian air transport)

- despite "ultra-high" dependability requirements

  like 10^{-9} probability of catastrophic failure conditions per flight hr

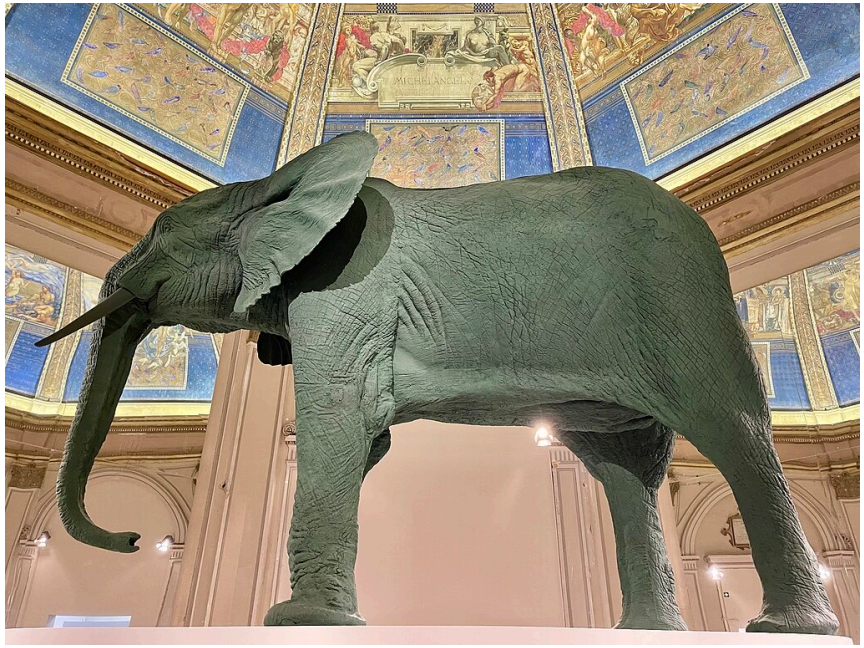
- so when a novel system comes along that requires UHD...

  e.g. "an automated car shall cause death at a rate ≤ 1 in 10^{-10} $mile^{-1}$ "

  ... we *rightly* demand a similarly stringent assurance regime

this should buy the public peace of mind... or should it?

There's an elephant in the room...



https://commons.wikimedia.org/wiki/File:The_elephant_in_the_room_at_Arsenale_(52196585578).jpg
license: https://creativecommons.org/licenses/by/2.0/deed.en