SSM: Metrics

I.G.Batten@bham.ac.uk

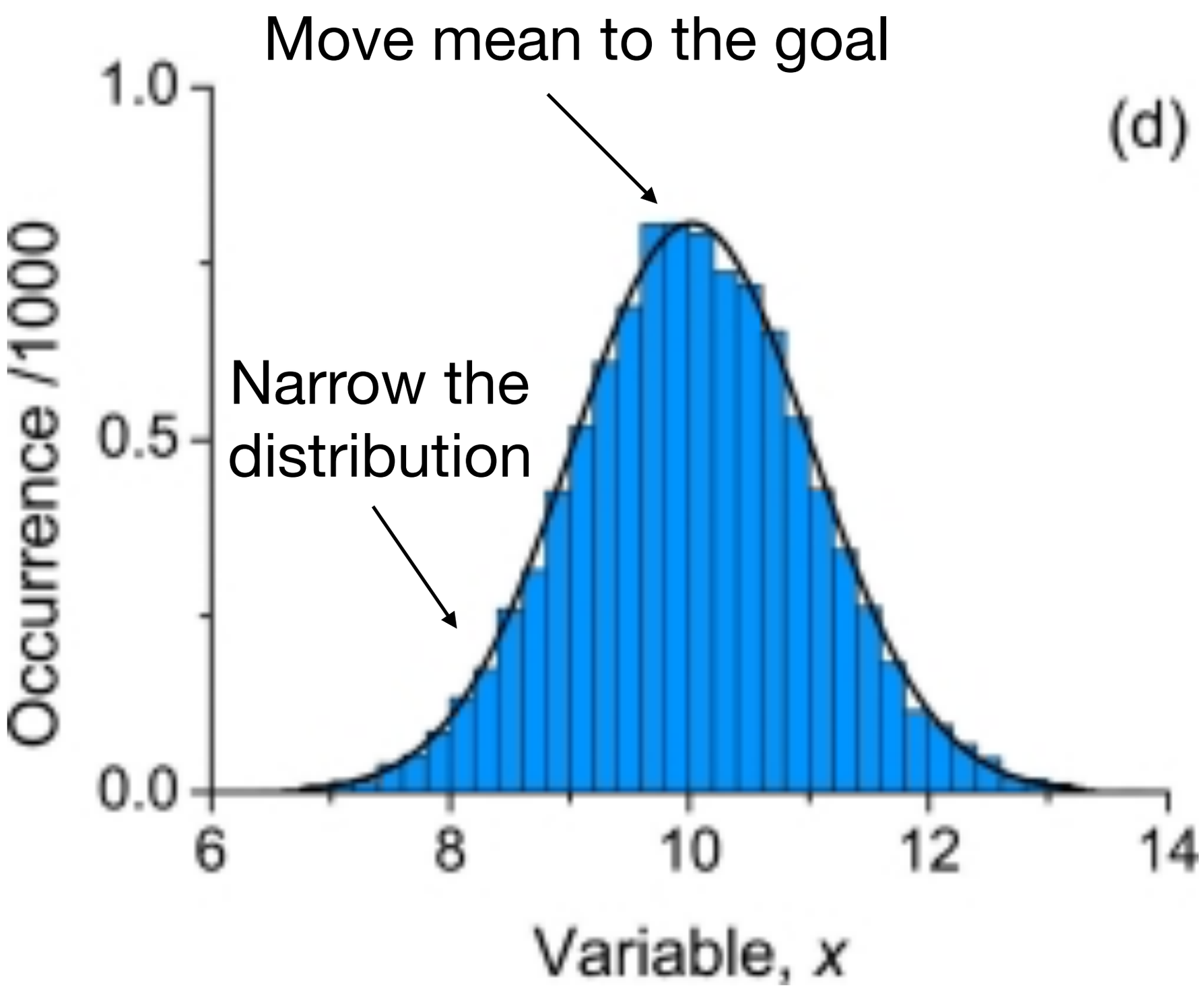
Purpose

- ISO 27001:2005 talks about plan-do-check-act improvement (which comes from ISO9001)
- ISO 27001:2013 is less prescriptive about the *how*, but still demands continuous improvement (so six-sigma, for example, is now compliant)
- How do we measure the effectiveness of our security system so that we can improve it?

The Problem

- Most of the things we are really worried about are rare, high-severity incidents
  - A few viruses (virii or viri is both wrong and very pretentious), the occasional phishing email: are these serious?
  - There will be constant ratting of the background radiation of the internet against your firewalls
  - And people will be constantly trying to break into ssh and web servers
- What should we measure?

Manufacturing is easy (!)



Security is harder

- Not a production line
- Measurement not an inherent part of the process
- Data collection harder and patchier

Proxy Outcomes

- Common problem in health trials
- Because we cannot measure what we want (reductions in long term mortality and long term morbidity) we instead measure a proxy for it (cholesterol, blood pressure, BMI).
- This is fine, as long as the proxy really is a very close correlate of the thing we really want to improve

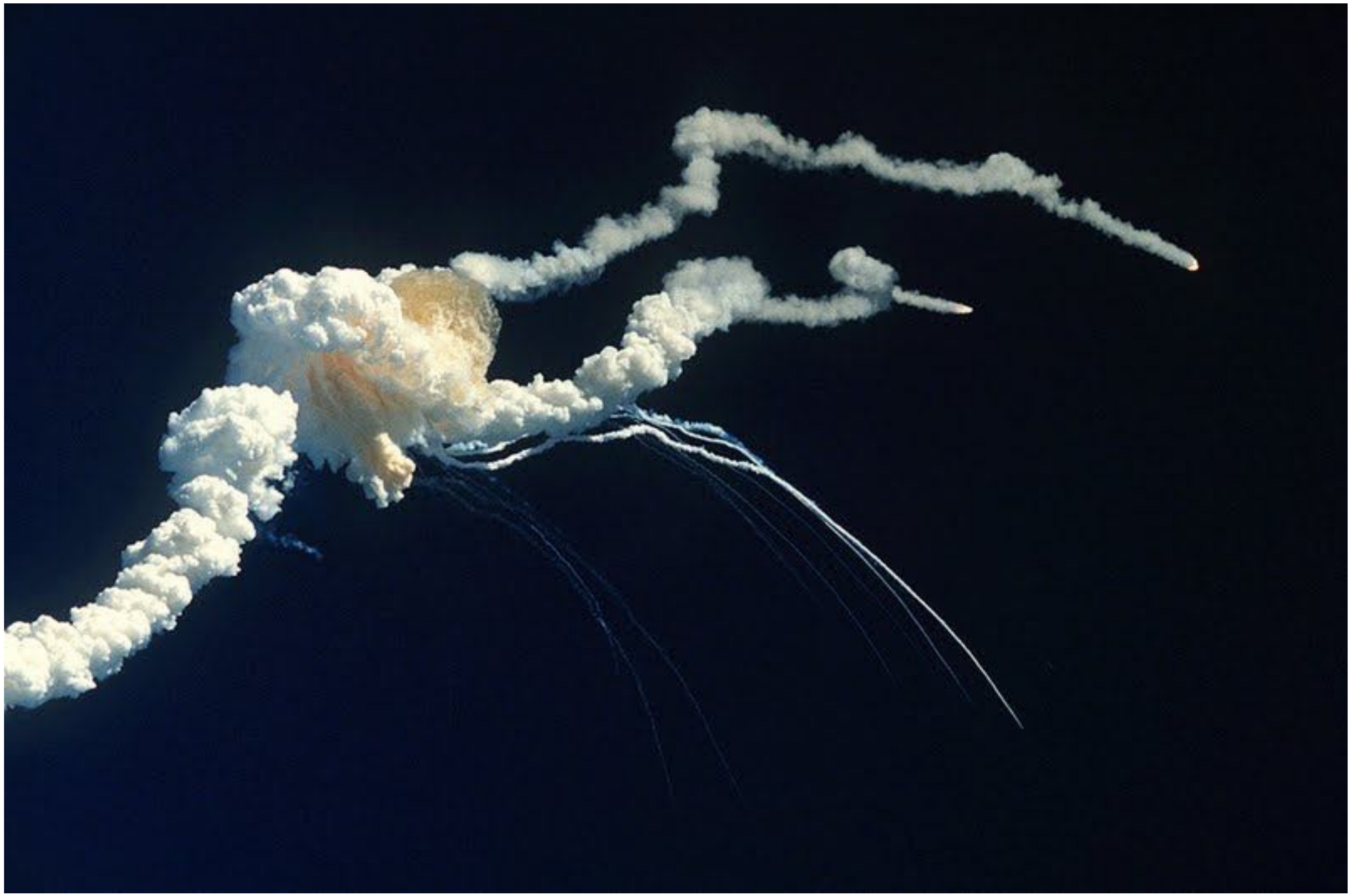
Proxy Outcomes

- Easiest to focus on things that we see a lot of: viruses hitting external email servers, packets hitting firewalls, systems being patched
- Is it better if those numbers go up, or down? Well, it all depends, and that makes use of them very dubious.
- Are we doing better or worse if we double the number of viruses we detect?
- Is our OS vendor releasing more security patches a good thing or a bad thing?

Some are OK…

- Measuring successful restorations (and more importantly failed restorations) is probably a reasonable measure of backup coverage
- Measuring downtime caused by disk failure is a reasonable measure of risk associated with storage redundancy
- But these are tenuous as security: this is more ITIL/ Business Continuity stuff

Who recognises this?

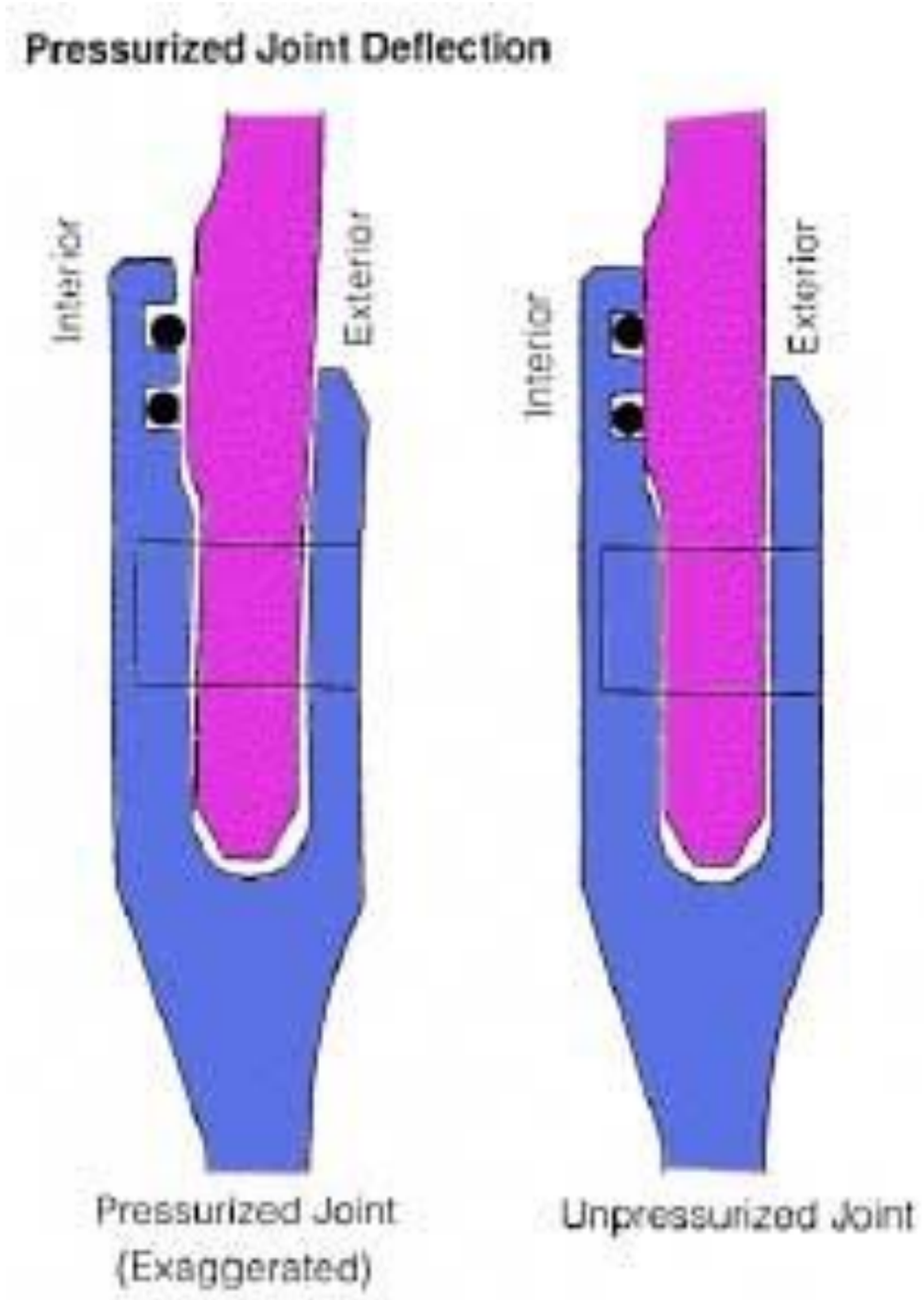


Safety Margins

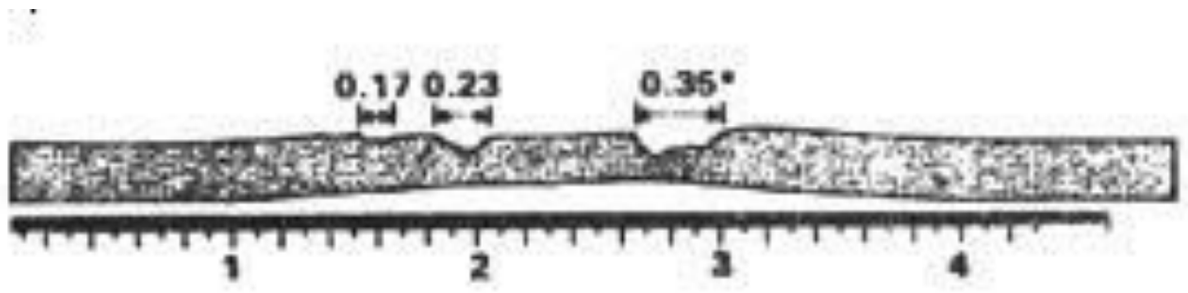
- Challenger accident, Jan 28 1986
- *Challenger*, a US space shuttle, exploded 73 seconds into mission STS-51L, killing everyone on board.
- Complete and utter failure of safety engineering
- Every engineer should read **Feynman's Appendix F** to the report at least once a year
- http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt

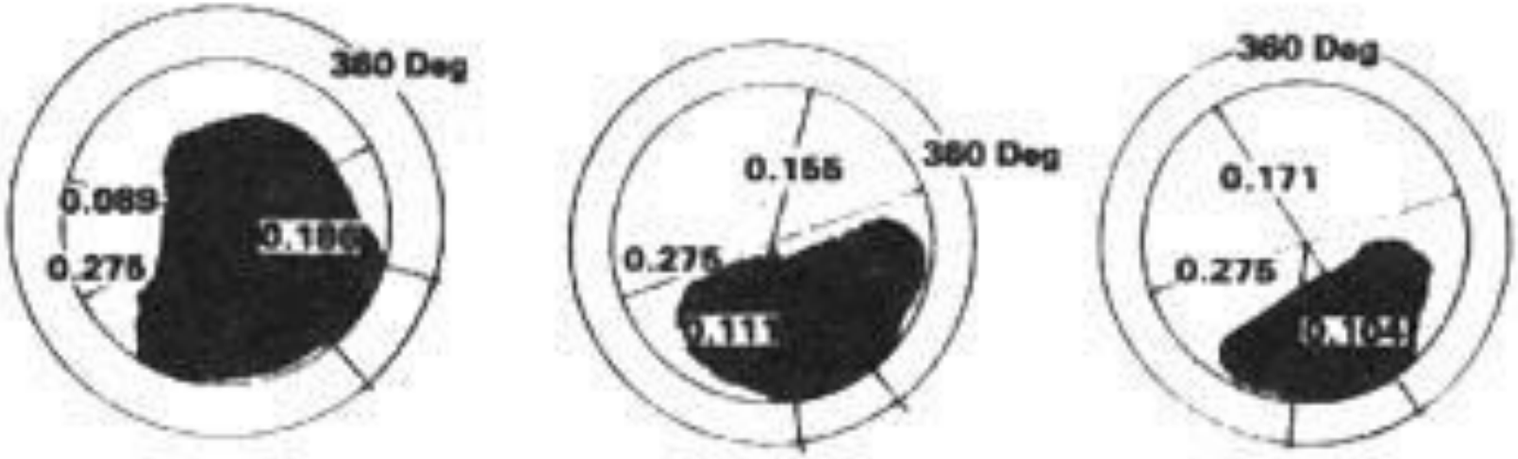
Myth of Safety Margin

- Accident caused by O Rings on large solid-fuel rocket failing
- Design said they should never be eroded



In fact they were being cut through by hot gasses, up to a third of their diameter being eroded.





In spite of these variations from case to case, officials behaved as if they understood it, giving apparently logical arguments to each other often depending on the "success" of previous flights. For example. in determining if flight 51-L was safe to fly in the face of ring erosion in flight 51-C, **it was noted that the erosion depth was only one-third of the radius. It had been noted in an experiment cutting the ring that cutting it as deep as one radius was necessary before the ring failed. Instead of being very concerned that variations of poorly understood conditions might reasonably create a deeper erosion this time, it was asserted, there was "a safety factor of three.**" This is a strange use of the engineer's term ,"safety factor." If a bridge is built to withstand a certain load without the beams permanently deforming, cracking, or breaking, it may be designed for the materials used to actually stand up under three times the load. This "safety factor" is to allow for uncertain excesses of load, or unknown extra loads, or weaknesses in the material that might have unexpected flaws, etc. If now the expected load comes on to the new bridge and a crack appears in a beam, this is a failure of the design. There was no safety factor at all; even though the bridge did not actually collapse because the crack went only one-third of the way through the beam. **The O-rings of the Solid Rocket Boosters were not designed to erode. Erosion was a clue that something was wrong. Erosion was not something from which safety can be inferred.**

“Defence in Depth”

- Common metric is to look at systems further in to measure effectiveness of outer perimeter
- So drop in IDS incidents on internal network implies that outer firewall is working
- Or does it imply that the IDS isn’t working?
- Or that the threat has changed?
- After all, the firewall is intended to pass **no** threats!

User Metrics

- Which of these seem like good metrics?
  - How often do users change their passwords?
  - How often do users forget their passes?
  - How often are laptops stolen?
  - How often are desks left unclear?

Good metrics

- Drive sensible behaviour
- Link clearly to security objectives, rather than just controls
- Have clear derivatives (ie, you know whether increase or decrease is better)

Five minutes…

- What would be some good metrics for the work you were doing for the exercise?
- Do they prove controls are working, or are just installed?
- Do they support policy?

Audit

- Internal audit is a very powerful tool
- Difficult in companies that don’t have a strong ISO9000 culture; internal audit teams are expensive and their skills are quite rare
- Also tend to be pariahs in the business: no-one likes the auditor when they turn up

Audit does two things

- Is the process being followed, with controls in place and records being kept?
  - This probably doesn’t require strong domain knowledge, and is about checking documents against reality
- Is the process worthwhile, with controls that meet the objectives?
  - Does require strong domain knowledge, and unlikely that your general-purpose audit team can help. Consultants and/or external auditors

Audit as Metric

- You can graph the number of successful audits, and the number of actions arising and being cleared
- Provided that your audit team is effective, this can work very well
- Probably only a solution for large companies, perhaps with a manufacturing slant

Financial Audit

- Note that today, your company's financial auditors will want to do an IT security audit as well.
- You need to pass this, but it will probably not be useful as a wider measure of effectiveness: baseline only.