Unjustified Justifications

SYSTEMS AND ENGINEERING TECHNOLOGY

Presented by

- David H Smith
- Principal Consultant
  - Frazer-Nash Consultancy Ltd
  - Mey House
  - Bridport Road
  - Dorchester
  - Dorset
  - DT1 3QY
  - Email: d.smith@fnc.co.uk
  - Tel: 01305 217910

Introduction

To provide examples of what can happen when safety

- exits the comfort zone
- encounters the not invented here syndrome
- is taken out of context

Standards

Defence Standard 00-56	RTCA/DO-254	IEC 61511
JSP 375	MIL-STD-882	RTCA/DO-178C
RTCA/DO-178B	JSP 430	ARP 4754A
IEC 61508	**There are too many standards**	MIL-STD-498
POSMS	JSP 454	IEC 61513
JAR 29	ISO 12207	ARP 4761
CAP 670	Defence Standard 00-55	JSP 520

Standards

Why can’t we have fewer standards?

Why does everyone have to do it differently?

There must be an easier way to do this

Standards

Unfortunately…

Standards

We can't even agree on basic definitions

Tolerable Risk

- *The maximum level of risk of a particular technical process or condition that is regarded as tolerable in the circumstances in question*
- *A level of risk between broadly acceptable and unacceptable that may be tolerated when it has been demonstrated to be ALARP*
- *Risk which is accepted in a given context based on the current values of society*
- *The maximum level of risk of a product that is acceptable to the Railway Authority*

Standards

Sometimes we just don’t seem to understand what needs to be done

Standards

- Good practice is not the same across industries
  - Some “good practice” might be considered out of date

Standards

- In some cases companies claim that there processes have been approved by a regulator
  - They therefore find it difficult to understand why an ISA would need to review and audit those processes

Standards

- Some systems were developed many years ago using the standards and accepted practice that was in place then
  - This is usually a problem, but not always

Standards

- Getting a contractor to sign up to a specific standard may not provide the outputs that are expected
- This can be the case when the contractor subcontracts all work
  - Especially if sub-contractors have no experience of that standard
  - Or the industry sector
- It can also be a problem if the contractor does not include the sub-contractor processes and outputs as deliverables

Standards

- There can also be problems if contractors fail to manage their subcontractors and how they are complying with the required standards

Standards

- For example, RTCA/DO-178B is only guidance
  - So it can be tailored
  - This might result in reduced levels of assurance

Standards

- Similarly, some standards require aspects such as Integrity Levels to be defined on a case by case basis
  - This again can lead to lower assurance than expected

Standards

- In some sectors suppliers provide some form of Certification
  - They can find it difficult to understand why other sectors cannot just accept such certificate and need to undertake audits, etc.

Standards

- Then there is the most common issue
  - *Sorry, we can't deliver on time and do all the safety work*

Standards

- Current guidance to Government Minister states that
  - *Standards are voluntary in that there is no obligation to apply them or comply with them, except in those few cases where their application is directly demanded by regulatory instruments*
  - *They are tools devised for the convenience of those who wish to use them*

Claims

Claims

- Some claims don’t address the requirements
- For example
  - *Validation activities will terminate when all the planned activities are complete*

Claims

- Sometimes the purpose of the safety case is not fully understood
- For example
  - *This final safety case provides a reasoned justification for the predicted achievement of acceptable safety integrity*

Claims

- Some claims appear to be wishful thinking rather than a reasoned argument
  - *A wrong setting could be made and go unnoticed, there is confidence that there will not be a problem*

Claims

- Sometimes there is a lack of understanding of basic terminology
- For example
  - *The transducer is a simple device, it only converts analogue data to digital data*
  - *…so we don't have to apply the full rigor of the standard*
  - *…it includes an FPGA*

Claims

- When software claim limits are used in Fault Trees this can result in strange claims
- For example
  - *The probability of system failure is 7.343232 x 10^{-31}*
  - *The probability of the test system not identifying a defective subsystem is 4.7 x 10^{-52}, approximately*
  - *This system has a probability of dangerous failure of 1.34 x 10^{-243} per year*

Claims

- Good intentions can be undermined by a lack of understanding of the requirements
- For example
  - *A contract said that there were no requirement higher than SIL 2, so the design used a mix of COTS and bespoke equipment*
  - *However SIL 4 requirements were identified following contract award, so an attempt was made to claim that the resultant risks could be addressed using SIL 2 functionality*

Claims

- Some suppliers seem to forget that different customers have different requirements
- For example
  - *They supply Boeing, Airbus and many others, if it's good enough for them, why isn't it good enough for you?*

Claims

- Sometimes initial claims are overtaken by events
- For example
  - *A Safety Case contained the claim that an item of equipment was considered to be COTS as it had been developed for another project*
  - *However the other project was cancelled, but the claim was kept in the safety case*

Claims

- Sometimes it seems like clutching at straws
- For example
  - *We've identified over 20,000,000 operating hours with no major failures*
  - *However the supplier recently changed the processor board and the FPGAs*
  - *As the part number did not change we still consider it to be valid data*

Claims

- There always seem to be problems with making ALARP arguments
- For example
  - A hazard analysis identified SIL 4 requirements
    - However the supplier did not have experience of developing such systems. They recognised that they could train our people, or recruit
    - They also recognised that they still needed relevant experience, which would take years to obtain
  - So they did a Cost Benefit Analysis
    - They worked out that it would cost ££££££££££s to do all that
    - But only £s to develop to SIL 2
  - And then claimed that therefore a SIL 2 system satisfied ALARP

Conclusions

- Transferable Safety?
  - Standards
    - Extreme Caution
    - Why do it?
  - Safety Cases
    - Yes and no
    - Introduces new risks
  - Competence
    - It depends…
- One way to really find out
  - See you in court

FRAZER-NASH CONSULTANCY

www.fnc.co.uk

SYSTEMS AND ENGINEERING TECHNOLOGY