Risk based Independent Safety Assessment

How to add value and reduce safety and project risks

David Bradley BSc CEng MIET

Praxis High Integrity Systems Limited

Introduction

Defining risk based Independent Safety Assessment

Real-life examples: findings and solutions

Impact of assessment

Benefit of assessment

Conclusion

What is risk based ISA?

Identify safety and project risks for ISA and client using selected tools and competent team

Use risks to inform:

Planning
Tools
Depth
Re-planning

Develop Claim Argument – assure assessment is complete

What is risk-based ISA? (2)

Clearly defined remit

Planned approach

Principles

ISA Toolkit

Trusted Specialists

Safety issues encountered in practice

Two contrasting examples discussed:

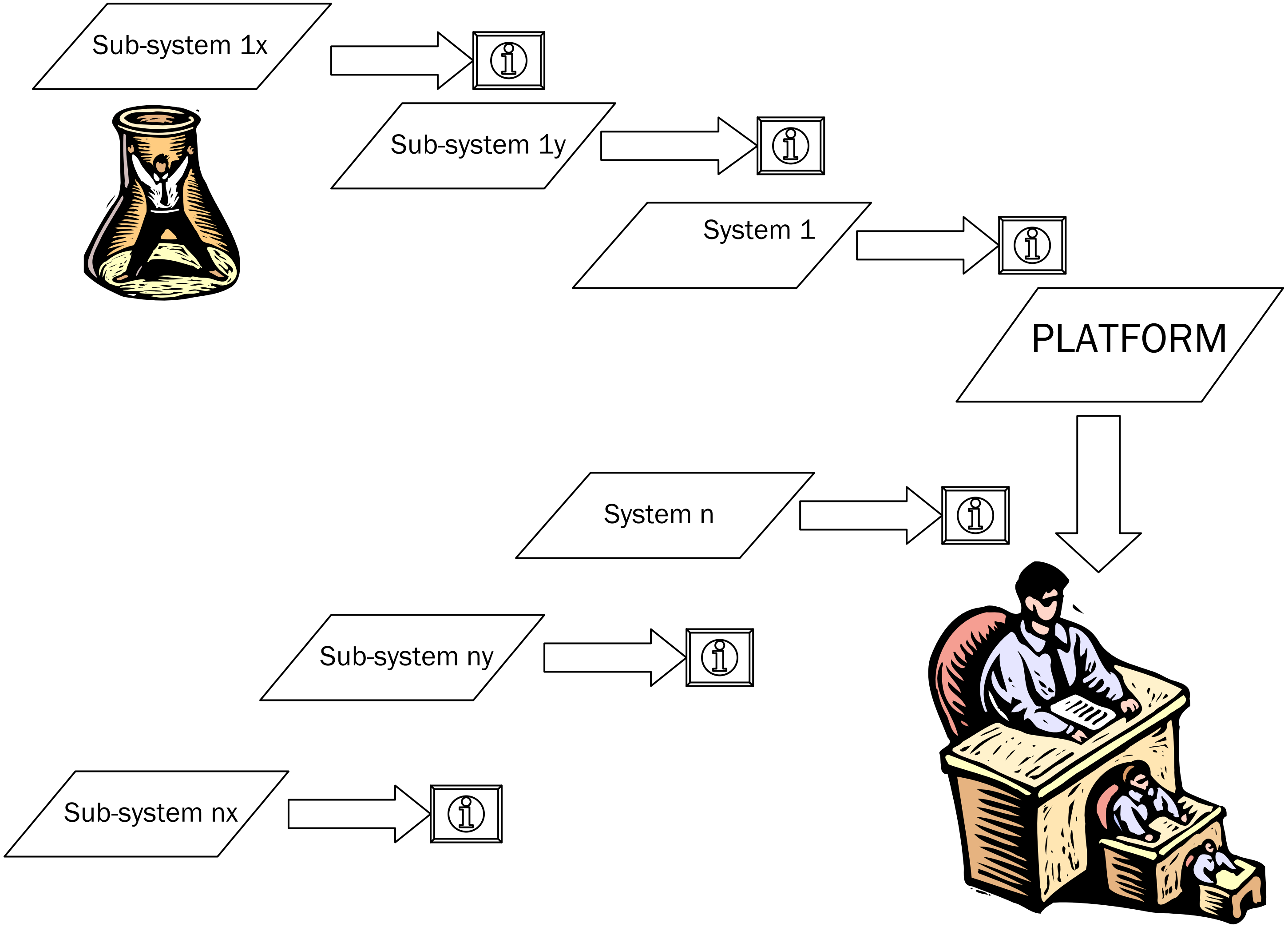
- Insufficient / late attention to system risks that impact platform
- Where the ISA identified vulnerable design in time to find solution

Followed by some perpetual problems

Example 1: identifying a problem but not the risk

- Designing a system that interfaces to weapons – required to safely interface
- Insufficient weapon information re functional safety – not contracted
- Problem recognised at interface level but not addressed for long period – until well beyond design commitment
- Potential major impact at platform level
- True ALARP solution achievable?

Developing in formation



Sub-system 1x

Sub-system 1y

System 1

PLATFORM

System n

Sub-system ny

Sub-system nx

Underlying problems

- ISA performed at platform level by individual skills –uncoordinated and with minimal system assessment
- Many competing issues at platform level, insufficient weight given to system / sub-system issues
- Responsibilities unclear – Platform, Weapon, System and Sub-systems
- Safety assessment of integrated systems performed after sub-system design commitment

How risk-based ISA deals with this

Coordinated assessment of all relevant aspects

Open-minded view, look across boundaries, challenge assumptions

Early involvement – reveal those problems early

Ensure adequate attention paid to the key risks and to their mitigation

Safety designed in, in preference to risk mitigated out

Rigorous processes being applied?

Example 2: The devil in the detail

- A sub-system design failing to meet integrity requirements
- Good architecture – second generation triple channel rail control product
- ISA risk-based assessment of modified / newly developed areas found:
  - Detailed design had ‘feature’ to improve built-in-test, involving links between channels in a 2 out of 3 voting function
  - Feedback monitoring of safe state not obviously robust
  - Insufficient safety analysis of common mode /cause failure performed to justify

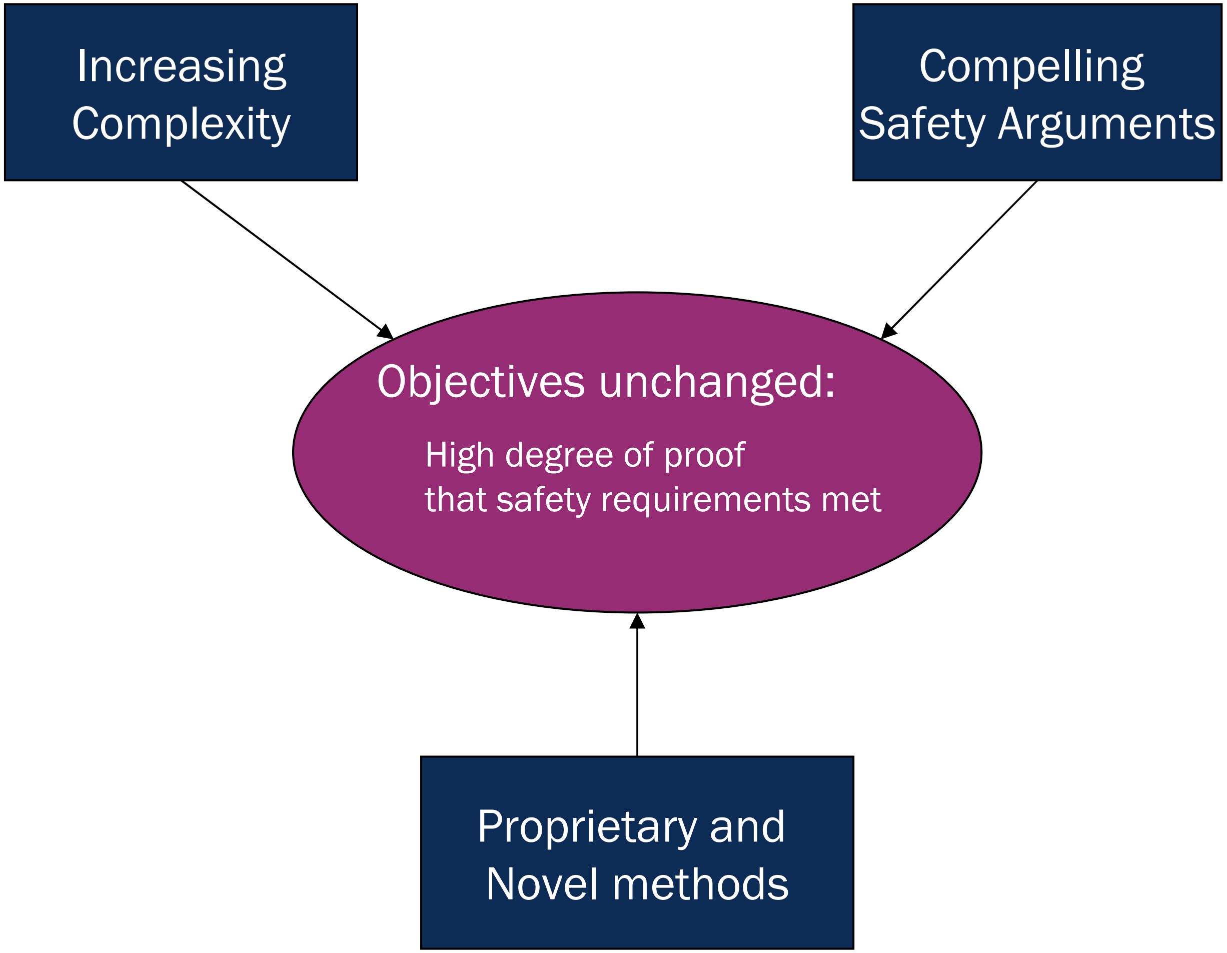
Problem solved

- Analyse, to justify to ISA, confirmed voting design to be vulnerable to single faults and common cause failure
- Design modified to remove specific inter-channel links, improve feedback design: greatly improved fault tolerance
- Found via early involvement with design, assess risk areas before design commitment
- One of several design improvements made during development as result of ISA challenge
- Robust system certified

Perpetual issues

- Safety risks arise at all levels:
  - Insufficient attention to cross-boundary risks and responsibilities
  - Difficult to get safety decisions made where cross-boundary issues
  - Assumptions made at all levels need to be challenged
  - Is the safety architecture adequate?
  - Is the implementation meeting the architecture requirements?
- Are all these risks being adequately assessed?

ISA in the modern context



Increasing Complexity

Compelling Safety Arguments

Objectives unchanged:

High degree of proof
that safety requirements met

Proprietary and Novel methods

The safety argument

- A safety case should present a compelling safety argument, not just a statement of compliance with standards
- Safety argument comprises a complex set of stronger and weaker arguments and supporting evidence, built over time
- A great deal of skill is required to construct and independently assess a sound and valid case for a complex system

ISA Adding value

Differences in interpretation can lead to conflict – these need to be identified and resolved

Need to flush out as early as possible

Need early agreement on use of novel methods

Provide a trusted escalation route in case of disagreement

The focus should remain on design for safety, supported by robust processes

Conclusions (1)

- Independent assessment must be performed with the capability to look at safety in the large and delve into detail
  - independence allows the focus to remain on designing in safety and mitigating risks
  - the design requirements, implementation and developing safety case must be scrutinised
  - rigorous processes must be assured

Conclusions (2)

- Risk-based ISA adds further value via
  - early identification of risks
  - early agreement on methods, design
  - facilitation of action to mitigate risks
  - systematic but risk-based assessment and auditing with clear evidential objectives

Praxis High Integrity Systems Limited

20 Manvers Street
Bath BA1 1PX
United Kingdom
Telephone: +44 (0) 1225 466991
Facsimile: +44 (0) 1225 469006
Website: www.praxis-his.com

Email: david.bradley@praxis-his.com