SAFETY SERVICES ORGANISATION

HAZARD LOGS & SAFETY CASES

SAFETY CASES

SAM CHURCHYARD – SENIOR CONSULTANT – SSO PE – JUNE 2023

RELEVANT DEFINITIONS

As defined in Def Stan 00-56:

- **Safety Case**: "A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment."

$\neq$

- **Safety Case Report**: "A report that summarises the arguments and evidence of the Safety Case, and documents progress against the Safety Programme."
  - A 'snapshot in time' of the current status of the safety case.

[1,2,3]

REFERENCES AND USEFUL DOCUMENTS

Useful documentation and resources:

- **DSA03 OME: part 1 OME Acquisition** (formerly JSP 520)
  - Available on gov.uk site: https://www.gov.uk/government/publications/dsa03-ome-part-1-ome-acquisition

[3,4,5,6,7]

CONTENTS – SAFETY CASES

Contents of this Lecture:

- Objectives of a Safety Case
- Why Safety Cases are considered good practice
- What evidence they should contain
- When they should be done in the lifecycle
- Safety Management Plans (SMP)
- Extent of the Safety Case
- OME review category
- OME specific contents
- GSN
- Assumptions, caveats and LoUs
- General warnings
- Review, ownership and acceptance

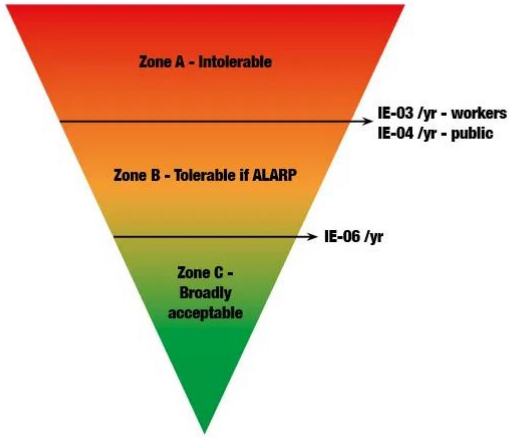
T

[8,9]

OBJECTIVES OF A SAFETY CASE

The purpose of a safety case is to:

- Document evidence that all risks are at least tolerable and ALARP.
- Document evidence that all safety requirements have been met.
- Describe the argument, with evidence, that the system is acceptably safe.
- It must also describe how the processes and assessments undertaken to reach that conclusion are sufficient.
- Provides documentary evidence.



The safety case report is created to tie all of this together, at a moment in time, to demonstrate that all safety activities and issues are at sufficient maturity.

[7,10,11]

OBJECTIVES OF A SAFETY CASE

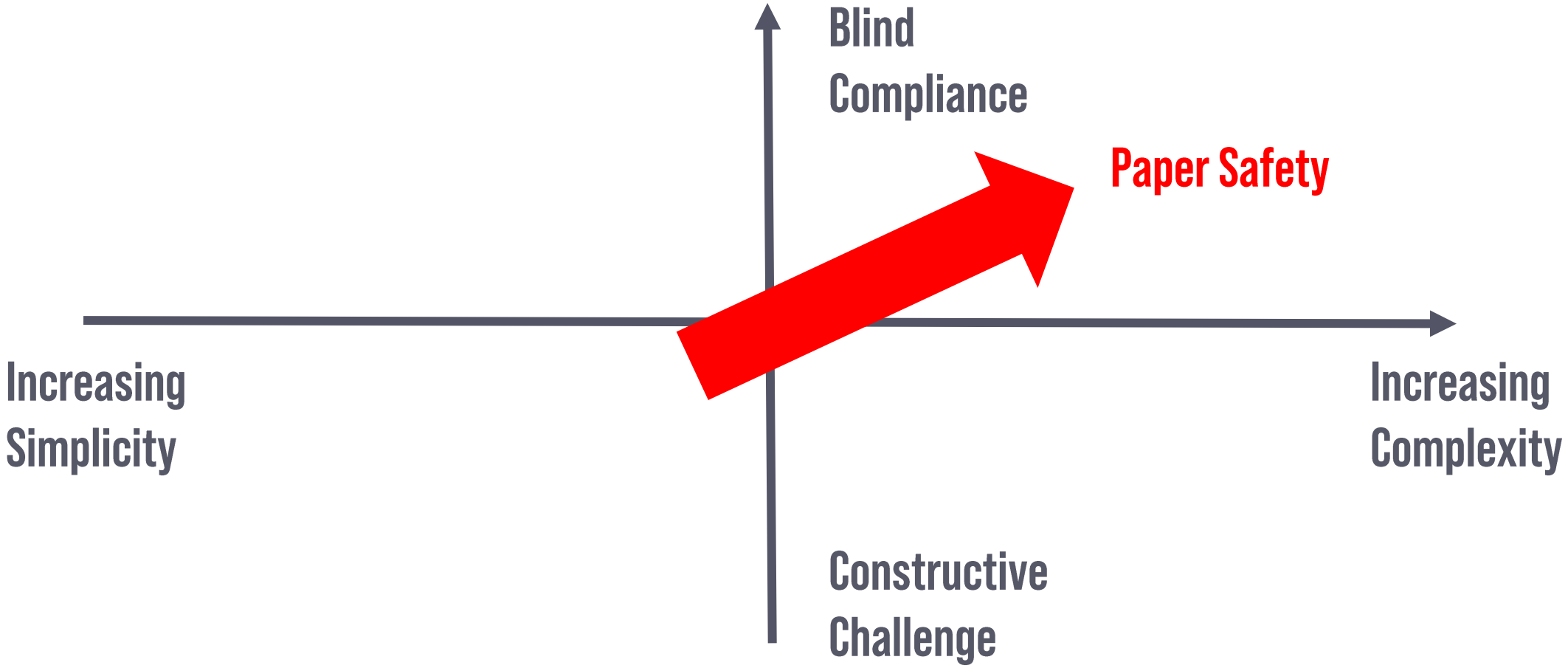
'Do the right thing'

Often in high hazard organisations 'doing the right thing' is put first and forefront which is obviously good.

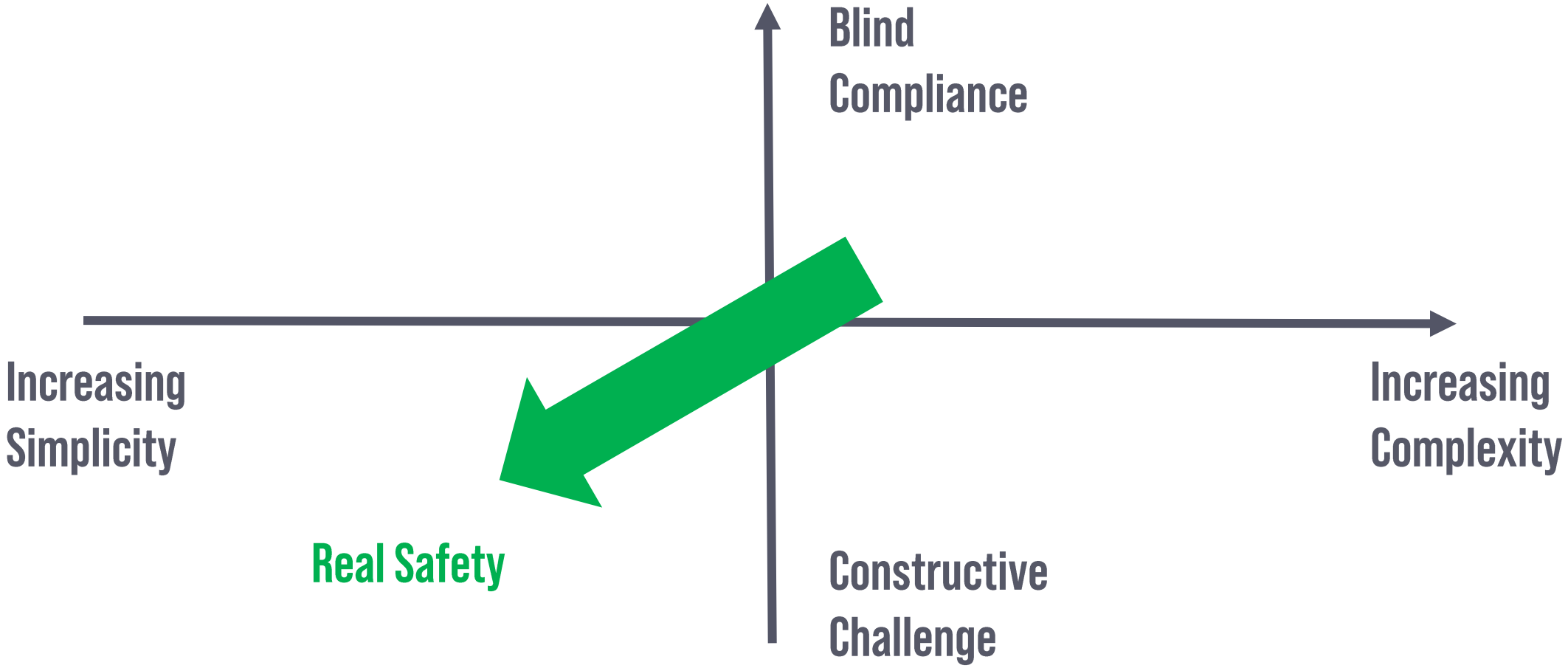
$$\sum_i \text{Reasonable}_i = \text{Unreasonable}$$

Unfortunately, many individually reasonable things can often, over time, lead to a safety case that is overly complicated and bureaucratic.

OBJECTIVES OF A SAFETY CASE



OBJECTIVES OF A SAFETY CASE



OBJECTIVES OF A SAFETY CASE

So how do we fix this?

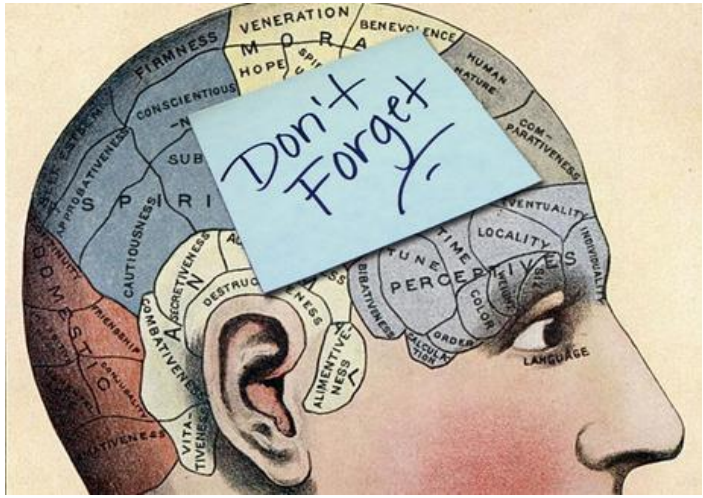
- From the Nimrod Review (Haddon-Cave QC):
  - Leadership
  - Independence
  - People (not process and paper)
  - Simplicity

1. Leaders *engaging* effectively with independent regulators early.
2. Leaders *empowering* their people by creating a culture of constructive challenge rather than blind compliance.
3. People *enhancing* simplified safety approaches that reduce complexity.
4. Regulators *expecting* simplified approaches that are fit for purpose.

SAFETY CASES AS GOOD PRACTICE

Safety Cases are considered best practice in many high hazard industries for the following reasons:

- Having effective Safety Cases reduces accidents.
- Allows a project to prioritise safety activities and allocate resource effectively.
- Improves corporate memory.
- Easily allows information to be applied to other systems and for lessons to be learnt for future projects.
- Good recording allows for engineering judgement to be used in safety decision making.



[7,12,13]

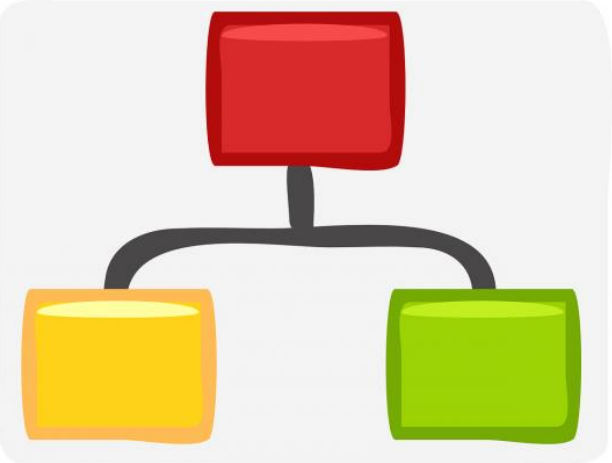
WHAT EVIDENCE SHOULD IT CONTAIN?

A Safety Case should argue and evidence the following key points:

- All safety requirements are suitable and met.
- The risk assessment is appropriate and suitably rigorous.
- The Safety Management System has been implemented correctly.

There are two types of safety evidence an SC should contain:

- Direct evidence – such as trials data, risk assessments, and calculations.
- Underpinning evidence – “measures that imply that the above are trustworthy” [27]



[7,14,15,27]

SAFETY CASES THROUGH THE LIFECYCLE

Point in Life Cycle – 'Gate'	Purpose of Safety Case
Initial Gate	Demonstrate that potential safety issues are understood and a strategy is in place to control them.
Assessment Phase	Document the safety merits, drawbacks and feasibility of options.
Main Gate	Weigh and eliminate options based on safety. Demonstrate the safety risks for the chosen option can be managed and controlled.
Demonstration & Trials	Demonstrate these activities can be undertaken safely, usually with additional controls.
Production	Demonstrate these activities can be undertaken safely. May also document how production will be controlled to ensure it does not degrade safety from the design.
System Acceptance	Demonstrate the system meets all its safety requirements.
User Trials	Demonstrate these activities can be undertaken safely, usually with additional controls.
Safety Submission for Hazards	Demonstrate that all hazards are managed iaw with MOD policy.
Introduction to Service	Demonstrate that the system is safe to use within its defined constraints. Also demonstrate that the facilities and management processes, such as training, maintenance regimes and logistics are sufficient to support safe use.
Disposal	Demonstrate disposal, or disposal strategy, can be conducted safely.

SAFETY MANAGEMENT PLAN (SMP)

"A document that defines the strategy for addressing safety and documents the Safety Management System [SMS] for a specific project."

The SMS is a little bit amorphous but is best thought of as:

'all that we do to ensure safety around here'

Depending exactly on your industry (e.g. general health and safety, OME, nuclear) there are different guidance documents that govern exactly what should be in an SMP.

Defence Safety Authority

SMPs can be written as stand alone documents, but can be incorporated in the Safety Case Report itself.

[3,17,18]

EXTENT OF THE SAFETY CASE

The depth and size of the safety case should be proportional.

A safety case should be scoped during the planning phase.

In this manner the amount of effort required for the safety assessment can be determined.

A safety case can range from a few pages long to multiple documents for more complex equipment.

There is no easy answer to this, judgement must be used!

[7,17,19,20]

OME REVIEW CATEGORY

As per DSA 03.OME Pt1 (JSP 520), it is necessary for an OME Safety Case Report to contain an OME Review Category.

The 5 review categories are:

- Credible Worst Case Consequence (40% weighting).
- System Maturity and Certification (10% weighting).
- Energetic materials (20% weighting).
- Munition Complexity and Integration (10% weighting).
- Perceived Public acceptability (20% weighting).

Review Category	Total Score
Low	< or = 5
Medium	> 5 and < 10
High	= or > 10

[7,17,19,20]

OME REVIEW CATEGORY

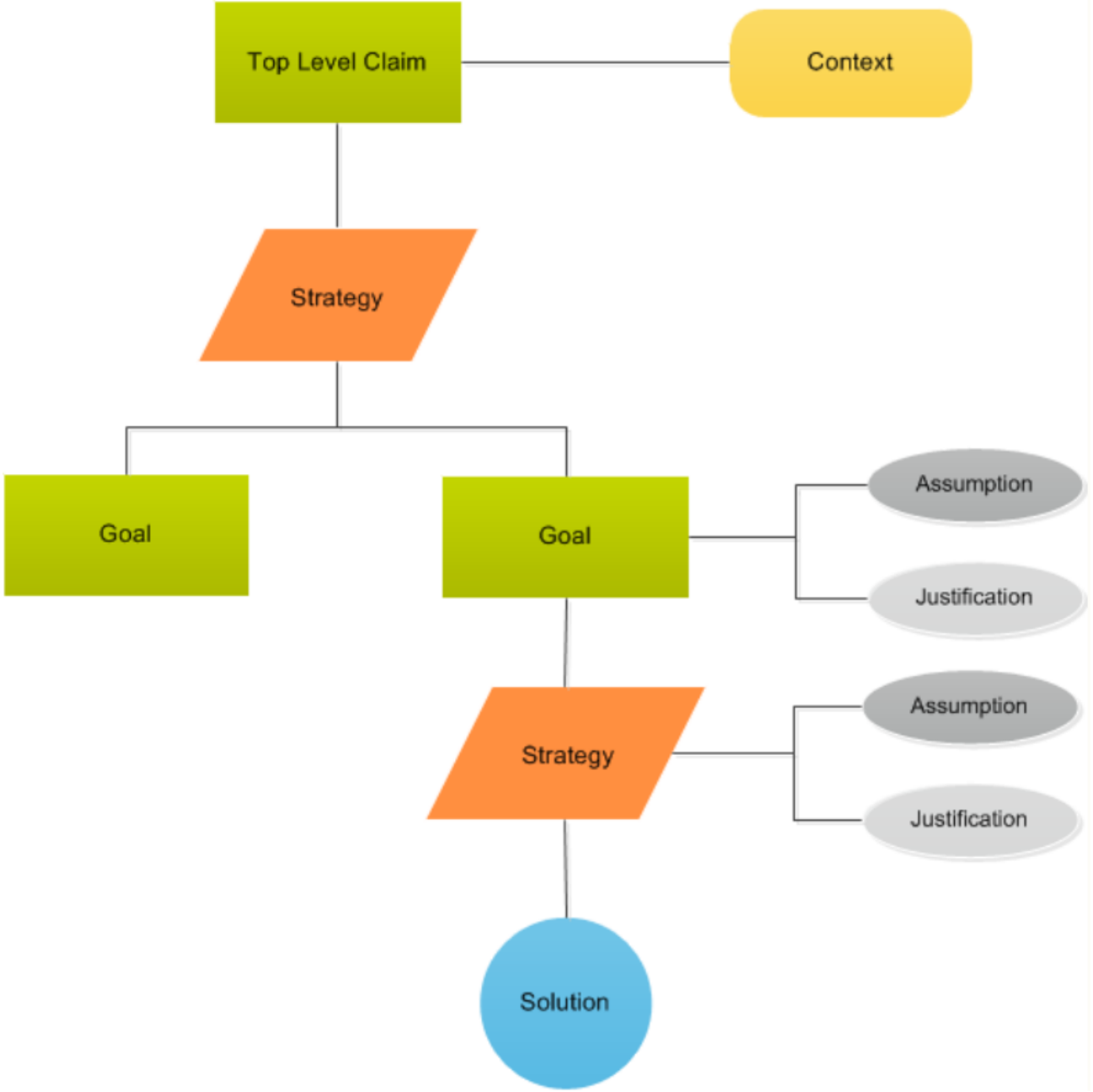
Factor	Review Level Indicators 16 14 12 10 9 8 7 6 5 4 3 2 1 0 Very Significant (Score 16 to 9)	Significant (Score 8 to 5)	Marginal (Score 4 to 2)	Insignificant (Score 1 to 0)	Score	Weighting	Weighted Score
4. OME Complexity and Integration	Complex OME (e.g. autonomous guided).	Complex OME (e.g. man-in-loop guided).	Non-complex but interacts with platform (e.g. decoy flare).	Non-complex (e.g. small arms ammunition).		0.1	
	Critical component new to military service.	Critical component new to UK MOD.	Similar to in-service items.	Identical to in-service items.			
	Safety Critical Software.	Complex Safety Related Software.	Simple Safety Related Software.	No Safety Related Software.			
	Significant OME / Platform integration issues – results in constraints in operation.	Significant OME / Platform integration issues – no operational constraints.	Simple OME / Platform integration.	No OME / Platform integration required.			
5. Perceived Public Acceptability	OME likely to provoke International TV Headline news. International implications.	OME likely to provoke headline national news and continuing local attention.	OME likely to provoke considerable local news with inside page national note.	OME likely to provoke no outside interest.		0.2	
TOTAL SCORE							
REVIEW CATEGORY (HIGH/MEDIUM/LOW)							

OME SAFETY CASE REPORT CONTENTS

The typical OME Safety Case Report will include:

- Part 1 – System Description
- Part 2 - Safety Requirements
- Part 3 – OME Review Category
- Part 4 – SMP
- Part 5 – Safety Assessment
- Part 6 – Disposal & Emergency Arrangements
- Part 7 – Operational Information
- Part 8 - Conclusions

GSN EXAMPLE



[7]

GOAL STRUCTURING NOTATION

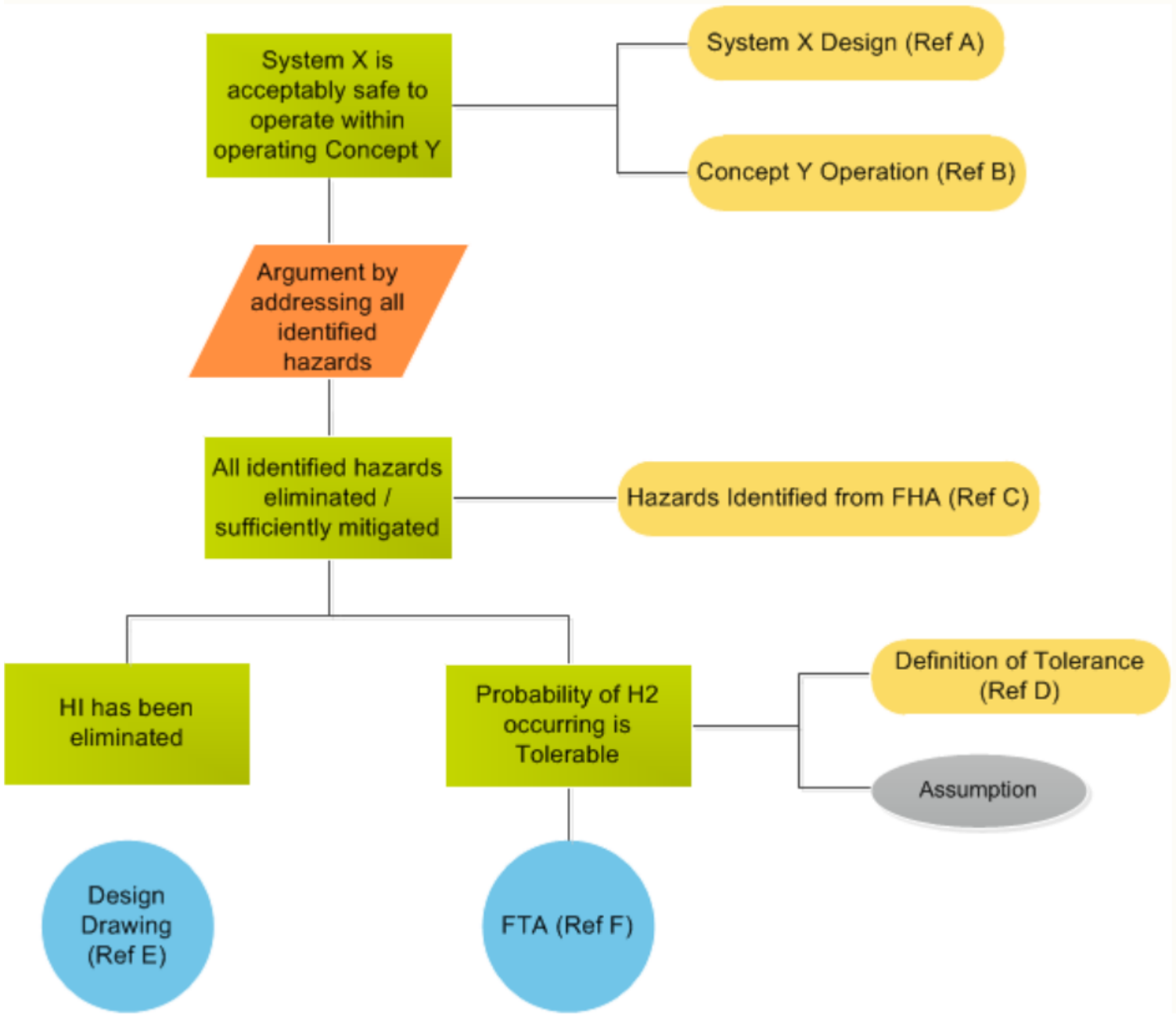
Goal Structuring Notation or GSN is a graphical means of representing an argument. Detailing an top-level goal at the top of the tree and breaking it down into sub-goals which can be directly evidenced.

It was developed from academic work on the nature of reasoning and the following 3 key elements:

- **Goal or claim**: refer to a property of the system i.e. “the weapon is acceptably safe”.
- **Evidence**: They support the goal or claim and can be facts, assumptions or sub-goals.
- **Arguments or strategy**: They link the evidence to the claim.

GSN EXAMPLE

Goal	A single positive statement of the objective acheived
Context	Statement/Reference which clarified contextual information in the claim/goal
Strategy	Description of the argument which explains the relationship between a goal and the set of sub-goals which describe why the writer believes the goal has been achieved
Solution	Reference to the information that supports the goal
Assumption	States why the strategy / goal is a solution
Justification	States any assumptions on which the strategy goal is based



[7]

HANDLING ASSUMPTIONS

Where there is no information it is acceptable to make assumptions but you must:

- Make it very clear an assumption is being made, when it is being made.
- Record all your assumptions.
- The Safety Case will rely on how credible these assumptions are so you should also:
  - Replace assumptions with evidence as soon as it becomes available.
  - Where this is not possible you must get your assumptions reviewed by stakeholders and subject matter experts.

[7,21,22]

CAVEATS & LOU

Where there is a lack of information and evidence but the project needs to progress, you can manage these gaps with safety case Caveats or Limitations of Use (LoU).

Example: The OME has not been subjected to vibration trials and so whilst it can be fired from a static vehicle for trials, it cannot be transported or fired on a moving vehicle.

Warning: They should not be used simply to rush the project through milestones, they need to be carefully considered and well thought out.

[7,23,24]

GENERAL SAFETY CASE WARNINGS

Unlike a lot of what I have spoken about, there aren't any real downsides to using the safety case approach. What follows are several pitfalls:

- The safety case is only as strong as the safety assessment.
- Include relevant authorities early.
- The safety case must be reviewed and updated regularly.
- Counter evidence should be gratefully included in the safety case.
- The safety case must be well documented and structured.

The Gordian Knot

[7,25,26]

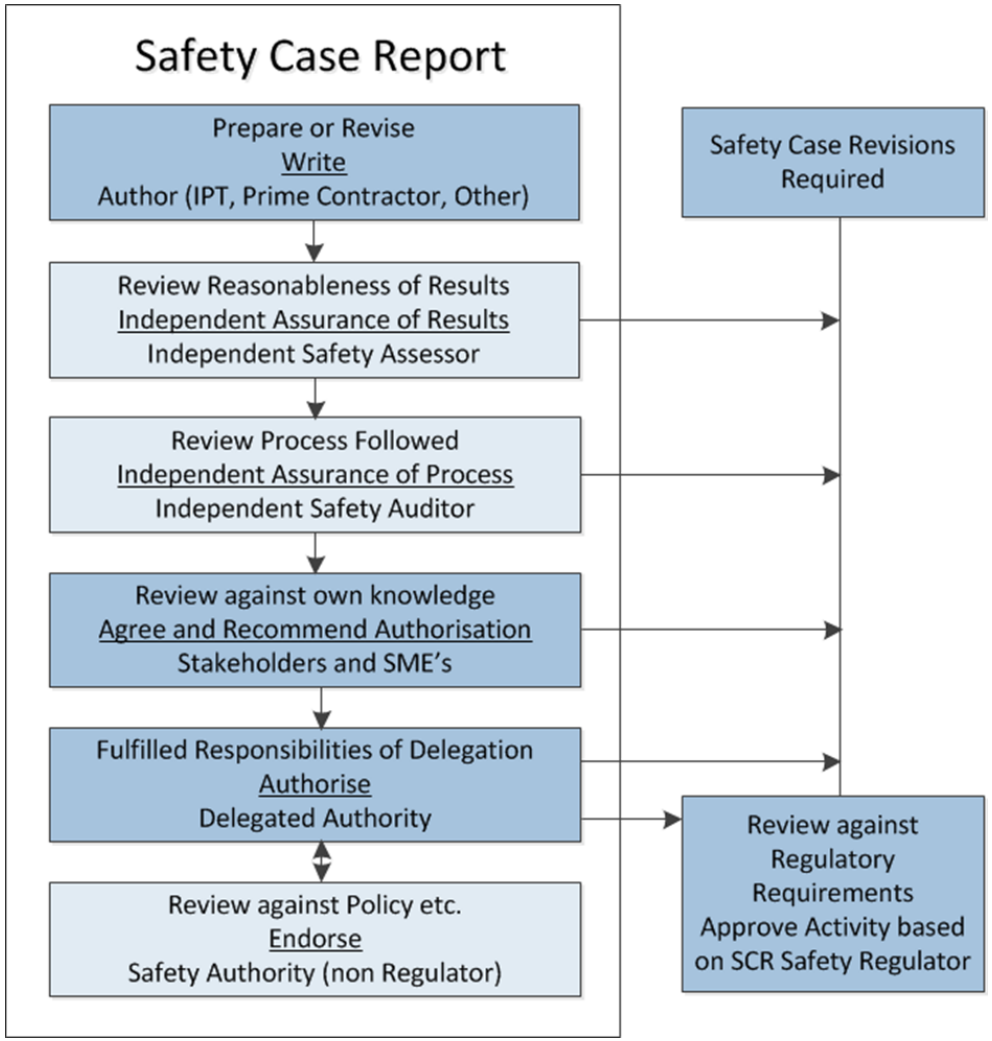
REVIEW, OWNERSHIP & ACCEPTANCE

The SCR should be reviewed and approved by the PSC, stakeholders and any independent assessors.

The Safety Delegation holder is the ultimate owner of the safety case.

It is possible that the safety case demonstrates the system is not acceptably safe.

Where the safety case meshes with other safety cases, there should be a clear hierarchy of safety cases.



NEXT STEPS...

That concludes the taught phase of the module!

REFERENCES

1. https://www.l-tron.com/How-to-document-a-crime-scene/
2. https://www.theverge.com/2020/2/12/21134272/nikon-d6-specs-price-release-date-announced
3. Def Stan 00-56: The standard for "Safety Management Requirements for Defence Systems".
4. https://www.kpcmhealthandsafetysigns.com/international-hazard-warning-symbol
5. https://www.repubblica.it/economia/2017/04/07/news/la_ue_cambia_i_simbol_sulle_etichette_rischio_discarica_per_molti_prodotti-162336907/
6. MOD Safety White Booklet: An Introduction to System Safety Management in the MOD Issue 4 Parts 1 and 2.
7. ASEMS Online POSMS - https://www.asems.mod.uk/guidance/posms
8. https://www.banham.co.uk/safes/what-to-consider-buying-safe/
9. https://www.wahl.co.uk/product/ultimate-case/
10. https://www.chemicalindustryjournal.co.uk/risk-and-tolerability-criteria-are-we-comparing-apples-and-pears
11. https://digitalagencynetwork.com/how-to-make-the-customer-journey-enjoyable/
12. https://www.psychologytoday.com/gb/blog/the-young-and-the-restless/201411/case-the-malleable-memory
13. https://www.changeboard.com/article-details/16963/decision-making-in-hr-and-recruitment-how-to-hire-the-right-candidate/
14. https://en.wikipedia.org/wiki/Bananarama
15. https://www.businessbullet.co.uk/business-analysis/the-hierarchy-of-requirements-and-how-it-impacts-requirements-gathering/
16. https://www.asems.mod.uk/sites/default/files/documents/SMP/smp12-g-02.pdf
17. DSA 03. OME Part 1 (Formerly JSP 520) – Defence Code of Practice (DCOP) for OME Acquisition. Defence Safety Authority, MOD. V1, 30/04/2020.
18. https://www.pinterest.co.uk/pin/325948091764656917/
19. http://www.mmvg.net/vehs.html
20. https://en.wikipedia.org/wiki/Trident_(missile)
21. https://www.saga.co.uk/magazine/money/personal-finance/making-money/selling-old-vinyl-records
22. https://www.bluecorona.com/blog/fake-google-reviews/
23. https://www.thinkdefence.co.uk/2011/12/uk-military-bridging-equipment-assault-bridging/
24. https://www.amazon.co.uk/PK-Supplies-Gaffa-Tape-Black/dp/B000KHDXZW

REFERENCES

25. https://www.pinterest.co.uk/pin/510947520195407876/

26. https://twitter.com/smallguybjj

27. P G Bishop, R E Bloomfield and P K D Froome. Justifying the use of software of uncertain pedigree (SOUP) in safety-related applications. Prepared by Adelard for the Health and Safety Executive. CONTRACT RESEARCH REPORT 336/2001. CRR336/2001: Justifying the use of SOUP in safety-related applications (hse.gov.uk)

28. Simplifying Safety. V0.3. Professor Andrew Sherry.

THANK YOU FOR LISTENING

ANY QUESTIONS?

SAFETY SERVICES ORGANISATION