# Safety Case Workshop

14-15 January 2014
A-P-T Research, Huntsville, AL

## Background

At the 2013 International System Safety Conference (ISSSC), the SAE International G-48 System Safety Committee accepted an action to investigate the utility of the Safety Case approach vis-à-vis ANSI/GEIA-STD-0010-2009. APT offered to organize and host a workshop for that purpose. Leaders in the field were invited to present at the workshop, and a panel was selected, led by Moderator, John Frost. Panel presenters included Dave West, SAIC; Don Swallom, U.S. Army AMCOM; John McDermid, Professor of Software Engineering at the University of York, UK; Barry Hendrix, Lockheed Martin; Dr. Homayoon Dezfuli, NASA; Robert Schmedake, Boeing; and Tom DeLong, A-P-T Research, Inc.

## Scope

To identify the best relative approach to benefit the system safety discipline and make a recommendation to the G-48 Committee in a continuation to define the best practices of system safety. Approaches reviewed and the findings of each are summarized below.

## Safety Cases: Purpose, Process, and Prospects

The basic concepts and processes of the Safety Case approach were briefed by John McDermid, University of York, UK. The basic elements of an effective system safety program defined by the Ministry of Defence (MoD) are shown in Figure 1. A Safety Case is defined as, "A structured argument supported by evidence, which provides a comprehensive and compelling case that a system is safe to operate in a given scenario." These arguments are defined at the beginning of a program to establish safety requirements which need evidentiary support to eventually conclude that the system is adequately safe.

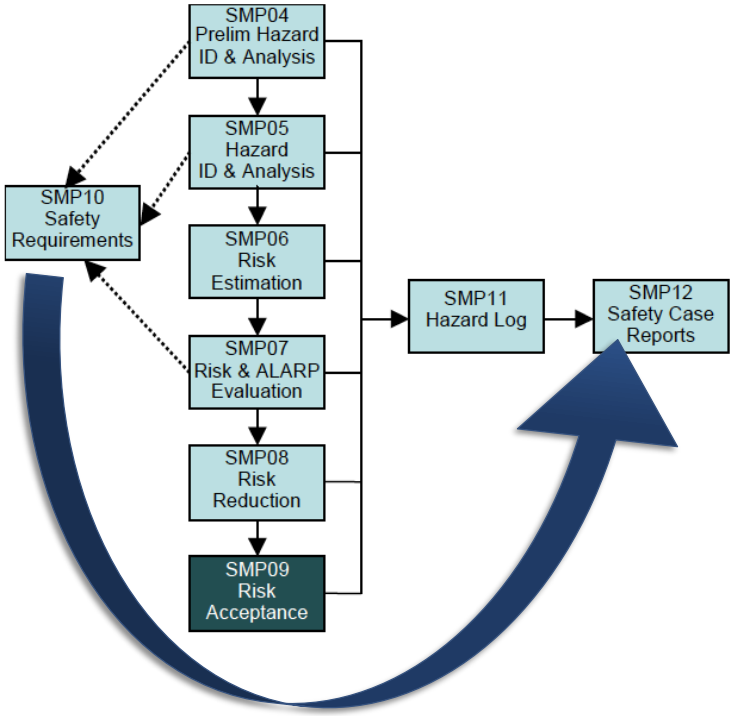



Figure 1. Safety Case Approach

The complete briefing is available at Appendix B.

## Findings

Comparison of existing ANSI-STD-0010 and MIL-STD-882 techniques found that the Safety Case approach includes the most critical elements of these approaches, as mapped by Figure 2.

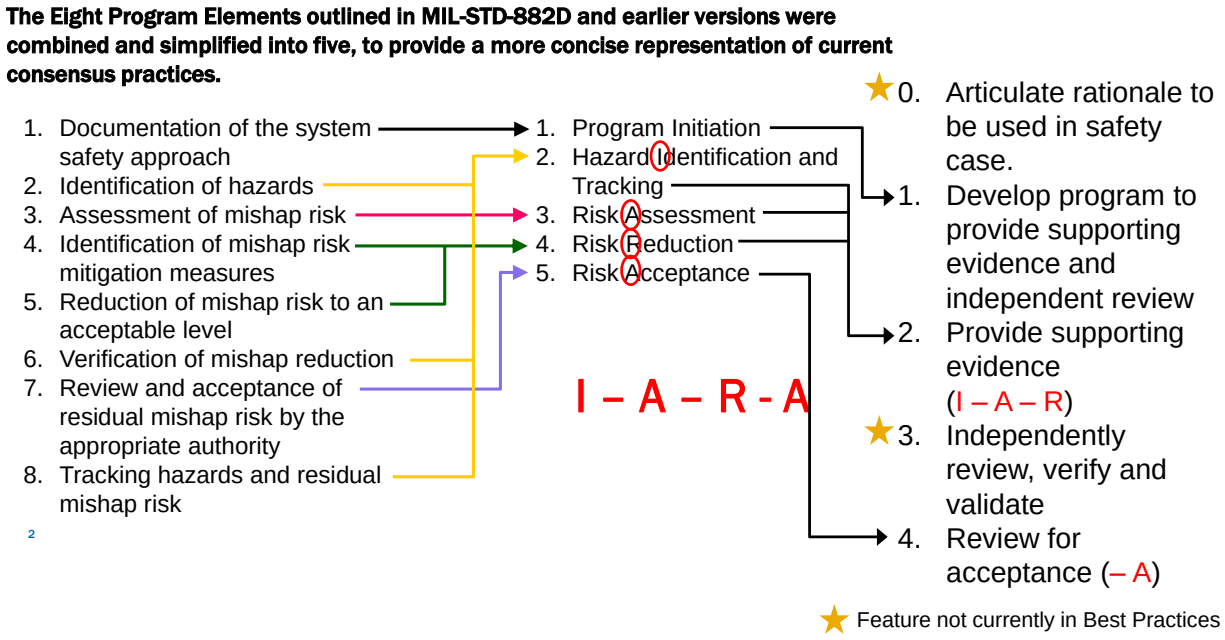



Figure 2. Traceability has been defined between ANSI-STD, MIL-STD, and Safety Case Approach

The structure, evidence-based approach to satisfying the safety arguments established at the start of the program offers benefits that were not included in other techniques. The benefits and observations identified with the Safety Case approach are summarized in Table 1.

Table 1. Strengths and Observations

| Strengths | Observations |
|---|---|
| 1. Includes clear, early definition of most compelling issues | Not included in ANSI or 882 |
| 2. Burden of proof is on the provider | |
| 3. Provides a baseline (normalcy map) for safety of the system | |
| 4. Explicit argument tying objective and robust evidence to support proof of claim | |
| 5. Essential narrative communicates effectively to decision makers, to risk takers, and to other stakeholders | |
| 6. Requires robust evidence to support key decisions (e.g., to operate systems) | |
| 7. Explicitly addresses the needs of the decision maker deciding whether to accept a system/permit a system to proceed to the next phase of development, or going to operation | |
| 8. The approach is highly tailorable to fit the need for evidence and the complexity of the system | All safety processes are tailorable; however, this seems to be more so because the arguments are unique to the decision |

| Strengths | Observations |
|---|---|
| 9. Inclusion of independence in review of the case (claims, arguments) | Not included in ANSI or 882 |
| 10. Evidence and independent review can aid in risk acceptance phase | Review panels or experts will develop consistent rules |
| 11. Encourages multiple approaches to capture evidence/facts, vs. assumptions | Existing SARs may not include all supporting evidence. |
| 12. Promotes a comprehensive assessment of the positive safety aspects of a design but does not overlook the negative aspect of the design | Fills potential gaps in 882 |
| 13. Facilitates incorporation of methods, processes, and tools from all existing sources | Freedom for broad tailoring |
| 14. Enables development of risk acceptance criteria in context of overall system risk | Enables focus on overall system level risk and does not mandate individual hazard risk assessment code |
| 15. Visibility of progress toward achieving and demonstrating safety objectives | Serves as a roadmap for the program manager |
| 16. Derived safety requirements from the statement of the arguments and hazard analysis can be put into systems engineering earlier than is currently being done | |
| 17. Earlier visibility of shortcomings (e.g., gaps in evidence) and understanding significance | |
| 18. International standardization of safety methodology | Save costs on multi-national programs |
| 19. Facilitates a holistic view of complex systems knowing that safety is an emergent property | |
| 20. Supports legal defense | List of hazards can impede legal defense |
| 21. Encourages system safety approach to become more evidence based as opposed to product-or-process driven | |
| 22. Is compatible with and unifies otherwise potentially fragmented system safety processes and approaches | |
| 23. Encourages systematic attempt to identify where claims may not be satisfied | |
| 24. | This method requires expertise in the system domain of the developed system |
| 25. | Requires up front work and may make reuse of prior analysis problematic. |
| 26. | Requires training and implementation strategies |
| 27. | Requires oversight (extensive) by qualified practitioners. |

An idealized concept of what should be included in the Safety Case approach was developed as, shown in Figure 3.

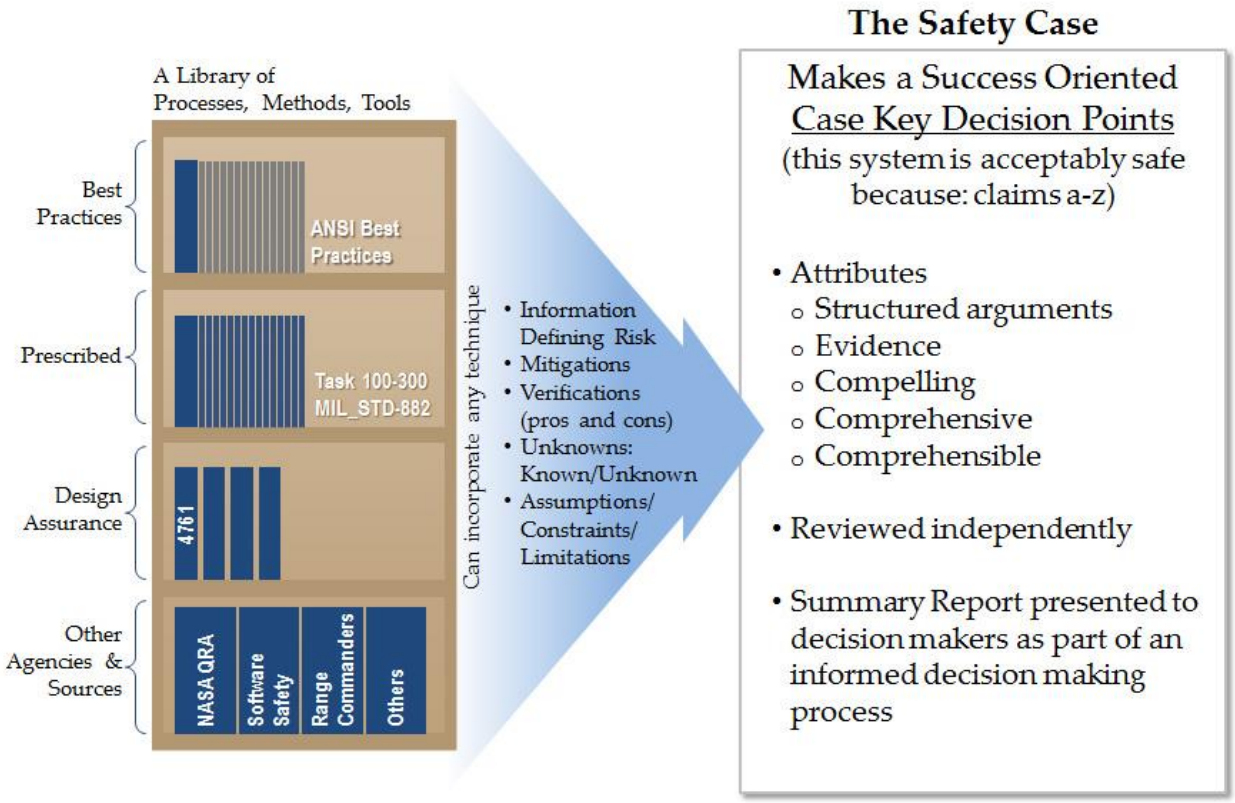



**Figure 3. What is the Safety Case ~ An Evidence Based Approach. Ideally, a Safety Case makes success oriented safety arguments, that are reviewed independently leading to risk informed decisions.**

## Recommendations

The workshop recommends that the G-48 Committee take steps to fully embrace the Safety Case approach as a recognized "best practice." It is also notes that multiple U.S. organizations, including NASA, major aerospace companies, and the Chemical Safety Board are already embracing the Safety Case approach.

Further, the workshop recommends that key features of the Safety Case approach be incorporated into existing approaches documented in ANSI/GEIA-STD-0010. These features include:

- Early identification of arguments required to demonstrate that a system is adequately safe.
- Development of compelling and comprehensive evidence to underpin the claims of safety.
- Independent review by qualified expertise prior to risk acceptance decisions.
- Incorporation of the evidence that the claims have been substantiated in safety assessments of the system.

# Appendix A: Approaches Reviewed

## The ANSI Process for System Safety Assurance - Dave West

The background and principles of the ANSI Standard (ANSI/GEIA-STD-0010-2009) developed by the G-48 were presented. The primary focus of this document was to simplify work elements and process flow, modernize the risk assessment matrix, and to introduce risk summing. The basic elements of an effective system safety program defined by the ANSI standard are shown in Figure 4.

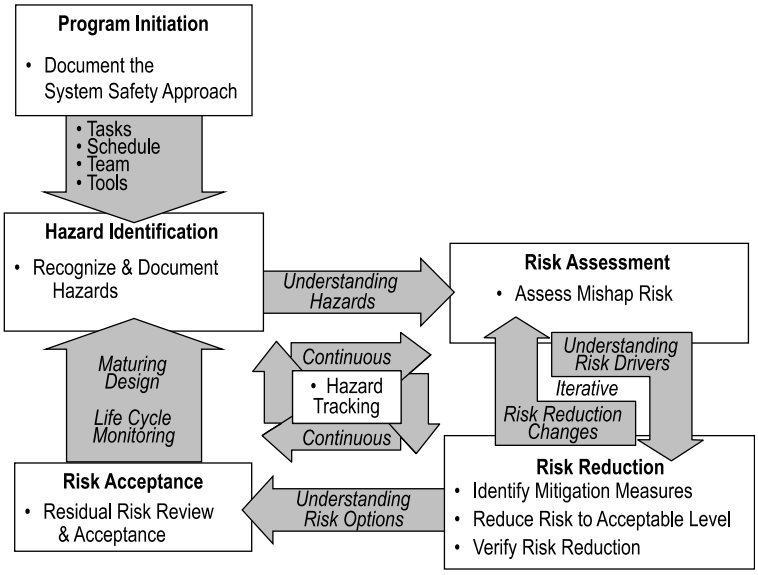



Figure 4. ANSI System Safety Approach

## The MIL-STD-882 Process – Don Swallom

The principles of MIL-STD-882E were presented by Don Swallom. The basic elements of the standard were briefed, as well as background information on the standard. The basic elements of an effective system safety program defined by the MIL-STD-882 are shown in Figure 5.

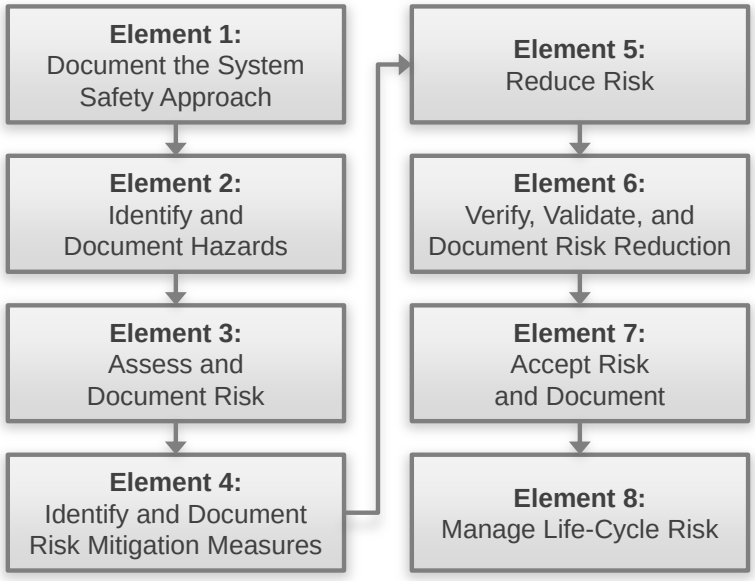



Figure 5. MIL-STD-882E System Safety Approach

## SAE ARP 4761 Process – Barry Hendrix

The SAE ARP 4761, SAE ARP 4754, IEEE STD 1228, and DO-178 process was briefed by Barry Hendrix. This document focuses on complex aircraft systems and the development of safety assessments which lead to certifications. The basic products include a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA), and System Safety Assessments (SSA). Residual risk is not part of ARP process as requirements must be met with few exceptions. The safety processes associated with aircraft systems are summarized in Figure 6.

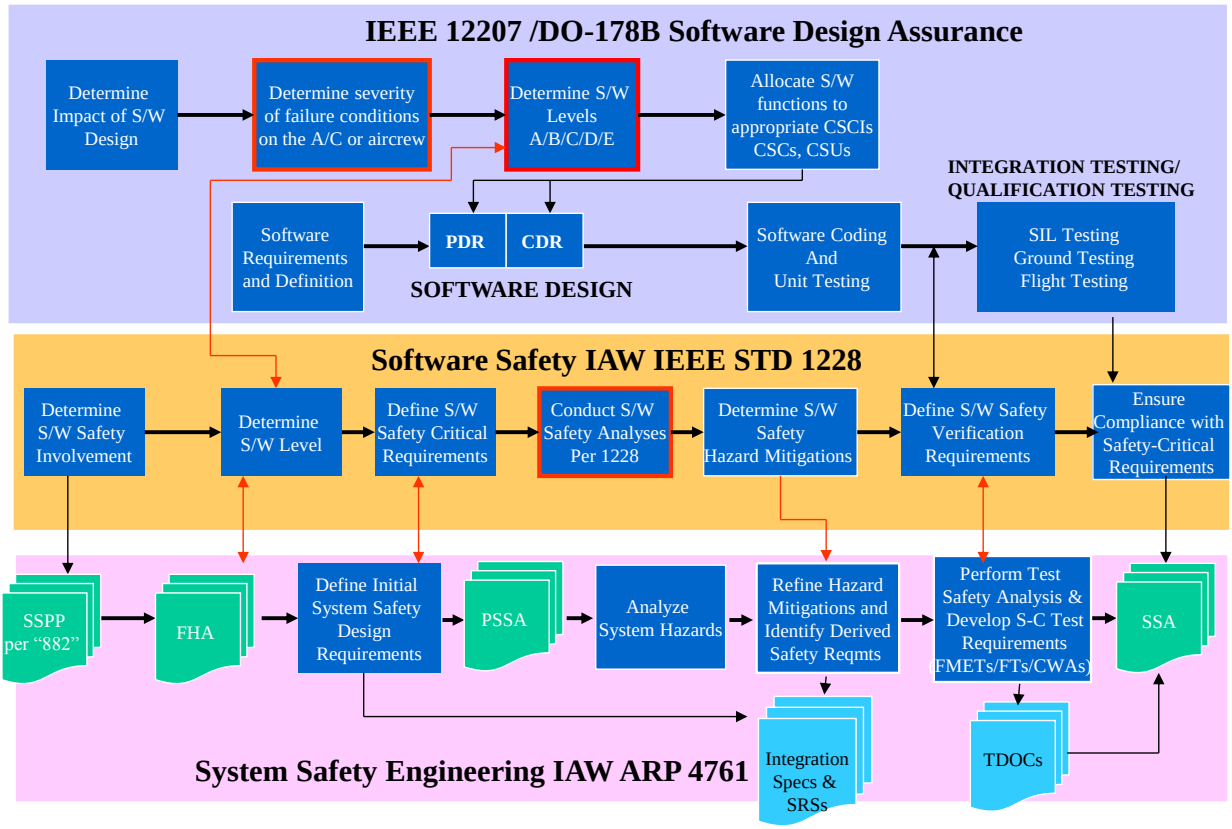



Figure 6. Top Level System Safety Process used by ARP

## Application of "Safety Case" at NASA – Dr. Homayoon Dezfuli

The NASA evolution of system safety and risk management, and the current thinking regarding system safety was presented. The NASA System Safety framework documented in NASA/SP-2010-580 is shown in Figure 7.

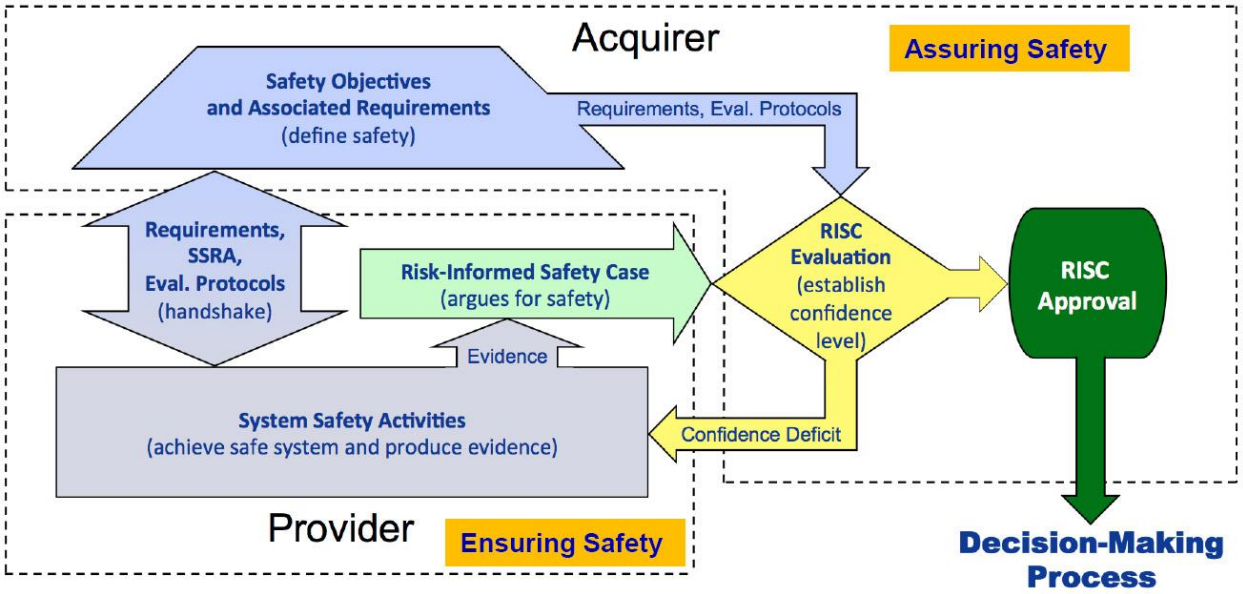



Figure 7. NASA System Safety Framework

Of note was a concept of how to account for Unknown/ Underappreciated (UU) risks. NASA recognized the need to consider the gap between the known risk and actual risk when applying safety thresholds and goals. The concept of safety performance margin is used to account for UU risks. This provides a rational basis for deriving verifiable requirements on known risks.

## Safety Case and Software Development – Robert Schmedake

The Safety Case approach and how it can be used in software development was discussed. Current methods in the standards are not bad; however, they are not sufficient in terms of software. The advantages of using the Safety Case approach include: defining explicit claims for the safety design up front; giving safety claims to build an argument; and providing evidence (analysis, inspection, demonstrations, and tests) to support the claim. The disadvantages include: the requirement for expertise in the system domain of the developed system. Also, it can make the reuse of prior analysis problematic since the original case would be specific to the original system context.

## Comparison of Methods – Tom DeLong

The various methods were summarized and discussed by the group. It was noted that in the United States, NASA and the FAA are going toward the Safety Case approach.

In the U.S., the Safety Assessment Report (SAR) comes closest to the Safety Case approach; however, a Safety Case is broader in scope than the SAR. A Safety Case is a structured argument, supported by evidence, which provides a comprehensive and compelling case

that a system is safe to operate in a given scenario. When compared to a SAR, the biggest difference is the use arguments and associated evidence to justify them.

When looking at U.S. Army systems, safety processes that seem to be working best include fuses, ignition systems, and insensitive munitions. These systems have rather complete requirements which are included in contracts, well defined processes to meet the requirements and demonstrate compliance, and a designated group of experts to validate compliance. The safety case approach can provide the same benefits for a broader group of material.

The Safety Case approach is a structured way of showing the work done on the safety program and highlights the importance of an independent evaluation group.

By defining arguments at the beginning of a program, safety could become the advocate rather than the protagonist. This approach could change the profession in profound ways by providing a positive front loaded approach.

## Appendix B: Safety Cases: Purpose, Process and Prospects

SAFETYCASE
WORKSHOP

# Safety Cases:
## Purpose, Process and Prospects

John McDermid, OBE FREng
University of York UK

# Outline

- Safety cases
  - Basic concepts
  - Purpose(s)
- Process
  - Used for system acceptance
  - Used for argument construction
- Prospects
  - Better safety cases
  - Integration of approaches
- Conclusions

# Safety Case Concept

- A safety case is:
  - A structured argument, supported by evidence, which provides a comprehensive and compelling case that a system is safe to operate, in a given scenario
- Compared to a safety assessment report (SAR)
  - Big difference is the argument (in the sense of a justification)
  - But what might we argue?

# Possible Arguments

- Examples might be
  - Completeness and quality of hazard identification
    - Including use of skilled people
  - Appropriateness of risk reduction
    - Including proper use of (MilStd 882) priorities
  - Tolerability of risk
    - More than just acceptance by authority, e.g. ALARP or cost-benefit analysis

In general, things which are often *implicit* in a SAR

# Purpose(s)

- Safety cases can be used for many purposes
  - Sub-systems rather than systems (like SSAR)
  - Through the process, e.g. preliminary safety case
    - Initially just the argument, to see if it would be acceptable if it could be supported by evidence at the end
  - Different roles
    - Overall system, e.g. aircraft, safety case
    - Integrated view, e.g. system of systems
    - Operational, e.g. for a mission

  Focus, for now, on system acceptance

# Safety Case and Reports

- A safety case is too big to deliver
  - No aircraft could lift its own (paper) safety case
- A safety case report is
  - A document which summarises the arguments and evidence of the safety, and documents progress against the safety programme
  - Really two roles
    - Deliverable summarising (final) safety case
    - Progress reports, including evidence generation

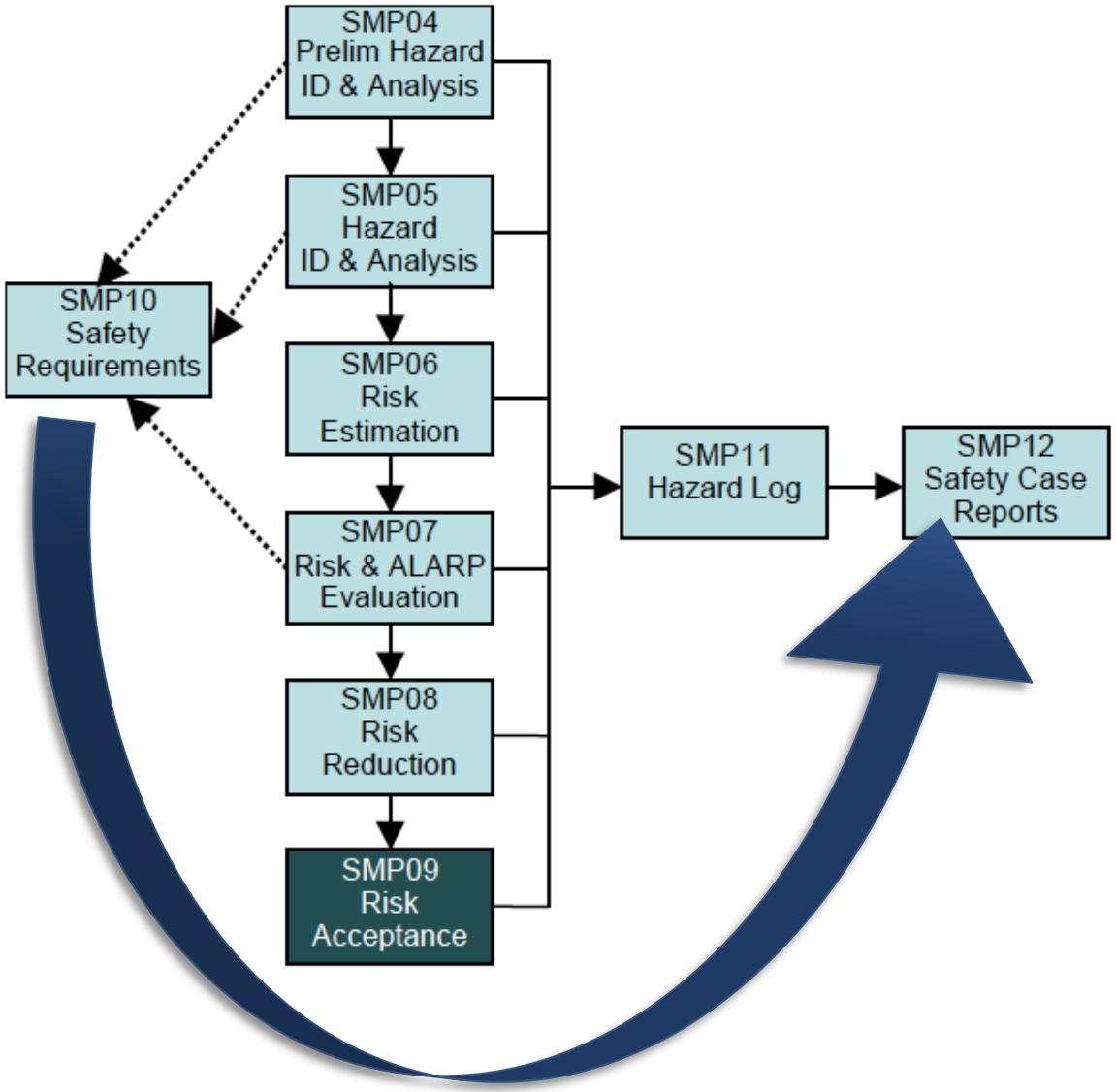
# Outline

- Safety cases
  - Basic concepts
  - Purpose(s)
- Process
  - Used for system acceptance
  - Used for argument construction
- Prospects
  - Better safety cases
  - Integration of approaches
- Conclusions

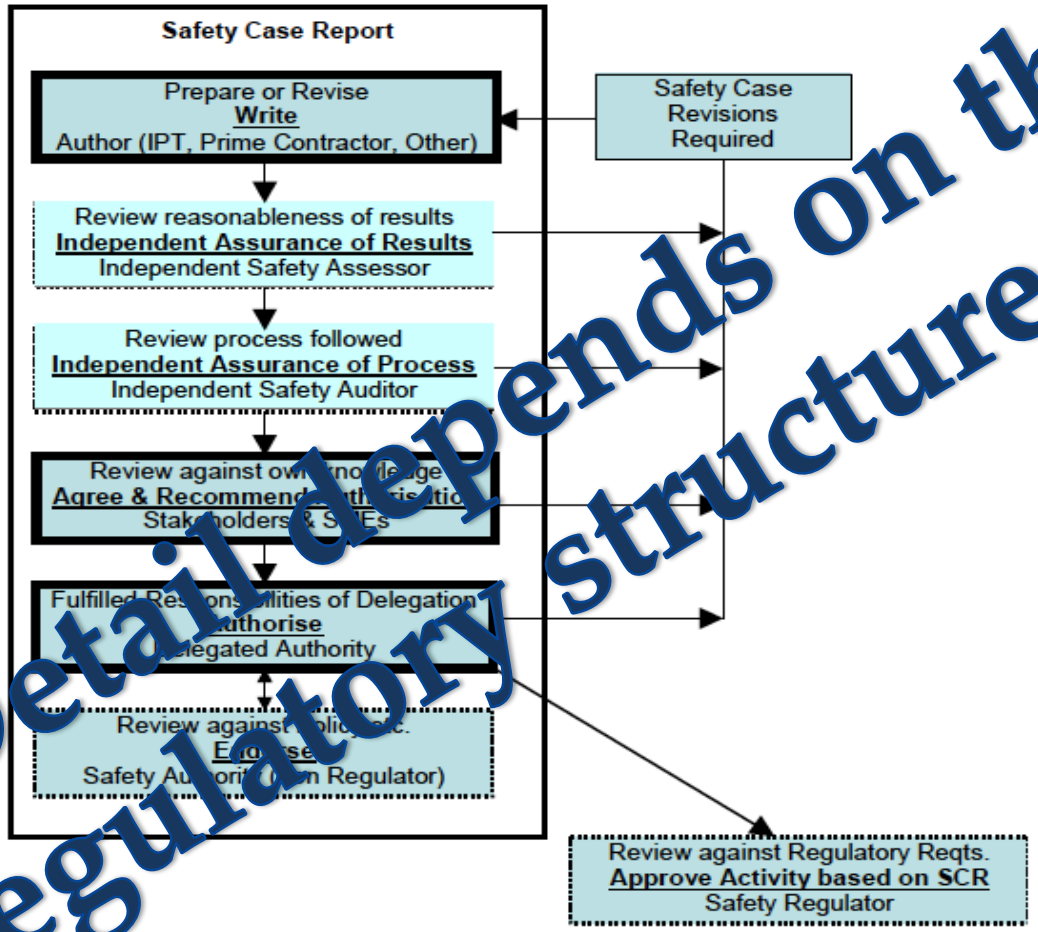
# MoD Process

- The MoD process is focused on acceptance
  - Used as an illustration as it is probably the closest approach to US DoD practices
    - Focuses on safety case report at the end
    - In practice, earlier drafts issued
  - Could also support uses in other domains
  - References to SMP are to Safety Management System Procedures out of MoD's POSMS (Project Oriented Safety Management System)

# Role of (Final) Safety Case

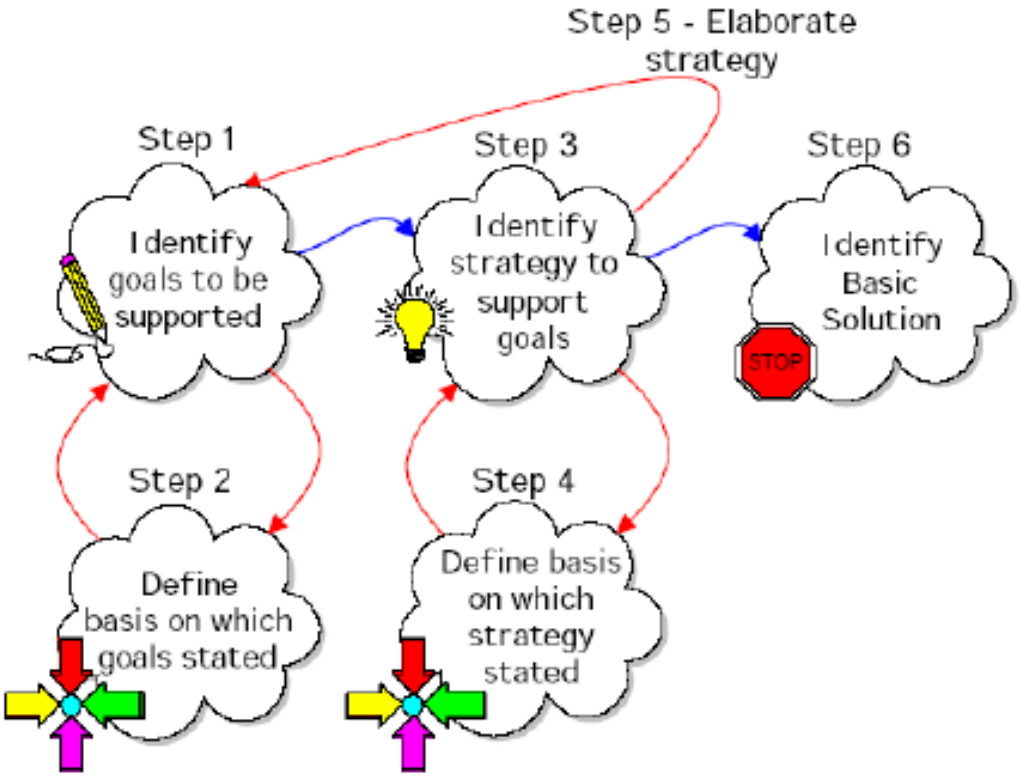


# Safety Cases and Reports




Detail depends on the regulatory structure, etc.

# Argument Construction Process (1)



# Argument Construction Process (2)

- The "process" is quite judgmental
  - Not unusual in safety engineering
  - Hence easy to do it wrong
  - Not very much guidance on "good practice'
- Available guidance
  - Some published "argument patterns"
    - Typical approaches, e.g. argument over hazards
  - Tim Kelly's thesis

    And see later

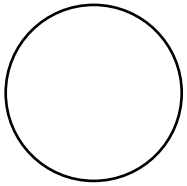
# Typical Safety Case Contents

- Following are key elements of most standards:
  - Scope
  - System Description
  - System Hazards
  - Safety Requirements
  - Risk Assessment
  - Hazard Control / Risk Reduction Measures
  - Safety Analysis / Test
  - Safety Management System
  - Development Process Justification
  - Conclusions

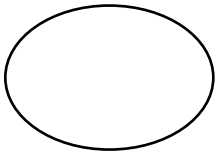
# Goal Structuring Notation

- Purpose of a Goal Structure
  - Diagrammatic notation to make argument clear

To show how **goals** are broken down into sub-goals,

and eventually supported by evidence (**solutions**) 

whilst making clear the **strategies** adopted,

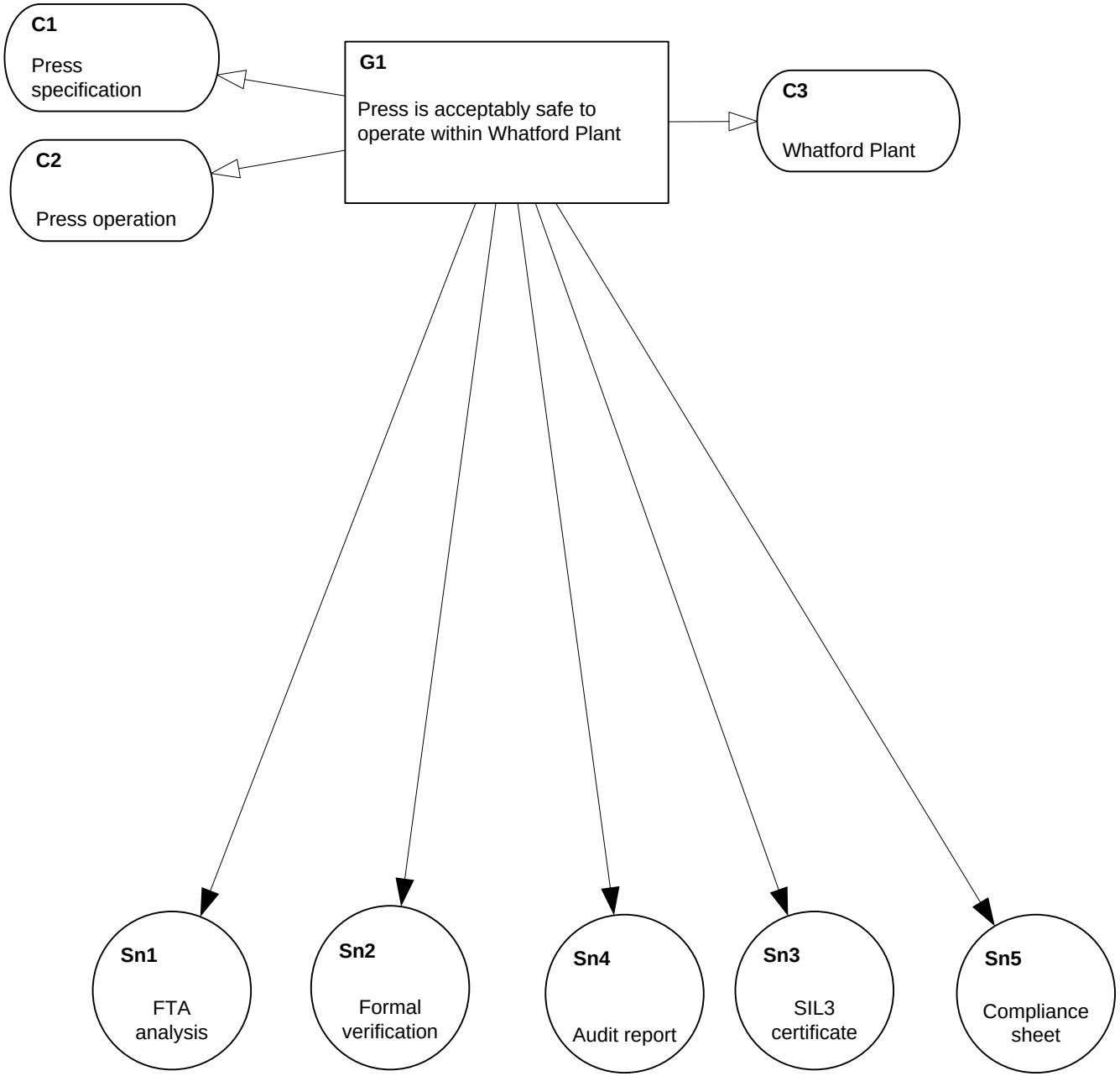
the rationale for the approach (**assumptions**, **justifications**)  **A/J**

and the **context** in which goals are stated

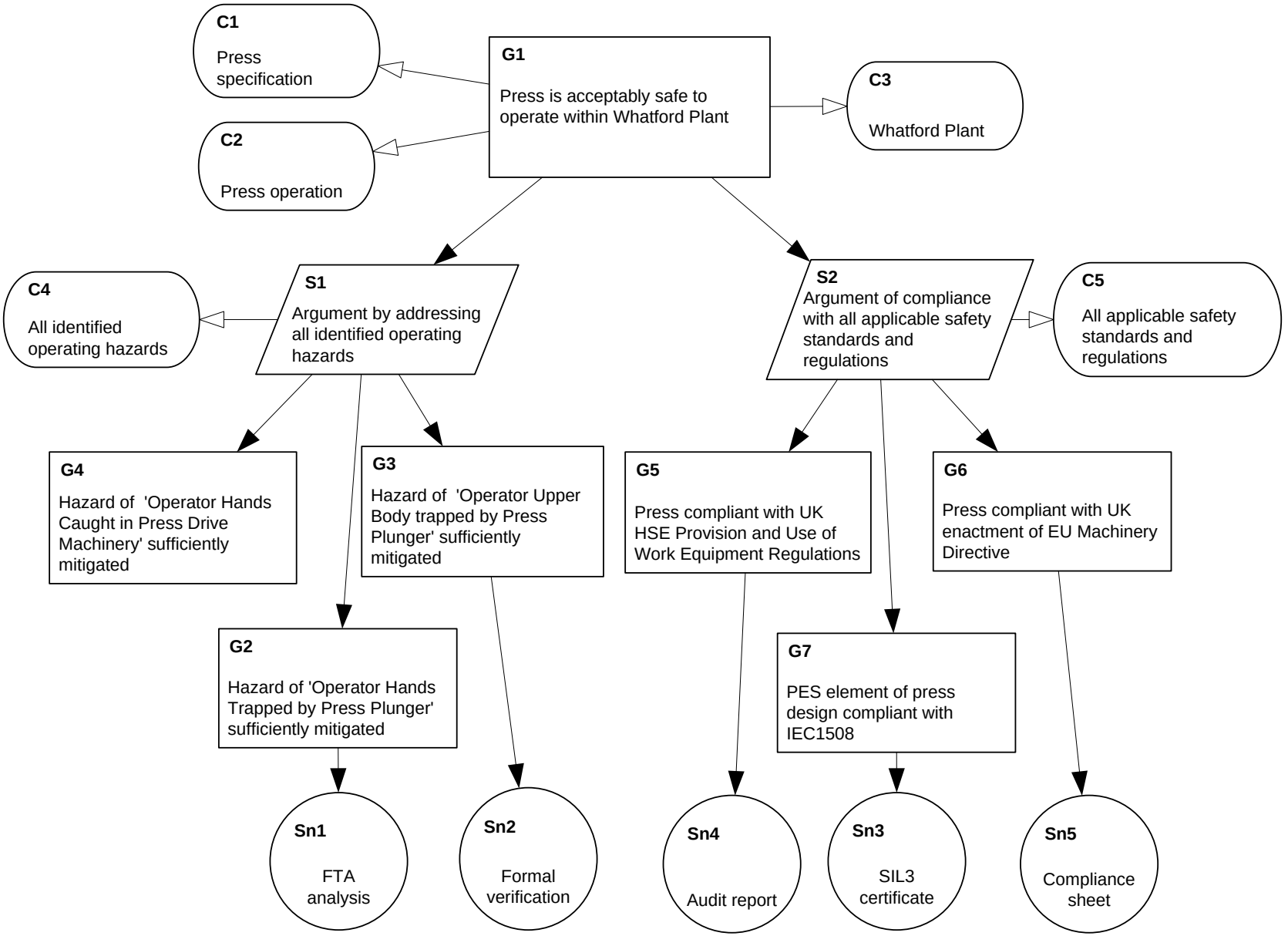
# Simple Example

- Example based on a hypothetical factory situation
  - Assumed to be at a town called “Whatford” in the UK
- The factory contains a metal press
  - Presses sheet steel to make car body parts
  - Has a single operator who inserts metal sheets and removes parts
  - Interlock to protect operator

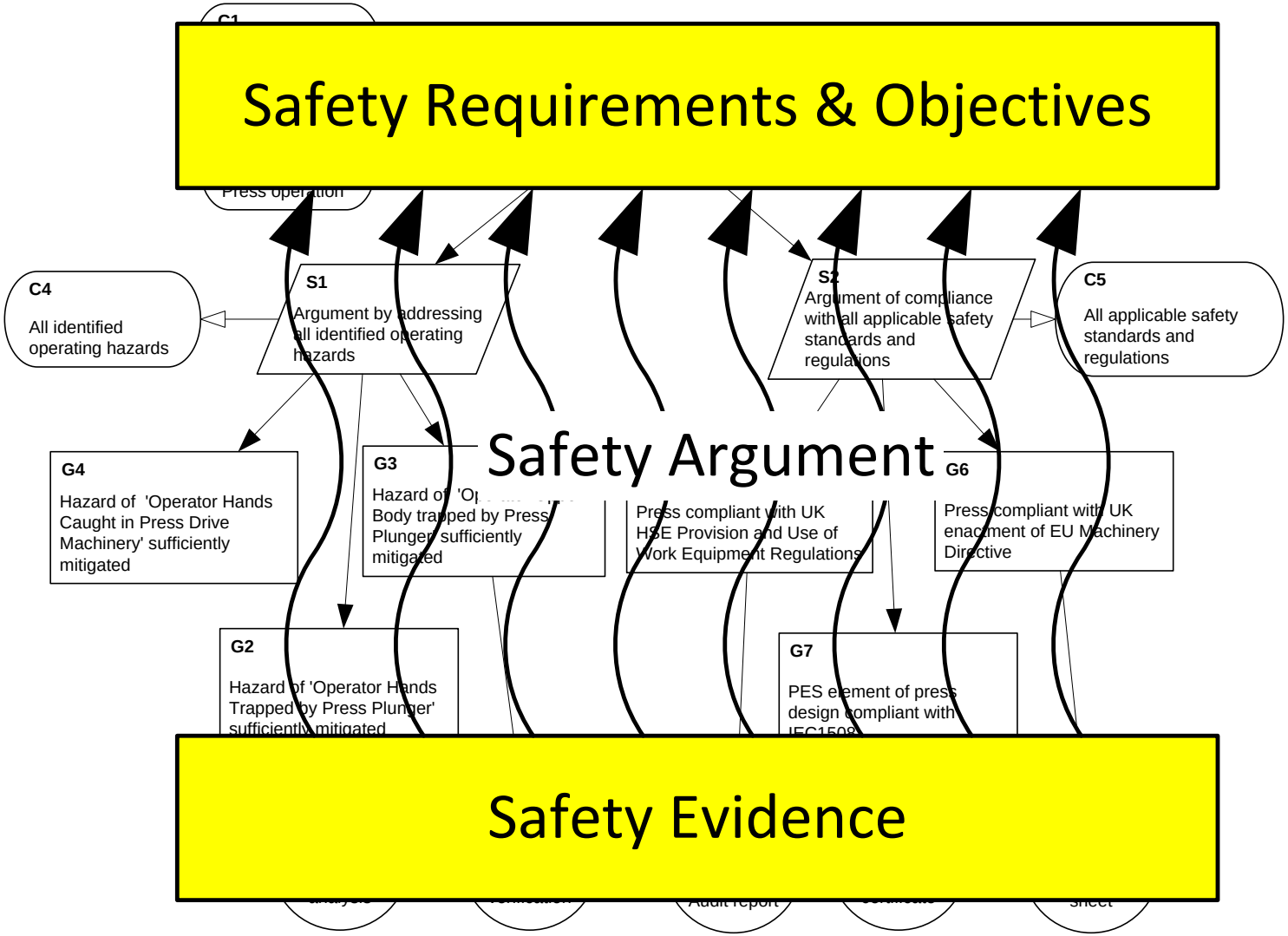
# A Simple Goal Structure



# A Simple Goal Structure



# Simple Goal Structure



# Outline

- Safety cases
  - Basic concepts
  - Purpose(s)
- Process
  - Used for system acceptance
  - Used for argument construction
- Prospects
  - Better safety cases
  - Integration of approaches
- Conclusions

# Better Safety Cases

- Learning from experience
  - Nimrod XV230 is salutary
- Pragmatism
  - Understanding when
    - Arguments add value, and when they don't
  - Understanding the nature of arguments
    - See next slide
  - Better reviewing
    - Make safety case report basis for "challenge"

# The “McDermid Square”

| | | Solution | |
|---|---|---|---|
| | | Familiar | Unfamiliar |
| Problem | Familiar | Minimal argument and standard evidence from the domain, e.g. stability certificate. | Focused argument on reasons for novel solution, plus the appropriate evidence. |
| | Unfamiliar | Minimal argument and standard evidence from another domain, e.g. railway safety case. | Extensive argument and evidence, with substantial independent scrutiny. |

# Integration of Approaches

- ANSI, MilStd 882, ARP
  - Familiar-Familiar – evidence standard documents, possibly only "argue" confidence in evidence
- UAS
  - Familiar-Familiar for "standard aspects"
  - Unfamiliar-Unfamiliar – e.g. sense and avoid
    - Argument that problem well enough characterised that solution will be adequate (safe)
    - Argument that solution works across **all** scenarios

# Outline

- Safety cases
  - Basic concepts
  - Purpose(s)
- Process
  - Used for system acceptance
  - Used for argument construction
- Prospects
  - Better safety cases
  - Integration of approaches
- Conclusions

# Conclusions

- Safety cases/reports **can** add value
  - Primarily arguments to articulate rationale in novel/complex systems/situations
  - Secondarily confidence (even in standard bits)
- Safety cases hard to construct well
  - Need to avoid them where they don't add value
  - Need better guidance on development/review
    - Safety case (argument) patterns helpful but insufficient
    - A good starting point would be a systematic review

# Goal Structuring Notation

» For the definition of the notation see:

http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

This is a “community standard” but it is quite stable

There are also support tools, some of which are linked from:

http://www.goalstructuringnotation.info/