Assurance Case

The verification/validation results we have

- Software requirements
- Risk analysis
- Model checking results
- Traceability analysis
- Testing result

Typical risk analysis report

Cause/Fault Tree Ref	Effect/Severity/Likelihood	Mitigation	Verification
Faulty data exchanged among redundant computers causes all computers to fail. This could occur because of Improper requirements, incorrect coding of logic, incorrect data definitions (e.g., initialized data), and/or inability to test all possible modes in the SW	Effect: Loss of operation of system during critical phase, leading to loss of life. Severity: Catastrophic Likelihood: Improbable Class: Controlled	a) Software safeguards reduce, to the maximum extent feasible, the possibility that faulty data sent among redundant computers causes them to fail b) Program Development Specifications and Functional SW Requirements c) Subsystem design and functional interface requirements are used in the design and development of the relevant SW	Extensive validation and testing are in place to minimize generic SW problems. The contractors must perform rigorous reviews throughout the SW definition, implementation, and verification cycles. These review processes cover requirements, design, code, test procedures and results, and are designed to eliminate errors early in the SW life cycle.

Typical risk analysis report

Cause/Fault Tree Ref	Effect/Severity/Likelihood	Mitigation	Verification
Faulty data exchanged among redundant computers causes all computers to fail. This could occur because of Improper requirements, incorrect coding of logic, incorrect data definitions (e.g., initialized data), and/or inability to test all possible modes in the SW	Effect: Loss of operation of system during critical phase, leading to loss of life. Severity: Catastrophic Likelihood: Improbable Class: Controlled	a) Software safeguards reduce, to the maximum extent feasible, the possibility that faulty data sent among redundant computers causes them to fail b) Program Development Specifications and Functional SW Requirements c) Subsystem design and functional interface requirements are used in the design and development of the relevant SW	Extensive validation and testing are in place to minimize generic SW problems. The contractors must perform rigorous reviews throughout the SW definition, implementation, and verification cycles. These review processes cover requirements, design, code, test procedures and results, and are designed to eliminate errors early in the SW life cycle.

Problems

- Ambiguities makes certification difficult

- Mitigation and verification actions are implicitly related to the causes

- The answers maybe somewhere but difficult to find

- Solution: make the relationships explicit

What is assurance case?

- A justified measure of confidence that a system will function as intended in its environment of use
- Measure of confidence
  - What level of confidence do we have as a result of various assurance activities?
- Justified
  - Why should we have a particular level of confidence?
  - What evidence is there to support this level of confidence?
  - Why do we believe the evidence?
- Function as intended
  - “as intended” by the system’s users as they are actually using it
  - Minimize impact of unusual (or unexpected) operational conditions
  - Minimize impact of vulnerabilities that can be exploited by hostile entities
- Environment of use
  - Not just the intended environment of use — the actual environment of use

Clarifications

- What assurance case is
  - Improves visual comprehension of existing arguments
  - Improves discussion and reduces time-to-agreement on what evidence is needed and what the evidence means (Having identified argument structure up front)
  - Recognition and exploitation of successful (convincing) arguments becomes possible (assurance case patterns)
  - Supports monitoring of project progress towards successful certification When problems arise it helps with diagnosis
  - When new functionality is added it can quickly pinpoint needed new evidence (and identify existing evidence that need not be reconsidered)
- What assurance case is NOT
  - A verified proof that a product is safe

Types of Assurance cases

- Safety assurance
  - Standard-based
    - Evaluate developer competence based on conformance to process standards
    - Adherence to good development processes is evidence of ability to produce good products
    - Pros: widely accepted, standardized
    - Cons: not suitable for new products with few practitioners
  - Product-based
    - Developers create an assurance case; independent assessors evaluate it.
    - Pros: agilely applicable to areas like aerospace, railways, nuclear power plants, off-shore oil, defense, medical devices, etc.
    - Cons: case by case study
- Confidence assurance
  - For tool developers

Goal Structuring Notation (GSN)

- Developed to help organize and structure Safety Cases in a readily reviewable form

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

and eventually supported by **evidence** ○

while making clear the argumentation **strategies** ▱ adopted,

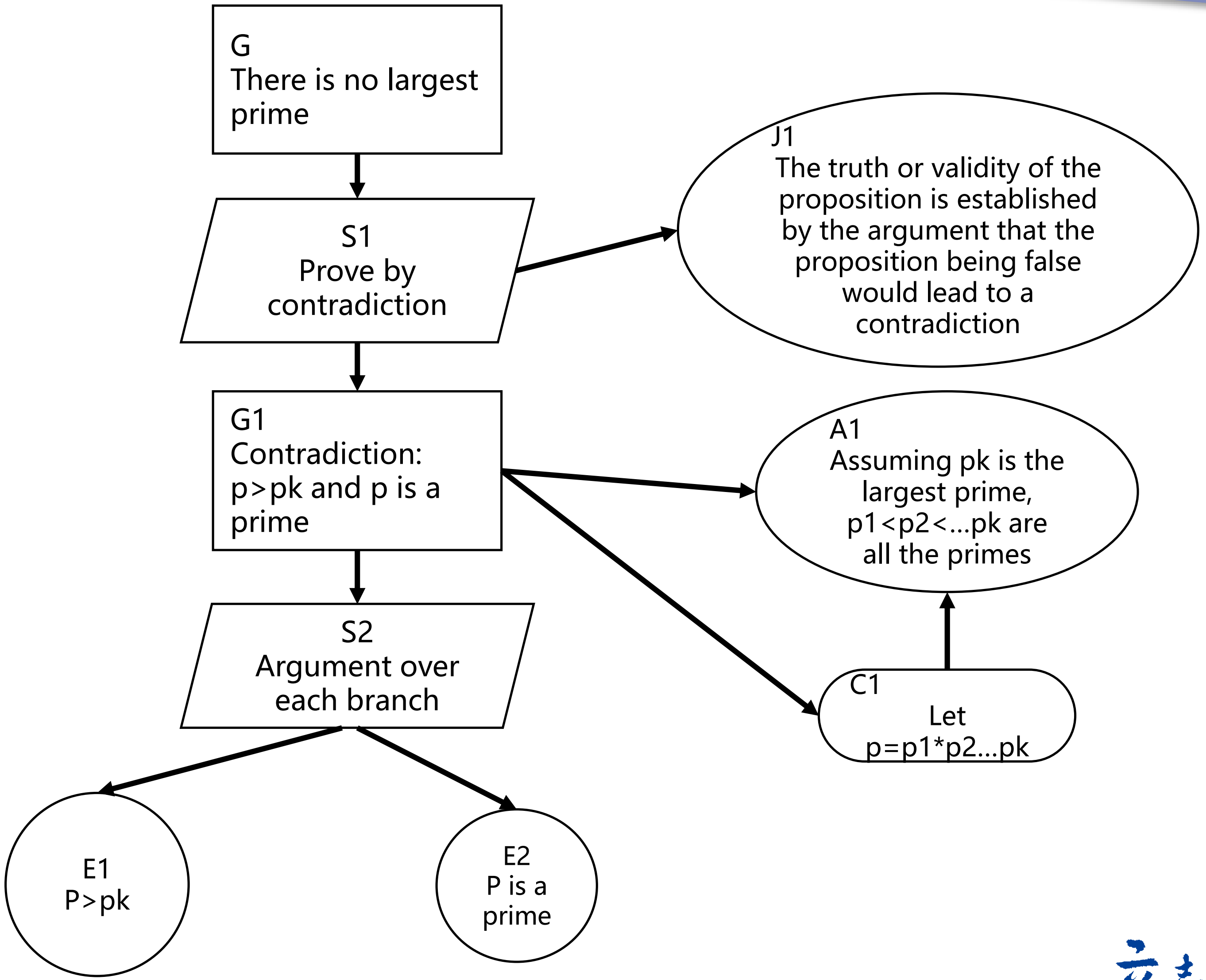
the rationale for the approach (**assumptions, justifications**) ⬭ A/J

and the **context** in which claims are stated ▢

Example

- Proposition
  - There is no largest prime number.
- Proof
  - Prove by contradiction
  - Assuming there is a largest prime
  - p1<p2<…<pk are all the primes
  - Let p=p1* p2* … * pk+ 1
  - p is not divisible by any prime
  - So p is a prime, larger than pk—a contradiction

GSN argument


G
There is no largest prime
S1
Prove by contradiction
J1
The truth or validity of the proposition is established by the argument that the proposition being false would lead to a contradiction
G1
Contradiction: p>pk and p is a prime
A1
Assuming pk is the largest prime, p1<p2<…pk are all the primes
C1
Let p=p1*p2…pk
S2
Argument over each branch
E1
P>pk
E2
P is a prime

How to construct assurance case

Suggested approach

- The GSN Six-Step Approach
  1. Identify Goals
  2. Define Basis for Goals
  3. Identify Strategies
  4. Define Basis for Strategies
  5. Elaborate Strategies
  6. Identify Basic Solutions/Evidence

- Notes
  - There are other valid suggestive approaches
  - A research topic

Step 1—Identify Goals - Phrasing

- Should be propositions (statements that can be true or false).
  - Noun-Phrase + Verb-Phrase
  - Noun-Phrase
    - System development – the design method, coding, requirements activities, etc.
    - System design – physical & functional properties of design
    - System operation and maintenance – procedures, roles, etc.
    - Testing, Safety and Hazard Analyses – e.g. fault trees, test results
    - Example
      - “Module XYZ123”， “Fault Tree for Top Event Y”，
      - “Testing Activity Z”
  - Verb-Phrases
    - Predicates over the subjects (qualification)

Step 1—Identify Goals - Phrasing

- In an appropriate tense for the intended time of reading.
  - Past tense for development: “System was written in SPARK-ADA subset.”
  - Present tense for system attributes: “Likelihood of Hazard X is 10^{-6}.”
  - Future tense for operation/maintenance: “Maintenance will be carried out every 30 days.”
- Should be positive statements of objectives achieved, not requirements
  - “Failure rate is less than 10^{-6}.” v.s. “Failure rate must be less than 10^{-6}.”
- Difficult to summarize?
  - Use references. i.e. “Requirement 6.3 (A-V Synchrony) has been met”

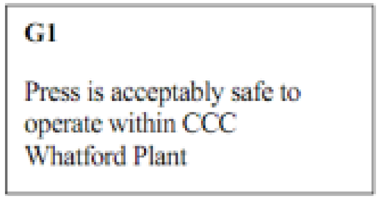
Step 1—Identify Goals - Examples

Subject <Noun-Phrase>	Predicate <Verb Phrase>
Component X	has no critical failure rates
All identified hazards for System Y	have been sufficiently mitigated
Non-destructive examination of weld-site Z	has been performed
Design A	employs triple modular redundancy

Wrong examples:

Claim:	Reason:
“Hazard Log for System Y”	Noun Phrase — describes an entity— not a statement
“Fault Tree for Hazard H-1”	As above
“Perform Fault Tree Analysis of Hazard H-1”	Verb Phrase — an action — not a statement
“How many failure modes does component X have?”	Question — not a statement

Step 1—Identify Goals - Examples



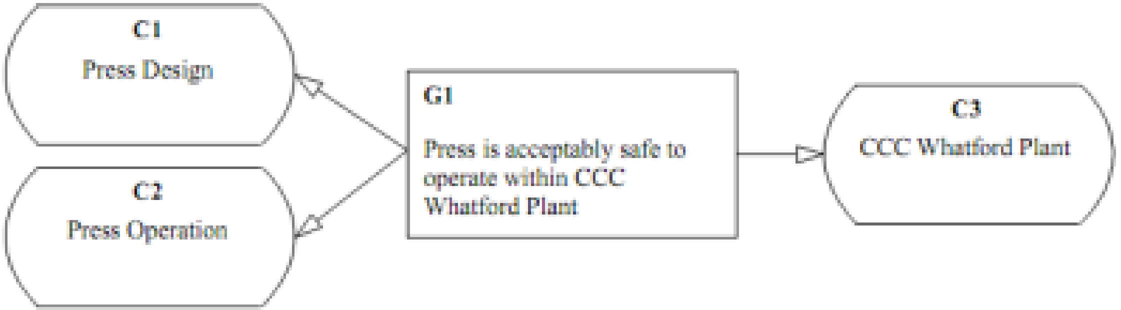
G1

Press is acceptably safe to operate within CCC Whatford Plant

Step 2 – Define basis for claims: Context

- Having presented a claim, make clear (unambiguous) the basis on which that claim is stated
    - When a claim talks of hazards, components, requirements, fault trees, acceptability, sufficiency … is it clear what is being referred to?
- Claims are rarely objective ‘context-free’ statements (especially when terms such as tolerable and negligible are used)
- The aim is to ensure that both writer and reader have same understanding
- Not helpful: “Requirement 6.3 has been met”
- Three Key Aspects
    - Information about the system under discussion
    - Information about the operation environment for the system
    - Information about the argument (terminology definition, etc.)

Step 2 – Define basis for claims: Context


C1
Press Design
C2
Press Operation
G1
Press is acceptably safe to operate within CCC Whatford Plant
C3
CCC Whatford Plant

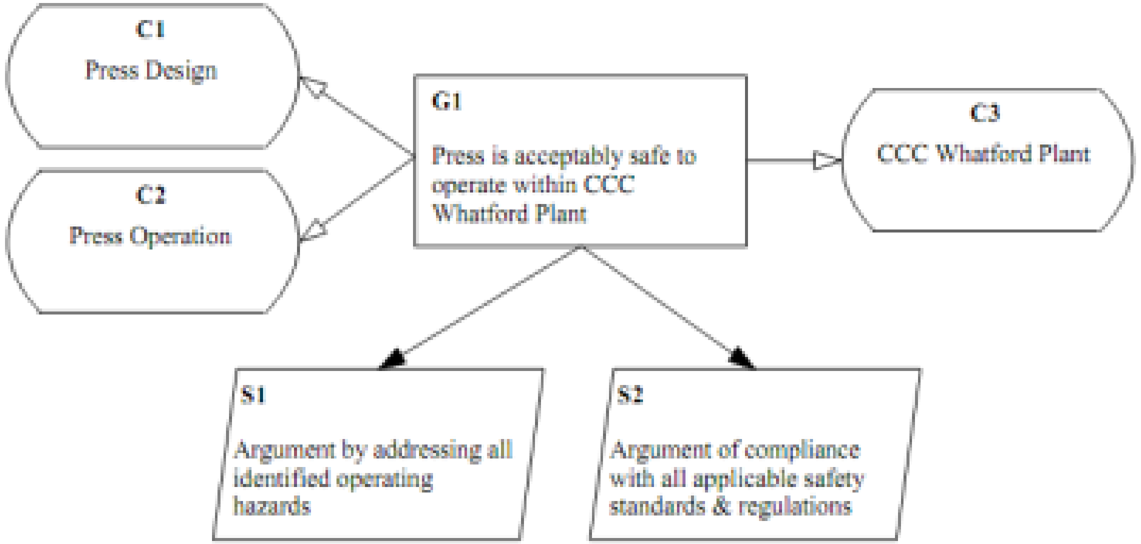
Step 3—Identify Strategies

- Q: When is it necessary to explicitly introduce a strategy node?
  - A1: Whenever you wish to explain the relationship between a claim and its sub-claims
    - Ask yourself whether the reader will understand how you have broken down the claim into sub-claims
  - A2: Whenever the strategy requires additional (contextual) information, justification or assumptions

Step 3—Identify Strategies - phrasing

- Strategies should not be imperative verb-phrases
  - e.g. “Use Historical Data”
- Strategies should be expressed from the perspective of the argument approach, not the design, testing, or analysis approach
  - e.g., “Argument by appeal to interlock” rather than “Interlocks used”
- Strategies should not contain claims
  - Should be possible to remove strategy nodes and not affect the argument being made

Step 3—Identify Strategies



C1
Press Design

C2
Press Operation

G1
Press is acceptably safe to operate within CCC Whatford Plant

C3
CCC Whatford Plant

S1
Argument by addressing all identified operating hazards

S2
Argument of compliance with all applicable safety standards & regulations

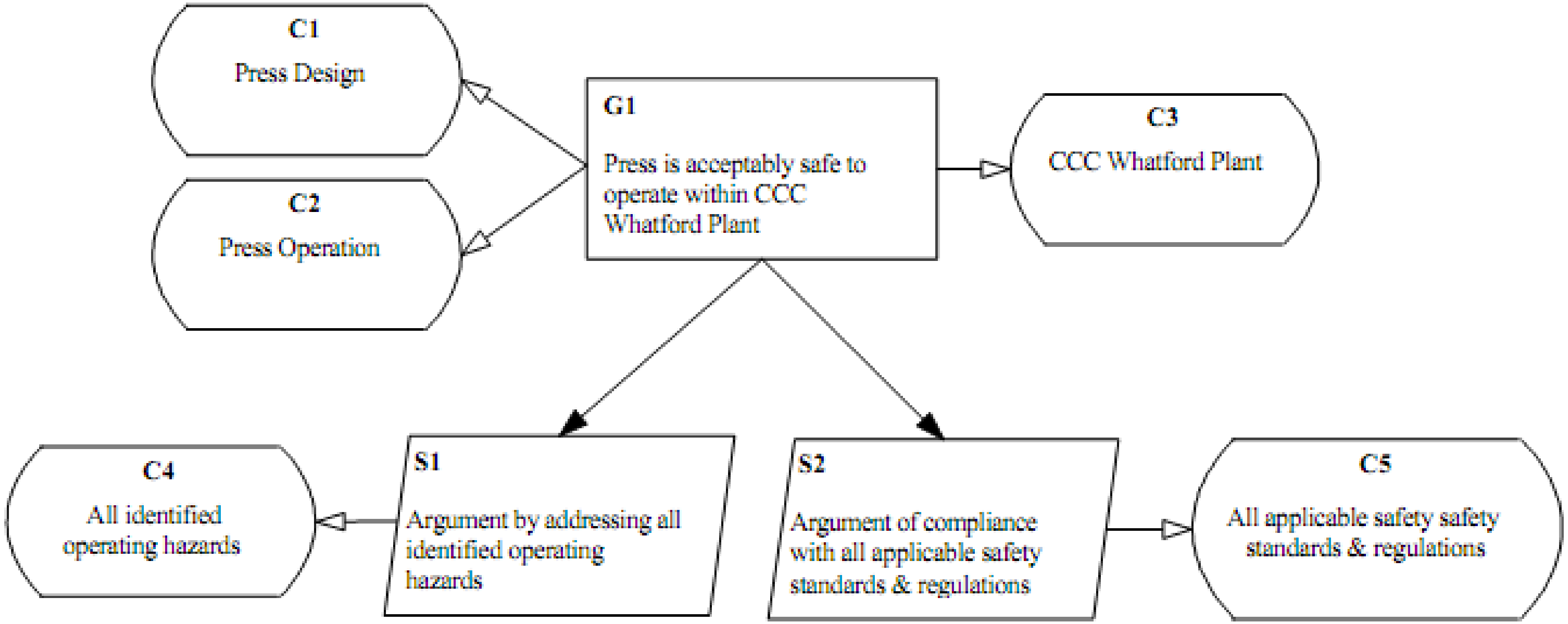
Step 4 – Define basis for strategy

- Contexts
  - Similar to contexts for goals, providing necessary contextual information (models, definitions, etc.)

- Rationales
  - Assumptions
    - Are there any assumptions on which the strategy/goal is being put forward as a solution to the parent goal?
  - Justifications
    - Why that particular strategy/goal is being put forward as a solution to the parent claim?

- Phrasing
  - Both assumptions and justifications are statements and should be expressed as claims.

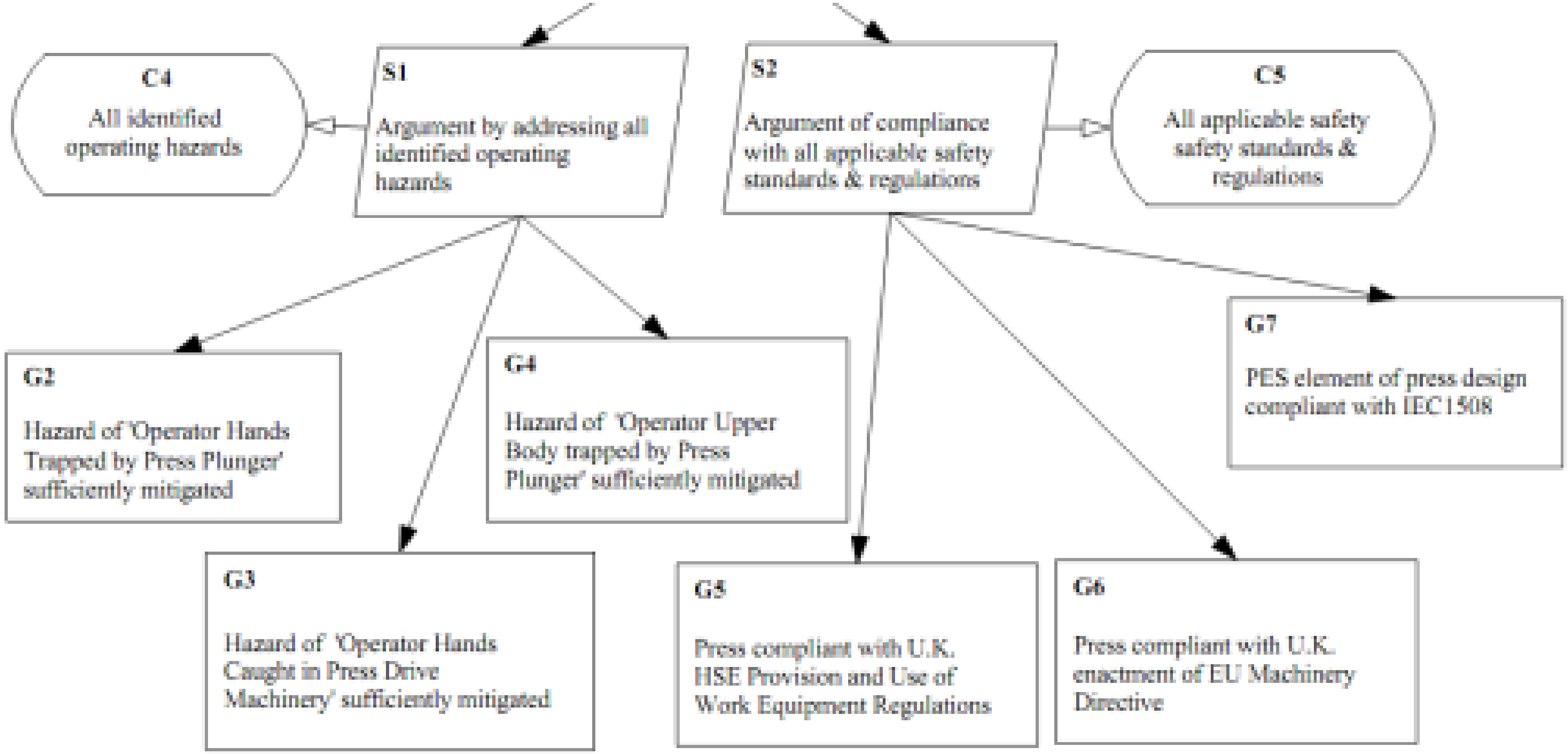
Step 4 – Define basis for strategy


C1
Press Design
C2
Press Operation
G1
Press is acceptably safe to operate within CCC Whatford Plant
C3
CCC Whatford Plant
C4
All identified operating hazards
S1
Argument by addressing all identified operating hazards
S2
Argument of compliance with all applicable safety standards & regulations
C5
All applicable safety safety standards & regulations

Step 5—Elaborating Strategies

- To develop subgoals/solutions to support strategies
  - Depending on the strategies, different structures may be put forward as goals.
    - E.g., if the strategy is "argument over all system safety properties," then each safety property is a subgoal to put forward.
    - E.g., if the strategy is "argument by quantitative analysis result," then quantitative claims must be put forward.
- Notes
  - Strategies are just a means of clarifying how goals/claims/solutions at different levels are related to one another.

Step 5—Elaborating Strategies



C4
All identified operating hazards

S1
Argument by addressing all identified operating hazards

S2
Argument of compliance with all applicable safety standards & regulations

C5
All applicable safety safety standards & regulations

G2
Hazard of 'Operator Hands Trapped by Press Plunger' sufficiently mitigated

G3
Hazard of 'Operator Hands Caught in Press Drive Machinery' sufficiently mitigated

G4
Hazard of 'Operator Upper Body trapped by Press Plunger' sufficiently mitigated

G5
Press compliant with U.K. HSE Provision and Use of Work Equipment Regulations

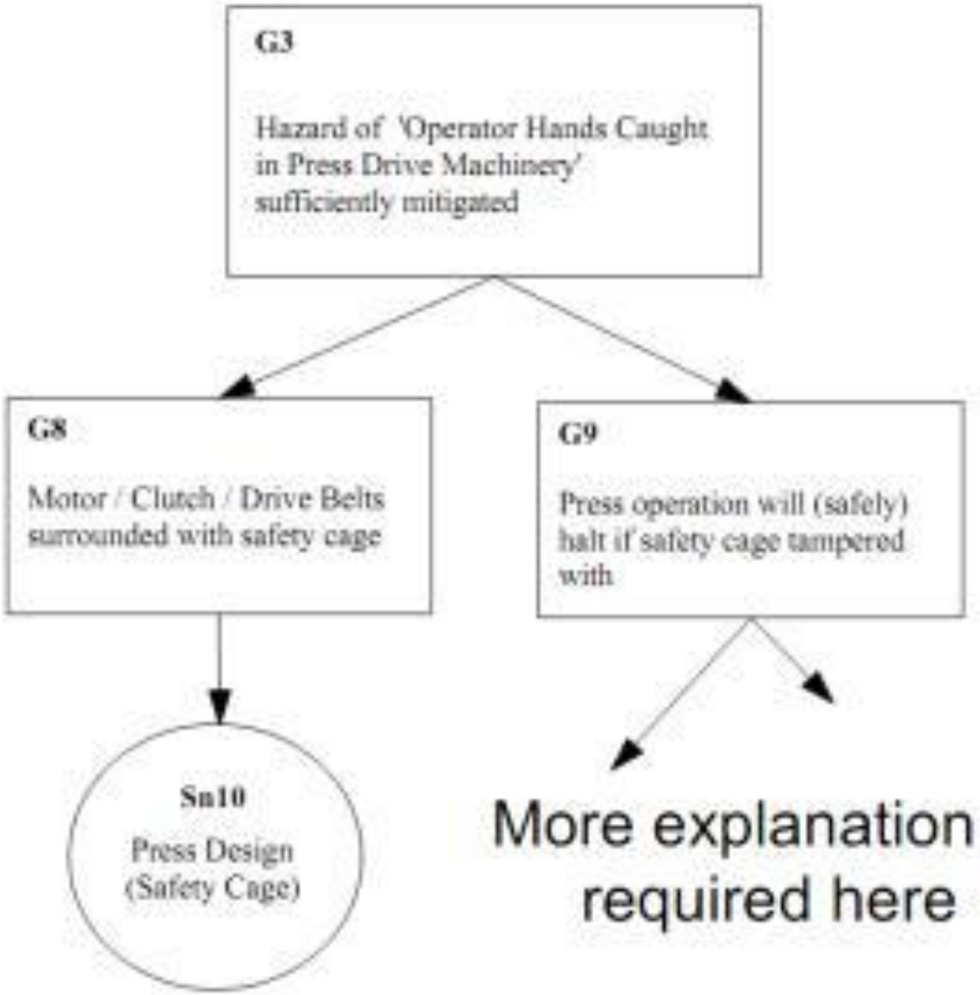
G6
Press compliant with U.K. enactment of EU Machinery Directive

G7
PES element of press design compliant with IEC1508

Step 6—Identifying Solutions/evidence

- Solutions/evidence
  - “Leaf goals” that do not need further explanation, expansion, or refinements.
  - Can be supported by direct reference to external evidence.
  - Come from
    - Test results, analysis reports, facts, etc.
- Watchout
  - Jumping to a solution too soon

Step 6—Identifying Solutions



G3

Hazard of 'Operator Hands Caught in Press Drive Machinery' sufficiently mitigated

G8

Motor / Clutch / Drive Belts surrounded with safety cage

G9

Press operation will (safely) halt if safety cage tampered with

Sn10

Press Design (Safety Cage)

More explanation required here

Assurance case recognition by FDA

- 510(k) submissions for infusion pumps are REQUIRED to have an assurance case
- The requirement may extend to all drug delivery devices
- The FDA encourages device manufacturers to submit safety assurance as part of pre-market submissions
- ISO/IEC 15026-2: Systems and software engineering — Systems and software assurance — Part 2: Assurance case

Conclusion

- Pros
  - is a way of organizing assurance arguments structurally.
  - applies mainly in safety-critical domains and for complex systems.
  - is an active research area.

- Cons
  - has limitations in building, reviewing, maintaining, and reusing.
  - has tool support, but not adequate.

References

- Insup Lee, Assurance Cases: An Introduction, University of Pennsylvania
- Charles B. Weinstock, Assurance Cases.Software Engineering Institute, Carnegie Mellon University, December 2008.
- George Cleland and Robin Bloomfield, Assurance Cases for Medical Devices: The ASCE Approach. Adelard LLP. Silver Spring, Maryland, September 28-29, 2010.
- Charles B. Weinstockand John B. Goodenough, Towards an Assurance Case Practice for Medical Devices. Technical Note, CMU/SEI-2009-TN-018.