# A Short Introduction to Assurance Cases

Ibrahim Habli

# Background

- Paradigm shift in many domains
  - Shift from a prescribed process to a product-oriented assurance
  - Shift from a tick-box to argument-based

- Different drivers:
  - Accidents
    - Piper Alpha, 1988
  - Different business model
    - Rail privatisation, 1992
  - Incidents and recalls
    - FDA, 2010
  - Complexity
    - Automotive, 2011

# Assurance Cases: Definition

- *"A reasoned and compelling **argument**, supported by a body of **evidence**, that a system, service or organisation will operate as intended for a defined application in a defined environment."*

- Often with a particular focus
  - Safety
  - Security
  - Dependability
  - Trust
  - …

[GSN Standard 2011]

# Assurance Cases: Structure

- Primary Claim, e.g.
  - The *contributions* made by the *BSCU software* to *S18 WBS hazards* are acceptable

- Argument, e.g.
  - Hazardous software contributions have been identified
  - Controls have been put in place to manage these contributions
  - Mechanisms are in place to monitor the performance of the controls and the system on an on-going basis

- Evidence, e.g.
  - Tests, analyses, reviews, simulation, expert judgements and compliance with best practice

# Assurance Case Arguments

- *"A connected series of claims intended to establish an overall claim"*

- Deductive argument: overall claim follows with necessity

  *All men are mortal.*
  *Aristotle is a man.*
  *----------------*
  *Therefore, Aristotle is mortal.*

- Inductive argument: overall claim follows with probability

  *System detects most faults via sensors.*
  *Collected sensor data shows lack of faults.*
  *--------------------------------------------------------------*
  *Therefore, System is very likely to be fault-free.*

- Unfortunately, assurance case arguments are predominantly inductive rather than deductive
  - and are often implicit!

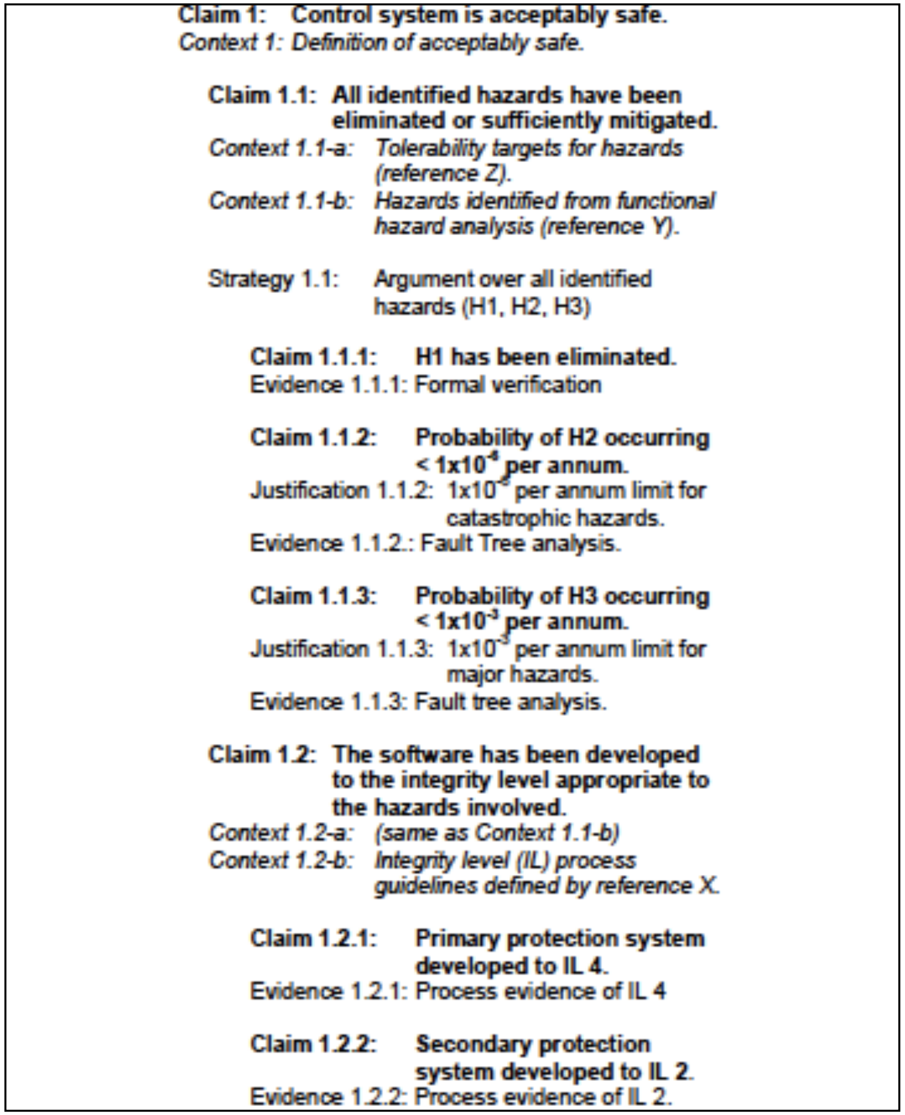
# Assurance Case Notations

- Clear representation is necessary
  - Comprehensible to all assurance-case stakeholders
  - Enable effective review and maintenance
- Main notations are:
  - Textual
  - Tabular
  - Graphical
- With increased interest in formalism
- Assurance cases for large scale and complex system will include most of the above notations

# Assurance Case Notations: Text

- Normal prose
  - Primary medium of expression in law and philosophy
- Structured prose
  - Explicitly denoting the critical parts of the argument
- Argument outline
  - Indentation, numbering and font changes

[Holloway 08]



**Claim 1: Control system is acceptably safe.**
*Context 1: Definition of acceptably safe.*

**Claim 1.1: All identified hazards have been eliminated or sufficiently mitigated.**
*Context 1.1-a: Tolerability targets for hazards (reference Z).*
*Context 1.1-b: Hazards identified from functional hazard analysis (reference Y).*

Strategy 1.1: Argument over all identified hazards (H1, H2, H3)

**Claim 1.1.1: H1 has been eliminated.**
Evidence 1.1.1: Formal verification

**Claim 1.1.2: Probability of H2 occurring < $1x10^{-6}$ per annum.**
Justification 1.1.2: $1x10^{-6}$ per annum limit for catastrophic hazards.
Evidence 1.1.2.: Fault Tree analysis.

**Claim 1.1.3: Probability of H3 occurring < $1x10^{-3}$ per annum.**
Justification 1.1.3: $1x10^{-3}$ per annum limit for major hazards.
Evidence 1.1.3: Fault tree analysis.

**Claim 1.2: The software has been developed to the integrity level appropriate to the hazards involved.**
*Context 1.2-a: (same as Context 1.1-b)*
*Context 1.2-b: Integrity level (IL) process guidelines defined by reference X.*

**Claim 1.2.1: Primary protection system developed to IL 4.**
Evidence 1.2.1: Process evidence of IL 4

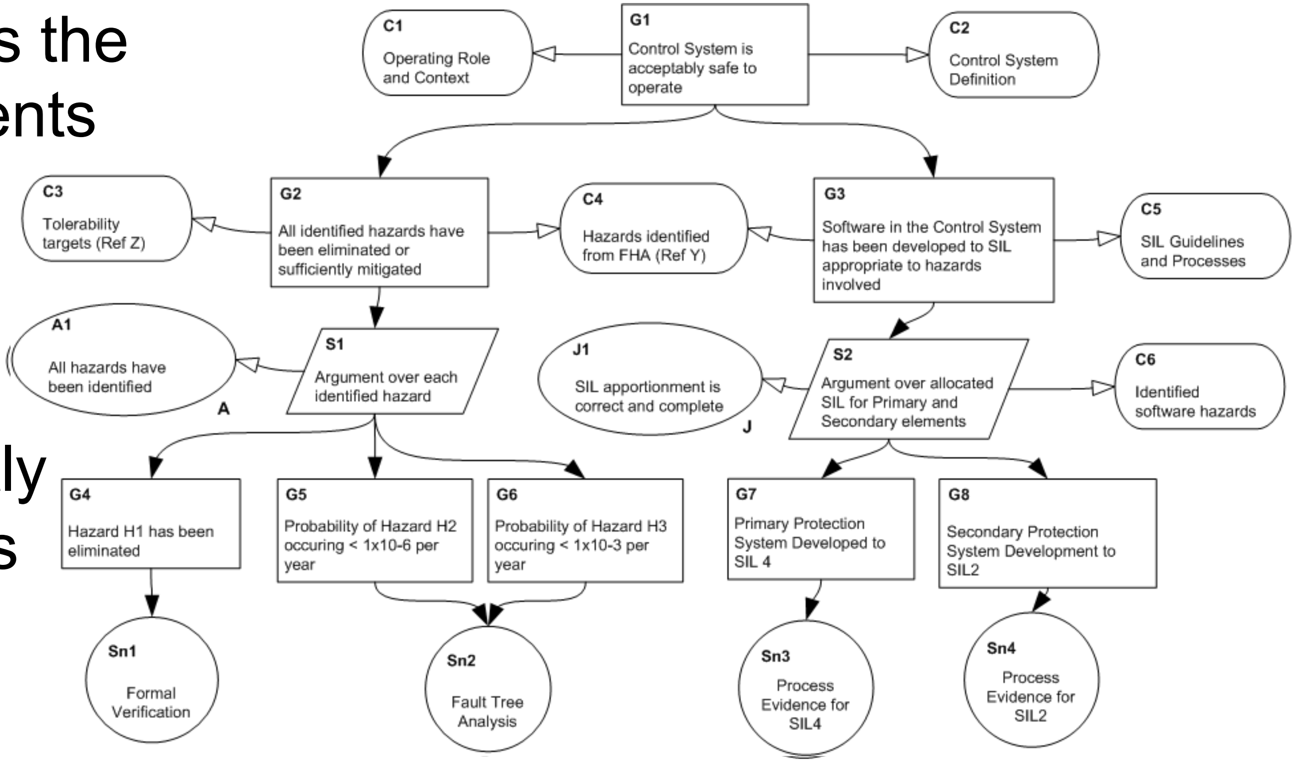
**Claim 1.2.2: Secondary protection system developed to IL 2.**
Evidence 1.2.2: Process evidence of IL 2.

# Notations: Graphical

- Two main notations:
  - Claims-Arguments-Evidence (CAE)
  - Goal Structuring Notation (GSN)

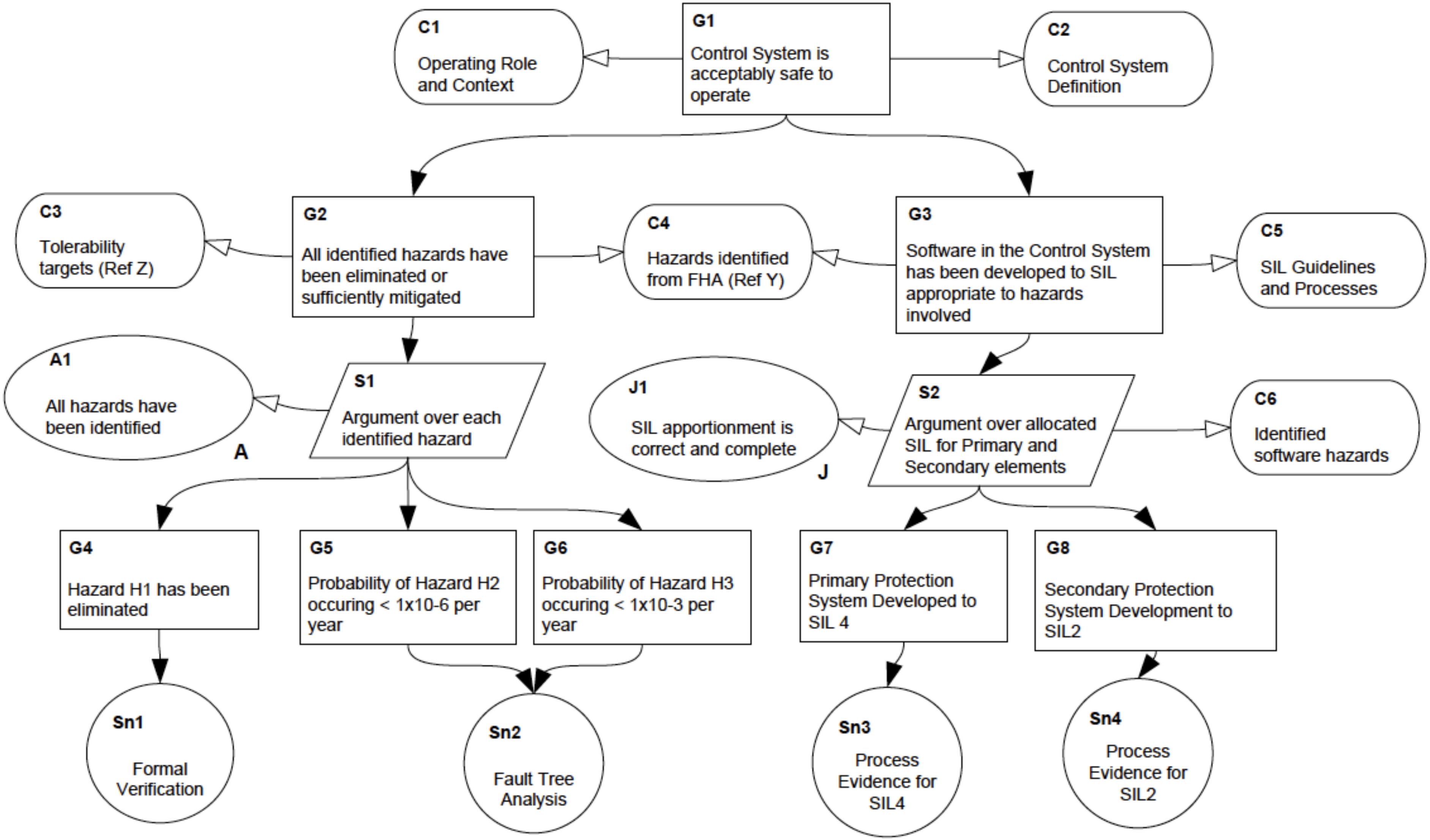
- GSN documents the individual elements of arguments

- More significantly the relationships between these elements

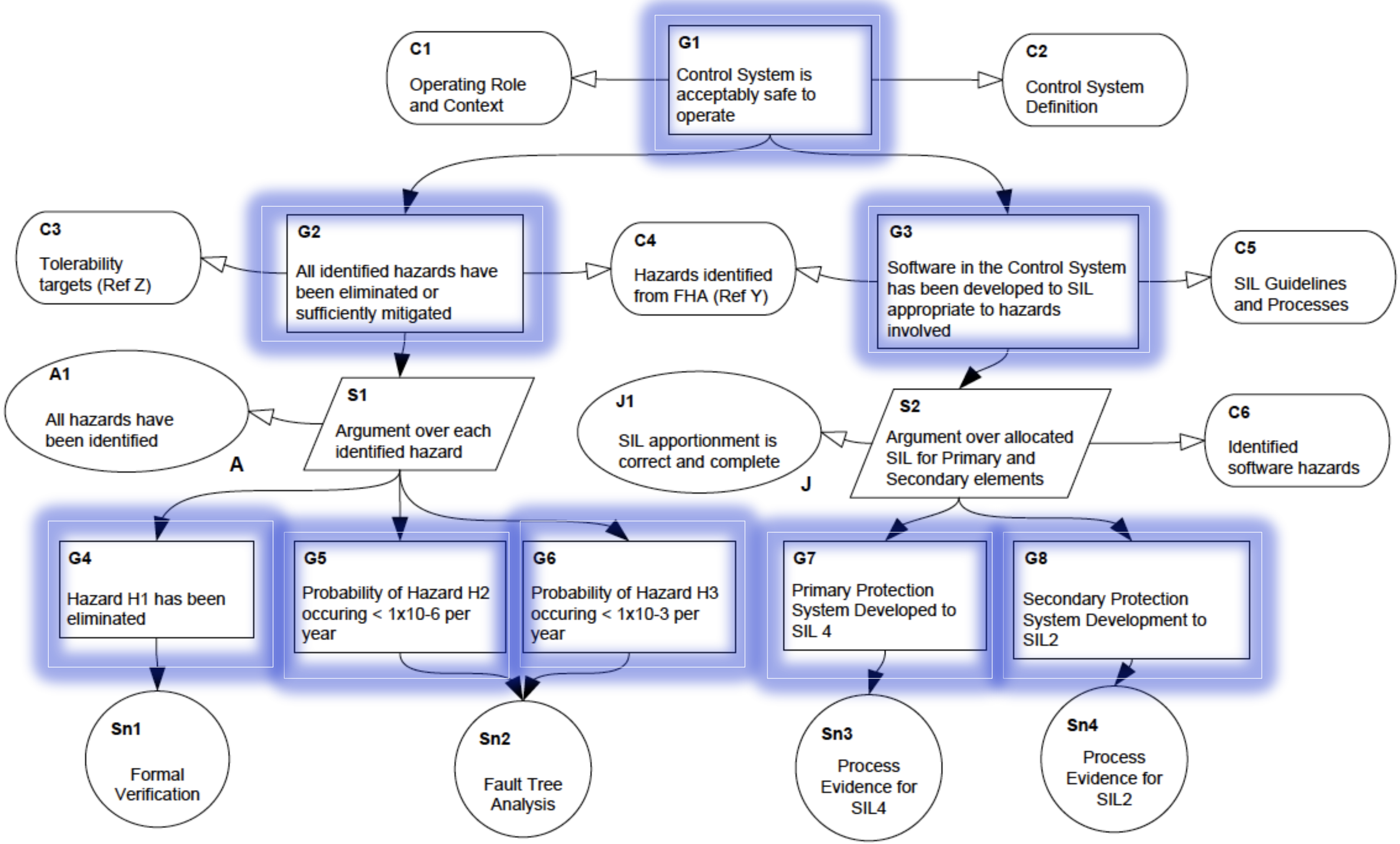

C1
Operating Role and Context
G1
Control System is acceptably safe to operate
C2
Control System Definition
C3
Tolerability targets (Ref Z)
G2
All identified hazards have been eliminated or sufficiently mitigated
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

[GSN Standard 2011]

# GSN: Goal Structure


G1
Control System is acceptably safe to operate
C1
Operating Role and Context
C2
Control System Definition
G2
All identified hazards have been eliminated or sufficiently mitigated
C3
Tolerability targets (Ref Z)
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

# GSN: Goals



G1
Control System is acceptably safe to operate

C1
Operating Role and Context

C2
Control System Definition

G2
All identified hazards have been eliminated or sufficiently mitigated

C3
Tolerability targets (Ref Z)

C4
Hazards identified from FHA (Ref Y)

G3
Software in the Control System has been developed to SIL appropriate to hazards involved

C5
SIL Guidelines and Processes

A1
All hazards have been identified

A

S1
Argument over each identified hazard

J1
SIL apportionment is correct and complete

J

S2
Argument over allocated SIL for Primary and Secondary elements

C6
Identified software hazards

G4
Hazard H1 has been eliminated

G5
Probability of Hazard H2 occuring < 1x10-6 per year

G6
Probability of Hazard H3 occuring < 1x10-3 per year

G7
Primary Protection System Developed to SIL 4

G8
Secondary Protection System Development to SIL2

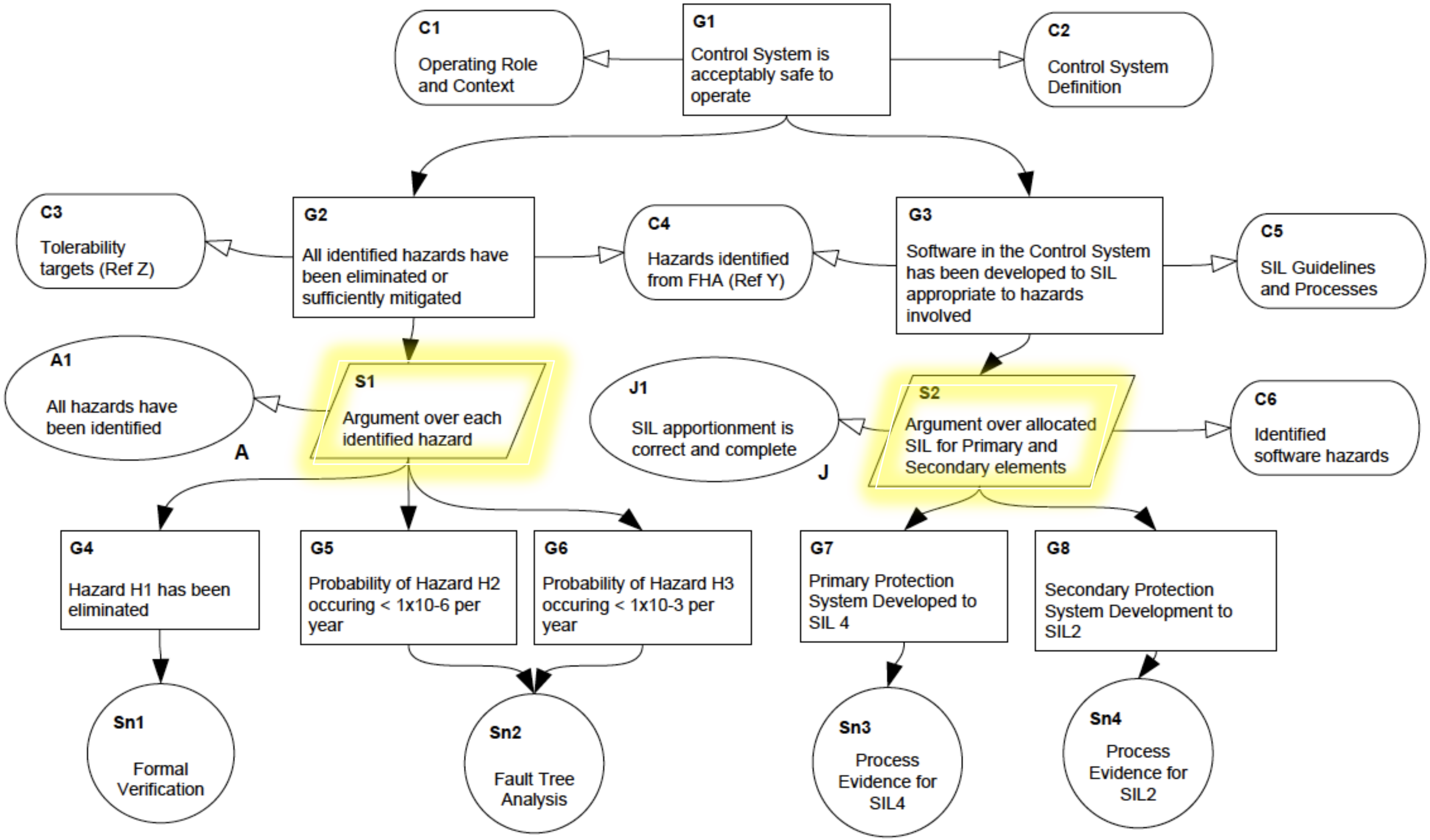
Sn1
Formal Verification

Sn2
Fault Tree Analysis

Sn3
Process Evidence for SIL4

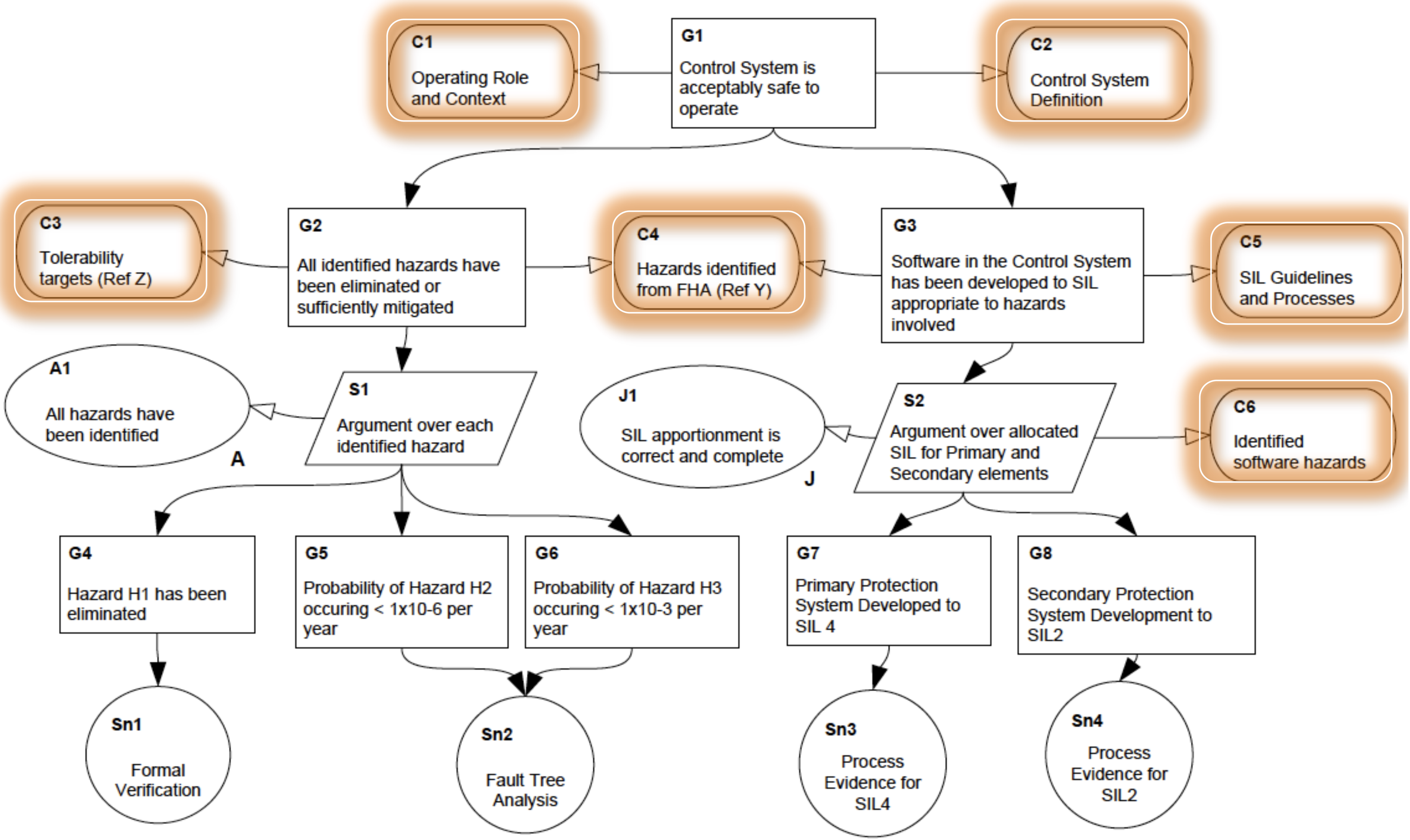
Sn4
Process Evidence for SIL2

# GSN: Strategies



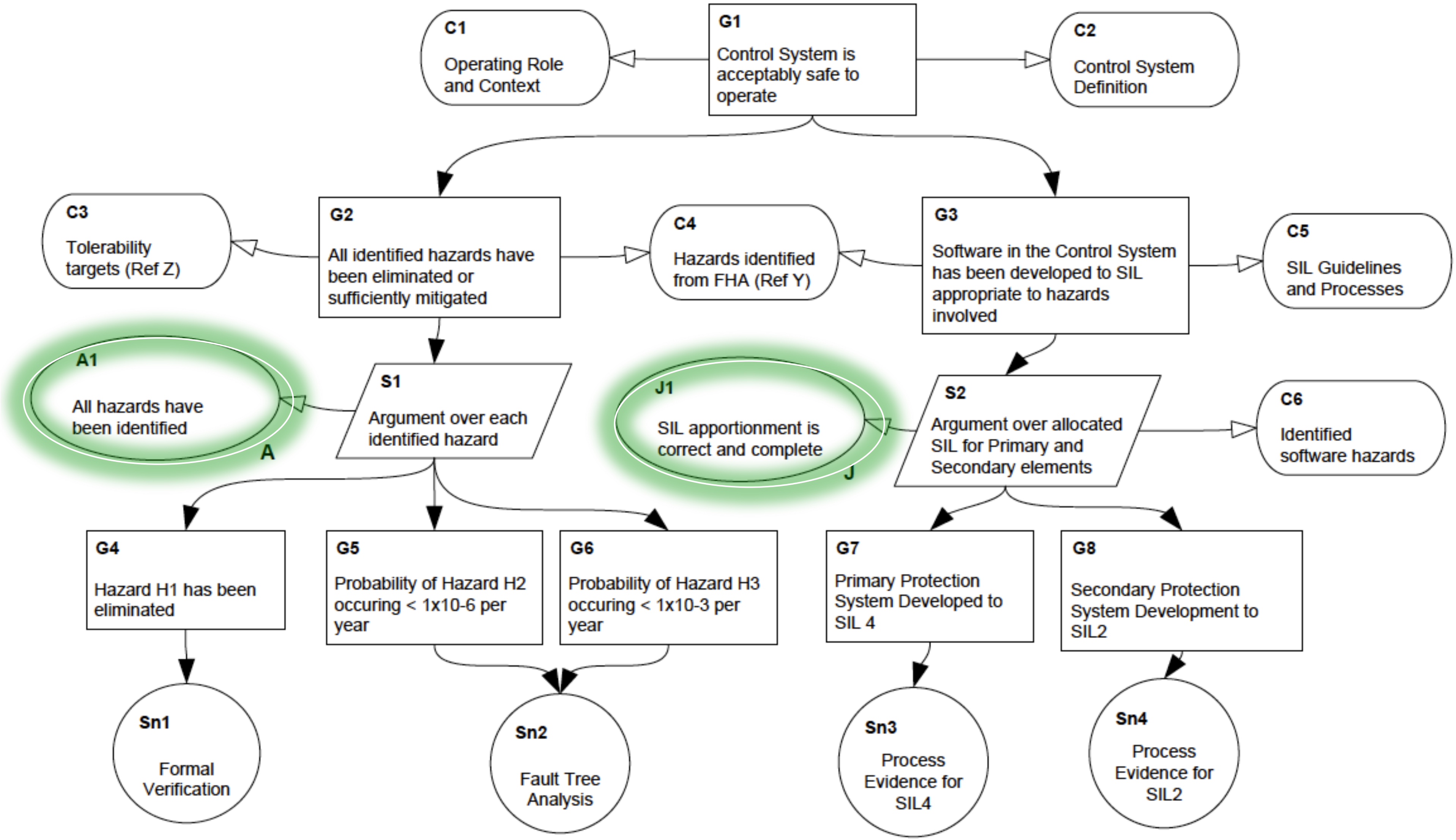
G1
Control System is acceptably safe to operate
C1
Operating Role and Context
C2
Control System Definition
C3
Tolerability targets (Ref Z)
G2
All identified hazards have been eliminated or sufficiently mitigated
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

# GSN: Context



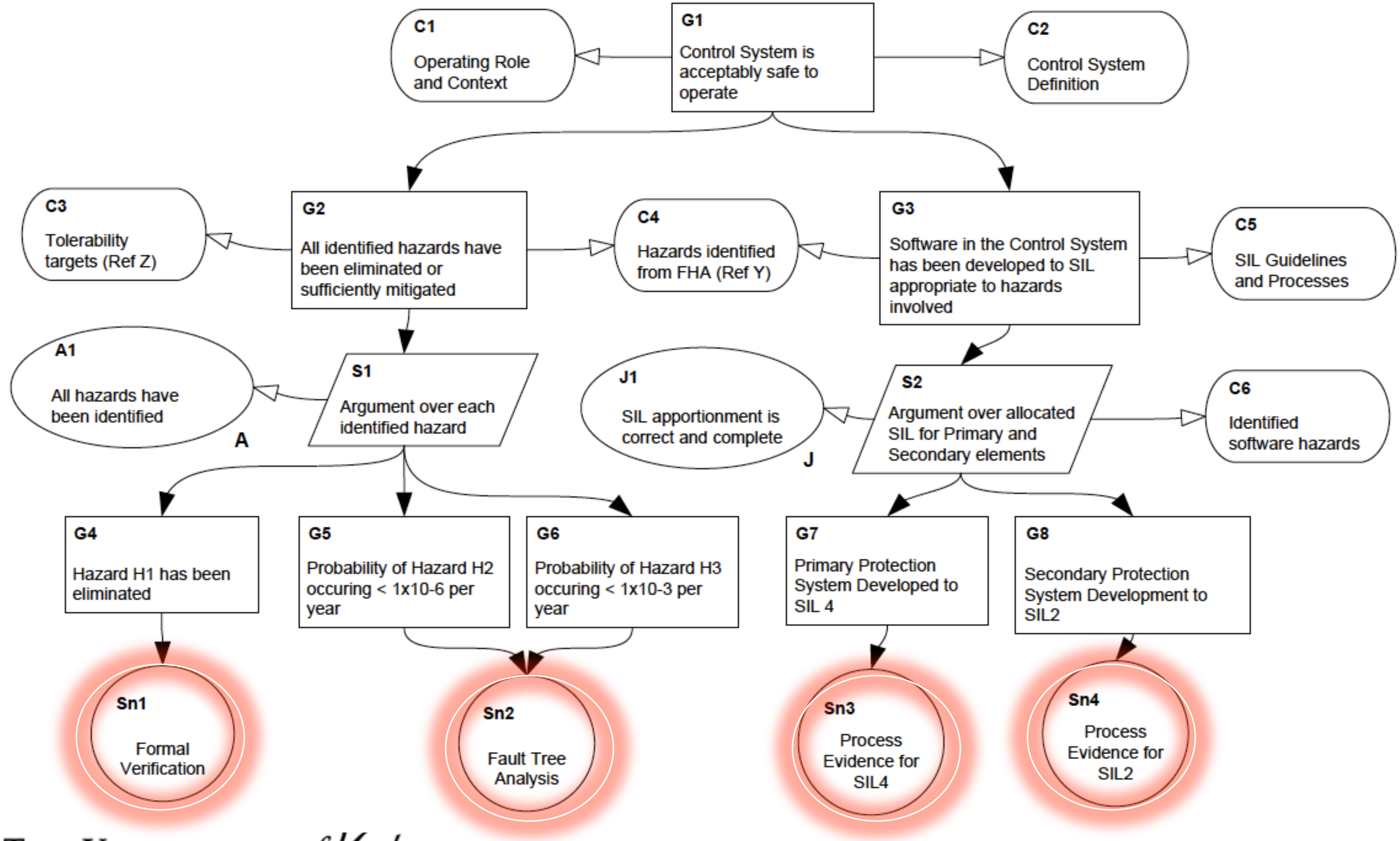
C1
Operating Role and Context
G1
Control System is acceptably safe to operate
C2
Control System Definition
C3
Tolerability targets (Ref Z)
G2
All identified hazards have been eliminated or sufficiently mitigated
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

# GSN: Assumptions/Justifications


C1
Operating Role and Context
G1
Control System is acceptably safe to operate
C2
Control System Definition
C3
Tolerability targets (Ref Z)
G2
All identified hazards have been eliminated or sufficiently mitigated
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

THE UNIVERSITY of York

# GSN: Solutions

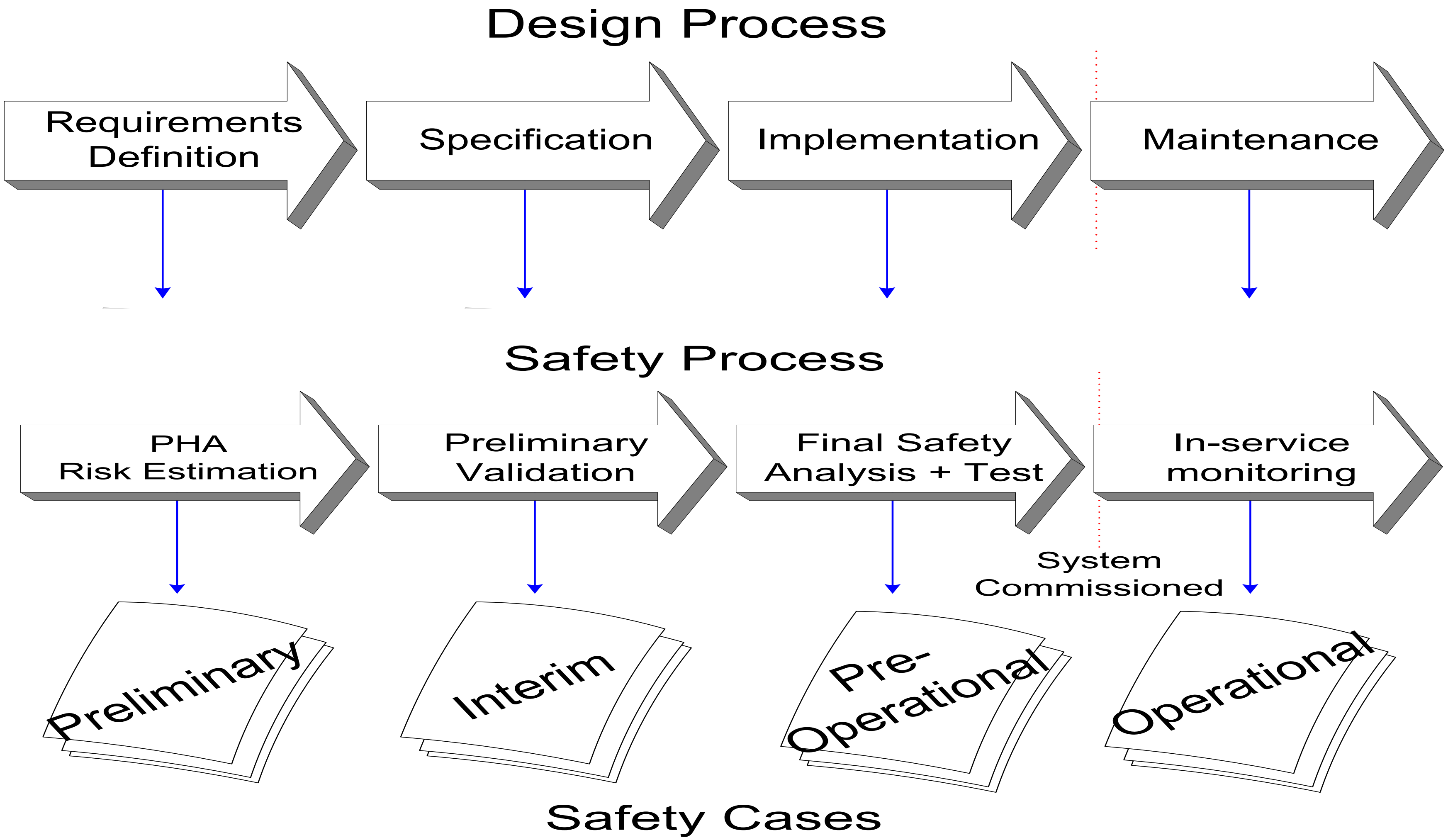

C1
Operating Role and Context
G1
Control System is acceptably safe to operate
C2
Control System Definition
C3
Tolerability targets (Ref Z)
G2
All identified hazards have been eliminated or sufficiently mitigated
C4
Hazards identified from FHA (Ref Y)
G3
Software in the Control System has been developed to SIL appropriate to hazards involved
C5
SIL Guidelines and Processes
A1
All hazards have been identified
A
S1
Argument over each identified hazard
J1
SIL apportionment is correct and complete
J
S2
Argument over allocated SIL for Primary and Secondary elements
C6
Identified software hazards
G4
Hazard H1 has been eliminated
G5
Probability of Hazard H2 occuring < 1x10-6 per year
G6
Probability of Hazard H3 occuring < 1x10-3 per year
G7
Primary Protection System Developed to SIL 4
G8
Secondary Protection System Development to SIL2
Sn1
Formal Verification
Sn2
Fault Tree Analysis
Sn3
Process Evidence for SIL4
Sn4
Process Evidence for SIL2

# Assurance Case Review

- Various issues to consider, including:
  - **Argument Comprehension**
    - Can the argument be fully understood by the reader?
  - **Sufficiency of argument**
    - Are the premises of the argument, taken together, strong enough to support the conclusion(s) being drawn?
  - **Integrity of evidence**
    - Has the evidence been developed and thoroughly reviewed by suitably competent and experienced personnel?

- Sadly, uncovering and understanding the arguments and evidence remain a key challenge for reviewers!

# Incremental Development



# Tool Support

- Improved presentation
  - e.g. through argument views
- Support for argument construction
  - e.g. structured expression and controlled vocabulary
- Support for review
  - e.g. syntactic checks of argument structure
- Support for reuse
  - e.g. argument patterns and modularisation
- Maintenance
  - e.g. change management and traceability

# Benefits

- **Making the implicit explicit**
  - Easier to review the arguments, question the evidence and challenge the adequacy of the reasoning presented
  - Creating greater transparency in the overall assurance process

- Aiding communication among stakeholders
- Integrating and assessing evidence sources
- Aiding safety management and governance
- …

[Health Foundation 2012]

# Challenges

- Removed from reality
- Approximation of truth
- Lack Empirical evidence
- Subjectivity
- Training needs
- Apologetic arguments
- Lack Scientific Assessment
- Paper exercise
- Capability of Tools
- Prescriptive arguments
- Lack of Examples
- Imbalance of skills
- Illusion of pictures
- Cost-effectiveness
- Wrong people

**and many more…**

Many potential benefits and challenges

Hence this workshop