Modellbasierte Safety-Cases für zuverlässige Softwaresysteme

Stefan Puchner, Bernhard Schätz, Stefan Wagner
Fakultät für Informatik, TU München

ADA-Workshop „Zuverlässige Software-Systeme“
Hochschule Regensburg, 18.06.2009

Zuverlässige Systeme: ISO 26262

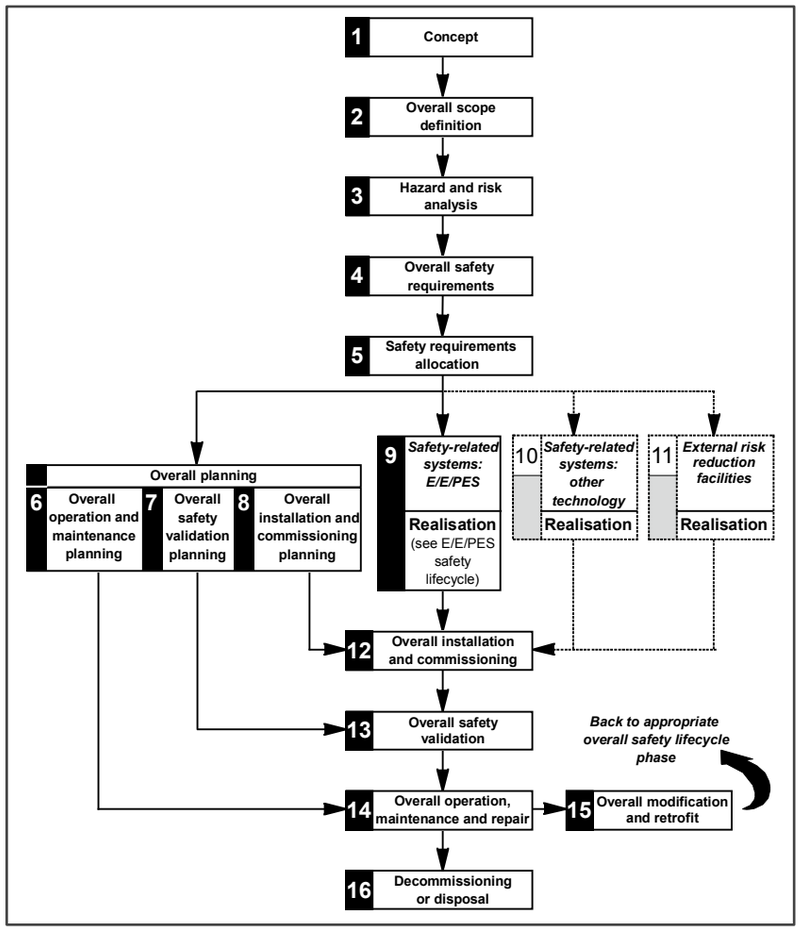


Table B.4 — Failure analysis (referenced by table A.10)

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1a Cause consequence diagrams	B.6.6.2	R	R	R	R
1b Event tree analysis	B.6.6.3	R	R	R	R
2 Fault Tree Analysis	B.6.6.5	R	R	HR	HR
3 Failure modes, effects and criticality analysis	B.6.6.4	R	R	HR	HR
4 Monte-Carlo simulation	C.6.6	R	R	R	R

a) Preliminary hazard analysis should have already taken place in order to categorise the software into the most appropriate safety integrity level.

b) Appropriate techniques/measures shall be selected according to the safety integrity level.

Table A.1 — Software safety requirements specification (see 7.2)

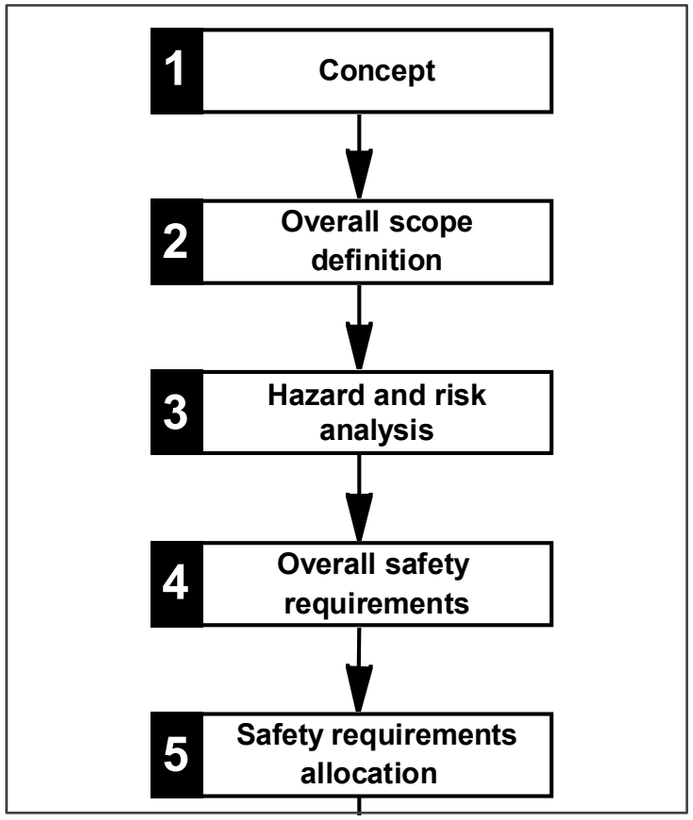
Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Computer-aided specification tools	B.2.4	R	R	HR	HR
2a Semi-formal methods	Table B.7	R	R	HR	HR
2b Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR

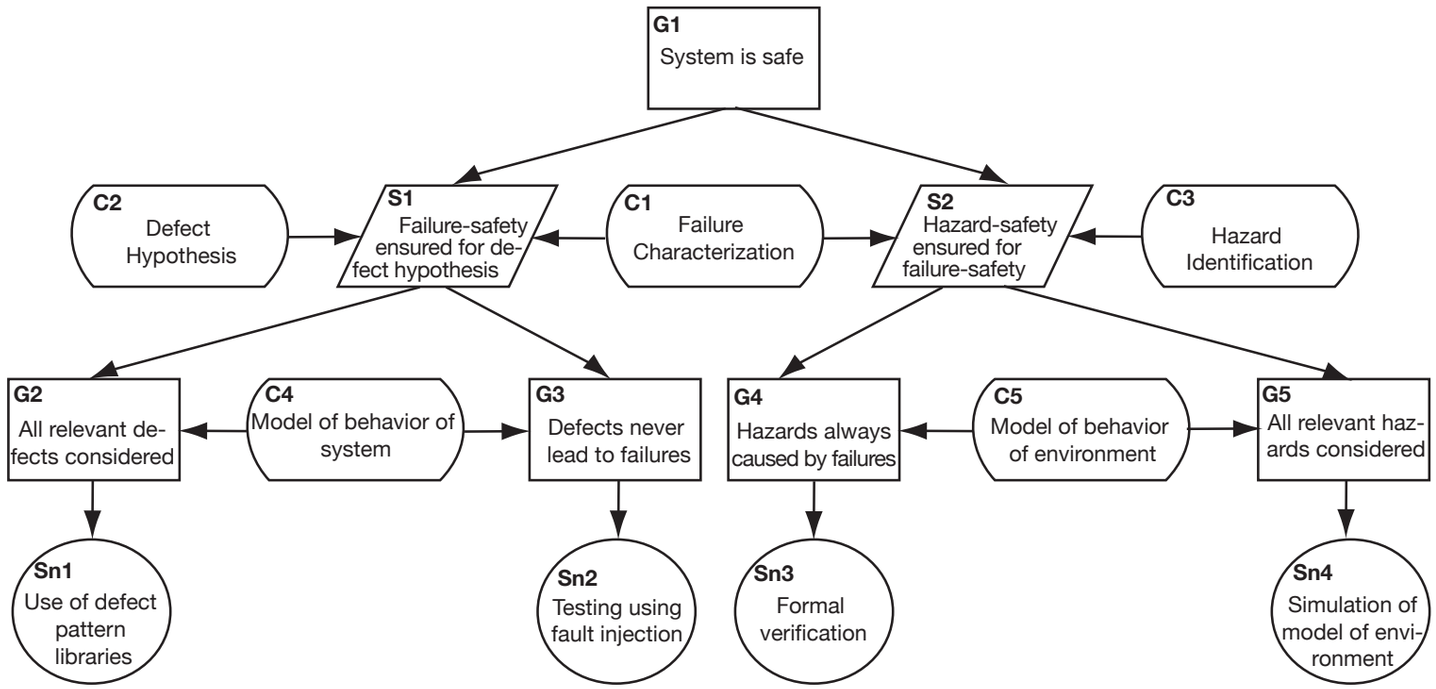
a) The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application.

ISO 26262: Zertifizierung sicherheitskritischer Automotive-Systeme

- Ziel: Nachweis der Sorgfalt bei Entwicklung, Betrieb und Wartung
- Fokus: Korrekte Entwicklung der sicherheitsrelevanten Systemanteile
  - Planung, Durchführung und Dokumentation der Entwicklungstätigkeiten
  - Definition anzuwendender Methoden und Verfahren
- Nicht im Fokus: Nachweis der Adequanz der sicherheitsrelevanten Funktionalität

Modellbasierte Safety-Cases: Ansatz

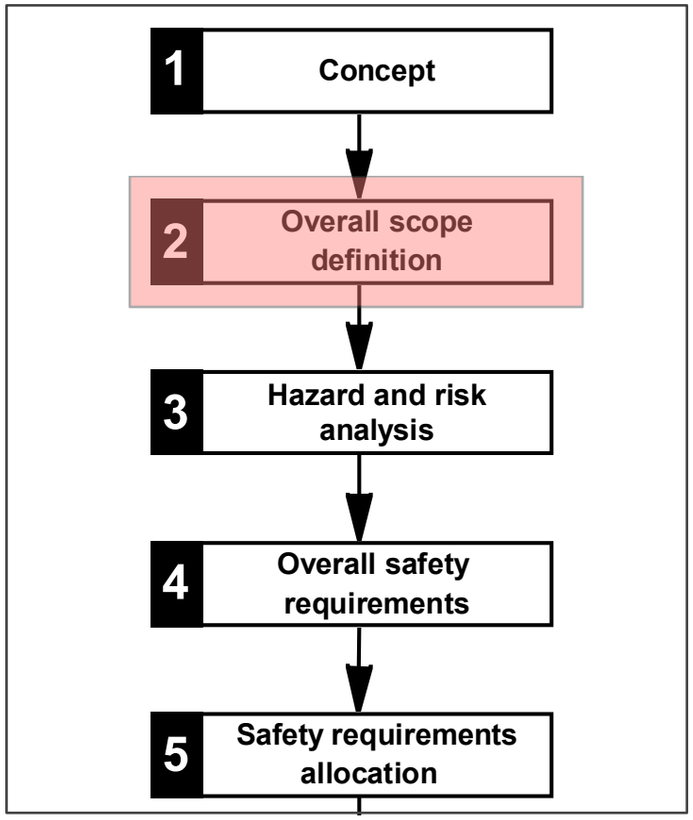


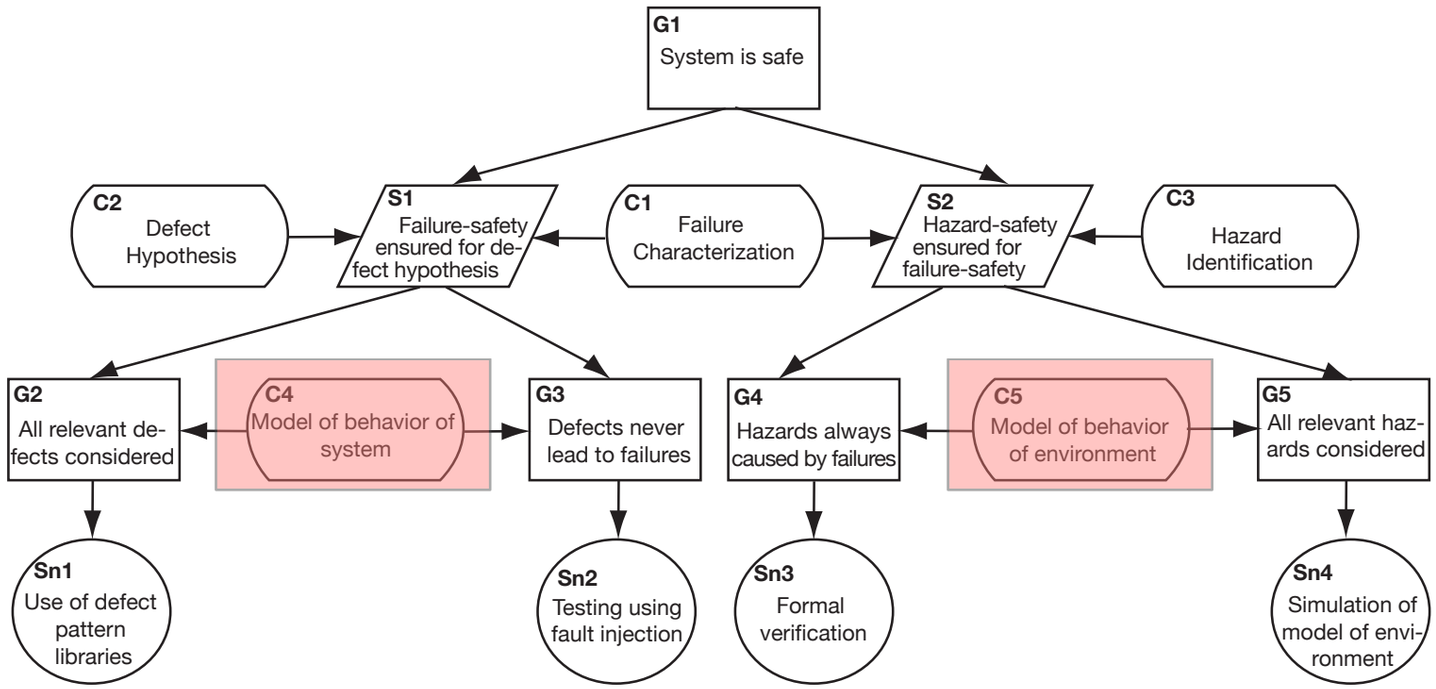


Safety Cases: Nachvollziehbare Argumentation

- Fokus: Entwicklung der adequaten Sicherheitsfunktion
- Prinzip: Schematisierte, nachvollziehbare und wiederverwendbare Argumentation
  - Definition eines Schemas: Konstruktion nach Standardstruktur
  - Einbettung in den Entwicklungsprozess: Modelle als Argumentationsbasis
  - Wiederholbares Verfahren: Verwendung von Argumentationsbausteinen

Modellbasierte Safety-Cases: Ansatz

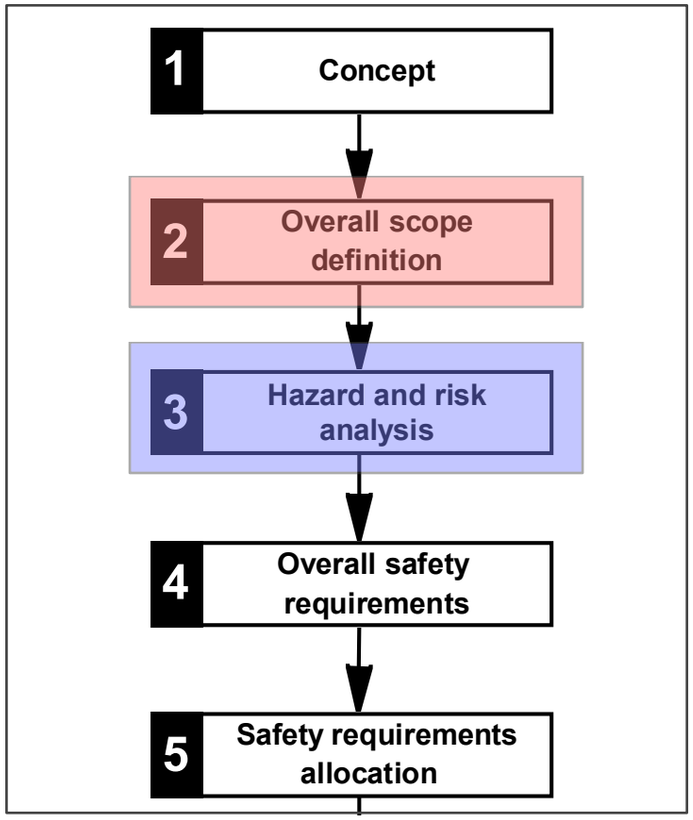


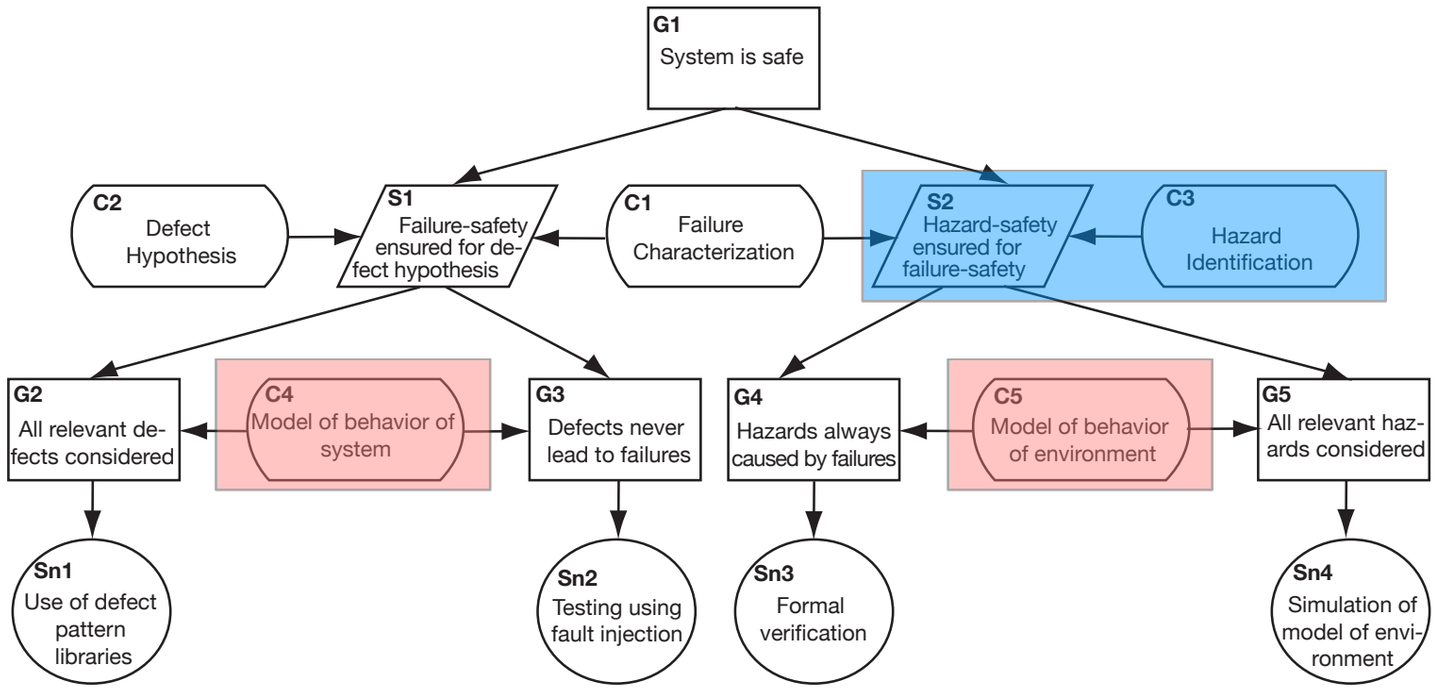


Safety Cases: Nachvollziehbare Argumentation

- Fokus: Entwicklung der adequaten Sicherheitsfunktion
- Prinzip: Schematisierte, nachvollziehbare und wiederverwendbare Argumentation
  - Definition eines Schemas: Konstruktion nach Standardstruktur
  - Einbettung in den Entwicklungsprozess: Modelle als Argumentationsbasis
  - Wiederholbares Verfahren: Verwendung von Argumentationsbausteinen

Modellbasierte Safety-Cases: Ansatz

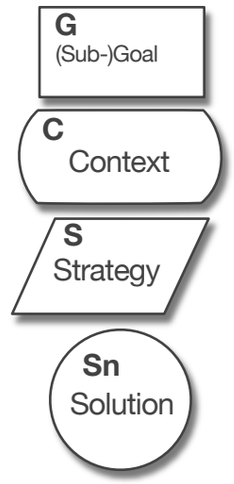




Safety Cases: Nachvollziehbare Argumentation

- Fokus: Entwicklung der adequaten Sicherheitsfunktion
- Prinzip: Schematisierte, nachvollziehbare und wiederverwendbare Argumentation
  - Definition eines Schemas: Konstruktion nach Standardstruktur
  - Einbettung in den Entwicklungsprozess: Modelle als Argumentationsbasis
  - Wiederholbares Verfahren: Verwendung von Argumentationsbausteinen

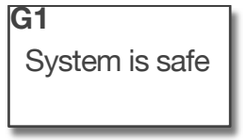
Modellbasierter Safety-Case: Struktur

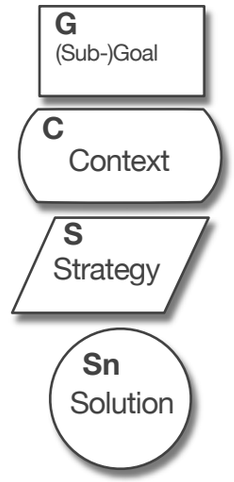


Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

Modellbasierter Safety-Case: Struktur





Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

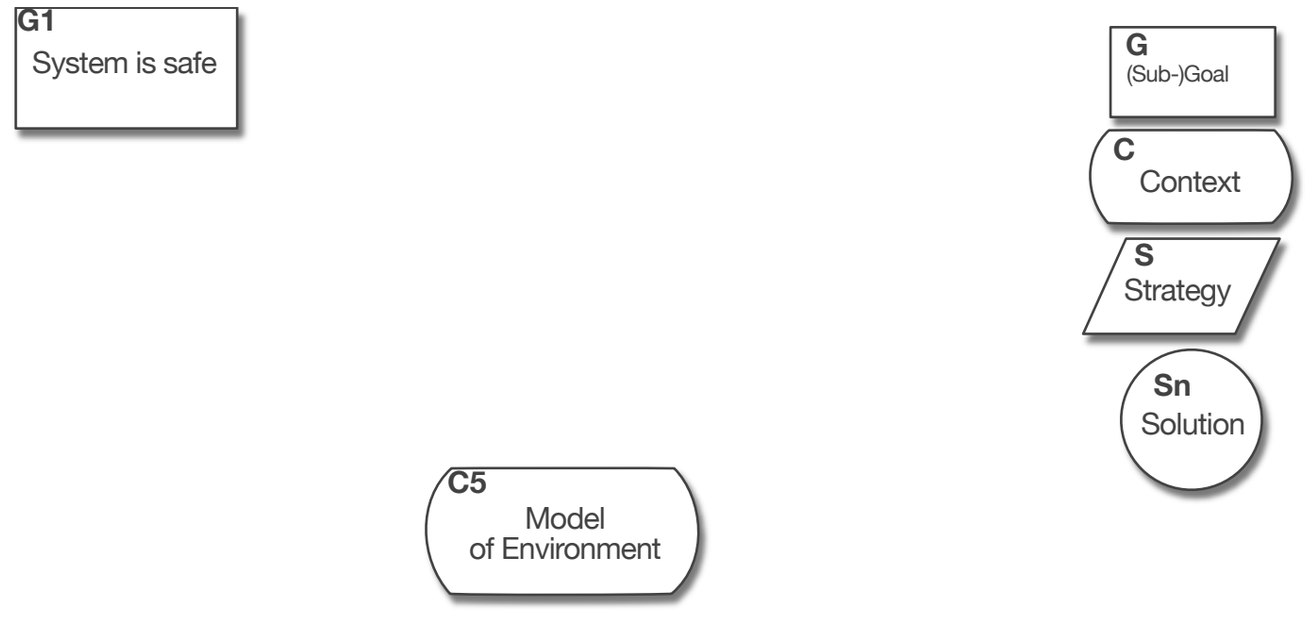
- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

Modellbasierter Safety-Case: Struktur

Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

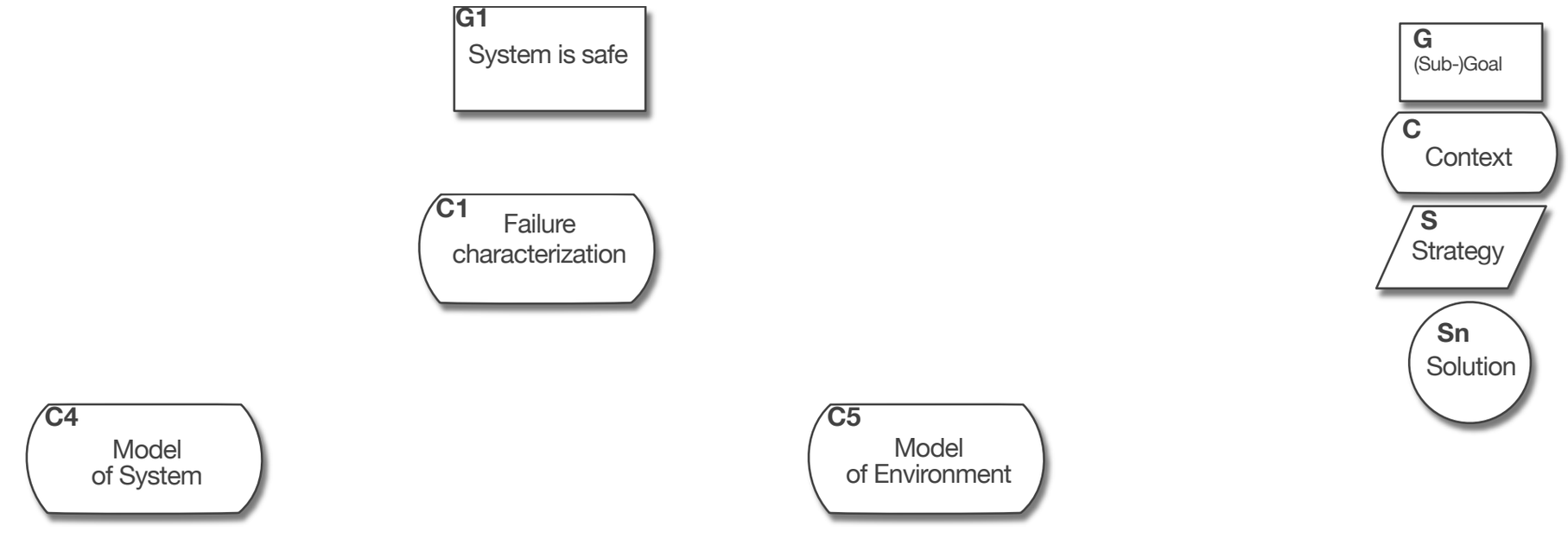
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

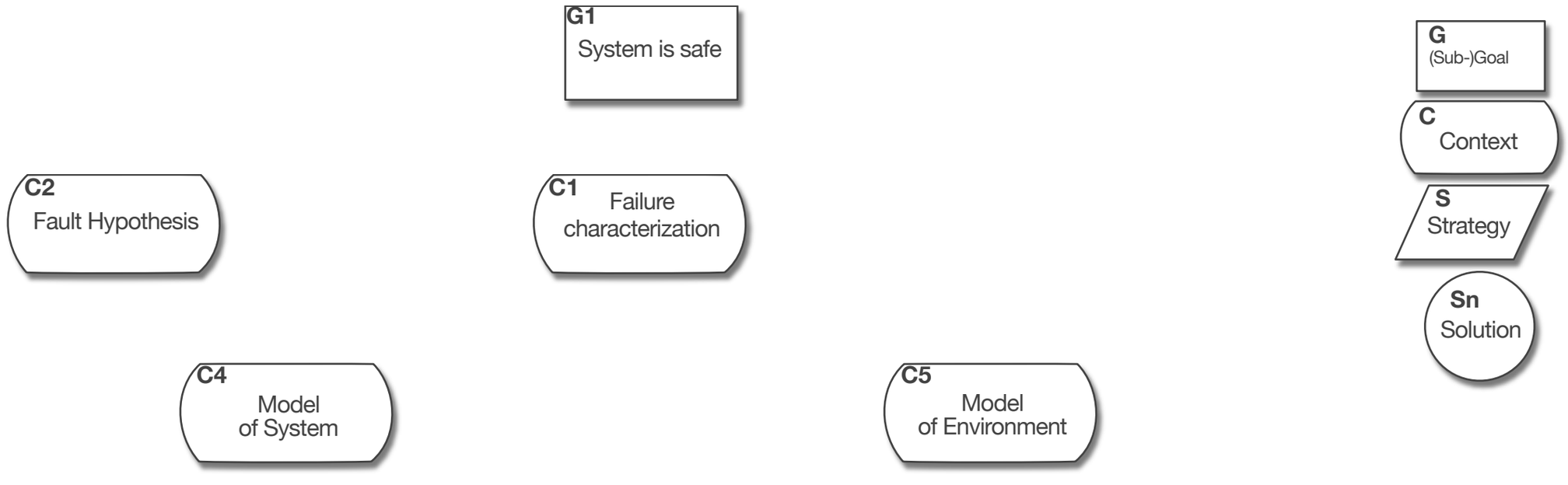
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

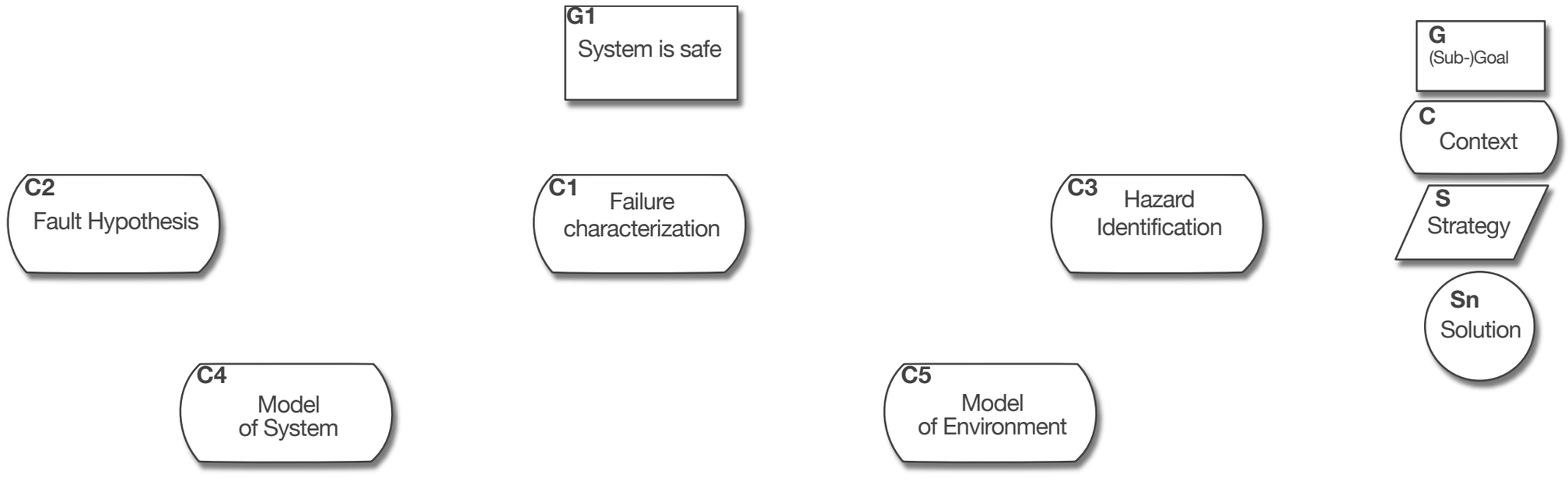
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

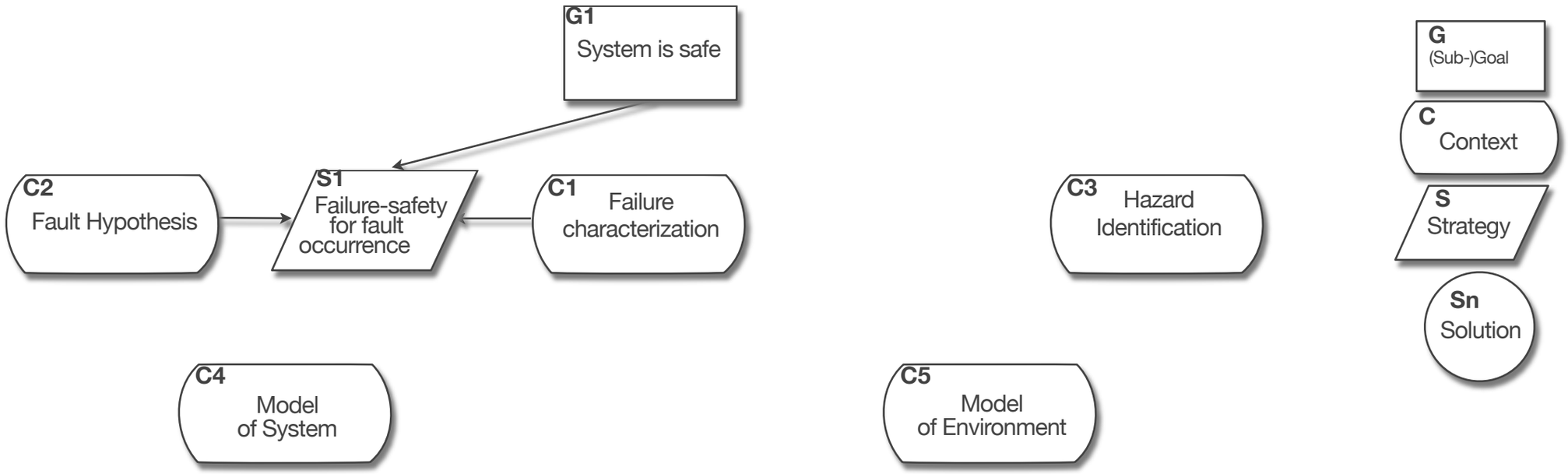
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

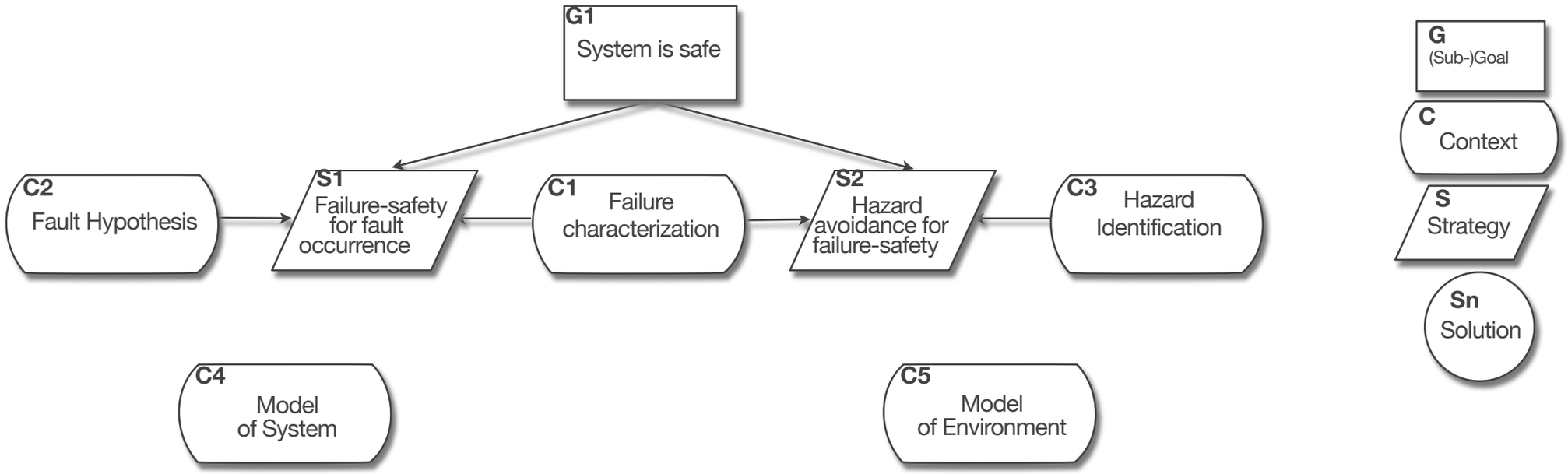
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

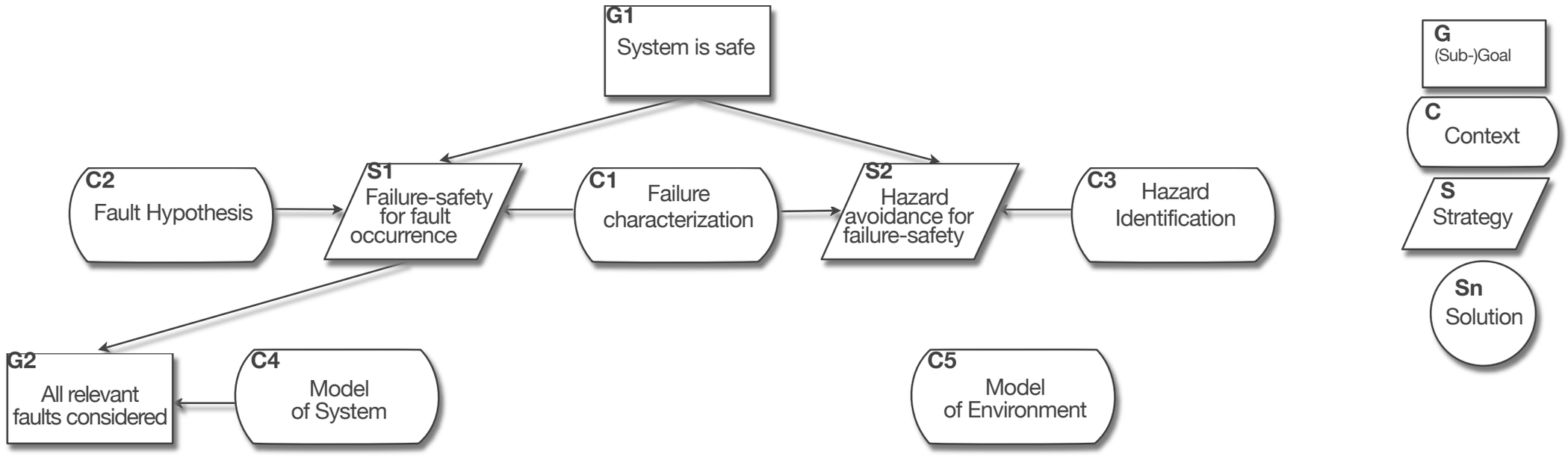
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

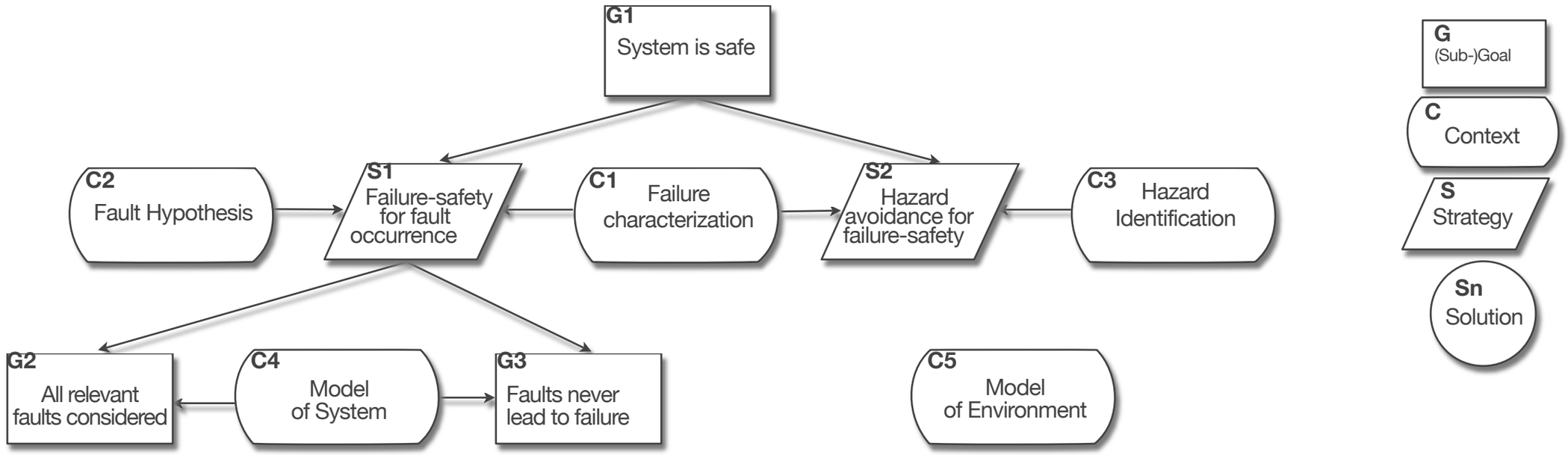
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

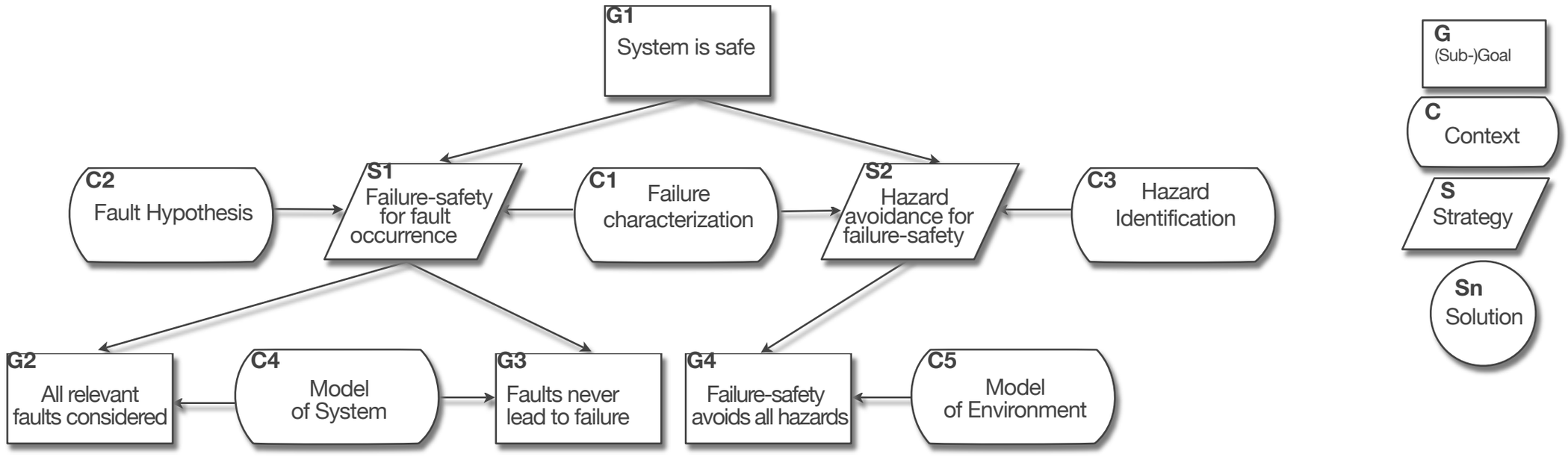
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

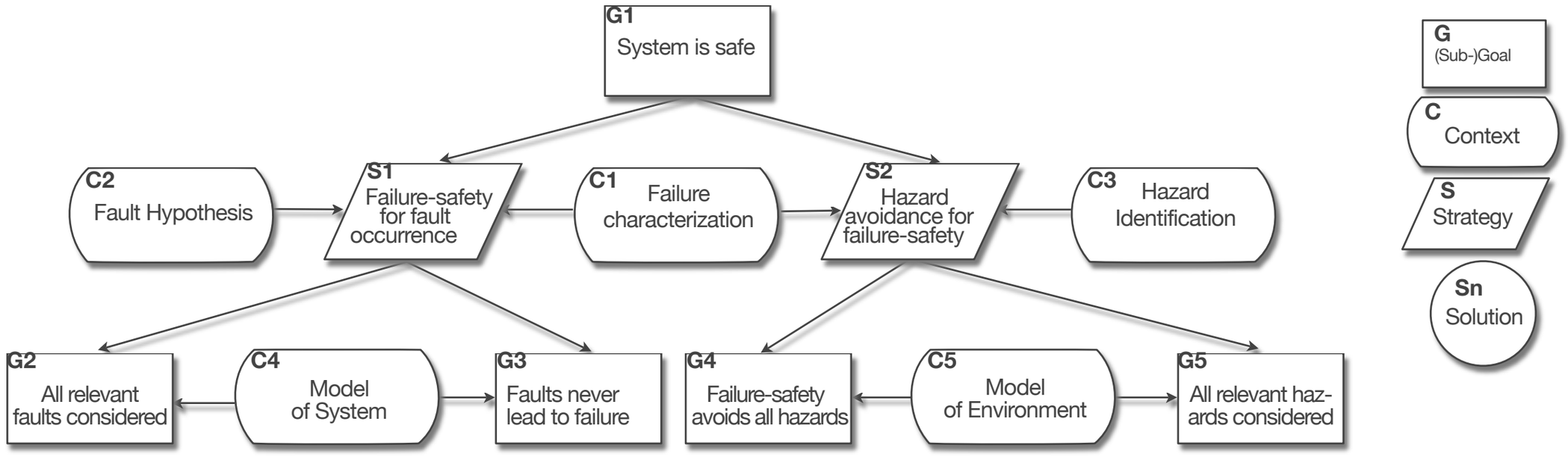
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

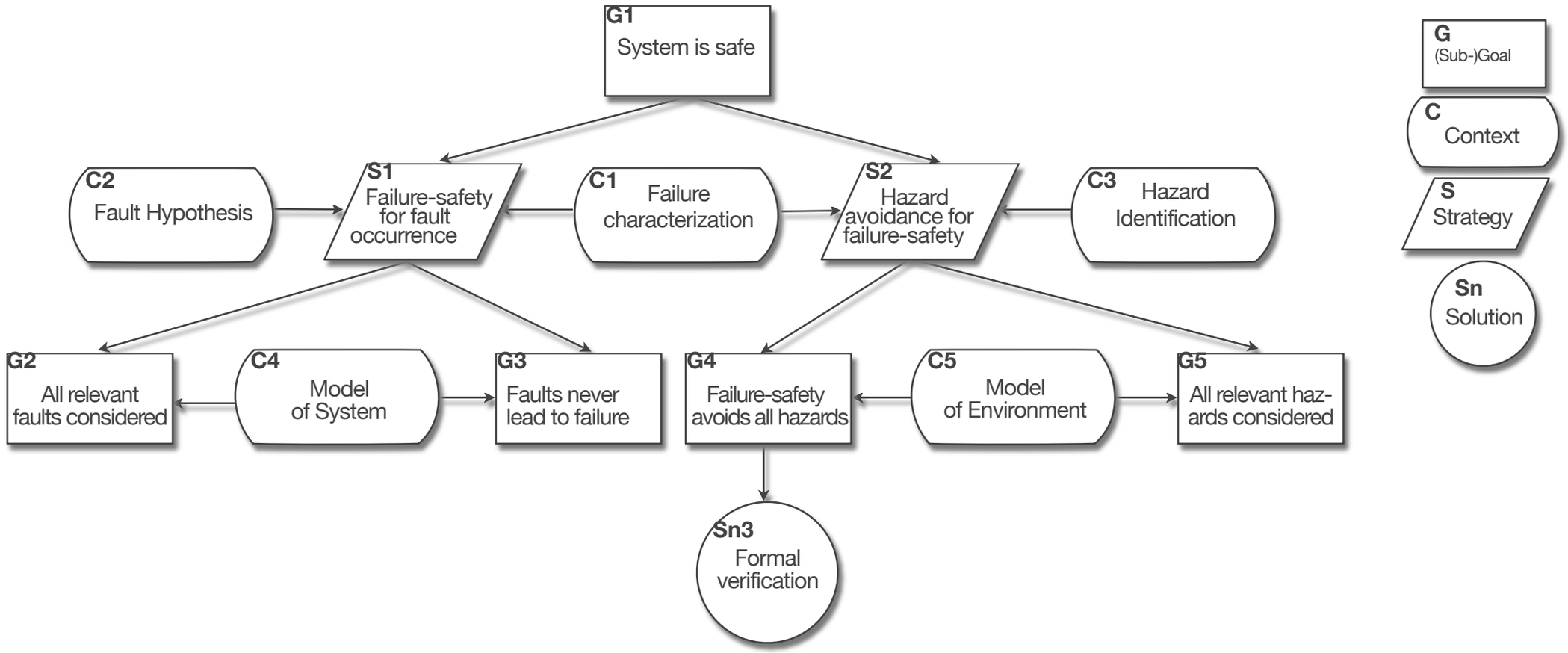
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

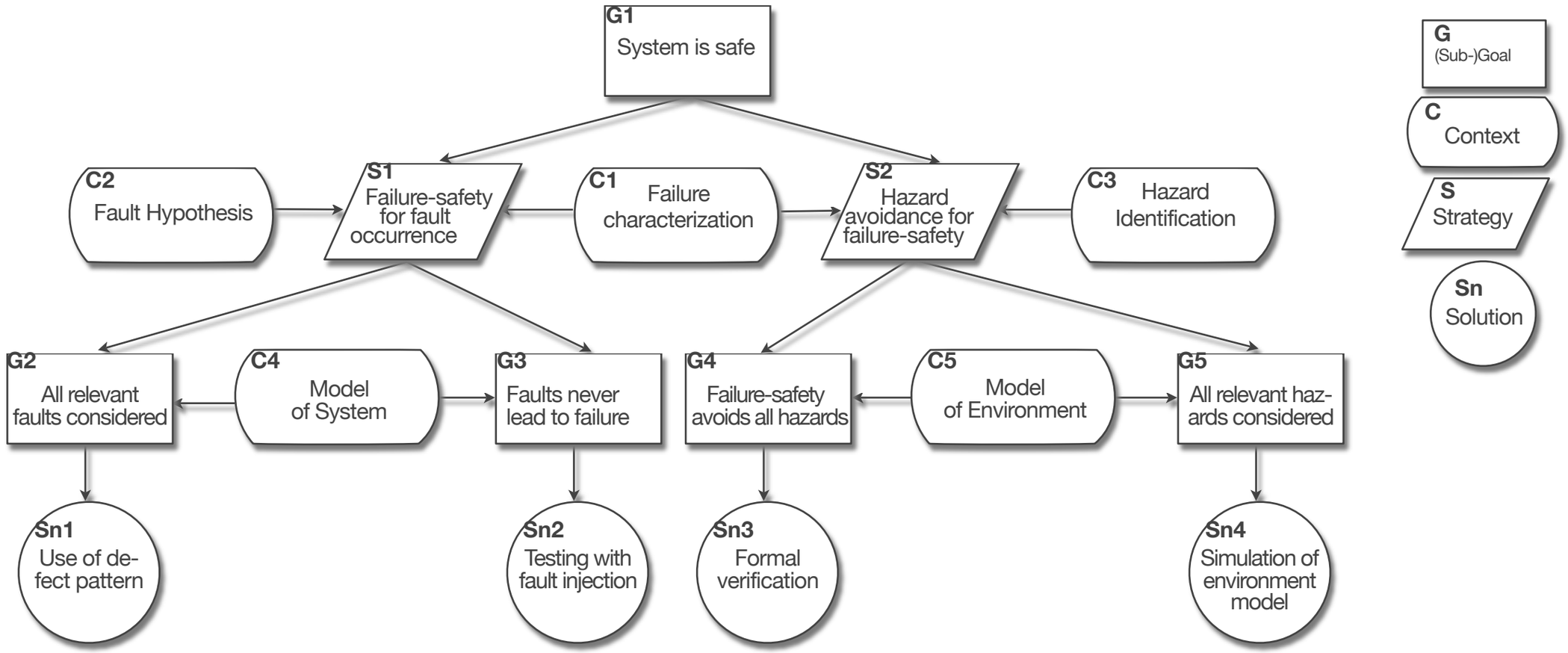
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

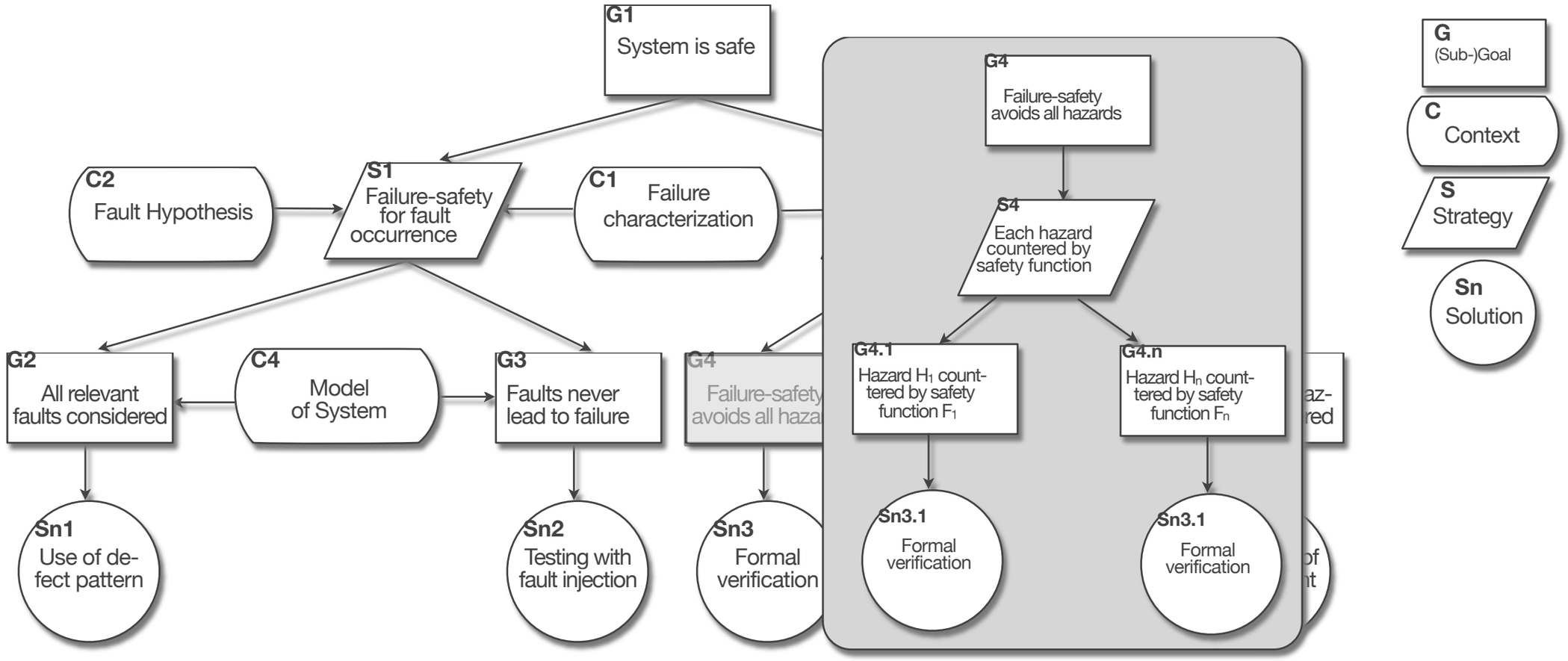
Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

Modellbasierter Safety-Case: Struktur



Gesamtstruktur: „Wie wird die funktionale Sicherheit erreicht“

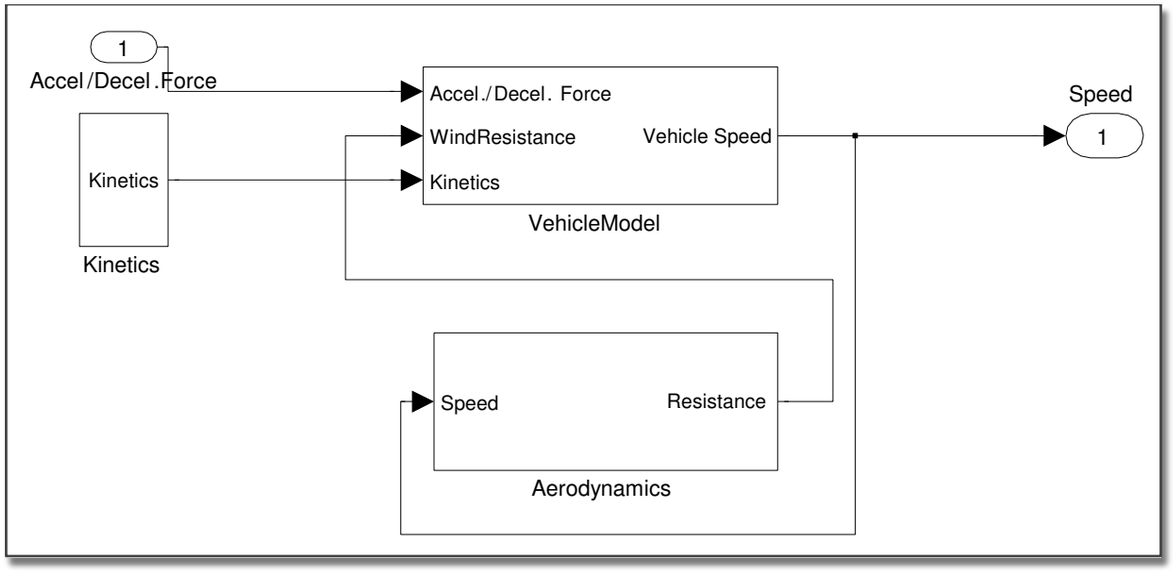
- Fokus: Standardisierte, strukturierte Argumentation
- Ansatz: Schematisierte, systemspezifische Konstruktion
  - Bausteine und Grundmuster (Ziele, Annahmen, Argumente, Verfahren)
  - Instantiierung für spezifisches System

Modellbasierter Safety-Case: Modelle

Modellspezifikation: „Welche Annahmen werden gemacht“

- Fokus: Explizite, formalisierte Annahmen
- Ansatz: Strukturierte, systemspezifische Modelle
  - Umgebungsmodell (Umgebung, Gerät, Nutzer)
  - Systemmodell (Software, Hardware, Mechanik)

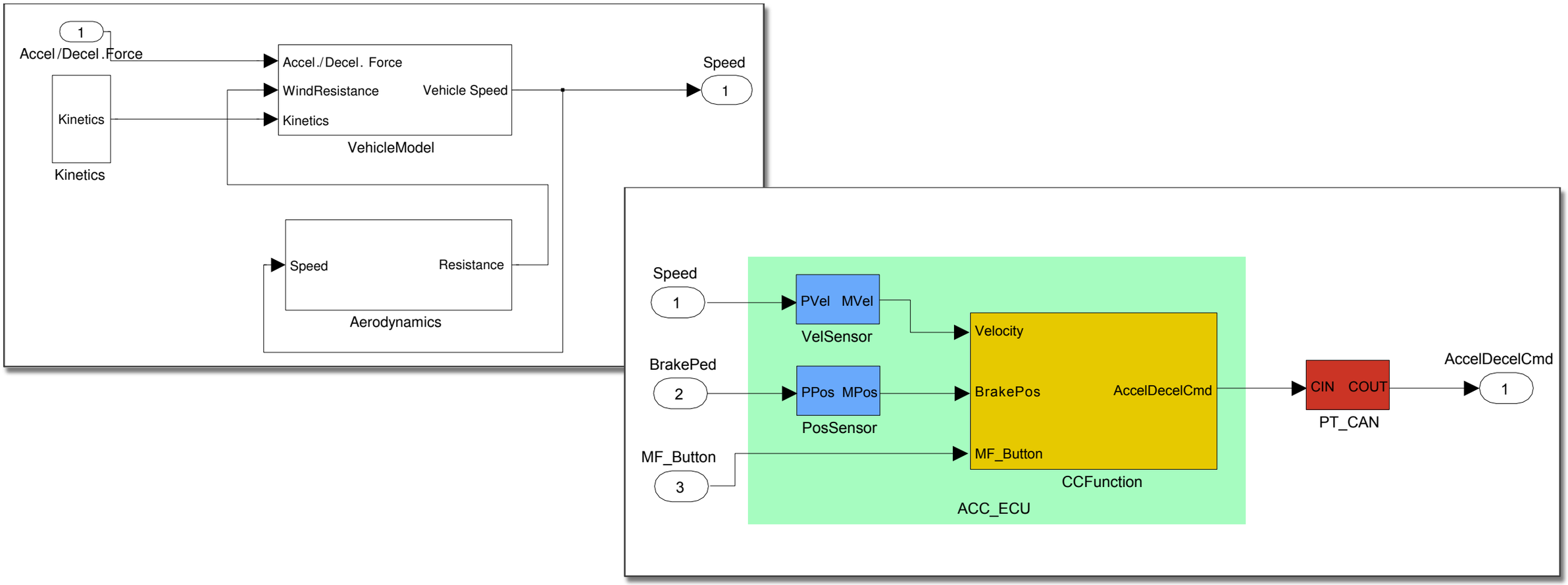
Modellbasierter Safety-Case: Modelle



Modellspezifikation: „Welche Annahmen werden gemacht“

- Fokus: Explizite, formalisierte Annahmen
- Ansatz: Strukturierte, systemspezifische Modelle
  - Umgebungsmodell (Umgebung, Gerät, Nutzer)
  - Systemmodell (Software, Hardware, Mechanik)

Modellbasierter Safety-Case: Modelle



Modellspezifikation: „Welche Annahmen werden gemacht“

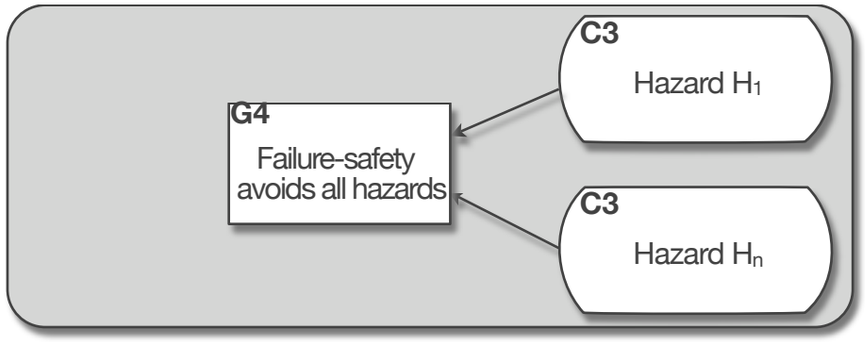
- Fokus: Explizite, formalisierte Annahmen
- Ansatz: Strukturierte, systemspezifische Modelle
  - Umgebungsmodell (Umgebung, Gerät, Nutzer)
  - Systemmodell (Software, Hardware, Mechanik)

Modellbasierter Safety-Case: Methoden

Gesamtstruktur: „Worauf basiert die Argumentation“

- Fokus: Bewährte, wiederverwendbare Argumentationen
- Ansatz: Generische, standardisierte Methoden
  - Argumentationsmuster (z.B. Argumentationsketten)
  - Lösungsmethoden (z.B. Fehlermuster, Analyseverfahren)

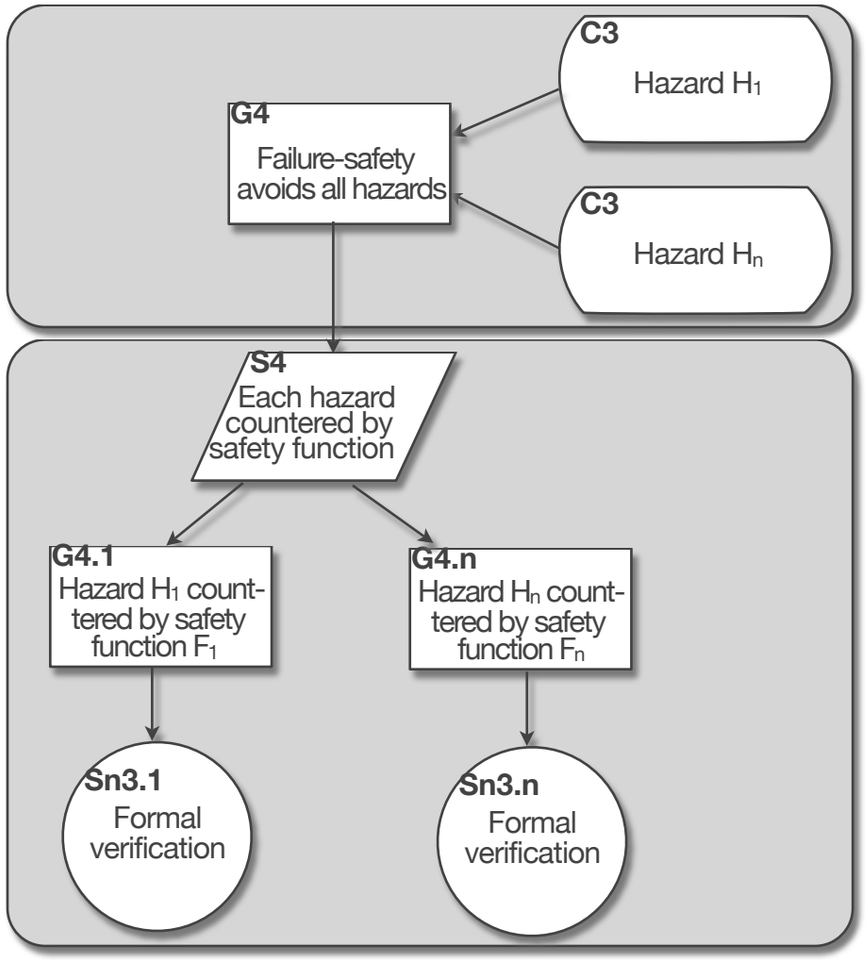
Modellbasierter Safety-Case: Methoden



Gesamtstruktur: „Worauf basiert die Argumentation“

- Fokus: Bewährte, wiederverwendbare Argumentationen
- Ansatz: Generische, standardisierte Methoden
  - Argumentationsmuster (z.B. Argumentationsketten)
  - Lösungsmethoden (z.B. Fehlermuster, Analyseverfahren)

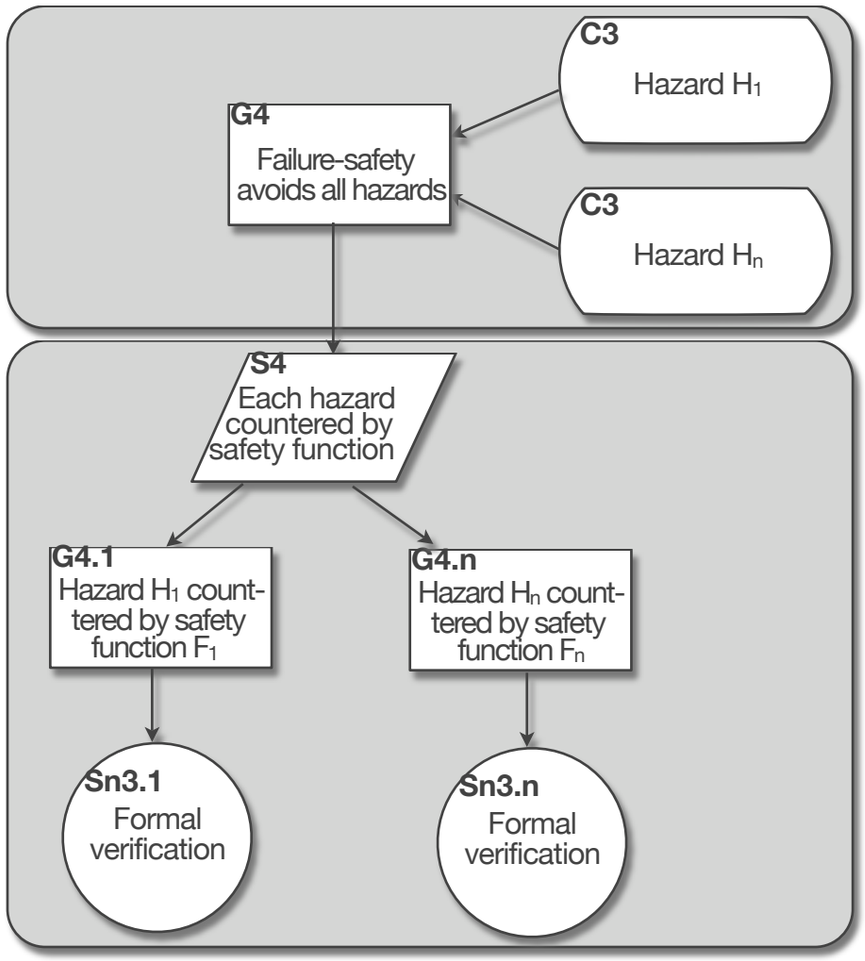
Modellbasierter Safety-Case: Methoden

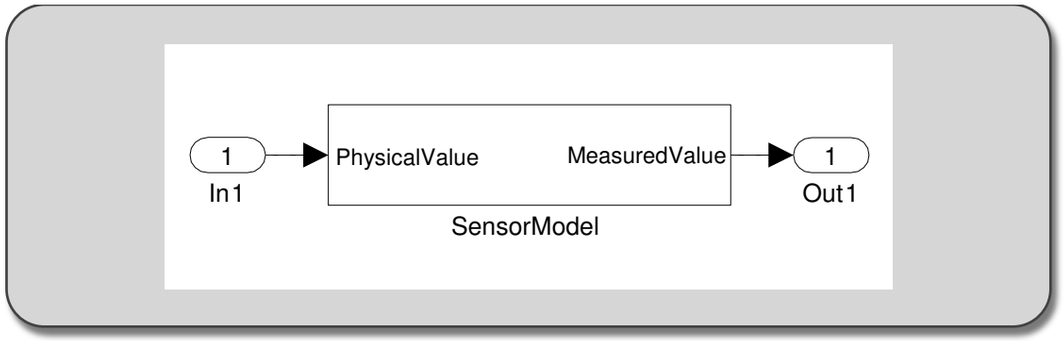


Gesamtstruktur: „Worauf basiert die Argumentation“

- Fokus: Bewährte, wiederverwendbare Argumentationen
- Ansatz: Generische, standardisierte Methoden
  - Argumentationsmuster (z.B. Argumentationsketten)
  - Lösungsmethoden (z.B. Fehlermuster, Analyseverfahren)

Modellbasierter Safety-Case: Methoden

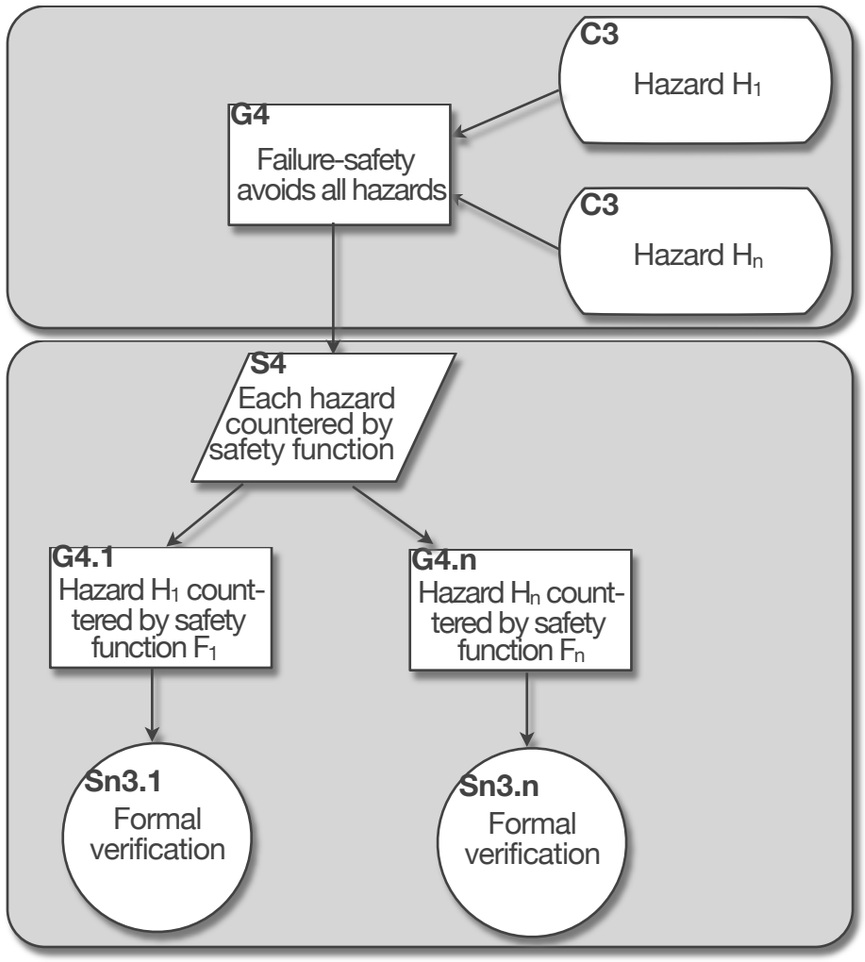


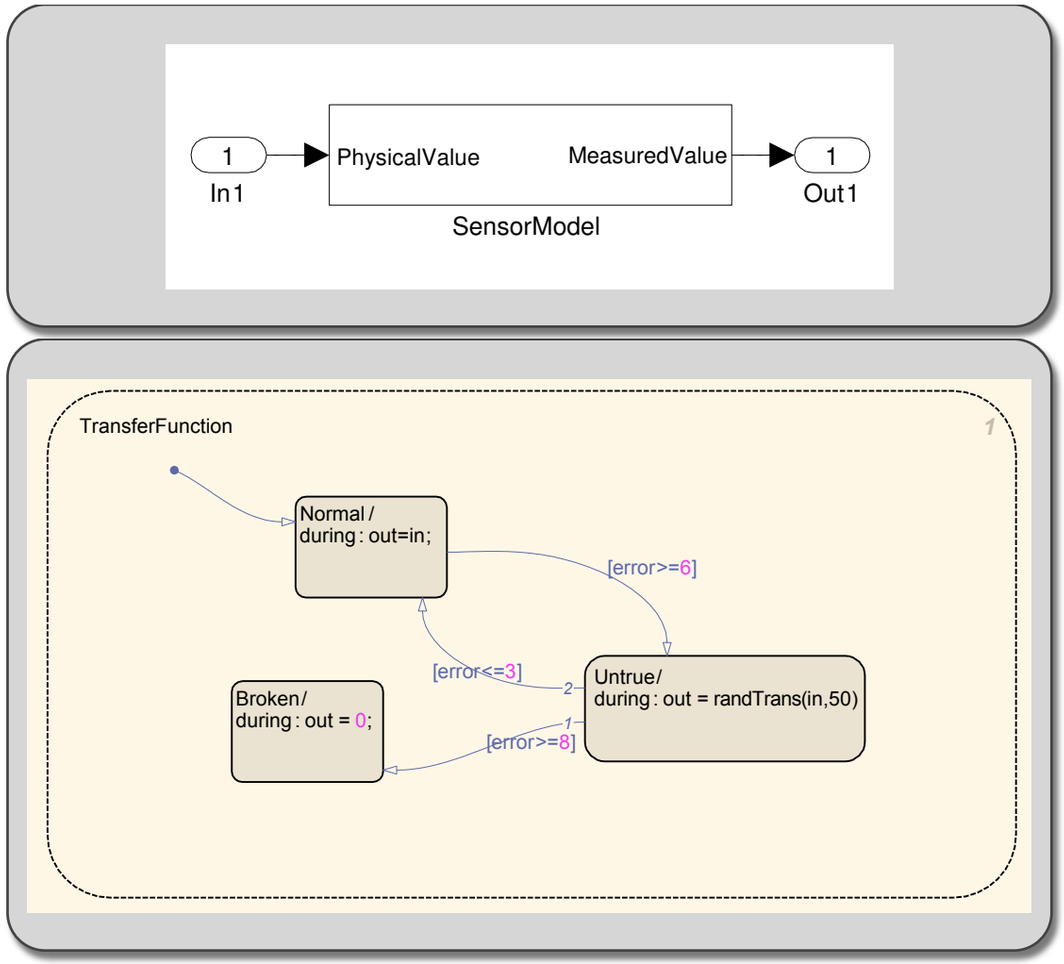


Gesamtstruktur: „Worauf basiert die Argumentation“

- Fokus: Bewährte, wiederverwendbare Argumentationen
- Ansatz: Generische, standardisierte Methoden
  - Argumentationsmuster (z.B. Argumentationsketten)
  - Lösungsmethoden (z.B. Fehlermuster, Analyseverfahren)

Modellbasierter Safety-Case: Methoden





Gesamtstruktur: „Worauf basiert die Argumentation“

- Fokus: Bewährte, wiederverwendbare Argumentationen
- Ansatz: Generische, standardisierte Methoden
  - Argumentationsmuster (z.B. Argumentationsketten)
  - Lösungsmethoden (z.B. Fehlermuster, Analyseverfahren)

Zusammenfassung: Modellbasierte Safety-Cases

Modellbasierte Safety-Cases:

- Ziel: Erweiterung aktueller Ansätze zur Systemqualifizierung
- Ansatz: Schematisierte Argumentation über Korrektheit der Sicherheitsfunktionen
- Prinzipien:
  - Konstruktion nach Standardstruktur
  - Modelle als Argumentationsbasis
  - Verwendung von Argumentationsbausteinen

- Erprobung: Safety Case für Automotive-Anwendung
  - Adaptive Geschwindigkeitsregelung
  - Werkzeuge: MATLAB/Simulink,Embedded Validator,TargetLink