A Safety Case Pattern for Model-Based Development Approach

(NFM, April 2012)

Anaheed Ayoub, BaekGyu Kim,
Insup Lee, Oleg Sokolsky

Department of Computer and Information Science

University of Pennsylvania

Penn Engineering

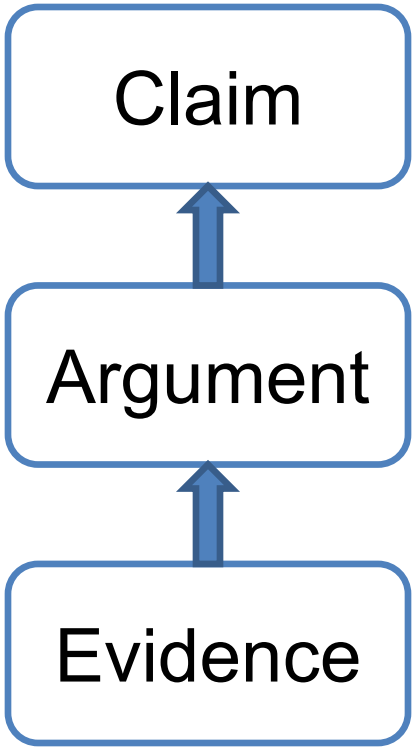
PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Motivation

- System assurance is a major issue in safety-critical applications
- Many safety-critical systems are reviewed and approved by regulators
- Domains:
  - Aerospace
  - Automobiles
  - Rail Systems
  - Energy (especially nuclear) systems
  - Medical systems
  - Weapons Systems

Assurance Cases

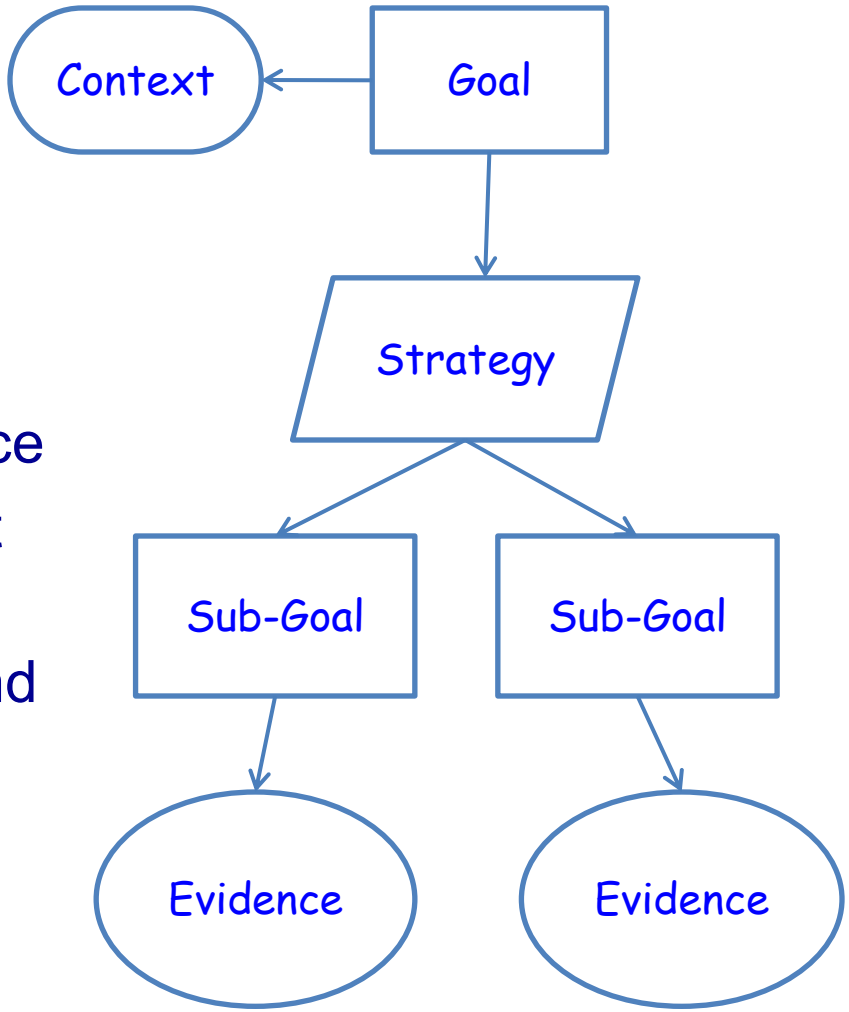
- An assurance case is a method for demonstrating the validity of a claim by providing a convincing argument together with supporting evidence.



FDA - Infusion Pump - Premarket Notification
[510(k)] Submissions DRAFT GUIDANCE, April 2010

Assurance Cases

- To construct an assurance case we need to:
  - make an explicit set of claims about the system
  - define the intended context
  - produce the supporting evidence
  - provide a set of arguments that link the claims to the evidence
  - make clear the assumptions and judgments underlying the arguments
- Safety case is a special kind:
  - Claims are limited to safety



Case Study: Infusion Pump

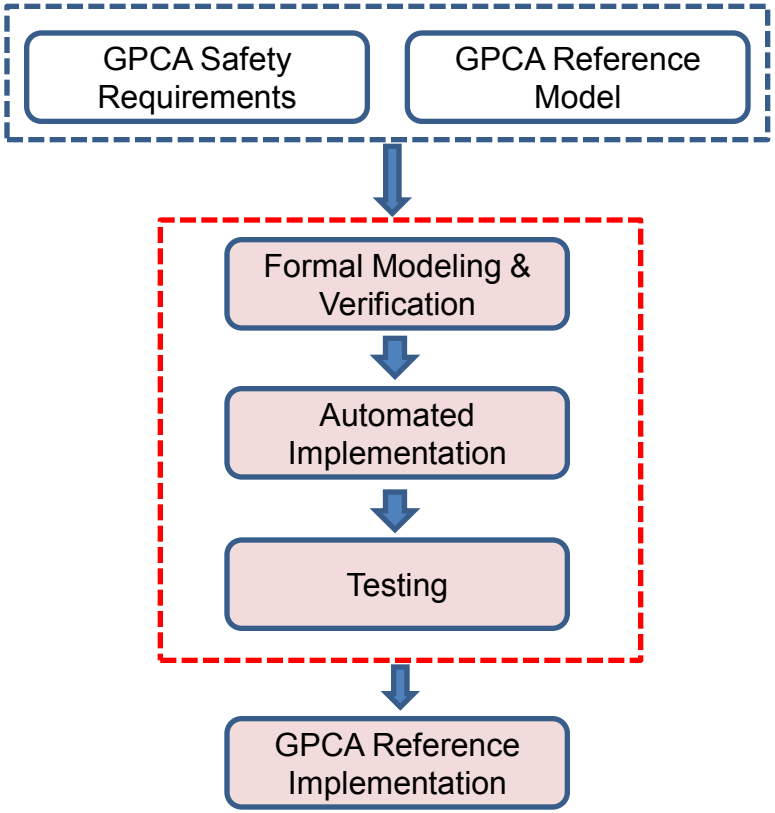
- Deceptively simple
  - 2005—2009: 56, 000 adverse event reports; 87 recalls
    - 1% deaths, 34% serious injuries

FDA, White Paper: Infusion Pump Improvement Initiative, April 2010.

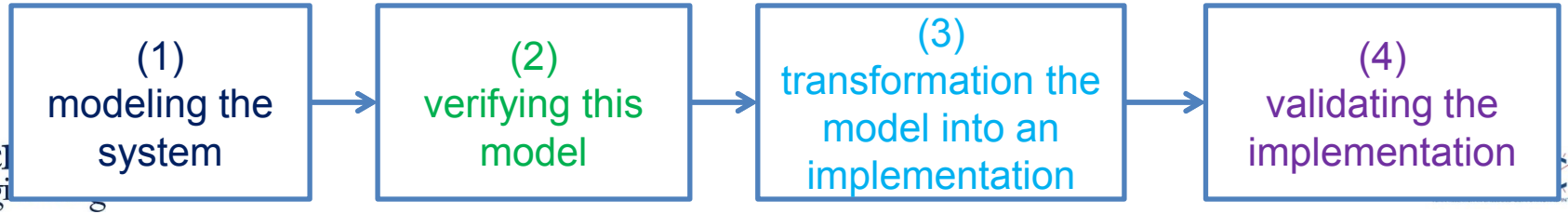
- Case study goals
  - Show how to do it right
    - Develop good requirements
    - Apply rigorous development
    - Explore assurance case construction
  - Provide guidance to manufacturers

GPCA reference implementation

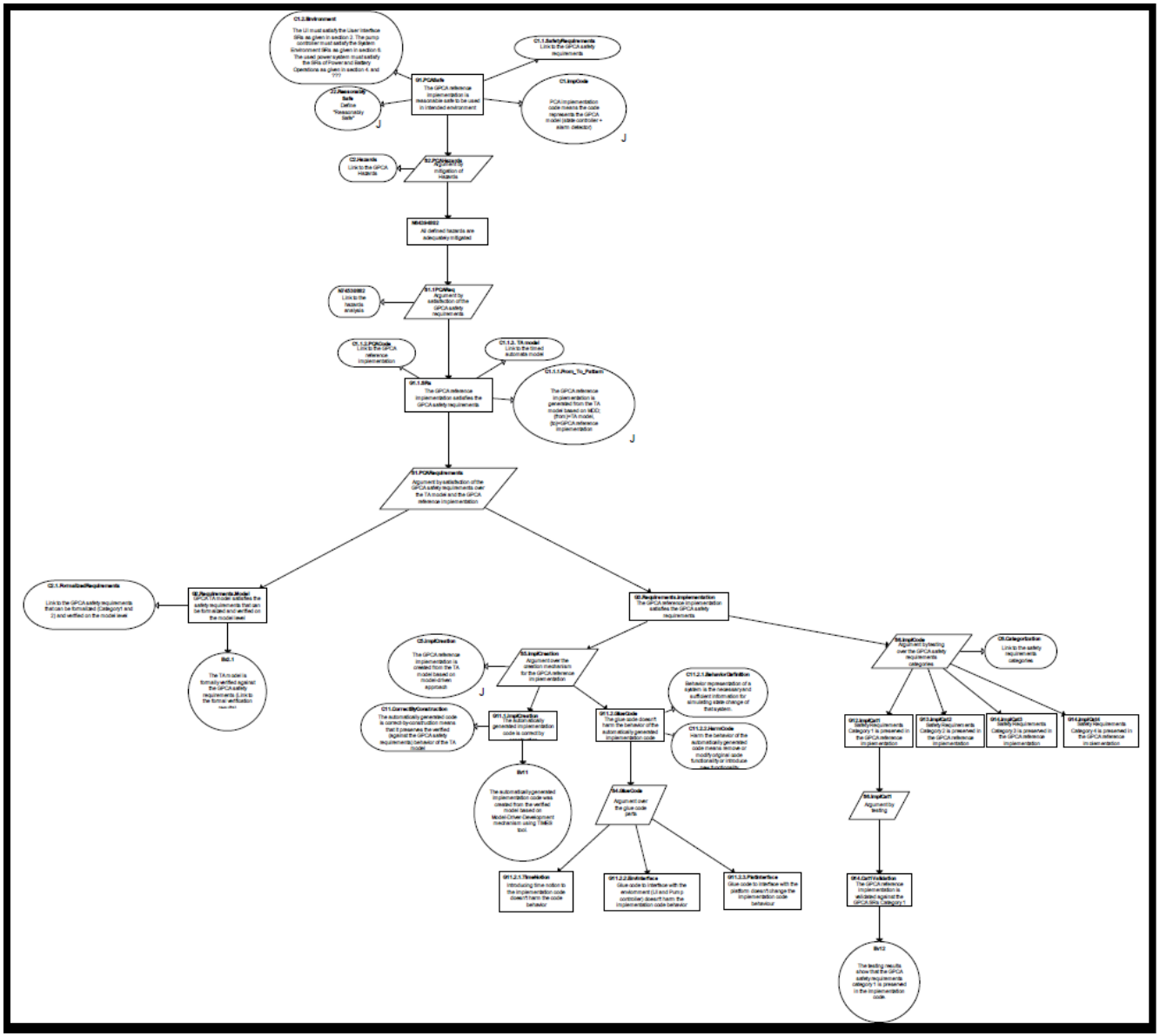
- FDA initiated
  - GPCA Safety Requirements
  - GPCA Reference Model (Simulink/Stateflow)
- Develop a GPCA reference implementation
- Construct a safety case for this implementation



Model-Based Development of GPCA Reference Implementation



The PCA Safety Case



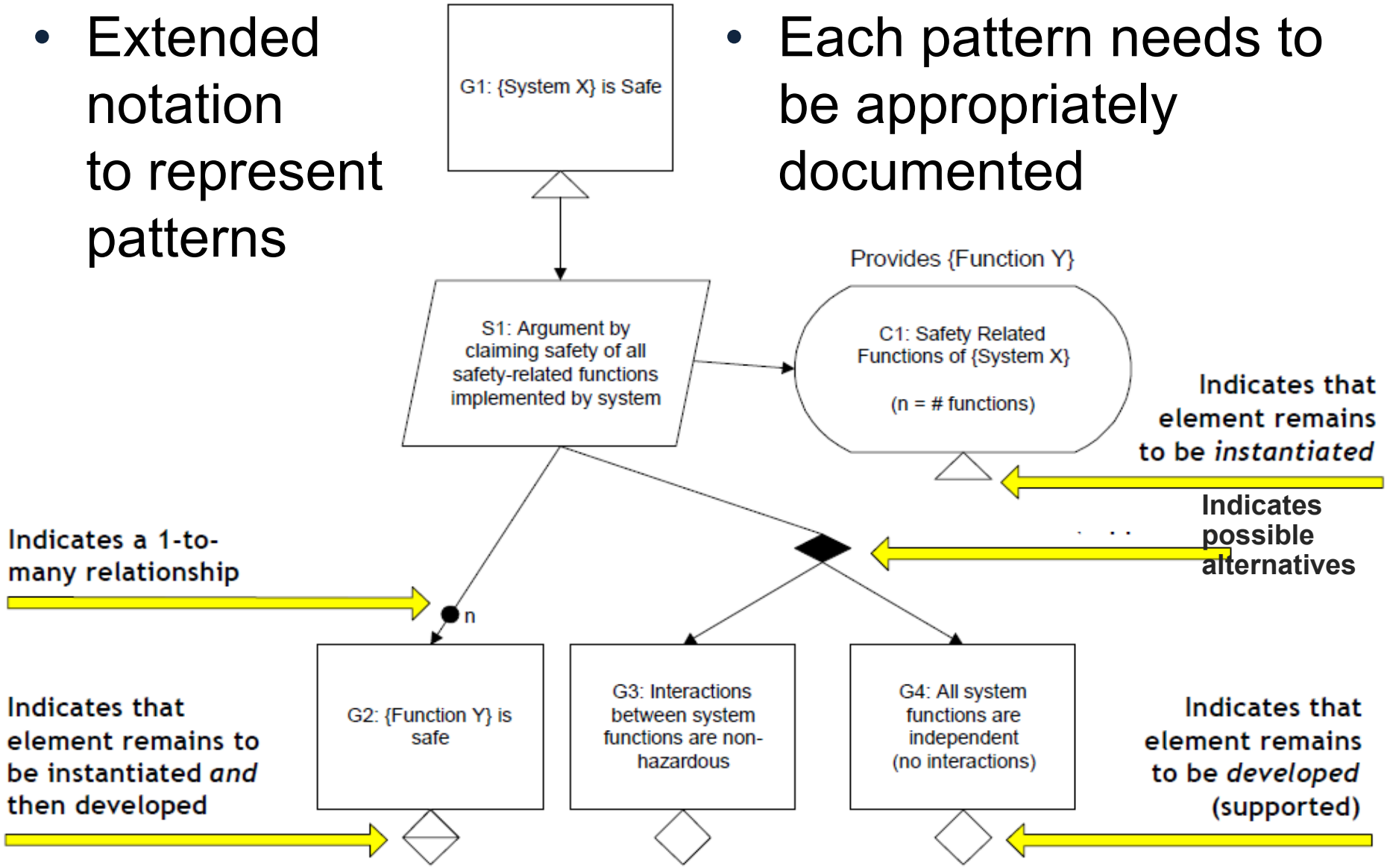
Safety Case Patterns

- Defined to capture successful (i.e., convincing, sound, etc.) arguments.
- Whenever a pattern is appropriate to a new safety case then it is instantiated within it.
- Therefore, safety case patterns allow reusing successful arguments among different safety cases.

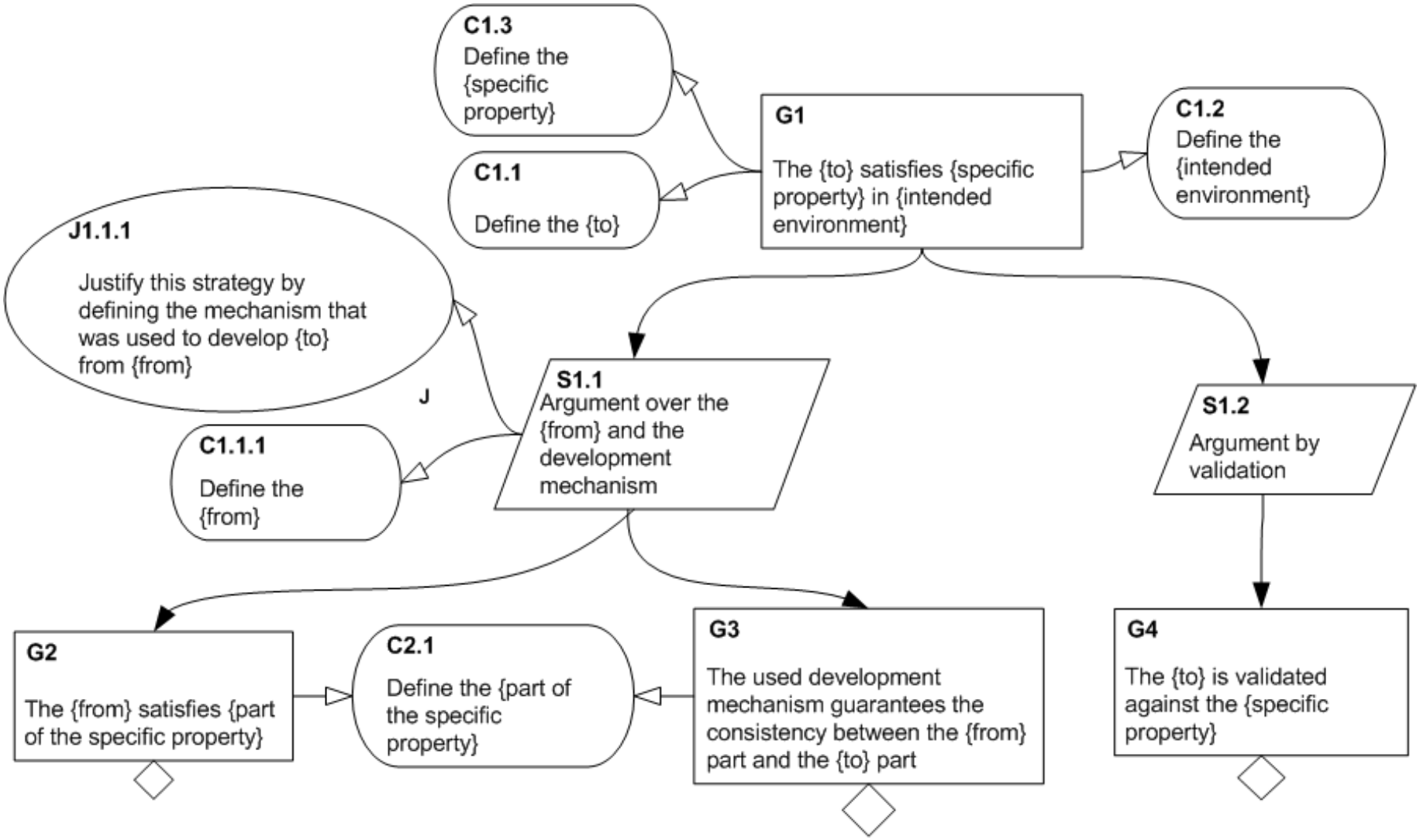
Tim Kelly, University of York, 1998

Safety Case Patterns -- Notation

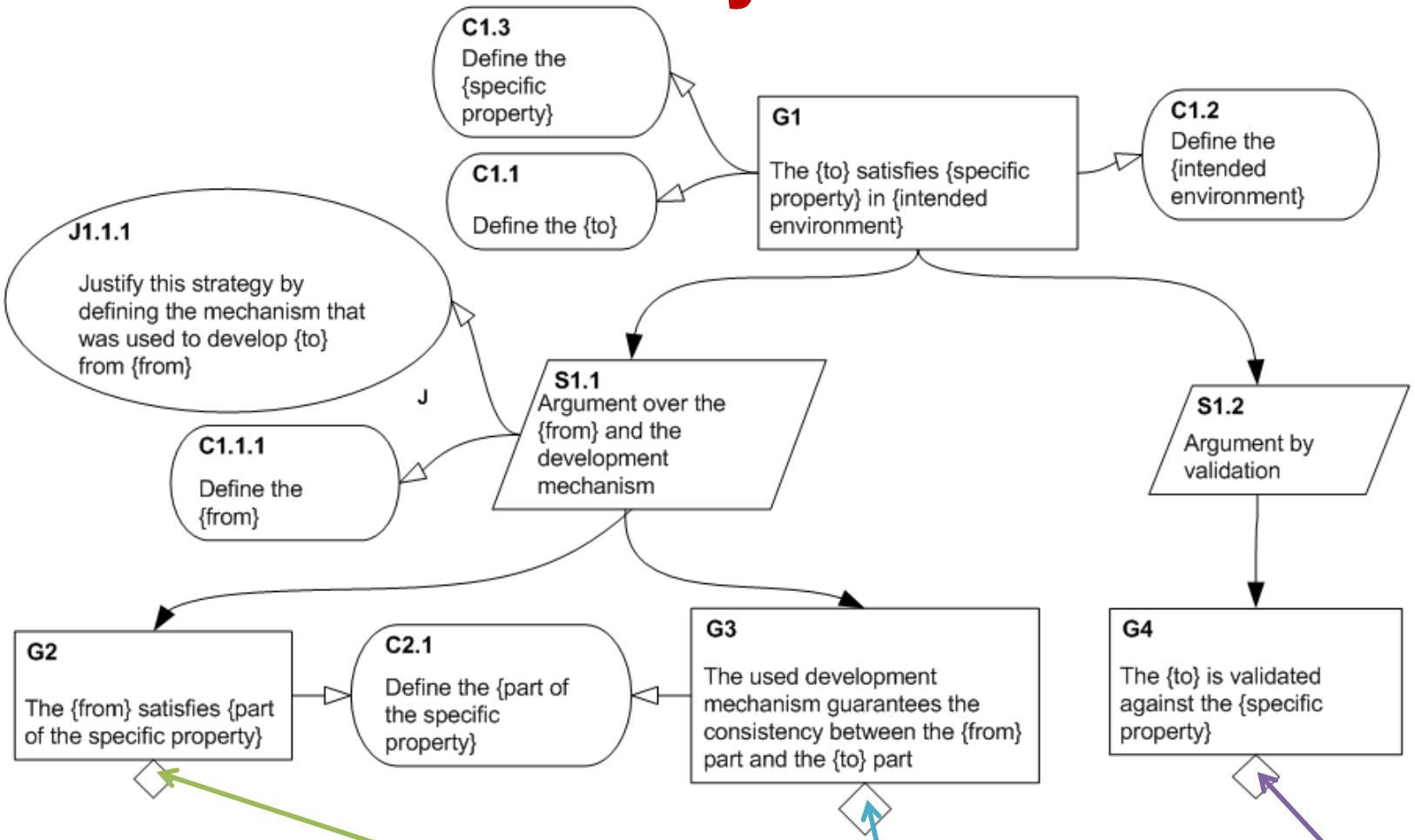
- Extended notation to represent patterns
- Each pattern needs to be appropriately documented



The PCA Safety Case – Safety Pattern

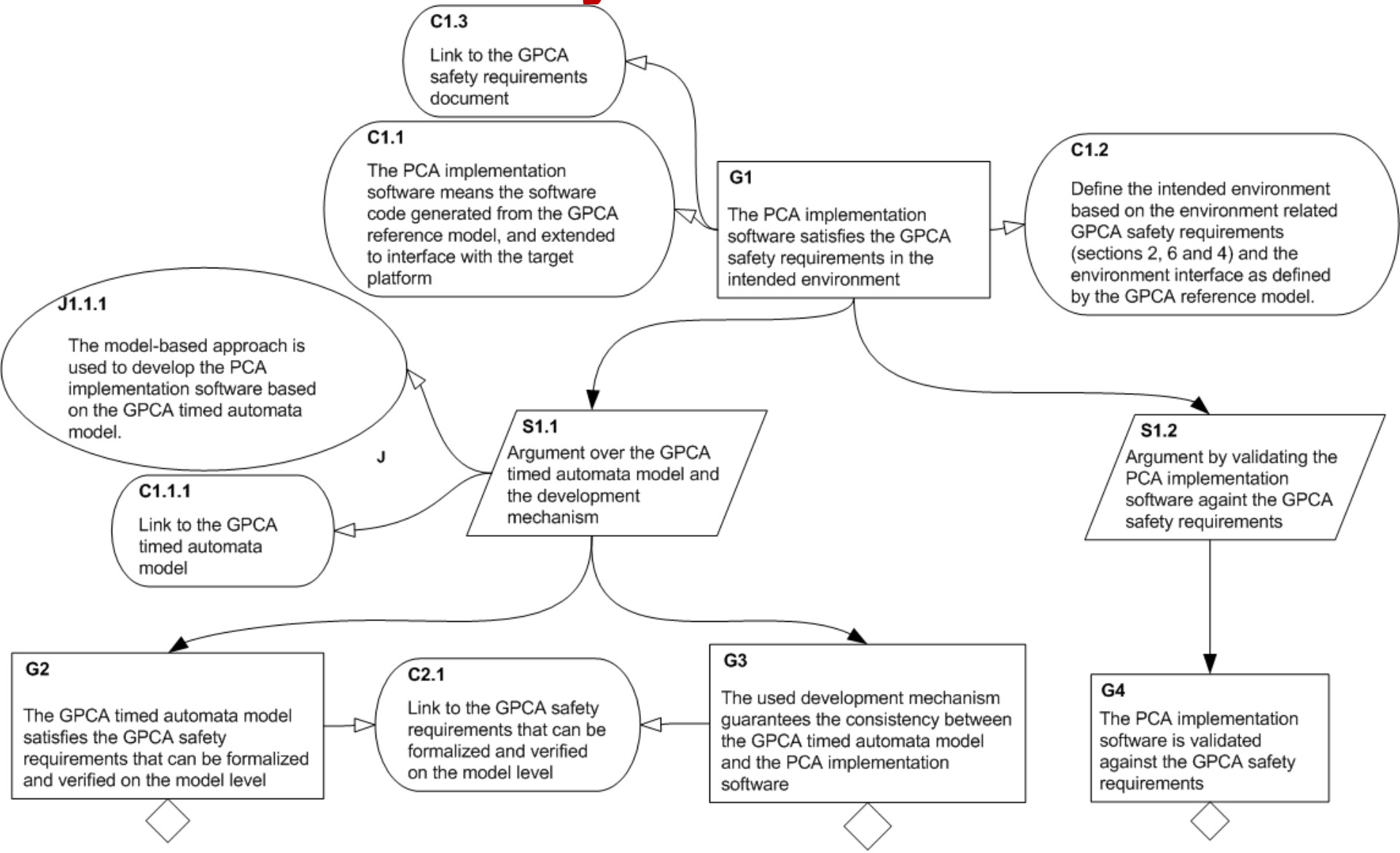


Mapping the Model-Based Approach to the Safety Pattern



(1) modeling the system → (2) verifying this model → (3) transformation the model into an implementation → (4) validating the implementation

The PCA Safety Case – Instantiation



Penn Engineering

PRECISE

Conclusion

- The main contribution of this paper is to define a safety case pattern
- This pattern is appropriate to be instantiated when implementations are developed using model-based approaches

Questions?