A Safety Case Pattern for Model-Based Development Approach

Department of Computer and Information Science
University of Pennsylvania
Anaheed Ayoub, BaekGyu Kim, Insup Lee, Oleg Sokolsky

In the premarket notification 510k [1], the U.S. Food and Drug Administration (FDA) recommends device manufacturers to submit infusion pump information through a framework known as an assurance case.

Assurance and Safety Cases

An assurance case is a way to demonstrate the validity of a claim by providing a convincing argument together with supporting evidence. The safety case is a special form of the assurance case that addresses safety.

Safety Case Patterns

Safety case patterns are defined to capture successful arguments that are used within the safety case. Whenever a safety case pattern is found to be appropriate to apply in a new safety case development, then it is instantiated within this new safety case. Therefore, safety case patterns allow reusing successful arguments among different safety cases.

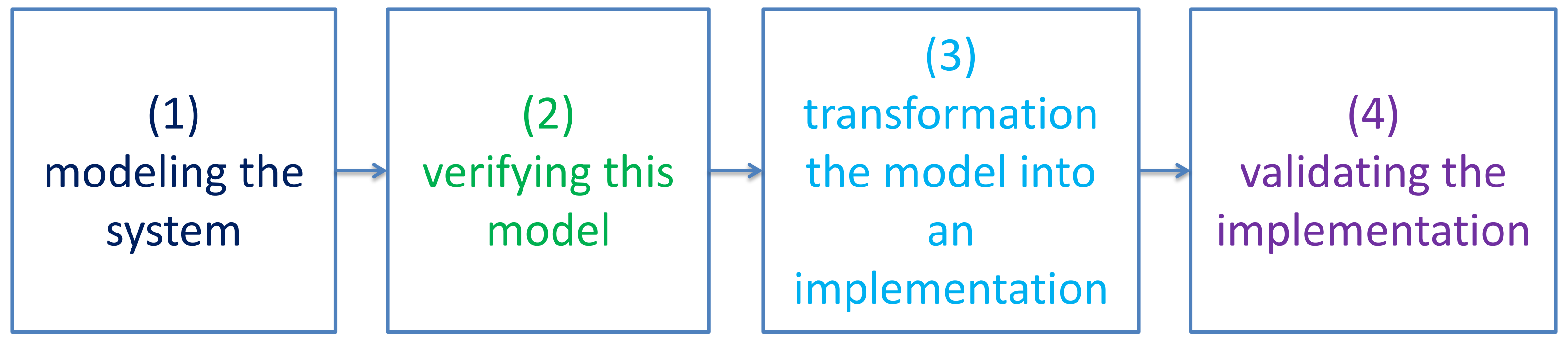
Ongoing Work

Our ongoing work is constructing a safety case for the Patient Controlled Analgesia (PCA) infusion pump system that we are developing. We applied the model-based approach to develop the PCA implementation.

Model-Based Development

Model-based development is the notion of building systems by constructing abstract representations of the system's behavior and translating them into something that executes on a target platform.

A typical model-based approach:



(1) modeling the system

(2) verifying this model

(3) transformation the model into an implementation

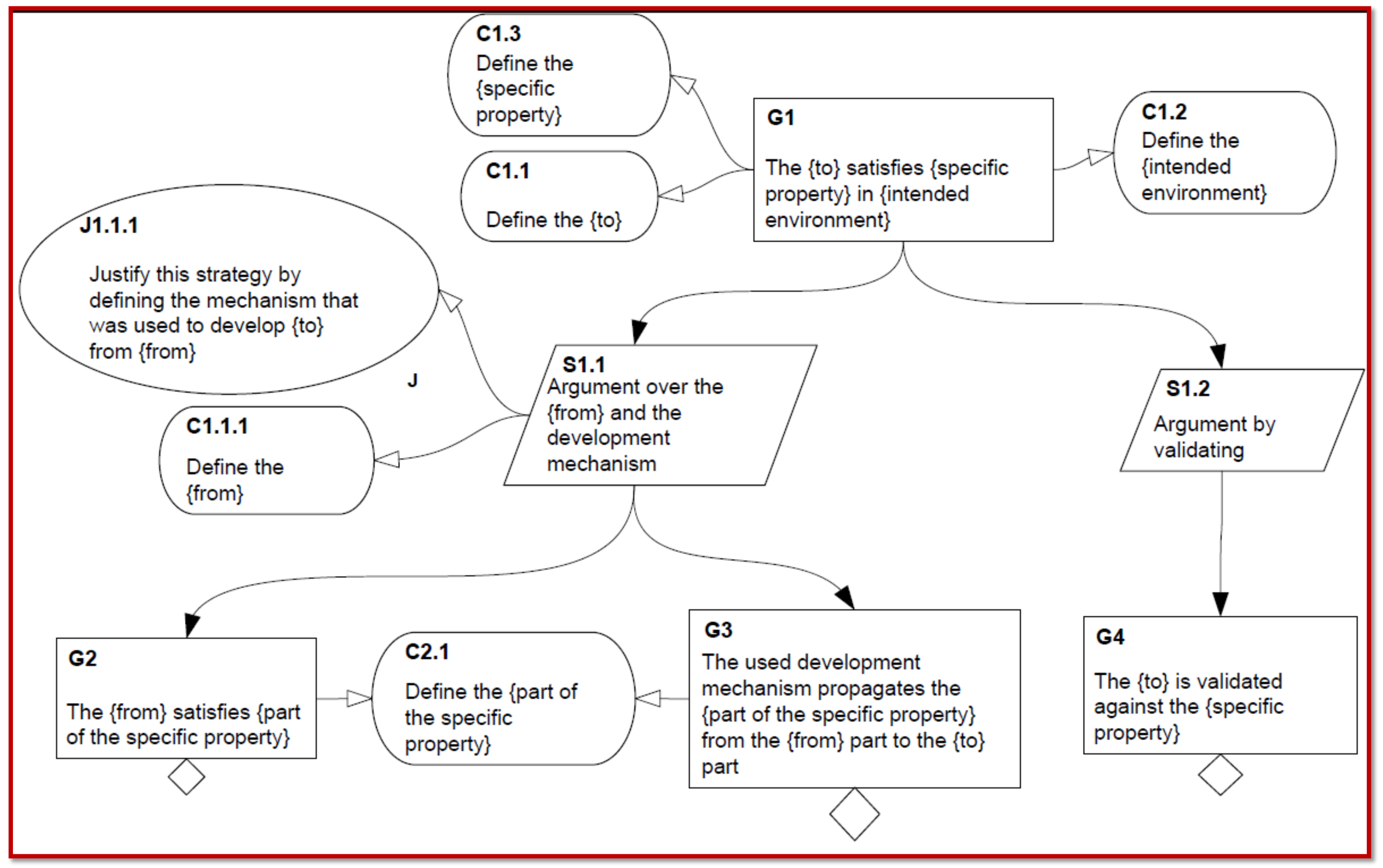
(4) validating the implementation

The Contribution

The main contribution of this work is proposing a safety case pattern that is appropriate to be used when the system is developed using the model-based approach.

The proposed pattern allows one to incorporate the belief in the model correctness obtained by verifying the system model (i.e., the second step of the model-based development approach is used to support goal "G2") and the belief in the development process gained by using a well-established development mechanism (i.e., the third step of the model-based development approach is used to support goal "G3"). In addition to arguing by validating the implementation (i.e., the fourth step of the model-based development approach is used to support goal "G4").

The Proposed Safety Case Pattern



C1.3
Define the {specific property}

C1.1
Define the {to}

G1
The {to} satisfies {specific property} in {intended environment}

C1.2
Define the {intended environment}

J1.1.1
Justify this strategy by defining the mechanism that was used to develop {to} from {from}

J

C1.1.1
Define the {from}

S1.1
Argument over the {from} and the development mechanism

S1.2
Argument by validating

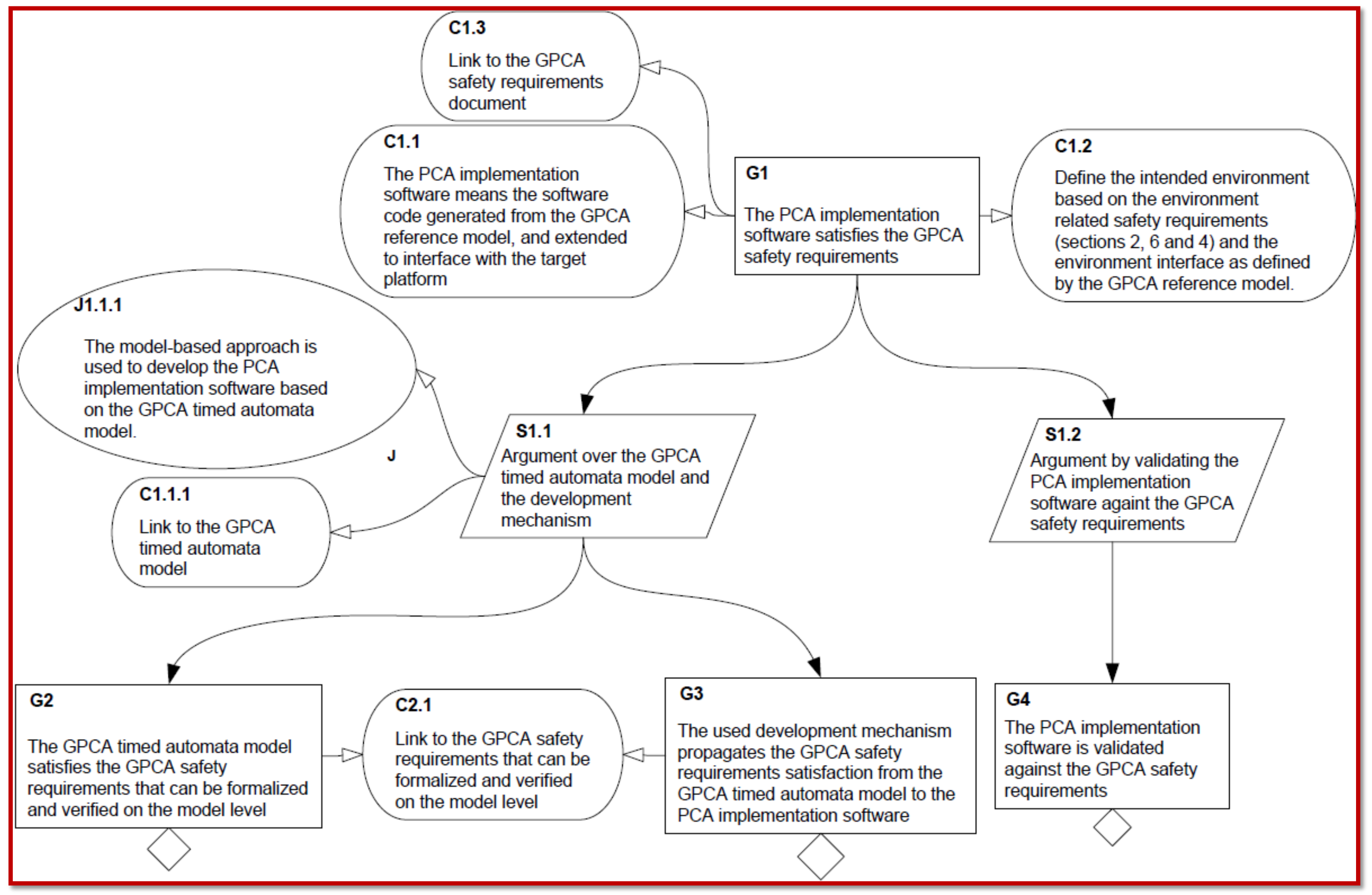
G2
The {from} satisfies {part of the specific property}

C2.1
Define the {part of the specific property}

G3
The used development mechanism propagates the {part of the specific property} from the {from} part to the {to} part

G4
The {to} is validated against the {specific property}

The Pattern Instance for the PCA Safety Case



C1.3
Link to the GPCA safety requirements document

C1.1
The PCA implementation software means the software code generated from the GPCA reference model, and extended to interface with the target platform

G1
The PCA implementation software satisfies the GPCA safety requirements

C1.2
Define the intended environment based on the environment related safety requirements (sections 2, 6 and 4) and the environment interface as defined by the GPCA reference model.

J1.1.1
The model-based approach is used to develop the PCA implementation software based on the GPCA timed automata model.

J

C1.1.1
Link to the GPCA timed automata model

S1.1
Argument over the GPCA timed automata model and the development mechanism

S1.2
Argument by validating the PCA implementation software againt the GPCA safety requirements

G2
The GPCA timed automata model satisfies the GPCA safety requirements that can be formalized and verified on the model level

C2.1
Link to the GPCA safety requirements that can be formalized and verified on the model level

G3
The used development mechanism propagates the GPCA safety requirements satisfaction from the GPCA timed automata model to the PCA implementation software

G4
The PCA implementation software is validated against the GPCA safety requirements

[1] U.S. Food and Drug Administration, Center for Devices and Radiological Health. Guidance for Industry and FDA Staff - Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions, April 2010.