Establishing Regulatory Compliance for Software Requirements

UNIVERSITY
OF TRENTO - ITALY

Silvia Ingolfo

John Mylopoulos

Alberto Siena

30th International Conference on Conceptual Modeling
Brussels, Belgium

October 31, 2011

“You say you got a real solution,
Well, we’d all love to see the plan.

You asked me for a contribution,
Well, you know… We’re all doing what we can”

- The Beatles -

Outline

- Introduction
  - What is the problem?
  - Motivation
  - Challenges
  - Our proposal
- Background
  - Argumentation Framework
  - Nòmos Framework
- Proposed Framework
- Compliance Process
  - Our approach
  - What is compliance
  - 5 steps of the process
  - Example
- Conclusions and Future Work

Introduction

- Problem

  Legal compliance of information systems

- Motivation

  Costs of compliance is high

  Costs of non-compliance is higher

Total cost per year per organization [1] **small-medium organization**
$3.5 million
$9.4 million
+ Fines, prosecutions + Revenue loss + Productivity loss + Business disruption

- Problem for organization

  Evaluate compliance of their software product

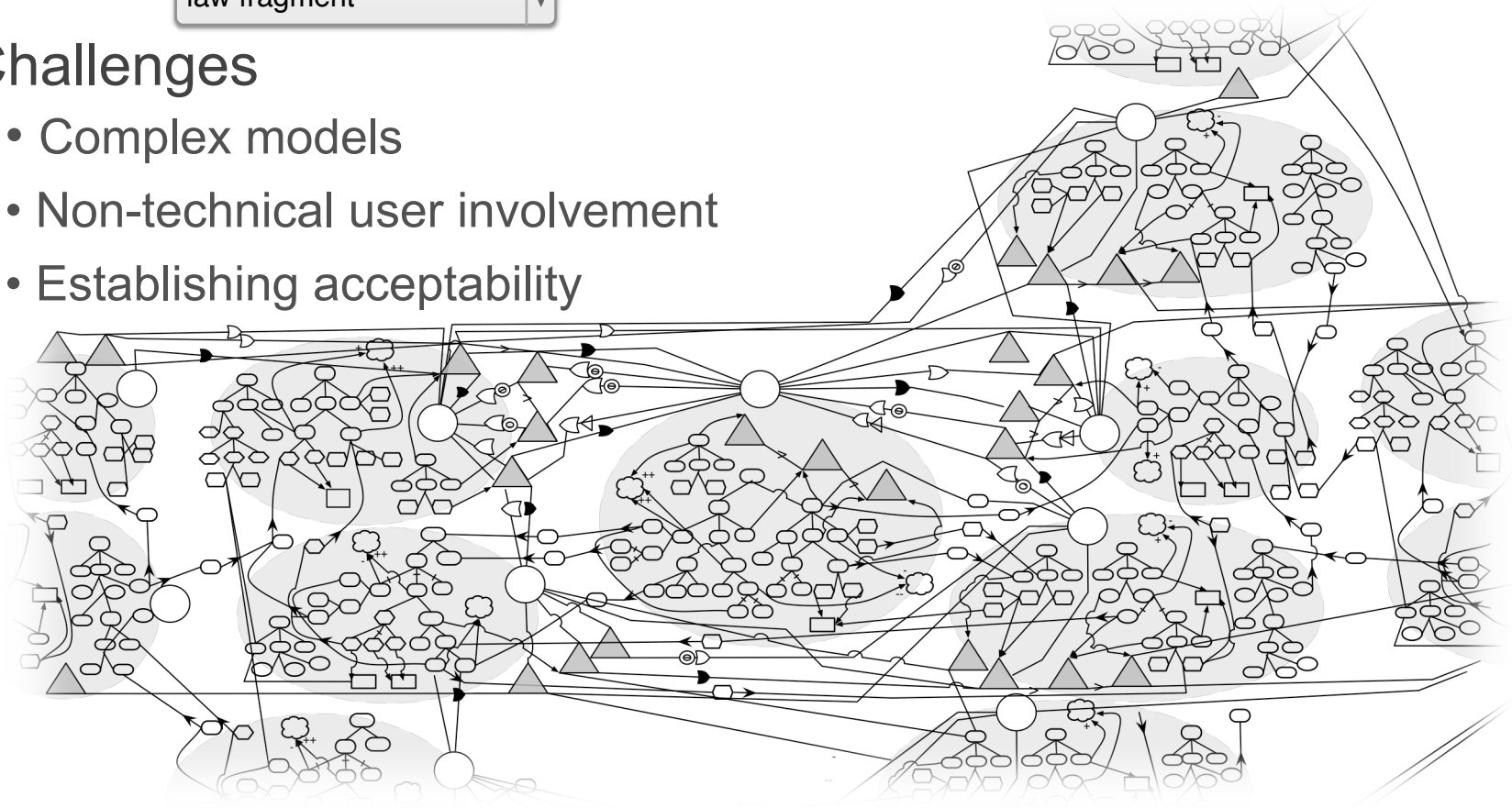
  → requirement phase

[1] Ponemon Inc, *The true cost of compliance. Research Report,* (2011)

Introduction

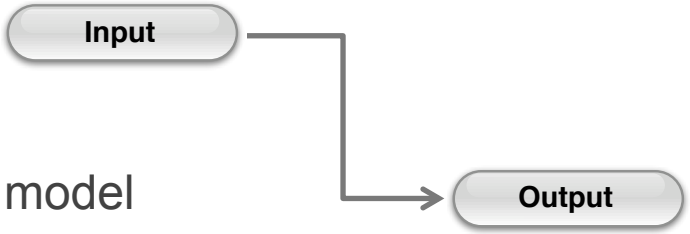
- The problem

- Challenges
  - Complex models
  - Non-technical user involvement
  - Establishing acceptability



Introduction – Our proposal

- **ARGUMENTATION** to establish acceptability
  - We need a systematic process for…
    1) … revising requirement
    2) … establishing acceptability of the model



- Systematic process for establishing compliance of a requirement model with a norm through argumentation

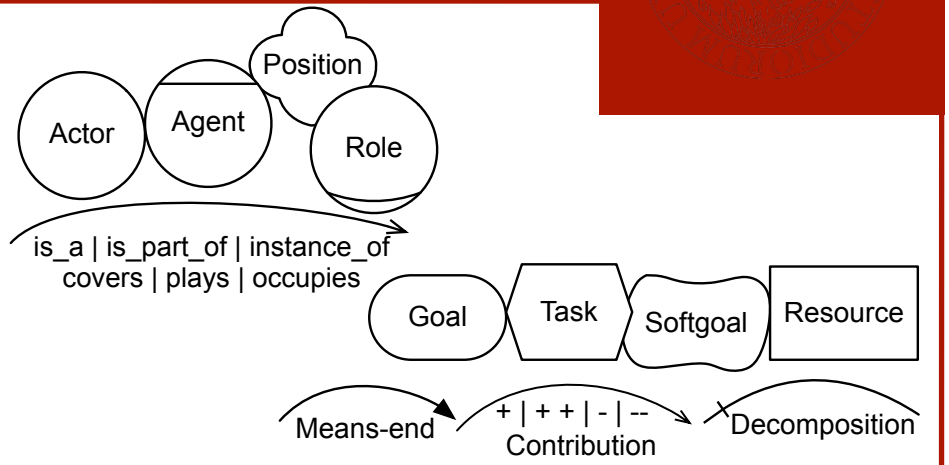
Nòmos Framework [3]

ACE Framework [2]

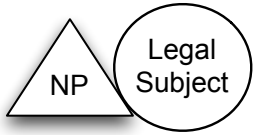
[2] I. Jureta, J. Mylopoulos, S. Faulkner, *Analysis of multi-party agreement in requirements validation*, IEEE Int. Conf. Req. Eng. Pp.57-66 (2009)
[3] A. Siena, *Engineering law-compliant requirements. The Nòmos Framework,* (2011)

Nòmos

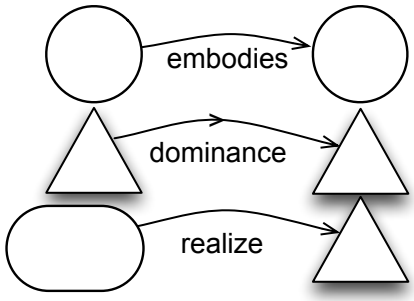
- Extension for i* [4]
  - Actors, Intentional Elements
  - Relations

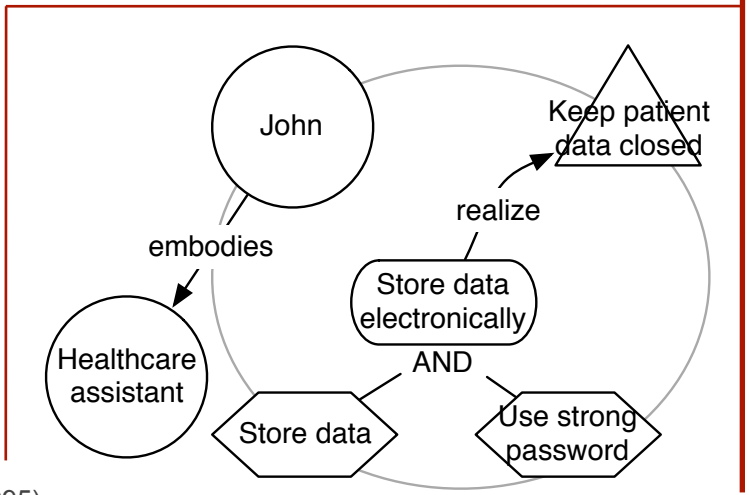


- Elements
  - Legal Subjects
  - Normative Propositions (NP)



- Relations
  - Embody
  - Dominance
  - Realization





[4] E. Yu, *Modeling Strategic relationships for process reengineering*, PhD Thesis (1995)

ACE argumentation

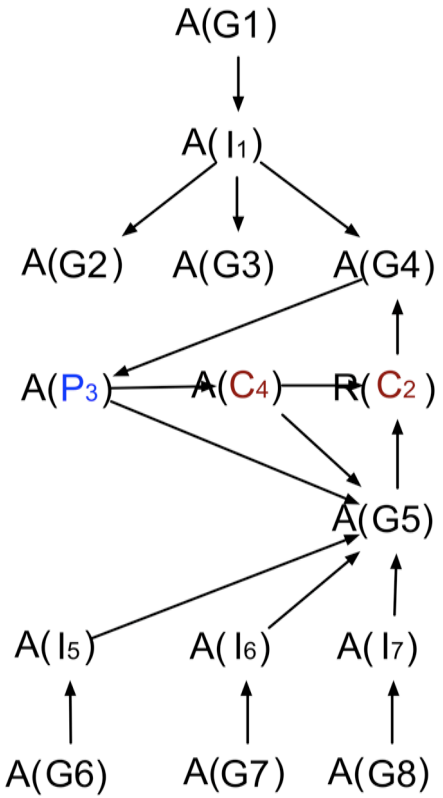
- Language of the ACE Framework

  Vertices
  - Information
  - Implication, Attack, Preference

- Algorithms
  - Retrieve Discussion
  - Evaluate Discussion (Accepted, Rejected)

- Example:

  "Build an audio player" [2]
  - Participants discuss topic
  - Information linked
  - Dialectic tree

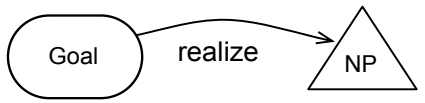


Proposed Framework

- Aim: compliance through argumentation
  - Combine ACE framework with Nòmos
    - + Syntax
    - + Algorithms
    - + Requirement model
    - + Legal concept

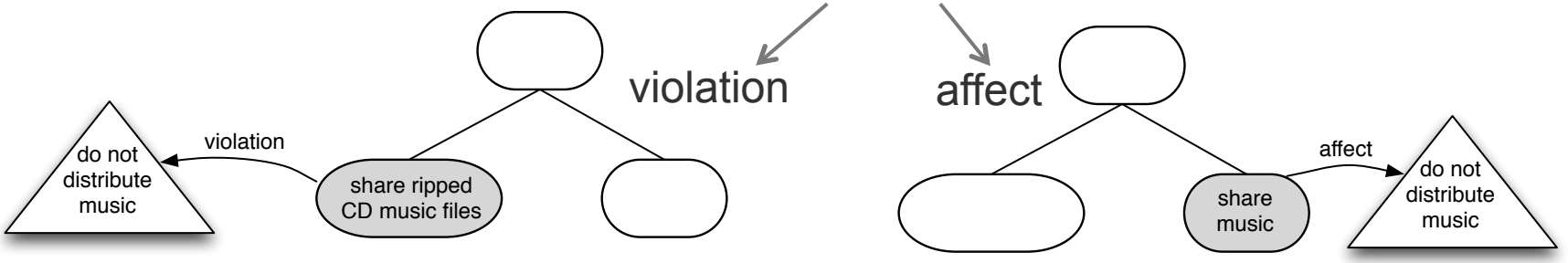
      Represent compliance

      − Represent non-compliance?



- Nòmos expansion to manage non-compliance

IRREGULARITIES: Situations where the model is / might not be compliant

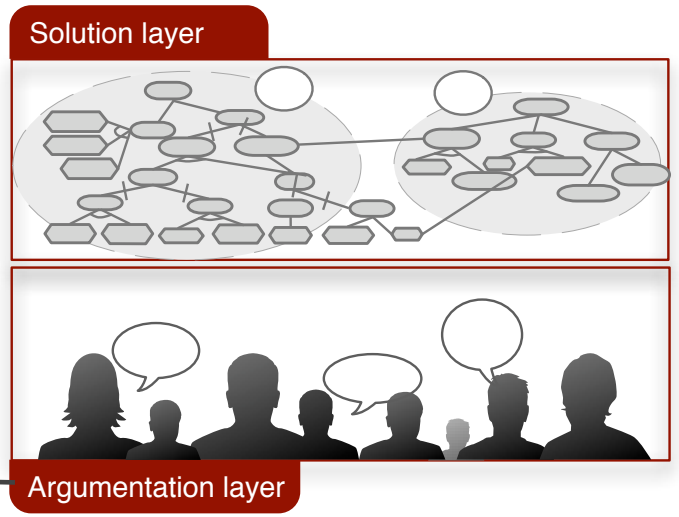


e.g. COPYRIGHT LAW:

"you CANNOT distribute the music or lyrics either for free, for no profit, or for profit"

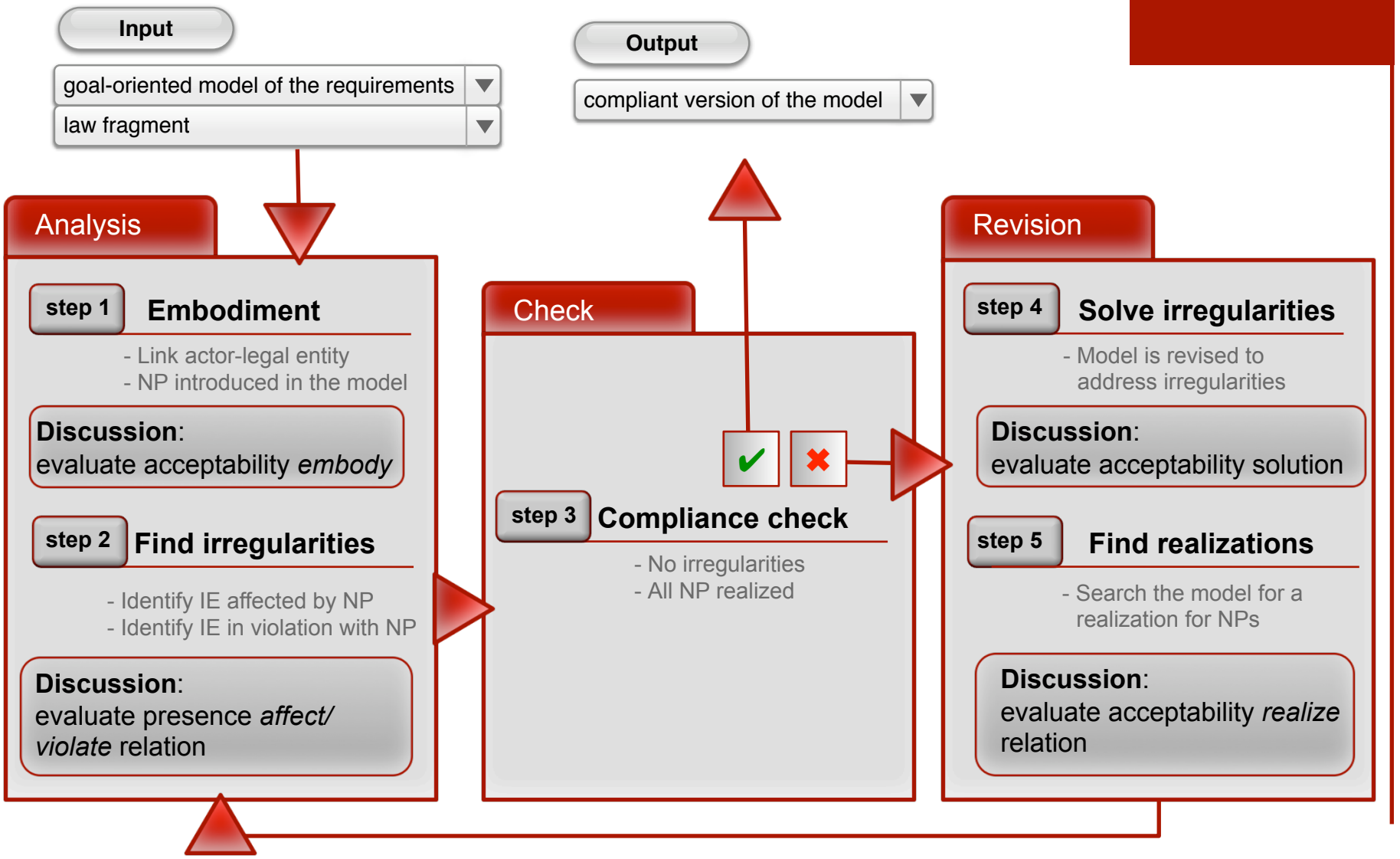
Compliance

- Compliance of a requirement model:
  - Norms respected [prove compliance]
    realize relation
  - Norms not infringed [confute nonconformity]
    affect, *violation* relation
- Reaching compliance through argumentation
  - Key: EVIDENCE OF COMPLIANCE from discussion
  - Participants - software engineers
    - stakeholders
    - lawyers
  - Too much information?



Traceability feature

Compliance Process



Compliance Process

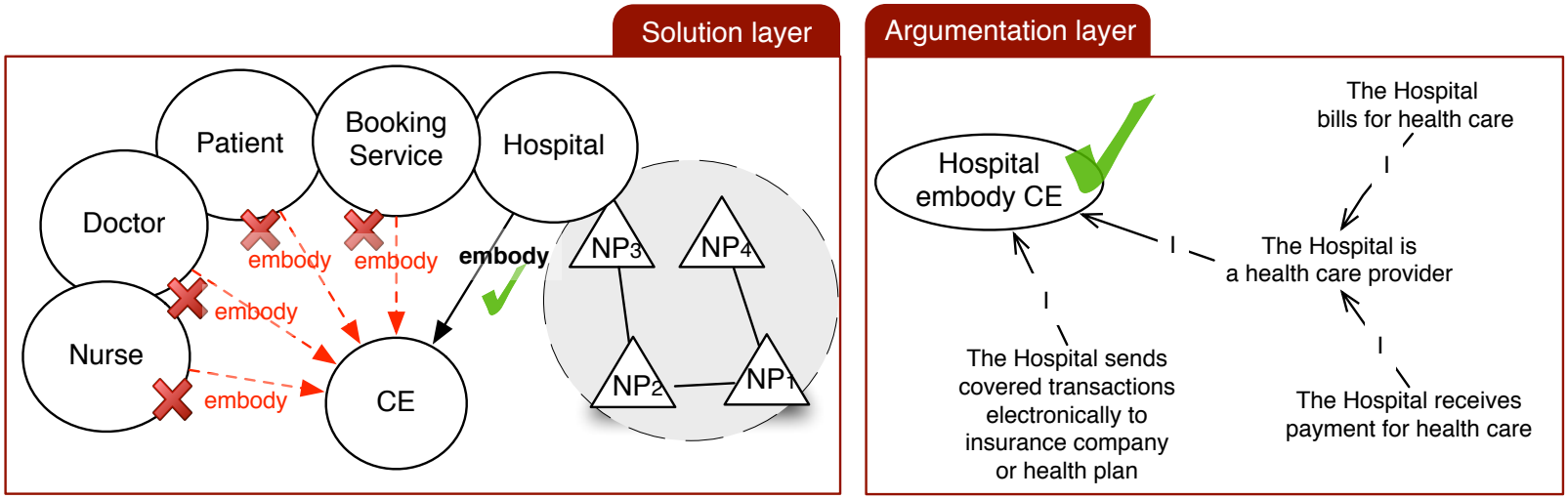
step 1 Embodiment

- Bind all actors with the appropriate legal subject
- *Discussion* evaluate acceptability

- Example in the Healthcare domain

Covered Entity (HIPAA §160.103)

"Any health care provider who bills an insurance company or health plan is a covered entity under HIPAA"

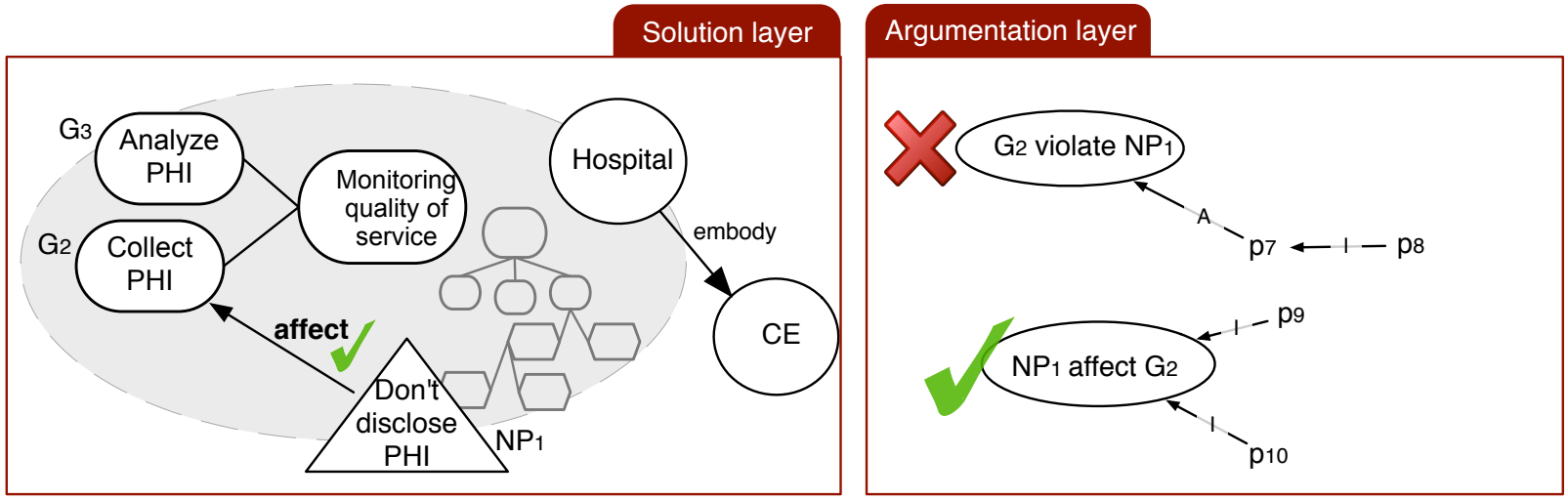


Compliance Process

step 2 Find Irregularities

- Identify all IE in the model that arise liability issues
- *Discussion* evaluate acceptability

- Example in the Healthcare domain:
  Actor: the Hospital

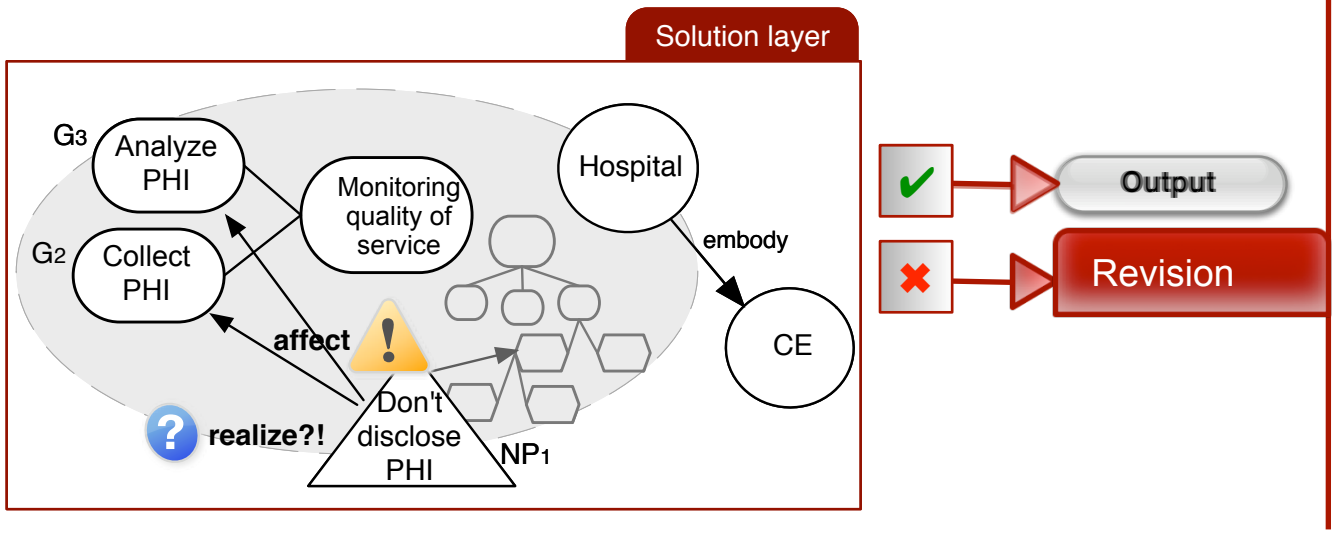


Compliance Process

step 3 Compliance check

- Norms not infringed? [no irregularity relations in the model]
- Norms respected? [all NP have a realization]

- Example in the Healthcare domain:
  Actor: the Hospital



Compliance Process

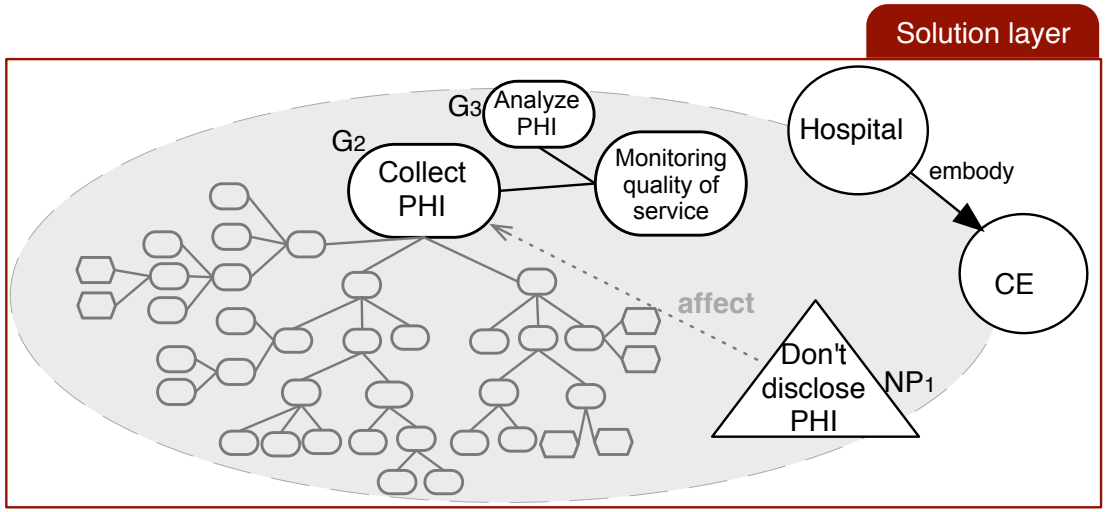
step 4 Solve Irregularities

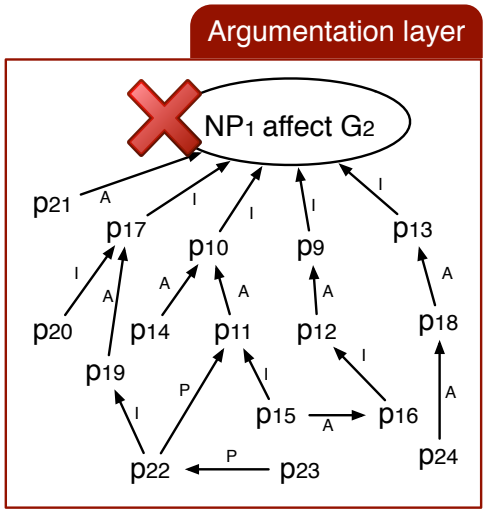
For every irregularity in the model

→ Revise the model until *discussion* accept the solution

- Example in the Healthcare domain:

Actor: the Hospital Irregularity: “Collect PHI” affected by “Don’t disclose PHI”





Compliance Process

step 5 Find Resolutions

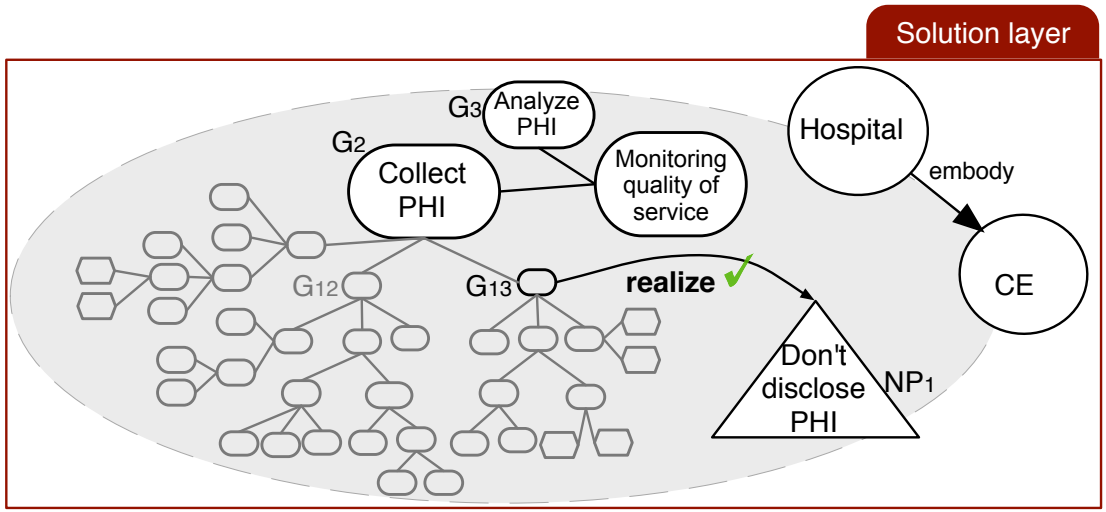
For every NP in the model

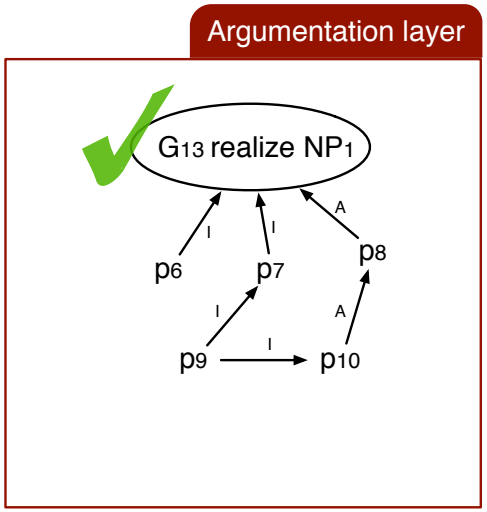
→ Search the model until all NP are realized

discussion evaluates acceptability

- Example in the Healthcare domain:

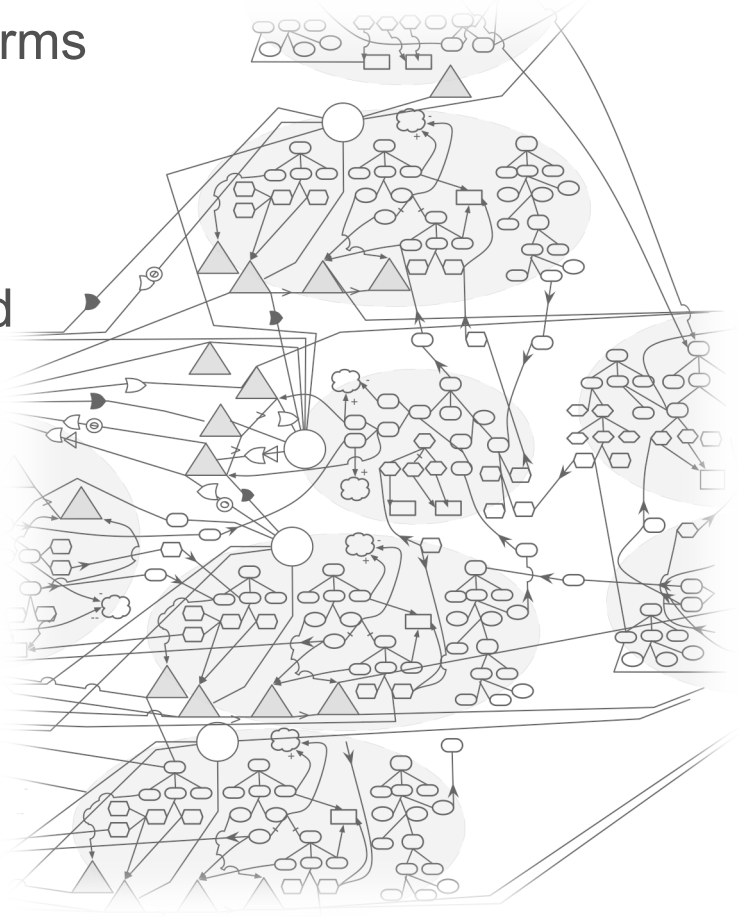
Actor: the Hospital Realization for "Don't disclose PHI"





Conclusions

- Problem
  - Aligning software requirements to norms
- Challenges
  - Complicated models to be accepted
  - Non-technical user involvement
  - Establishing acceptability
- Our proposal: ARGUMENTATION



Conclusions and Future Work

- Our contributions:

  SYSTEMATIC PROCESS TO ESTABLISH

  1. ACCEPTABILITY OF A COMPLICATED MODEL
  2. COMPLIANCE OF A REQUIREMENT MODEL

+ Flexibility	– Unbounded length
+ General approach	– Possible failure
+ Usability	
+ Traceability of decisions	

- Future work
  - Industrial case study
  - Improve process
  - Manage law evolvability
  - Tool support

Questions?