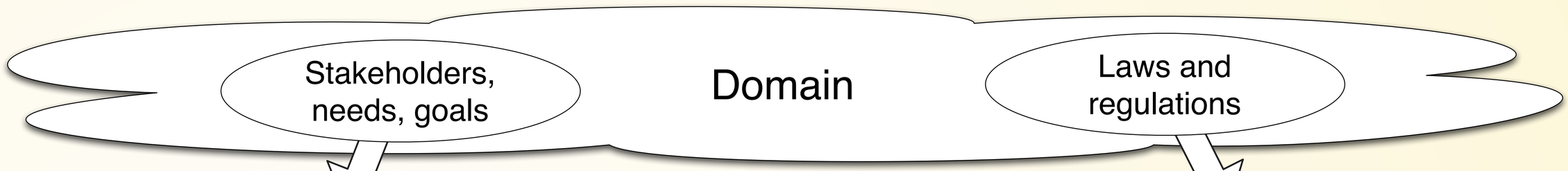
FONDAZIONE BRUNO KESSLER
RICERCA SCIENTIFICA E TECNOLOGICA

UNIVERSITY OF TRENTO - Italy

Alberto Siena, John Mylopoulos, Anna Perini, Angelo Susi

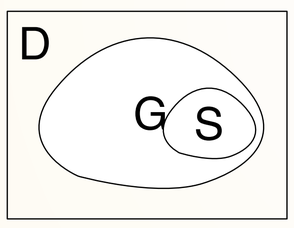
Towards a Framework for Law-Compliant Software Requirements

NIER@ICSE

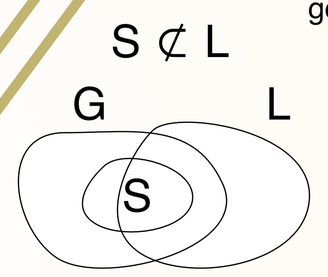


In a given domain, the system's requirements are represented as goals that stakeholders **want**

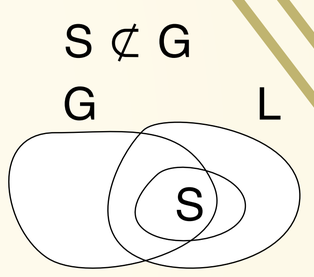
Given a certain domain (D), and a set of requirements represented as goals (G), the requirements specification problem consists in finding a subset S of G, where some properties hold (e.g., cost, security, risk, ...)



The problem arises: if we derive requirements from goals, we risk to be not aligned with law. If we incorporate directly law prescriptions, we risk to fail in matching stakeholders goals.

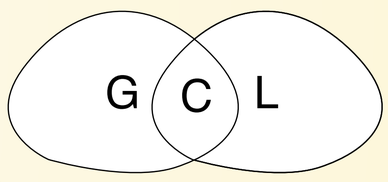


D, R ⊭ L



Laws describe a world that differs from the one desired by stakeholders

The of states of the world described by law statements (L) may differ from that described by goals (and also *conflict* with it). The states, in which goals and laws match (C) are those in which the compliance property holds.



C = G ∩ L

Intentional compliance: assignment of responsibilities such that if every actor fulfils its goals, then compliance is achieved.

Fundamentals of a process

Domain characterization 1

(Preliminary gathering of knowledge about the domain, its stakeholders, goals, and existing laws

Input: none

Output: preliminary goal model of the domain

Law modeling 2

Legal domain exploration; collection of applicable laws; law modeling using a formal language (Nomos)

Input: preliminary goal model of the domain

Output: model of applicable laws

Intentional compliance modeling 3

Refinement of the law models with the information collected in step 1; matching of law subjects with stakeholders; linking of goals with legal prescriptions

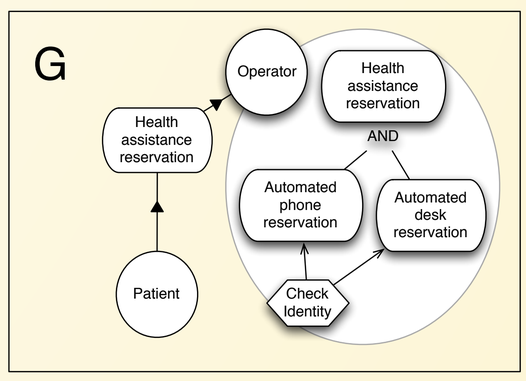
Input: preliminary goal model of the domain and of applicable laws

Output: model of compliant requirements

Conceptual tools: Goal-oriented modeling language

i****: concepts of*** Goal, Actor, strategic dependency between actors

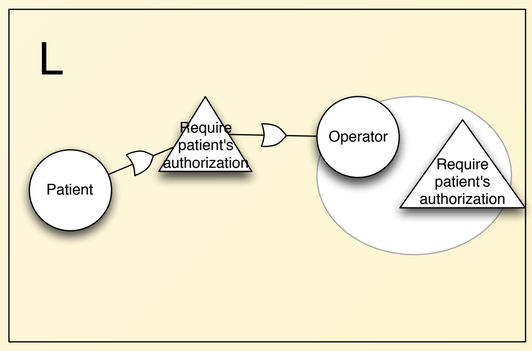
In a health care domain, a hospital wants to set up a centralized reservation system; it wants to support both reservations via phone and at the desk.



Conceptual tools: Ontology of legal concepts

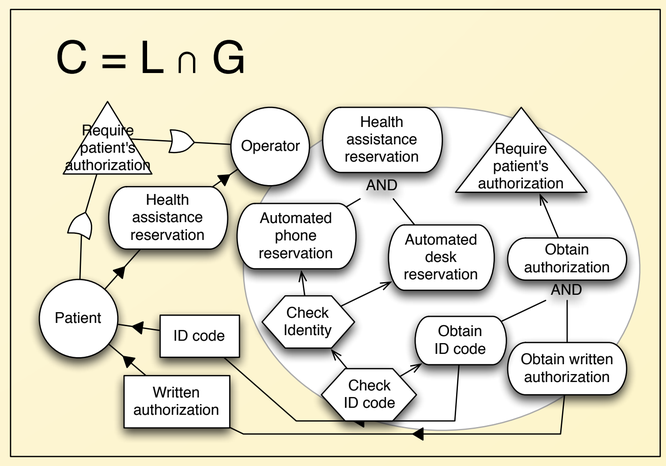
Hohfeldian taxonomy: *Claim, Duty, Privilege, No-claim, Power, Liability, Immunity, Disability*

Italian law DL196 lays down privacy constraints for treating patients personal data. Among them, operators of health care call centers have to explicitly request data treatment authorization to the patients



Conceptual tools: Laws and goals

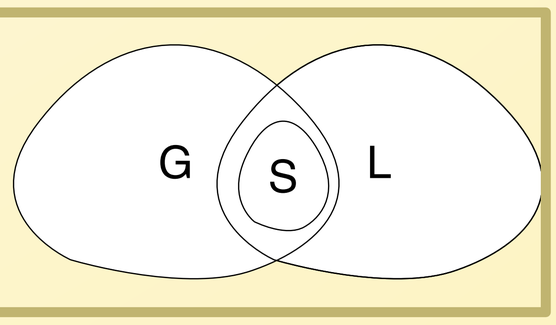
As a result of the legal prescription, the identity of the patients is checked in an anonymous way: an Id code is requested to the patient, without actual data exchange with the call center operator.



The requirements specified at the end of the process have both the properties: they match the stakeholders goals and comply with law

Requirements Specification

Properties of the Nomos models:
Traceability
Documentability
Risk safety
Security



References

Alberto Siena, John Mylopoulos, Anna Perini, and Angelo Susi**. The Nomos framework: Modelling requirements compliant with laws**. Technical Report TR-0209-SMSP, FBK – Irst, http://disi.unitn.it/asiena/files/TR- 0209- SMSP.pdf, 2009.
A. Siena, J. Mylopoulos, A. Perini, A. Susi. **From Laws to Requirements**. 1st International Workshop on Requirements Engineering and Law (Relaw'08), held at the RE 2008. September, 2008. Barcelona, Spain.

Ongoing/future work

- Formalization. Properties of law compliant models have to be formalized: traceability, documentability, risk-safety, ...
- Analysis. We are currently exploring how automation can support analyst in checking compliance properties
- **Case studies**! The Nomos framework has to be applied to a real and extended case study.