Towards a Formal Framework for Normative Requirements Elicitation

Nick Feng, **Lina Marsso**, Sinem Getir Yaman, Beverley Townsend,

Ana Cavalcanti, Radu Calinescu, Marsha Chechik

September 13, 2023

Normative Requirements

- Capture social, legal, ethical, empathetic, cultural aspects of systems
- Specified by stakeholders with non-technical expertise
  - Designers, regulators, ethicists, etc.
- Hard to get right
  - Stakeholders from different fields, different vocabularies
  - Their views are often conflicting or redundant

DAISY robot from RoboStar
University of York, UK

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders

Contribution: FormaTive

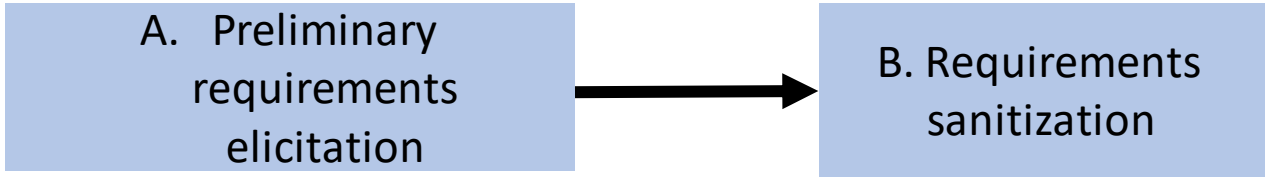
A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders

A. Preliminary requirements elicitation

Specification of normative rules for a software system in **SLEEC DSL**

Contribution: FormaTive

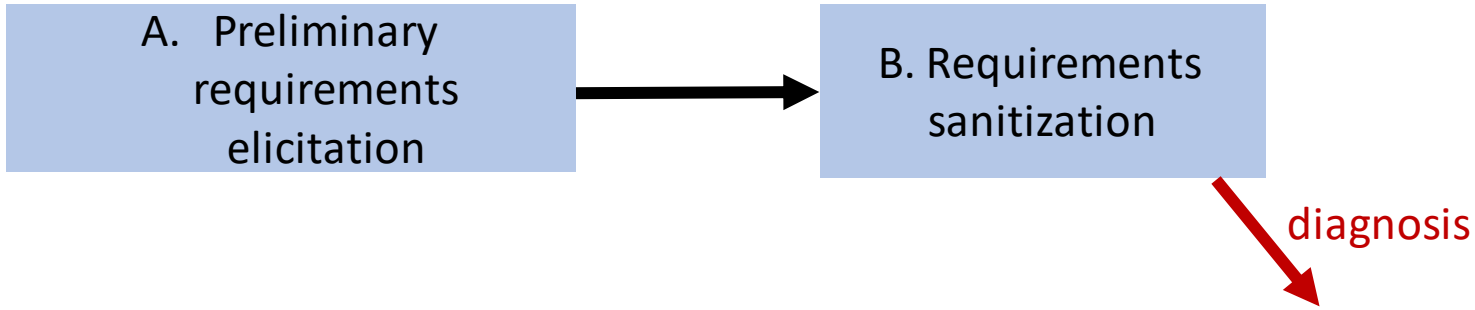
A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders



Specification of normative rules for a software system in **SLEEC DSL**
Automates: (i) the identification of conflicts, redundancies,

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders

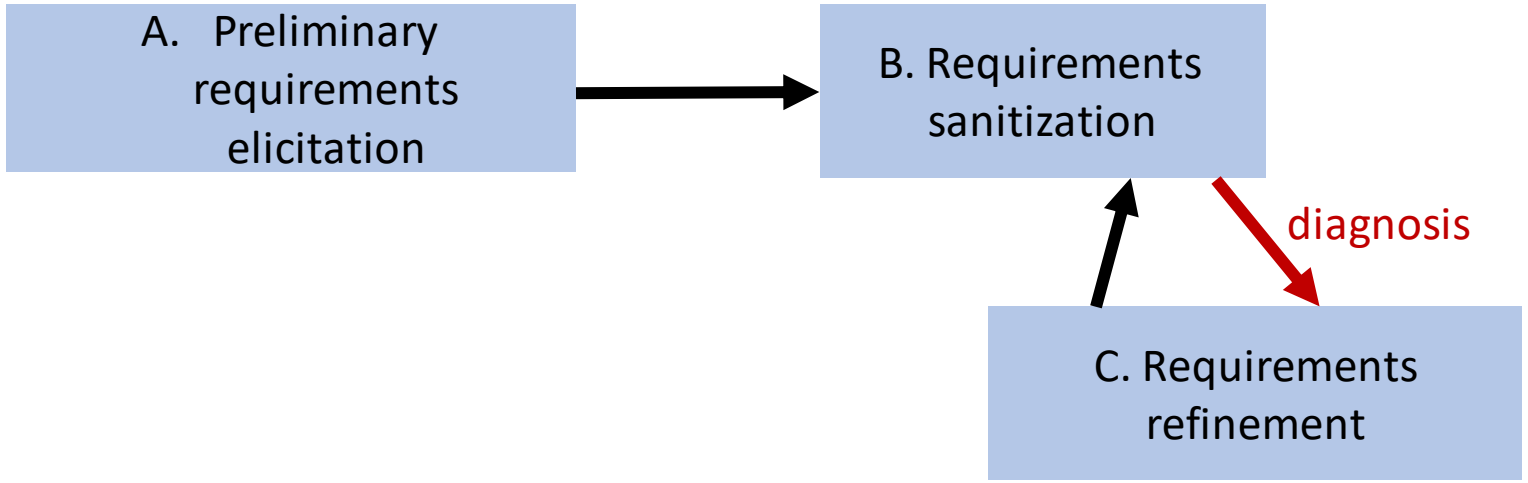


Specification of normative rules for a software system in **SLEEC DSL**

Automates: (i) the identification of conflicts, redundancies
(ii) the synthesis of feedback helping to understand/resolve problems

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders

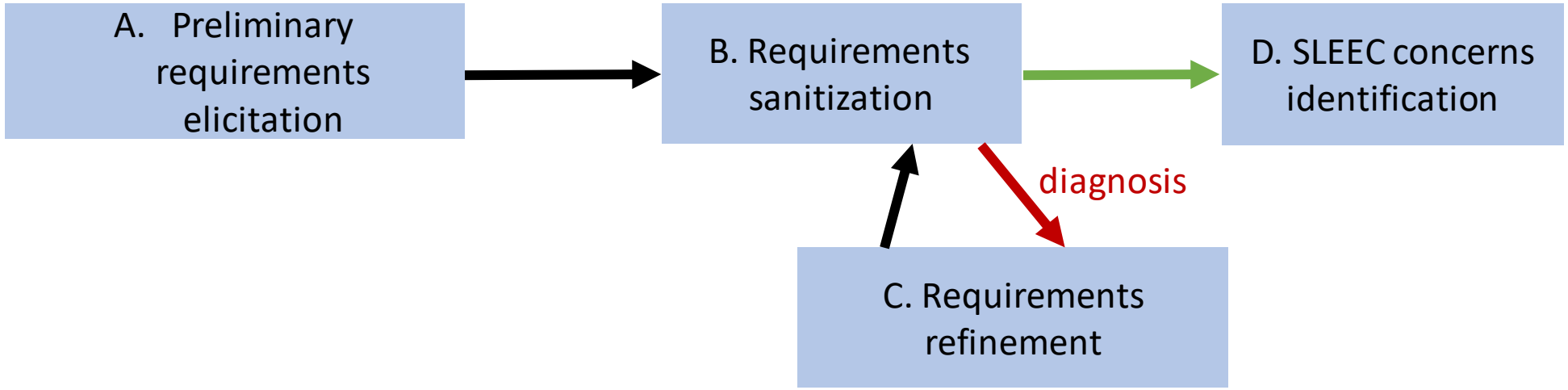


Specification of normative rules for a software system in **SLEEC DSL**

Automates: (i) the identification of conflicts, redundancies
(ii) the synthesis of feedback helping to understand/resolve problems

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders



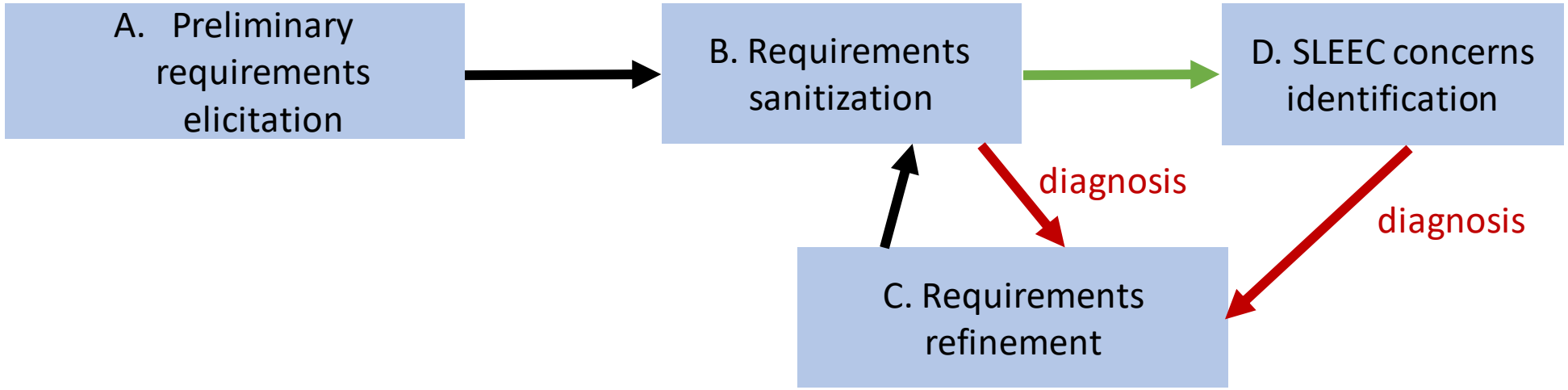
Specification of normative rules for a software system in **SLEEC DSL**

Automates: (i) the identification of conflicts, redundancies, and concerns

(ii) the synthesis of feedback helping to understand/resolve problems

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders



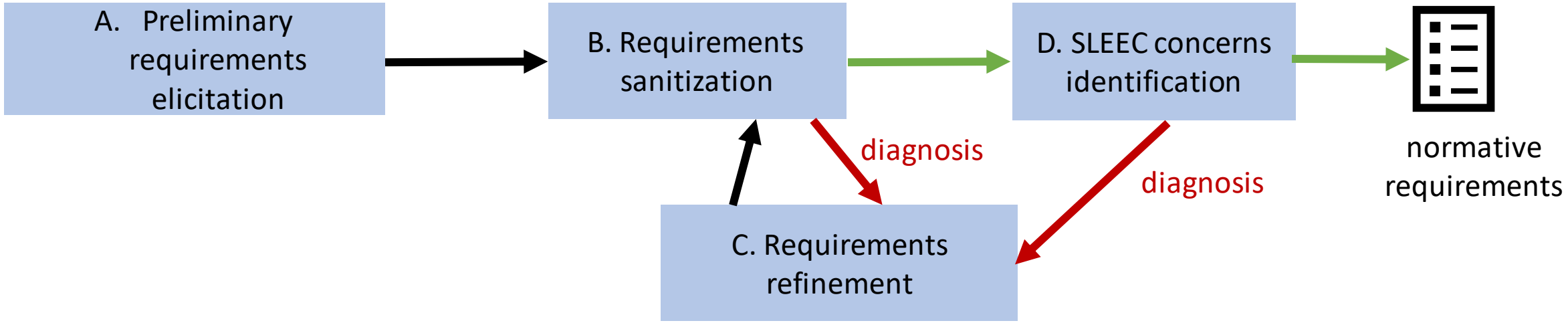
Specification of normative rules for a software system in **SLEEC DSL**

Automates: (i) the identification of conflicts, redundancies, and concerns

(ii) the synthesis of feedback helping to understand/resolve problems

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders



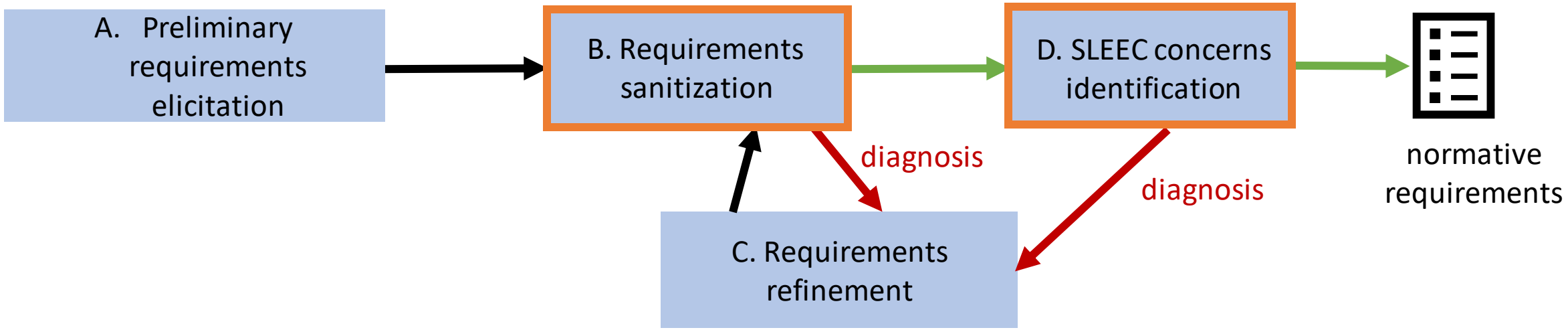
Specification of normative rules for a software system in **SLEEC DSL**

Automates: (i) the identification of conflicts, redundancies, and concerns

(ii) the synthesis of feedback helping to understand/resolve problems

Contribution: FormaTive

A tool-supported **Formal** framework for norma**Tive** requirements elicitation for *non-technical* stakeholders



Specification of normative rules for a software system in **SLEEC DSL**

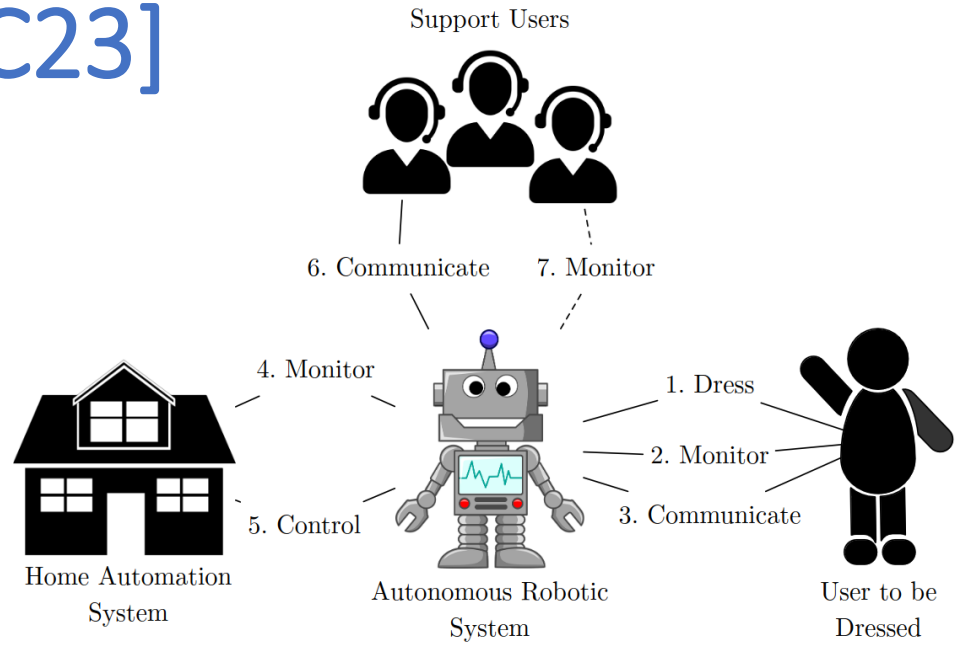
Automates: (i) the identification of conflicts, redundancies, and concerns

(ii) the synthesis of feedback helping to understand/resolve problems

Outline

I. Background: SLEEC DSL
II. Requirement sanitization
III. SLEEC concerns identification
IV. Implementation
V. Preliminary evaluation
VI. Future research directions

Background: SLEEC DSL [GYBJCC23]



Definitions

event DressingStarted
event CurtainOpenRqst
event CurtainsOpened

measure userUnderdressed: **Bool**
measure roomTemperature: **numeric**

Rules

Rule1 **when** DressingStarted **then** DressingComplete **within** 2 **minutes**
unless (roomTemperature < 19) **then** DressingComplete **within** 60 **seconds**

Rule2 **when** CurtainOpenRqst **and not** UserUnderdressed **then** CurtainsOpened **within** 2 **minutes**
unless (roomTemperature < 19)

[GYBJCC23] S. Getir-Yaman, C. Burholt, M. Jones, R. Calinescu, and A. Cavalcanti. "Specification and Validation of Normative Rules for Autonomous Agents", FASE 2023.

Requirements Sanitization

Redundant rule is a logical consequence of other rules

Conflicting rule cannot be triggered together with other rules

Checking *r5* redundancy in the rule set R via satisfiability:

$\neg$ *r5* $\cap$ (R $\setminus$ *r5)*

Redundant SLEEC rule:

r5 when DressingStarted and (({roomTemperature} < 16) and {userUnderDressed})
then DressingComplete within 1 minutes

---

r1 when DressingStarted then DressingComplete within 2 minutes
unless ({roomTemperature} < 19) then DressingComplete within 90 seconds
unless ({roomTemperature} < 17) then DressingComplete within 60 seconds

Redundancy Diagnosis

Redundant SLEEC rule:

r5 when DressingStarted and (({roomTemperature} < 16) and {userUnderDressed})
then DressingComplete within 1 minutes

---

r1 when DressingStarted then DressingComplete within 2 minutes
unless ({roomTemperature} < 19) then DressingComplete within 90 seconds
unless ({roomTemperature} < 17) then DressingComplete within 60 seconds

Redundancy Diagnosis

Redundant SLEEC rule:

r5 when DressingStarted and ({roomTemperature} < 16) and {userUnderDressed})
then DressingComplete within 1 minutes

---

r1 when DressingStarted then DressingComplete within 2 minutes
unless ({roomTemperature} < 19) then DressingComplete within 90 seconds
unless ({roomTemperature} < 17) then DressingComplete within 60 seconds

({roomTemperature} < 16) ==> ({roomTemperature} < 17)

Redundancy Diagnosis

Redundant SLEEC rule:

r5 when DressingStarted and ({roomTemperature} < 16) and {userUnderDressed})
then DressingComplete within 1 minutes

---

r1 when DressingStarted then DressingComplete within 2 minutes
unless ({roomTemperature} < 19) then DressingComplete within 90 seconds
unless ({roomTemperature} < 17) then DressingComplete within 60 seconds

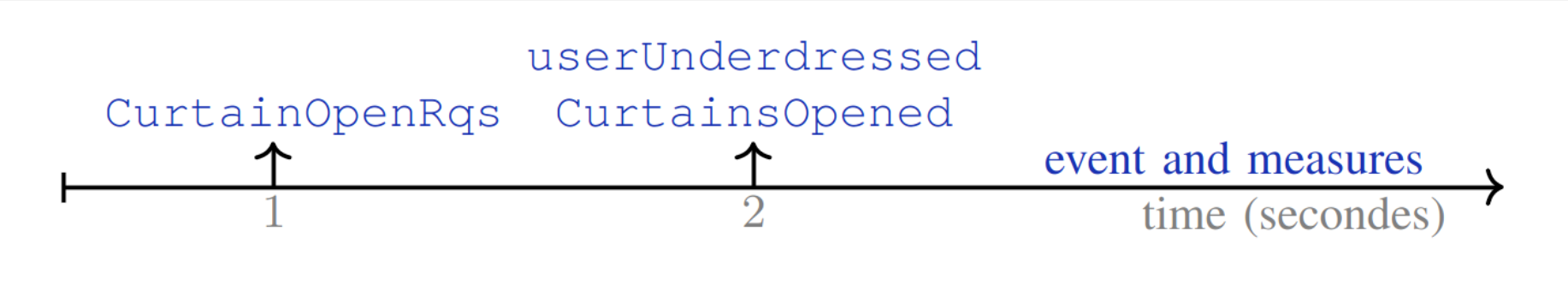
within 1 minutes <==> within 60 seconds

({roomTemperature} < 16) ==> ({roomTemperature} < 17)

SLEEC Concerns Identification

- A SLEEC concern specifies a behavior to avoid
  (e.g., a failure to protect user privacy)
- Contextualize high-level SLEEC concerns
  (operating environment and normative capabilities)

- *C:* **when a user open curtains then the user is underdressed**
- Checking whether *C* is raised while respecting the rule set R via satisfiability: R ∩ *C*



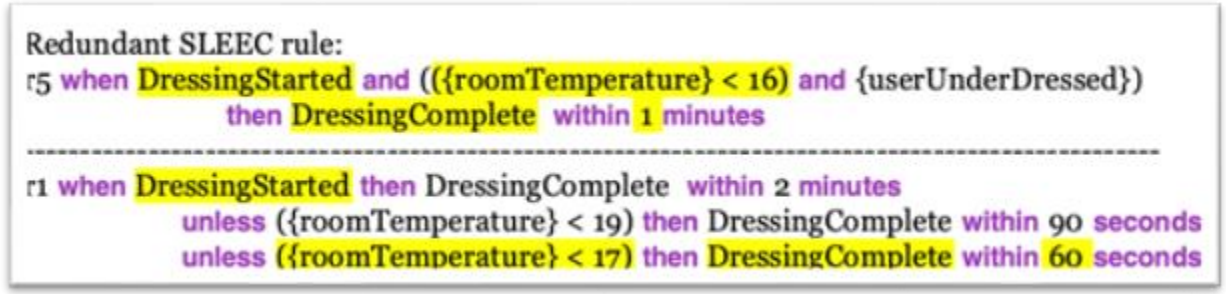
Implementation

Automated reasoning tool

B. Requirement sanitization

D. SLEEC concerns identification

- Compiles each SLEEC DSL rule into FOL*
- Interprets redundancy, conflict, concerns definitions as FOL* constraints
- Uses LEGOS (the FOL* satisfiability checker [FMSC23]) to identify the problems
- Provides a user-friendly diagnosis



[FMSC23] N. Feng, L. Marsso, M. Sabetzadeh, and M. Chechik. "Early verification of legal compliance via bounded satisfiability checking", CAV 2023.

Preliminary Evaluation 1/3

Case studies:

- ERA: Elderly robot assistant
- DR: Dressing robot

System	#event	#measures	#rules	#defeaters	#redudancies	#conflicts	#concerns
ERA	7	5	4	6	0	0	1
DR	9	4	12	11	3	1	1

Six stakeholders:

- Philosopher - Computer Vision expert
- Robotists - Sociologist - AI expert

Preliminary Evaluation 2/3

RQ1: How effective is our framework in detecting redundancies, conflicts, and concerns compared to manual analysis?

participant	redundancies	conflicts	concerns
ground truth	0	0	1
Roboticist	**2**	**1**	**0**
Computer vision expert	**1**	0	1
Philosopher	**1**	0	**0**
AI expert	**1**	0	1
Roboticist	0	0	1
Sociologist	**1**	0	**0**
FormaTive	0	0	1

Preliminary Evaluation 3/3

RQ2: How effective is the diagnosis produced by our framework in helping the user understand the causes of redundancies, conflicts, and concerns?

29 out of 30 cases (96%) the participants correctly explain the causes given the diagnosis produced by FormaTive

Summary

Early results:

Formal analysis provided by FormaTive is usable by non-technical stakeholders and more effective than manual analysis!

Remaining research question:

RQ3: How efficient and effective is the FormaTive framework in eliciting redundant-, conflict-, and concern-free normative requirements?

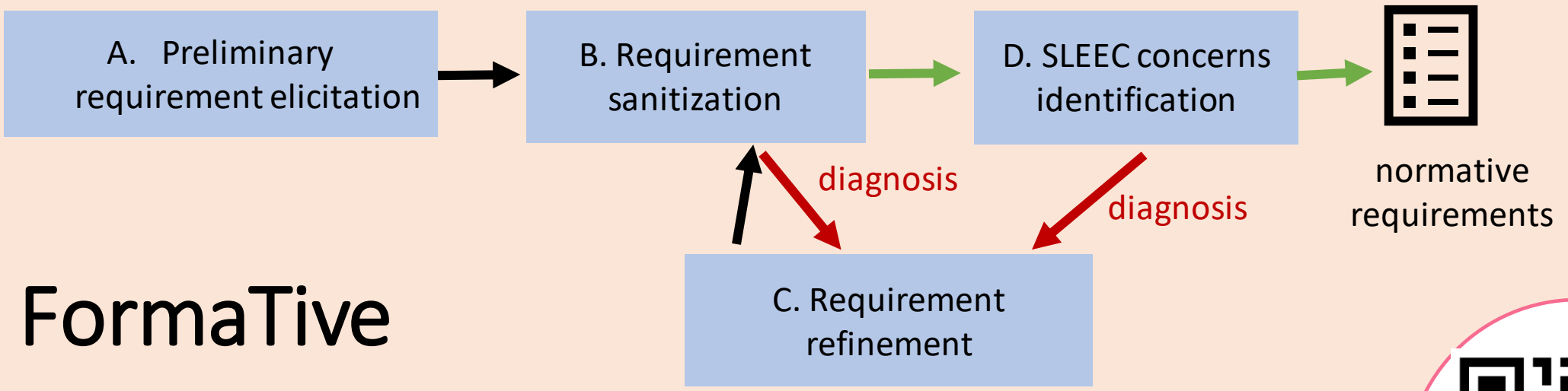
Future Research Directions

1. Conduct an extensive study to assess the efficiency of the overall framework
   (evaluating iterations for eliciting requirements and quality)

2. Generate and suggest patches to resolve the identified issues.

3. Provide more detailed diagnoses for raised concerns
   (e.g., information on requirements that partially address concerns)

Nick Feng
Lina Marsso
Sinem Getir Yaman
Beverley Townsend



FormaTive

Automated reasoning tool support for:

- the identification of conflicts, redundancies, and concerns
- the synthesis of feedback helping **non-technical stakeholders** to understand/resolve problems

Thank you! ☺

Ana Cavalcanti
Radu Calinescu
Marsha Chechik