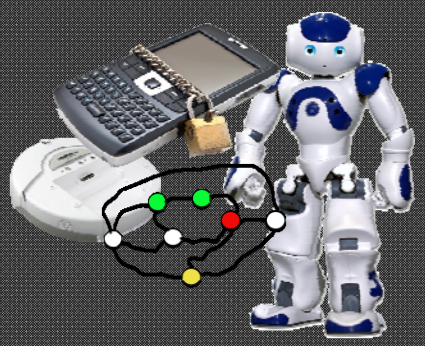
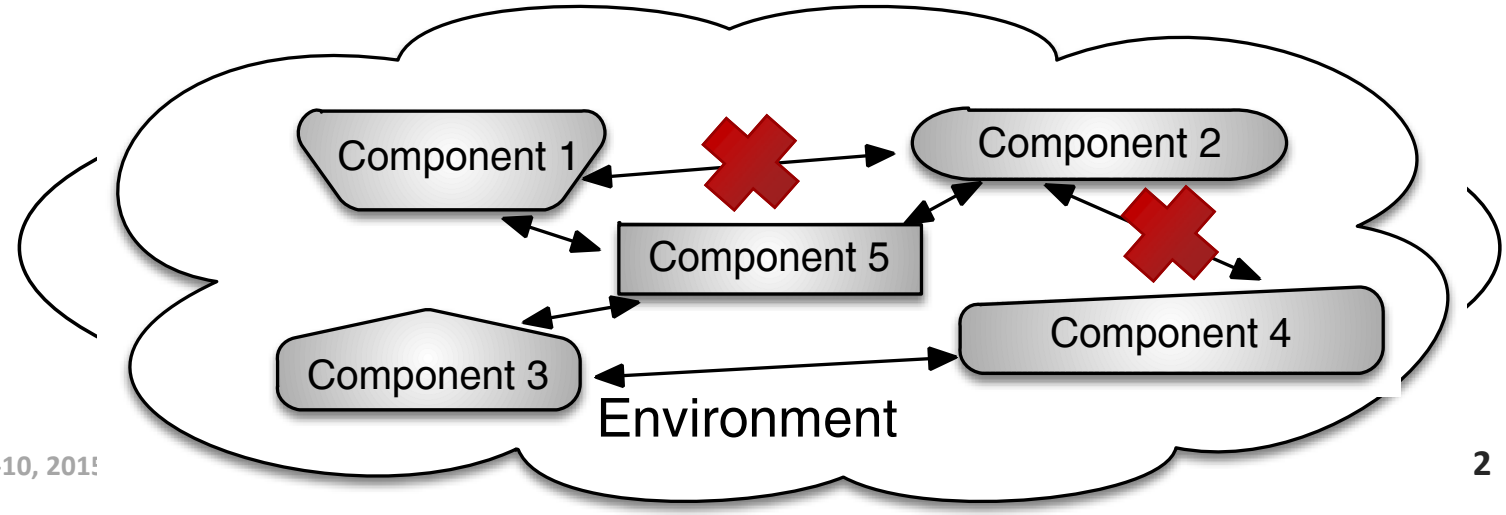
Requirements-Driven Mediation for Collaborative Security

Amel Bennaceur
The Open University, UK

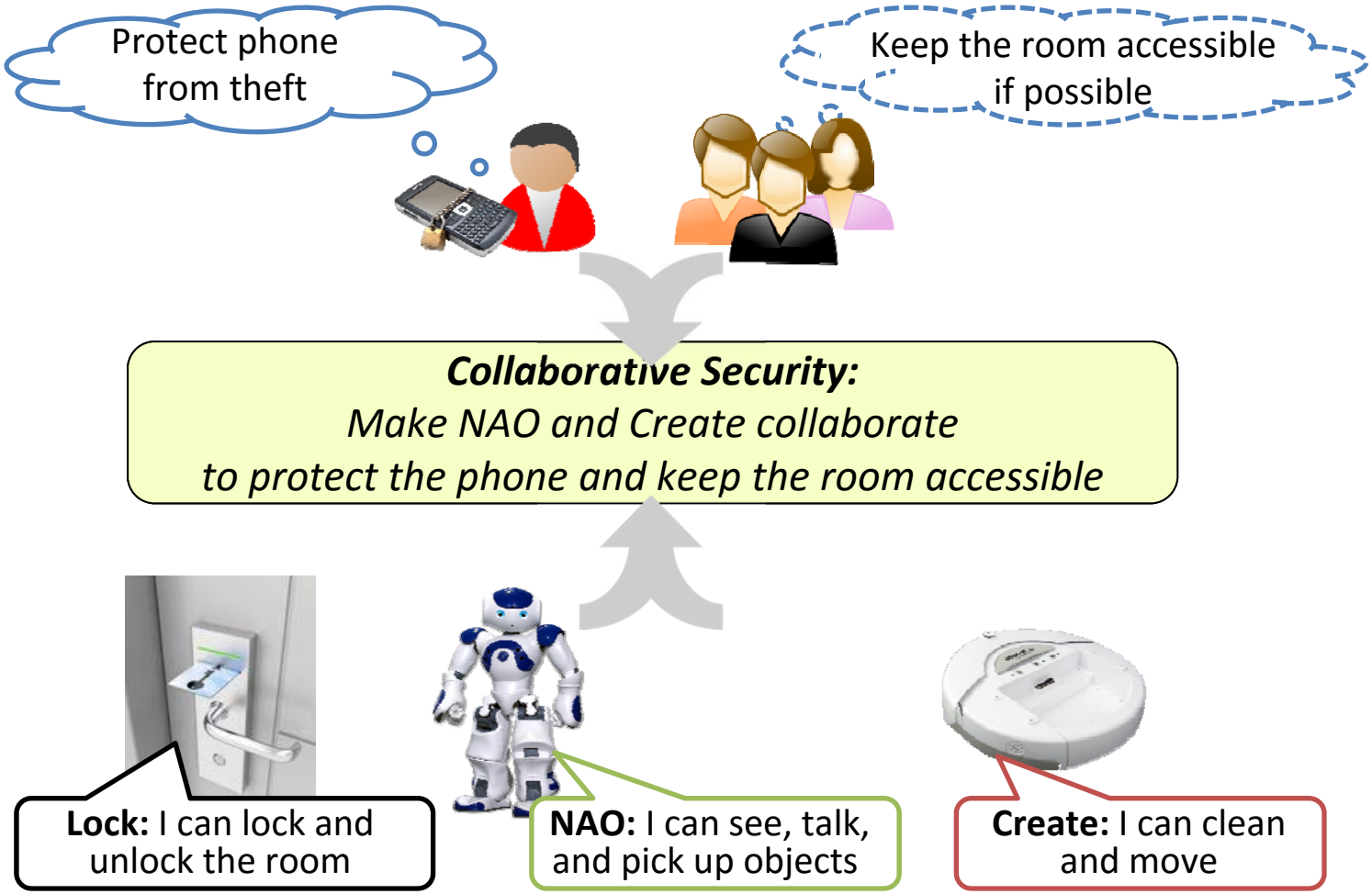


Collaborative Security

- Making multiple, heterogeneous, software-intensive components collaborate in order to meet security requirements
  - The boundary of the systems is uncertain
  - The components can change
  - The components are designed and implemented independently



Collaborative Security - Example



Adaptive Security meets Collaborative Adaptation

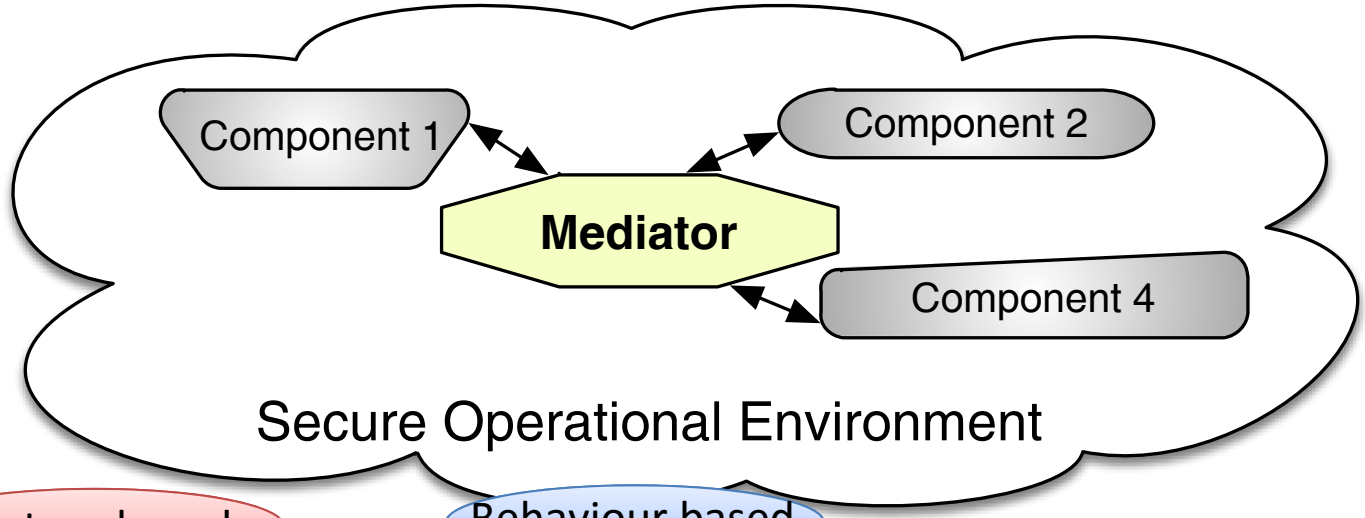
Adaptive Security	Collaborative Adaptation

- Reasoning about assets, threats, attacks, and vulnerabilities
- Identify the security controls necessary to keep security requirements satisfied
- How to enact these security controls?

- Reasoning about dynamic discovery and composition
- Making multiple components collaborate
- How to reason about assets, threats and security controls?

Collaborative Security à la Michael Jackson

$R = \{R_s, R_1, \ldots, R_m\}$: partially ordered set of requirements
$\mathcal{S} = \{C_1, \ldots, C_n\}$: set of components' capabilities
E : environment properties

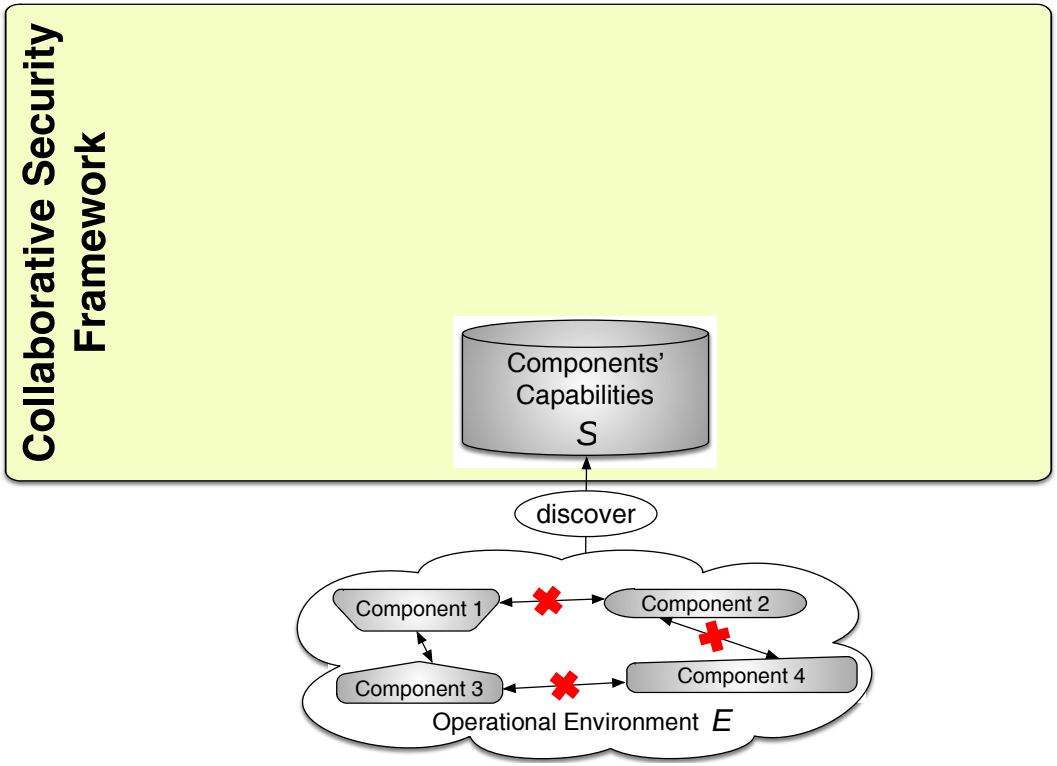


Feature based

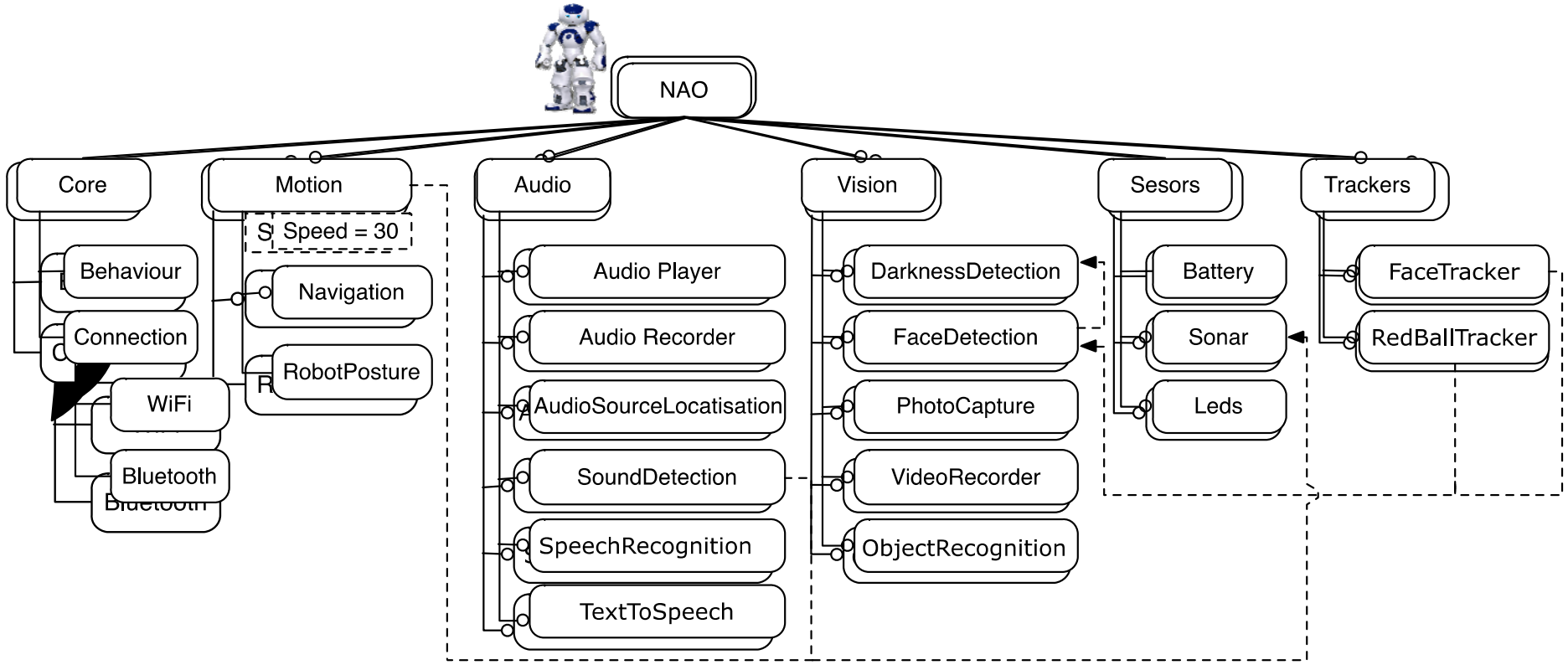
Behaviour based

Find $\mathcal{C} \subseteq \mathcal{P}(\mathcal{S})$ and synthesise M such that $\mathcal{C}, M, E \vdash R$ $\forall \mathcal{C}' \subseteq \mathcal{P}(\mathcal{S}), \mathcal{C}', M, E \not\vdash R$

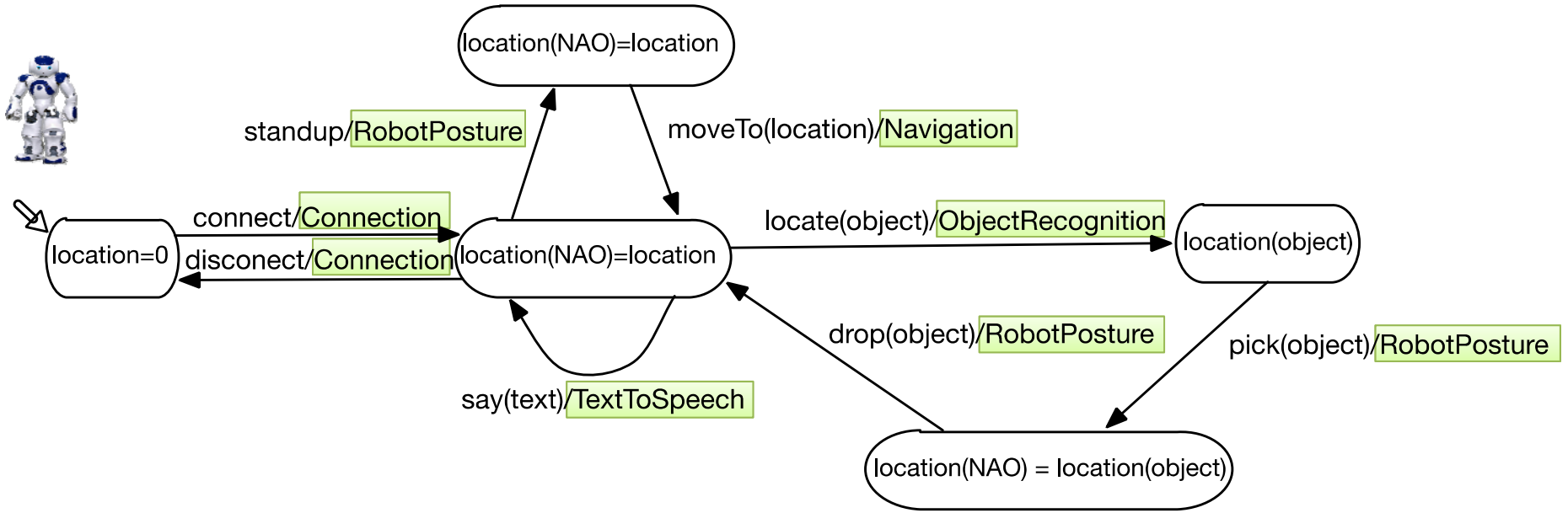
Collaborative Security Framework



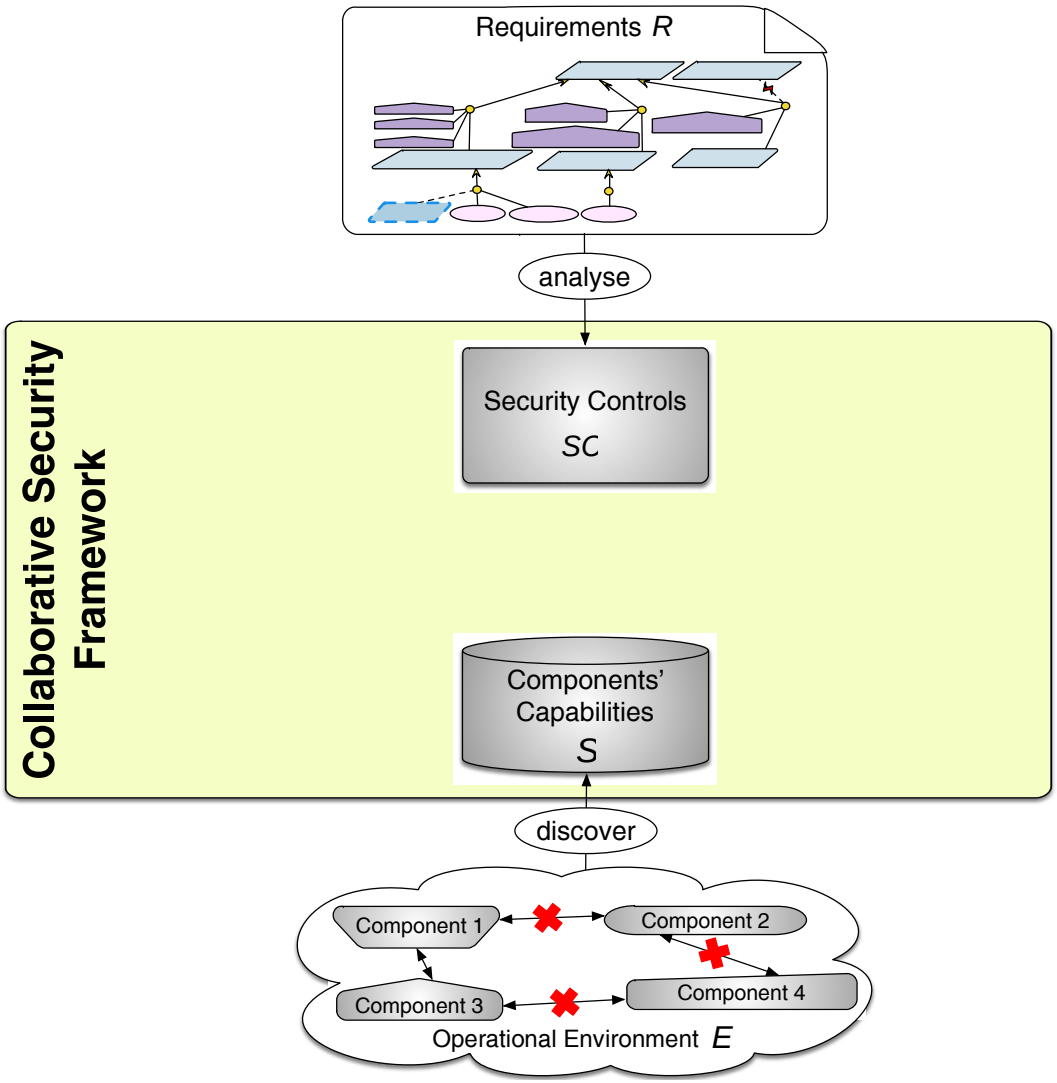
Capabilities as Featured Transition Systems



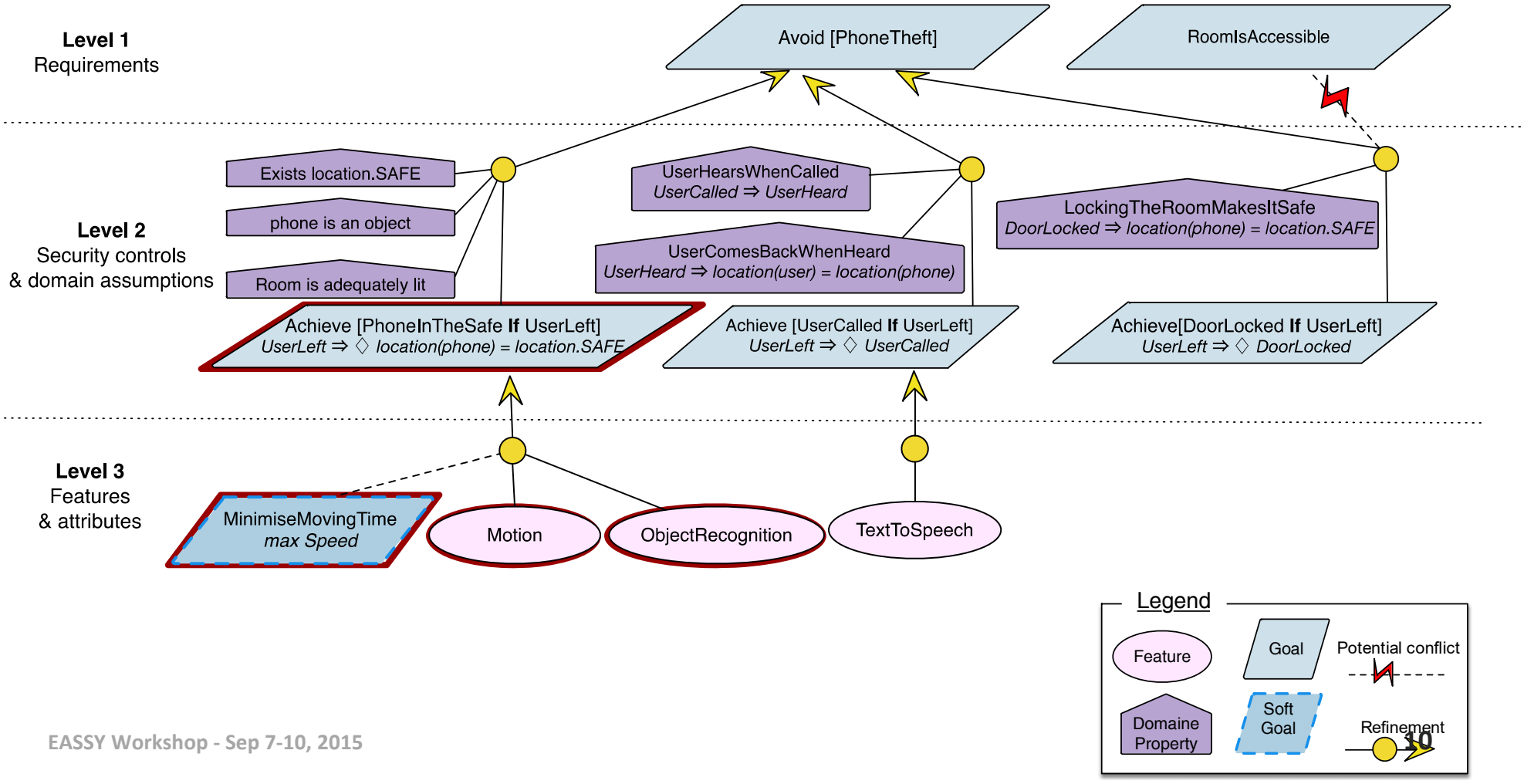
Capabilities as Featured Transition Systems



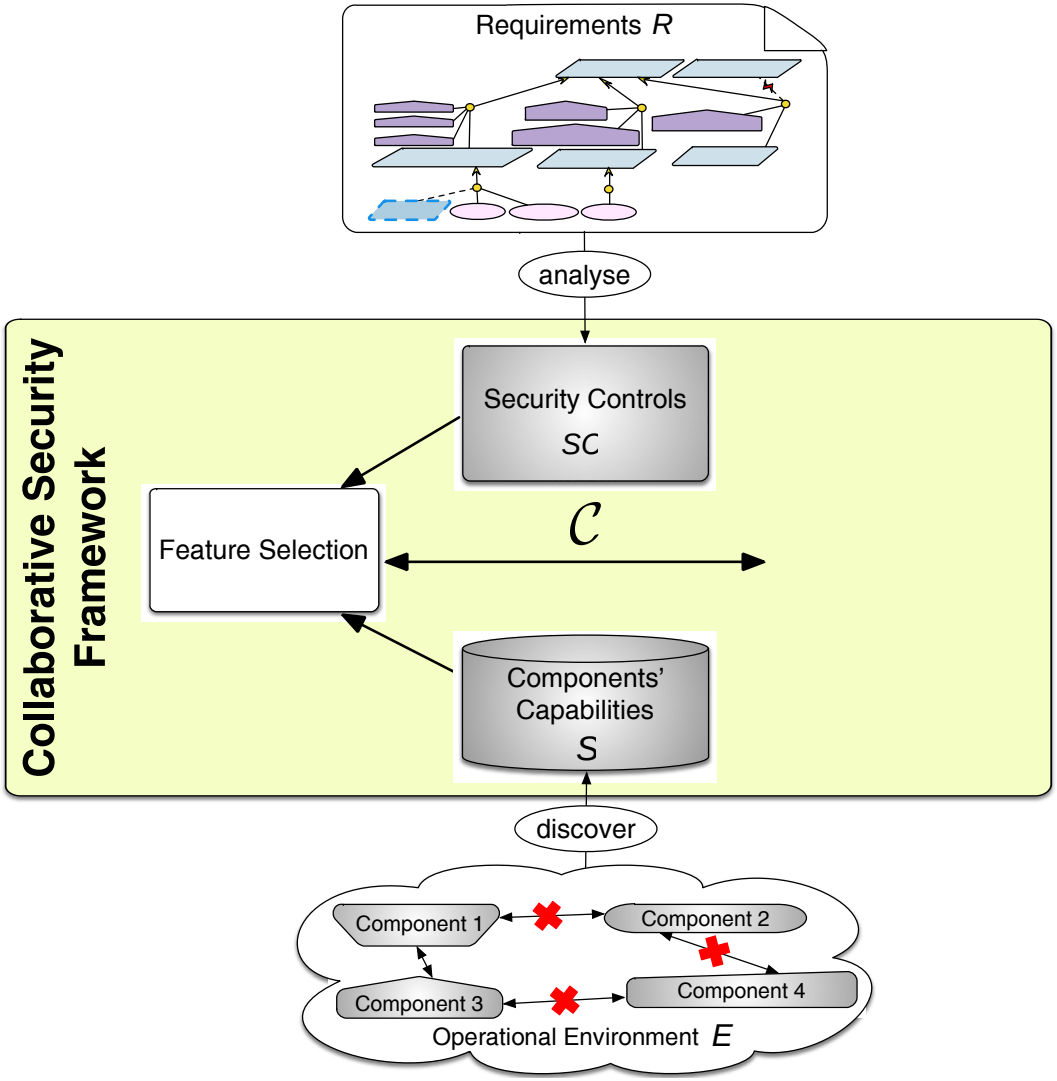
Collaborative Security Framework



Identifying Security Controls



Collaborative Security Framework



Feature Selection using Constraint Programming

Reason

$X = \{x_1, x_2, ..., x_n\}$

$D(X) = \mathcal{P}(\mathcal{F}_1) \times \mathcal{P}(\mathcal{F}_2) \times \cdots \times \mathcal{P}(\mathcal{F}_n)$

Feature-based Constraints $\mathcal{C}_1, \mathcal{C}_2$

Optimisation functions $g_{A_1}, g_{A_2}, \ldots, g_{A_l}$

CP Solver

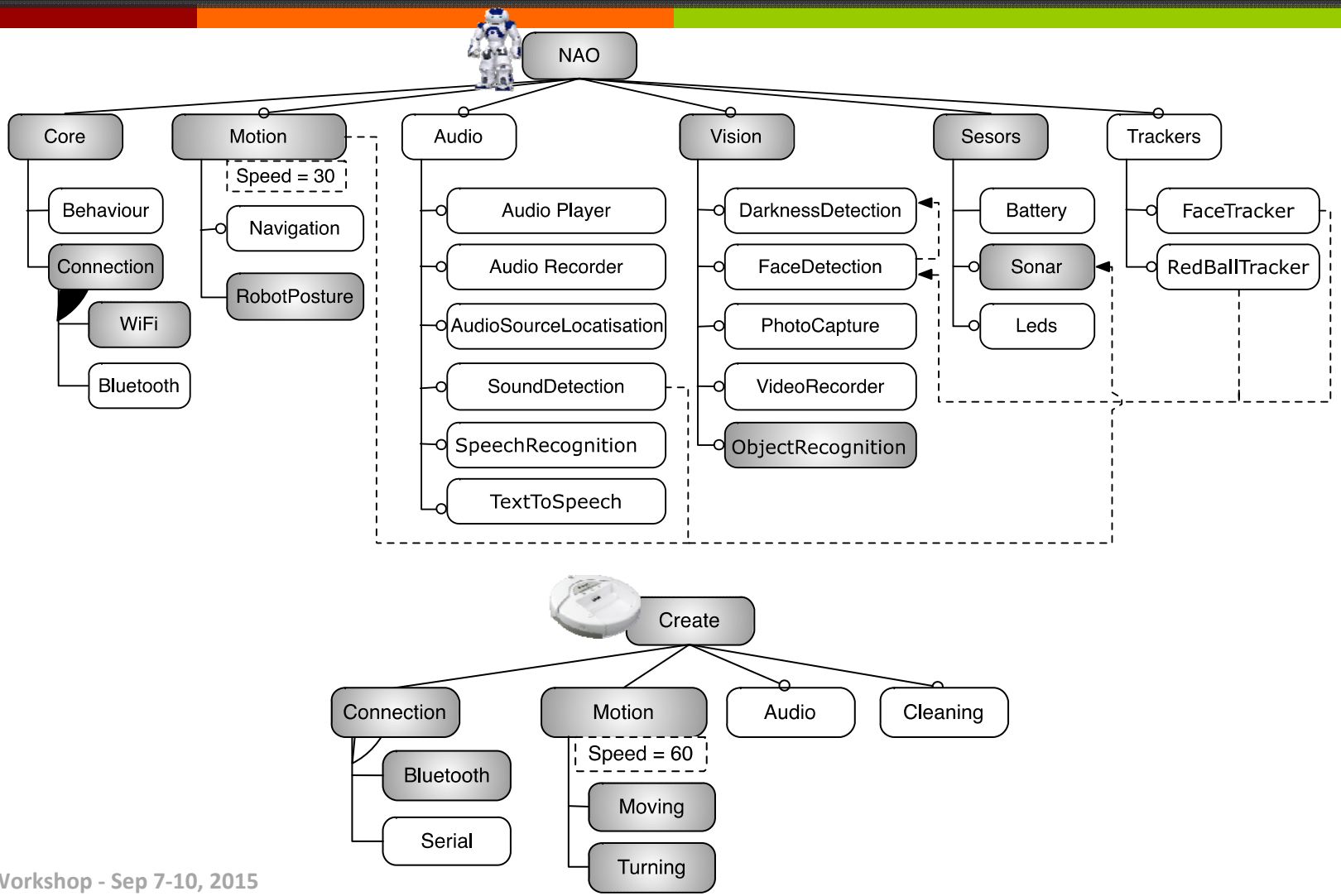
$f_1, f_2, \ldots, f_n$

$\mathcal{C}_1$: **Subsumes** the features of a selected security control provided some domain properties

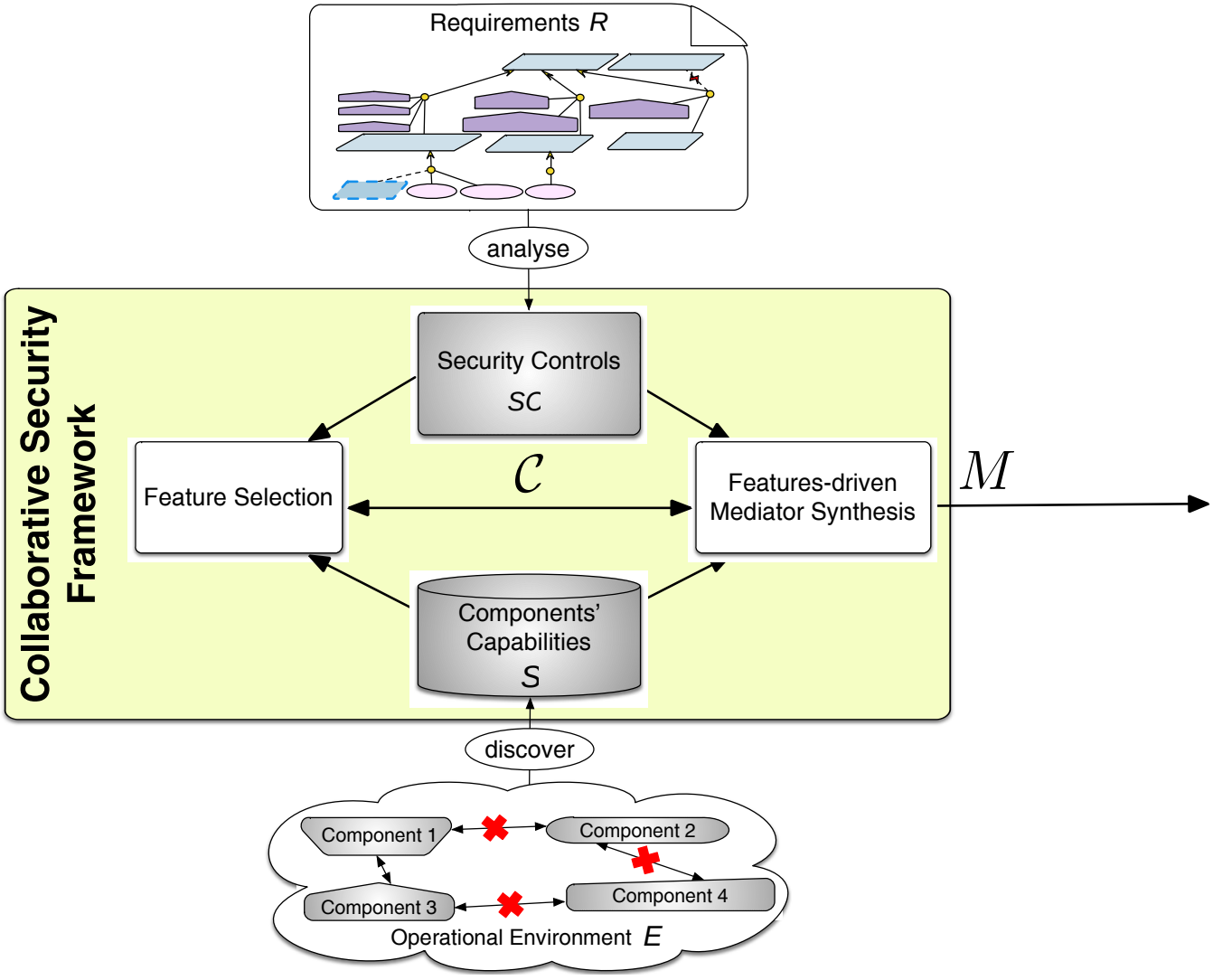
$\mathcal{C}_2$: **Respects** the constraints between features

Feature Selection

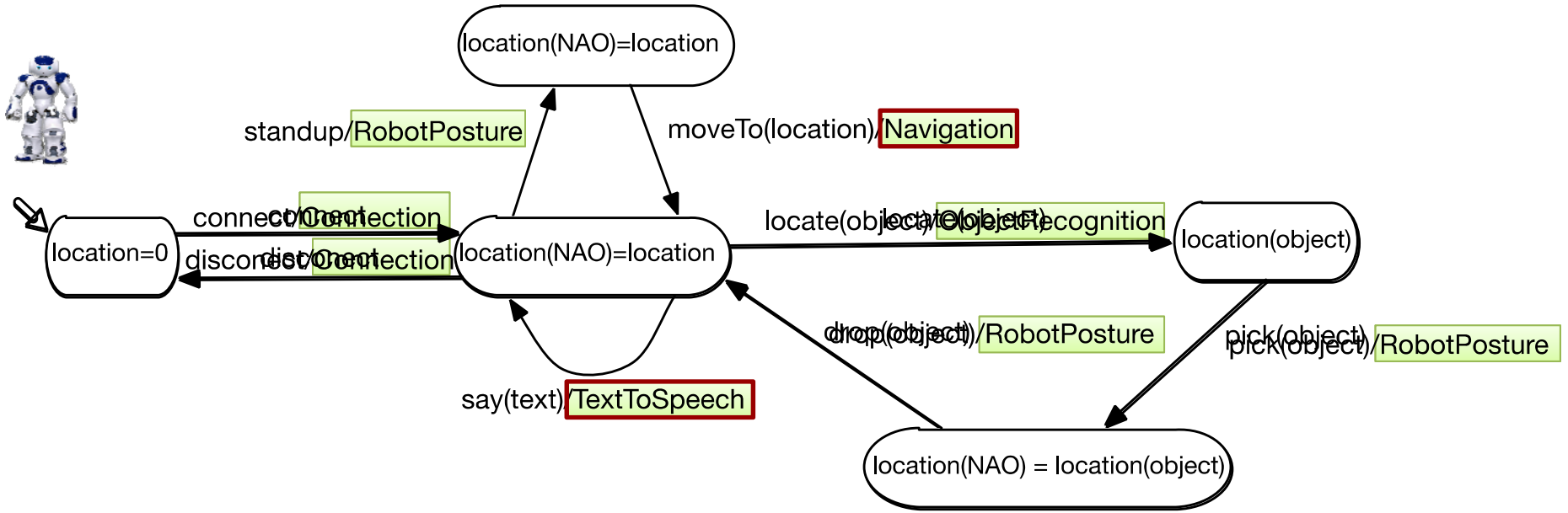
Reason



Collaborative Security Framework

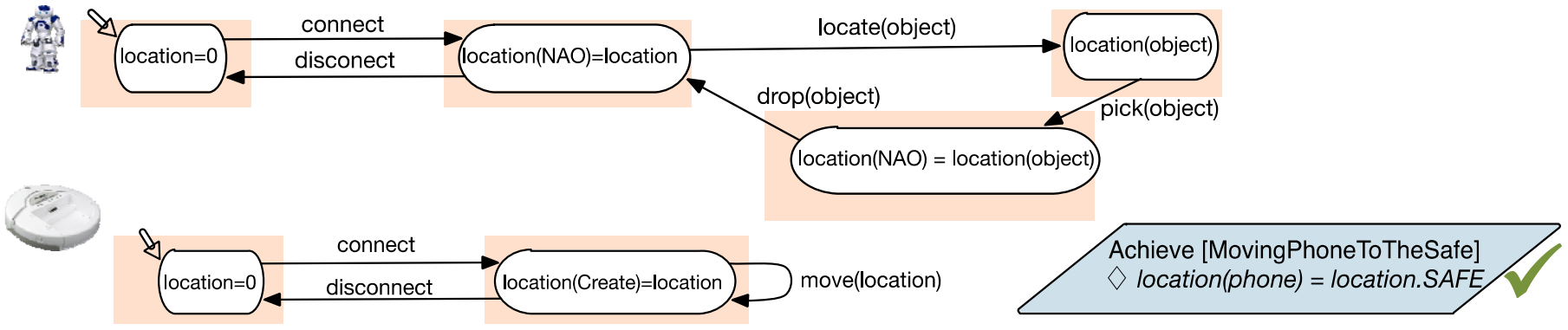


Projection of Featured Transition Systems



Feature-based Mediation

Synthesise



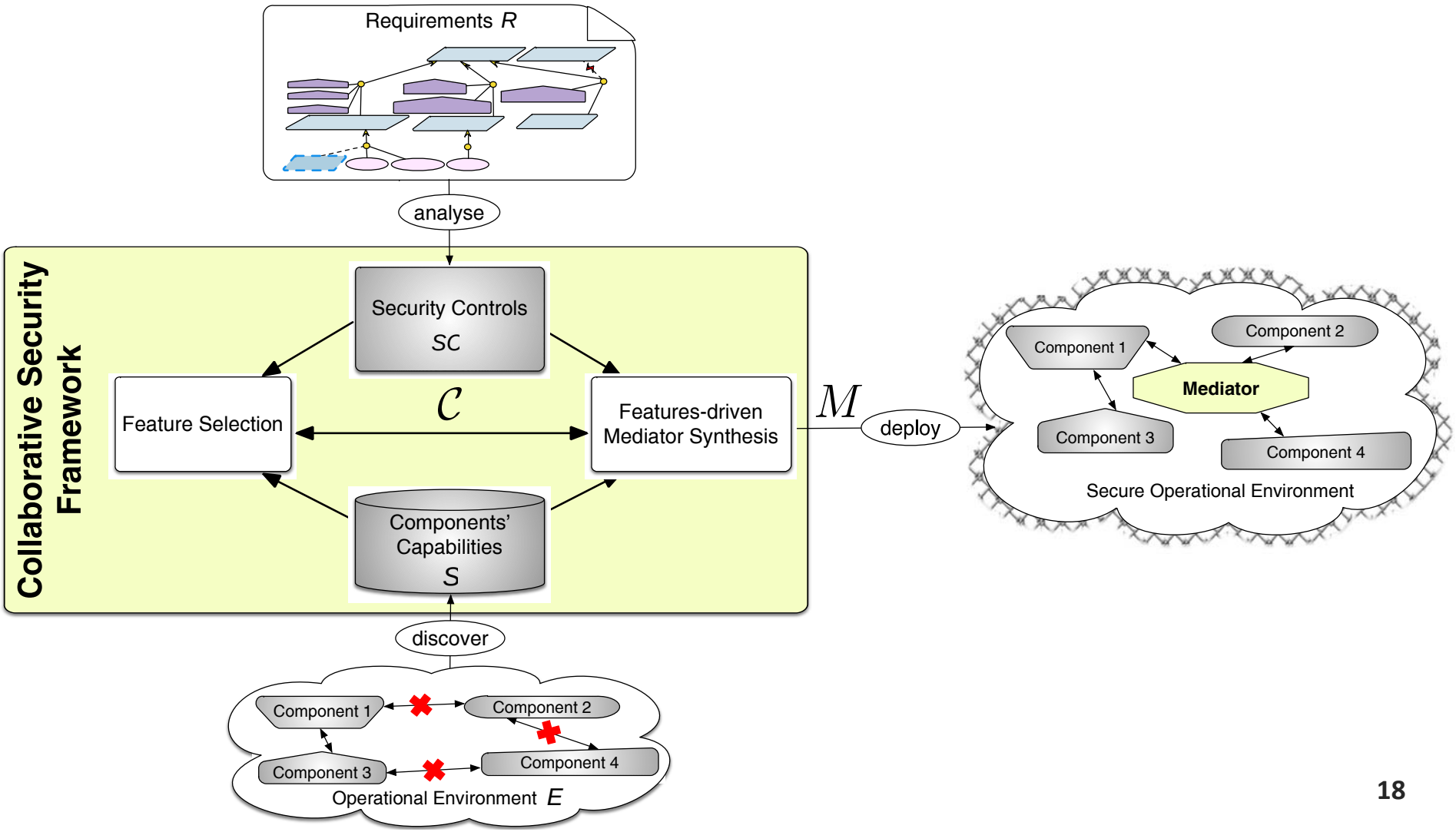
Features-driven Mediator Synthesis

Synthesise

- Use the selected features to project the behaviour of the components
- Synthesise, if possible, a mediator that enables the composed system to reach

$$fts_{1|f_1} \parallel fts_{2|f_2} \parallel \ldots fts_{n|f_n} \parallel M \models_B G_s$$

Collaborative Security Framework



Tool Support

http://sead1.open.ac.uk/fics/

Summary

- Features and behavioural models to reason about and achieve collaborative security
- Capability selection (and mediation) as a multi-objective optimisation problem
- Features to scope components' behaviours and reduce the space for mediation

Open Questions

- Can collaboration be applied to other types of requirements besides security ?
  - Yes but security exacerbates and opens many issues that make collaboration more challenging, e.g., dealing with change and assurance
- What are the limitations of the approach?
  - Predefined set of security control
  - Shared vocabulary between the specification of security controls and capabilities
  - Independent iterations between feature selection and mediator synthesis
  - individual components are trustworthy and implement the capabilities advertised

Open Questions

- How about the user?
  - How to explain the choice and implementation of the security control?
  - Is the user just another component?
- Where do the models come from? What is the impact of their inaccuracy on the model?

Thank you

www.amel.me

http://sead1.open.ac.uk/fics/

Adaptive Security and Privacy
www.asap-project.eu