Global Design for Secure Socio-Technical System

PhD Candidate: Tong Li

Supervisor: John Mylopoulos & Fabio Massacci

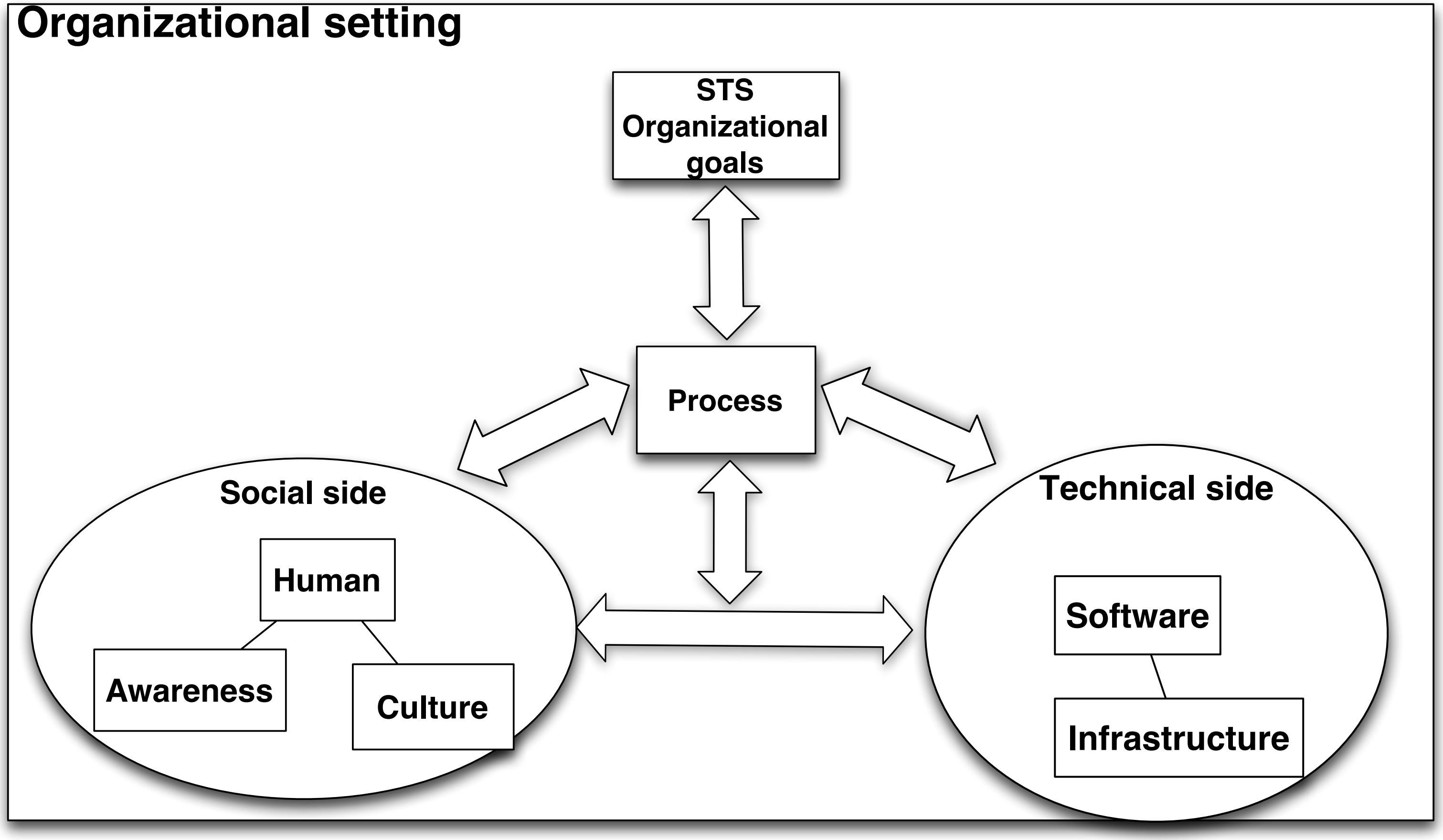
2013.02.08 @Molveno

Syllabus

- Motivation
- State of the Art
- Research Problem
- Research Approach
- Illustration
- Research Schedule
- Conclusion

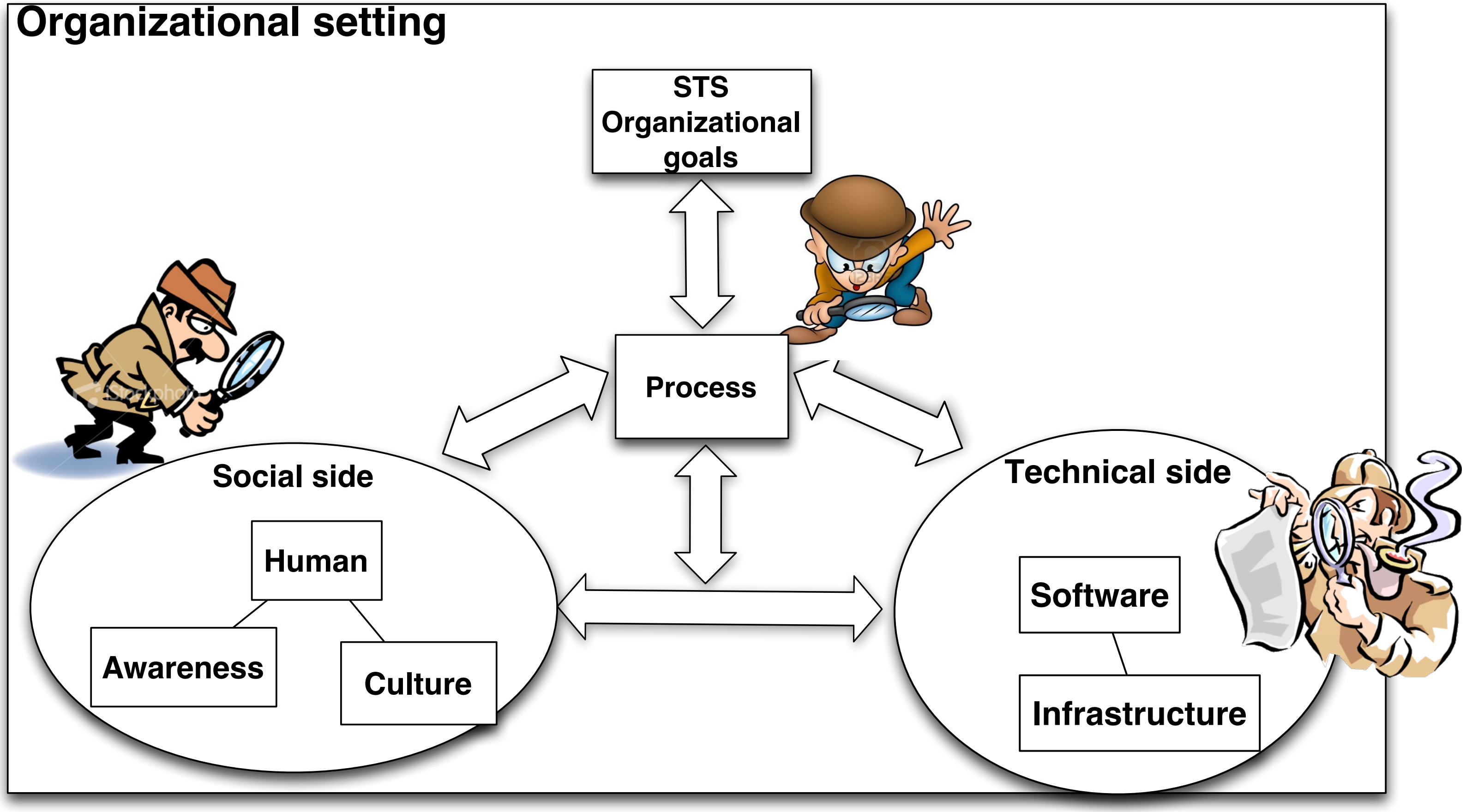
Motivation

- Socio-Technical System (STS)



Motivation

- How to secure STSs?



Organizational setting

STS Organizational goals

Process

Social side

Human

Awareness

Culture

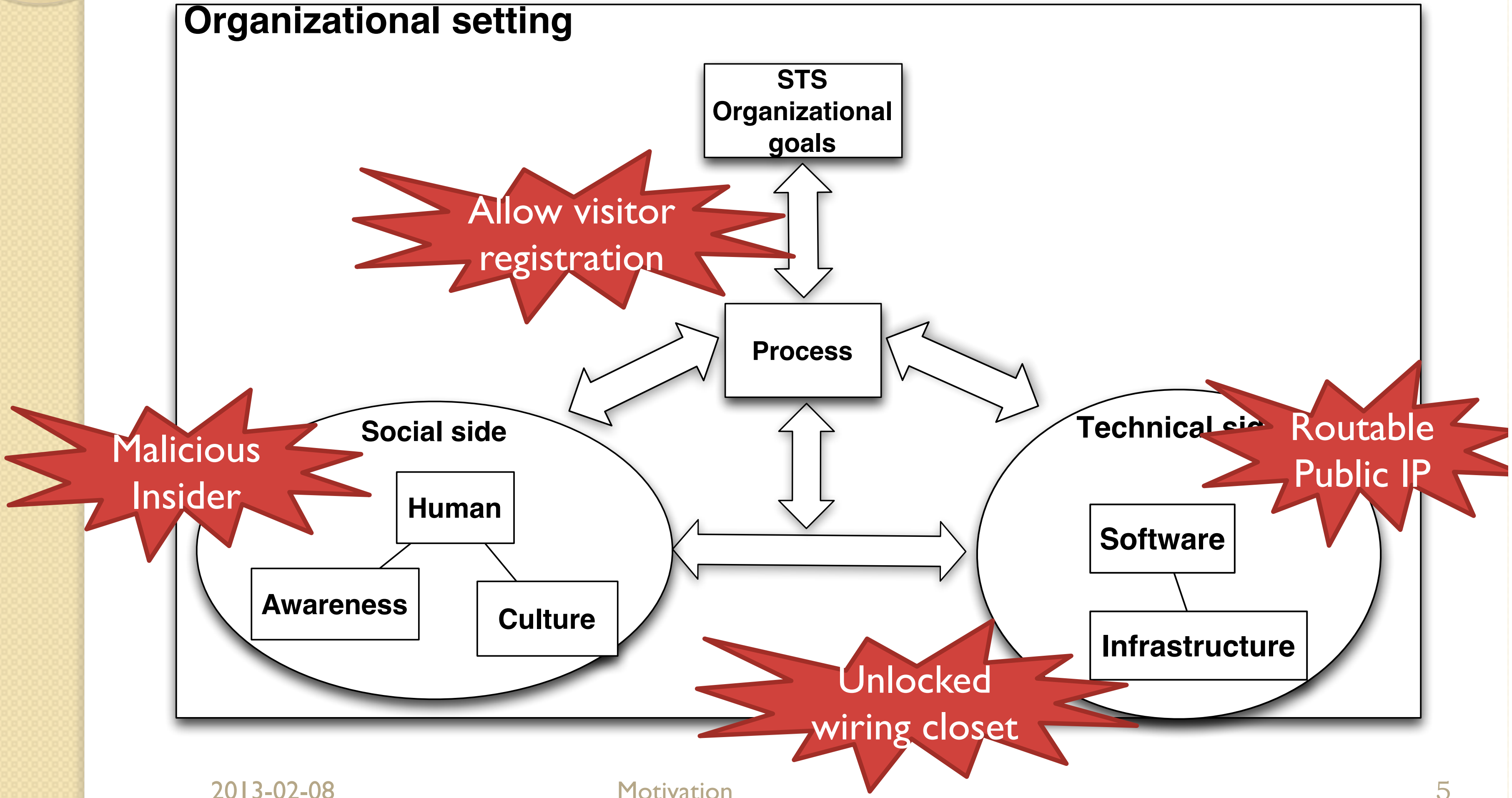
Technical side

Software

Infrastructure

Security Scenario

- **JSTOR Statement: Misuse Incident and Criminal Case --- more than 4.5 million articles are illegally downloaded**



State of the Art I
Security Analysis in Organizational Level

- Liu et al. model actors' social interactions, in which they analyze the vulnerable points.
- Mouratidis and Giorgini propose Security Tropos to capture organizational security issues.
- Giorgini et al. explore the trust, ownership and delegation relationships in the organizational level.
- Dalpiaz et al. elicit security requirements through three views: social view, resource view and authorization view. They represent those requirements by using commitments (SecCo).

State of the Art II
Security Analysis on Business Process

- Altuhhova et al. align BPMN constructs to ISSRM model to support modeling security concepts in business process models.
- Rodriguez et al. propose an extension on BPMN to model secure requirements for the business process.
- Herrmann and Herrmann propose MoSSBP, which provide the security analysis process for business process domain.
- Taubenberger and Jurjen exploit the semantics of business process to evaluate the adherence of security objectives in business process domain.

State of the Art III
Security Analysis for Software

- **SRE techniques**:
  - Misuse Case(Sindre2001), Abuse Case(McDermott1999), Attack Tree(Schneier1999), Obstacle/Anti-goal(Lamsweerde2002,2004), Anti-requirements/Abuse Framework(Lin2003)
- **SRE process**:
  - CLASP(Viega2005), SQUARE(Mead2005), SREP(Mellado2007)
- **Security development in SDLC**:
  - UMLSec(Jurjen2002), Security Pattern(Schumacher2002), Security Architecture Pattern(Riccardo2008), Microsoft SDL(2010)

State of the Art IV
Multi-view Security Analysis

- Mouratidis and Jurjen integrate Security Tropos with UMLSec, which translates organizational security requirements to design level.
- Paja et al. transferring SecCo organizational security requirements to the business process domain.
- Mana et al. defines security semantics for the business process, and further transfer them into the software development.
- Muller et al. manually derive software security requirements by referring to related business process model.

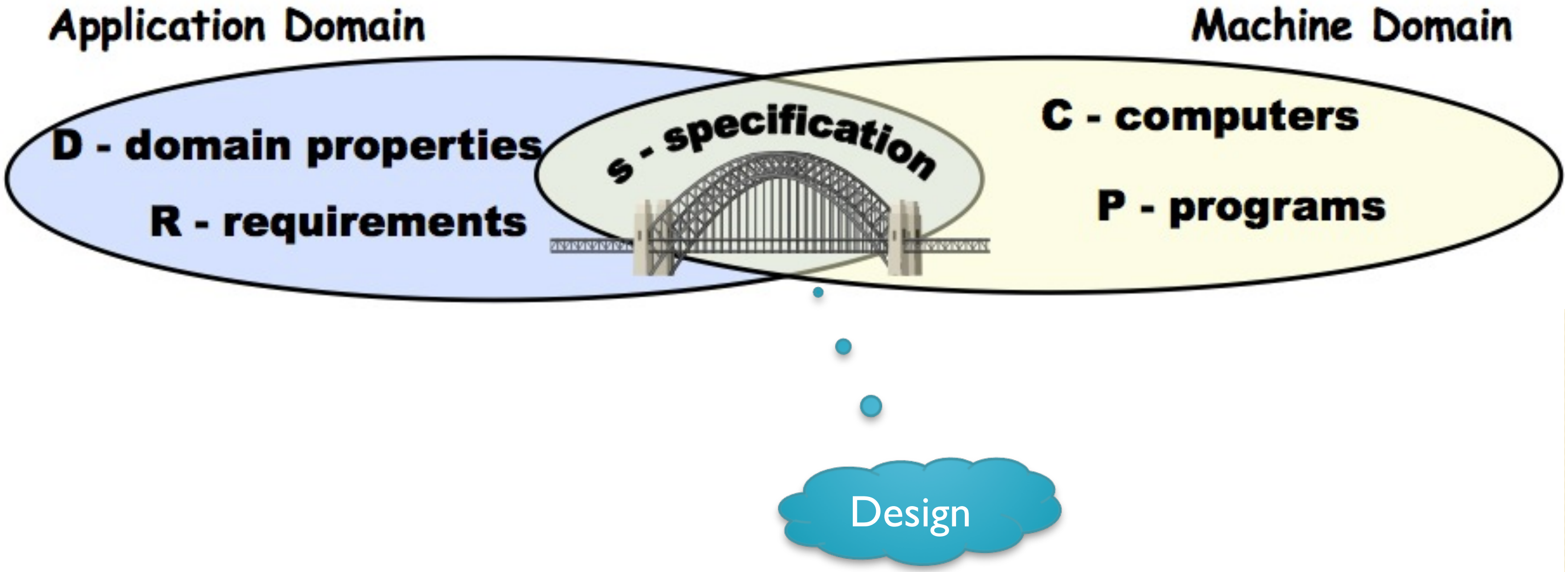
Research Problem

- Coordinate the security designs of all related domains to deliver secure STSs.
  - Business process
  - Software
  - Infrastructure

Preliminary

- Problem model

$$D, S \vdash R$$

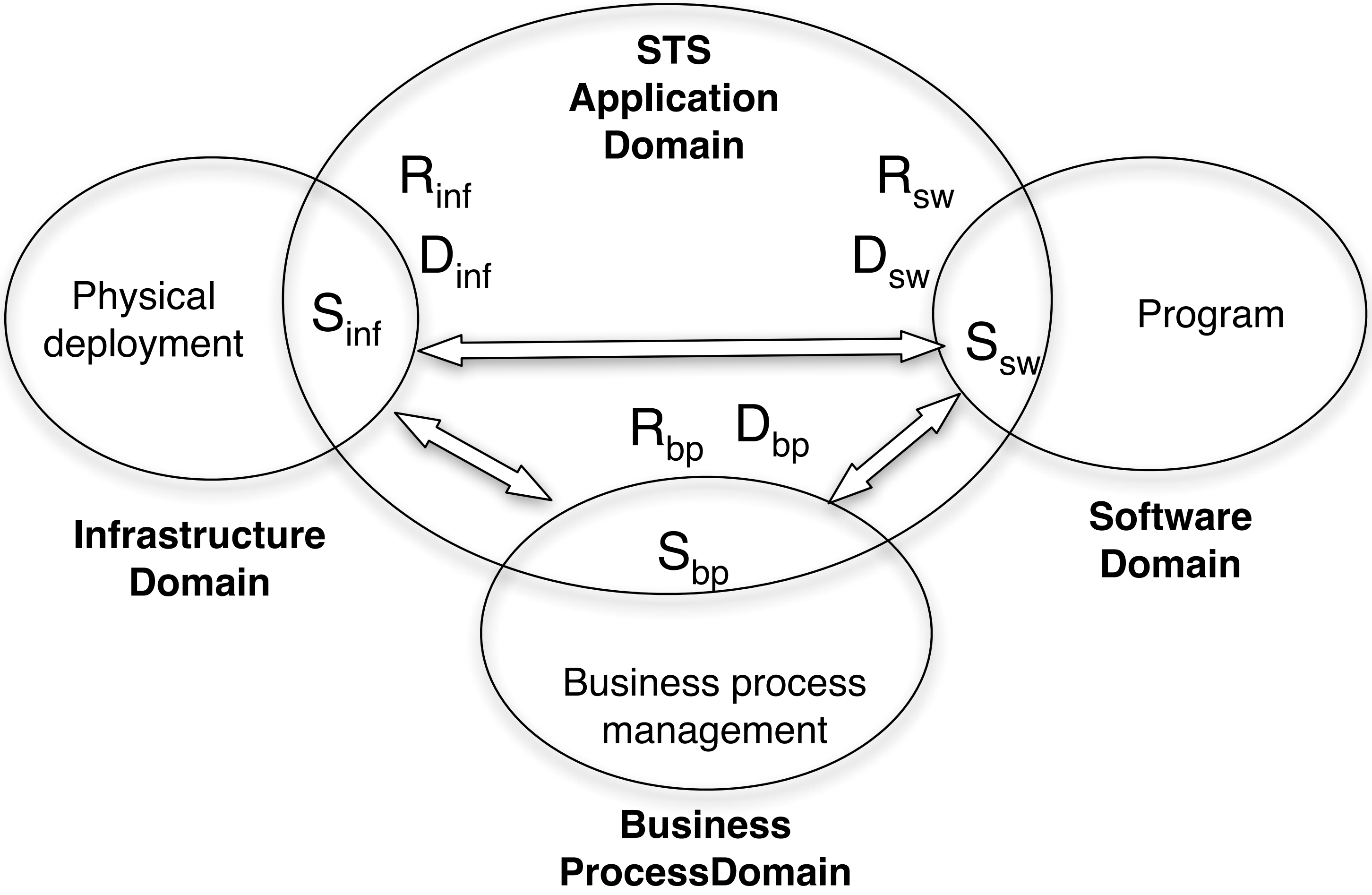


Reformed Problem Model

- Treat each component of STS as a separate problem domain.
- The design of a STS is the combination of all three specifications.
- Examine the interrelationship among specifications in each domain.

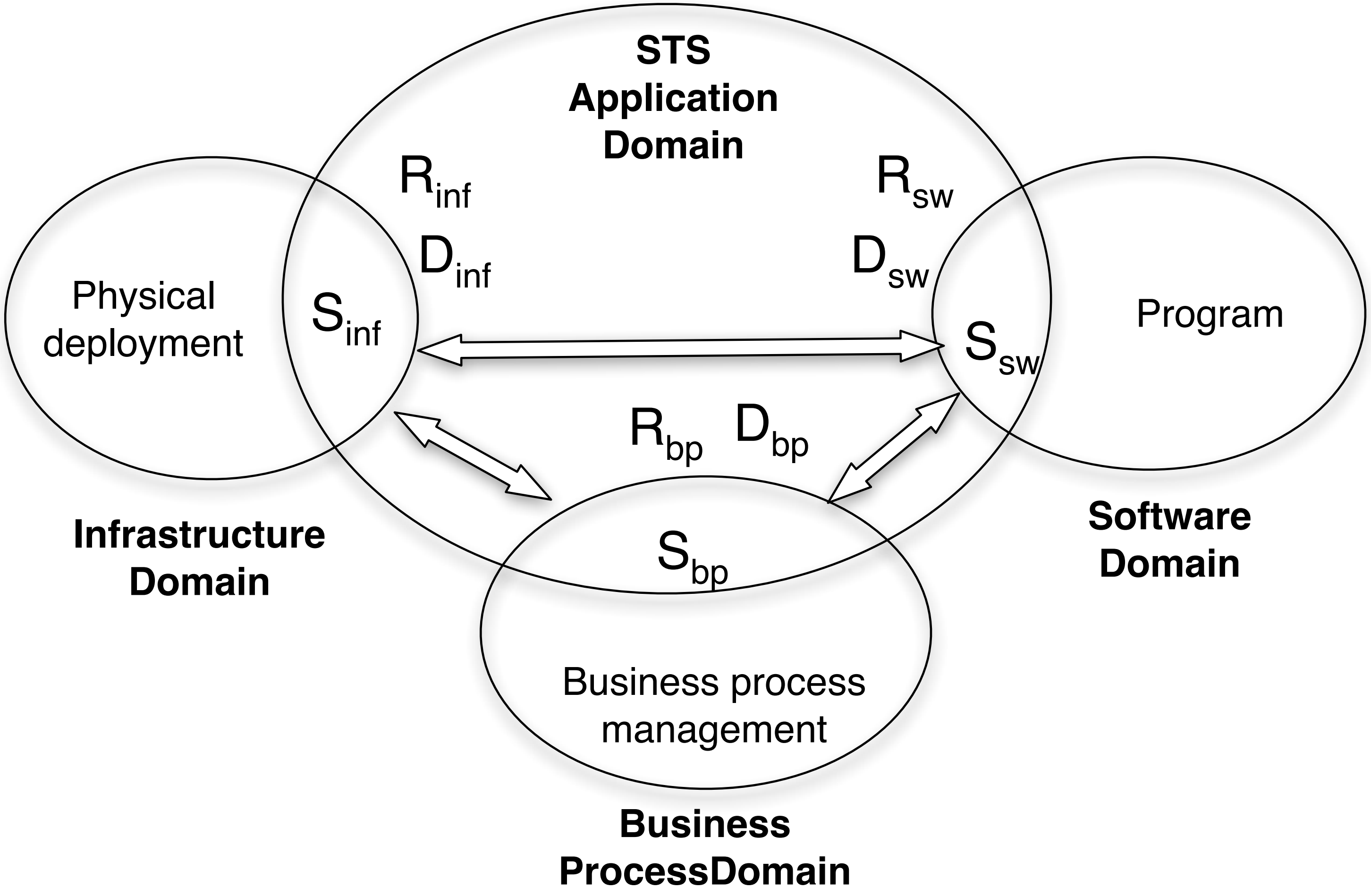
Problem Overview

- The design of a STS is the combination of all three specifications.



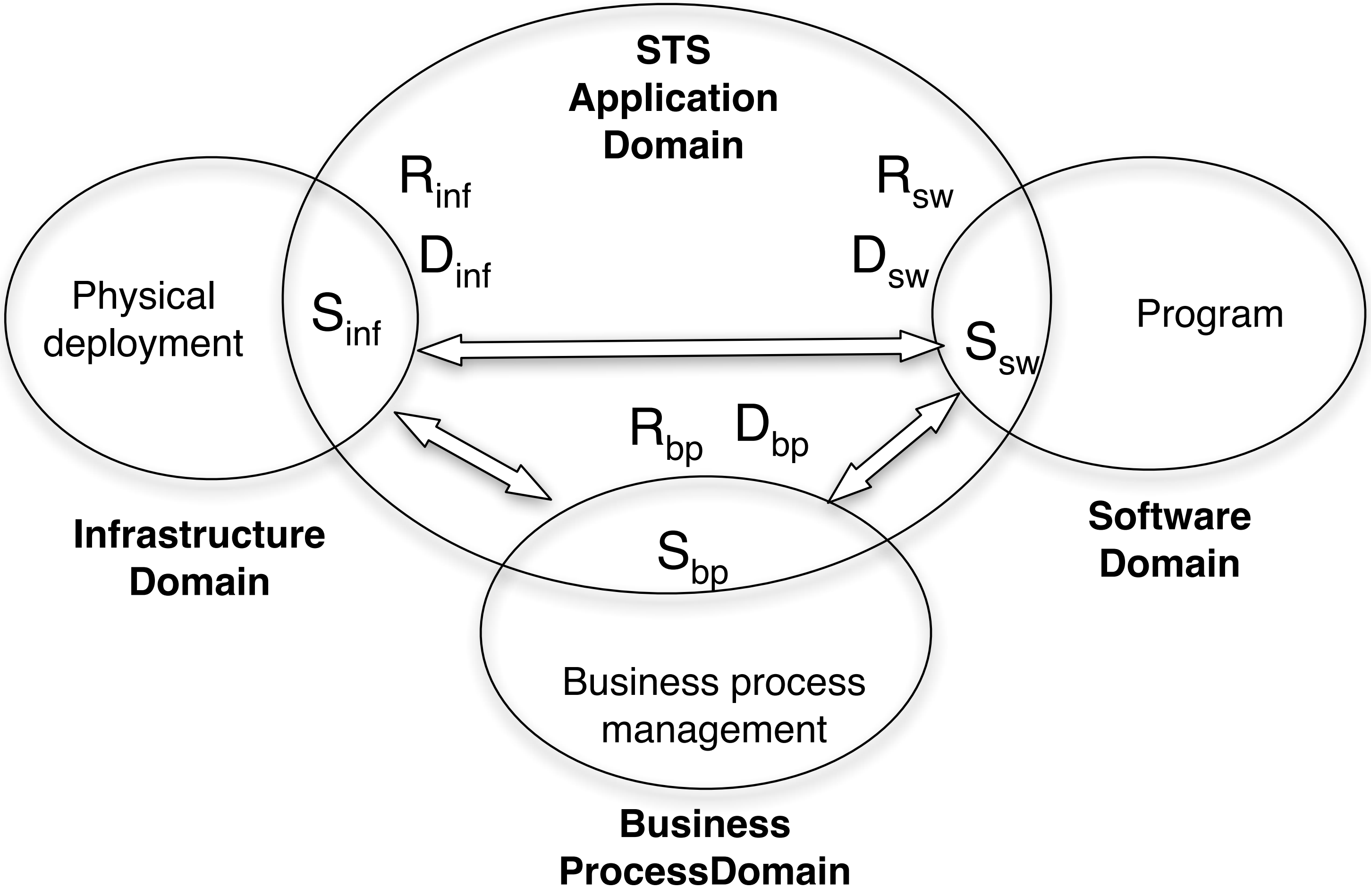
Problem Overview

- Treat each component of STS as a separate problem domain.



Problem Overview

- Examine the interrelationship among specifications in each domain.

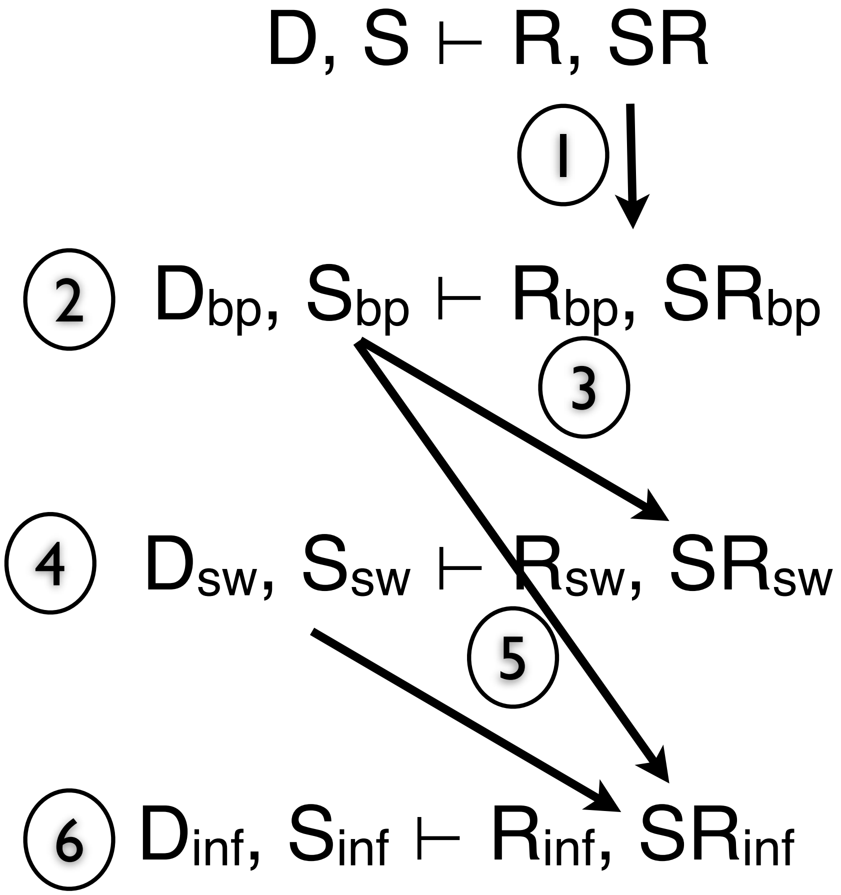


Research Questions

- Basic questions:
  - What are the interrelationships among each domain?
  - How to orchestrate the security analysis and design in different domains?
  - How to adapt designs to handle system changes?
  - How to support real secure system development?
  - What about the correctness and effectiveness of the proposed method?
- Further question:
  - How to derive secure design in each domain?

Research Approach

- System Design Hierarchy



$D, S \vdash R, SR$

1

2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$

3

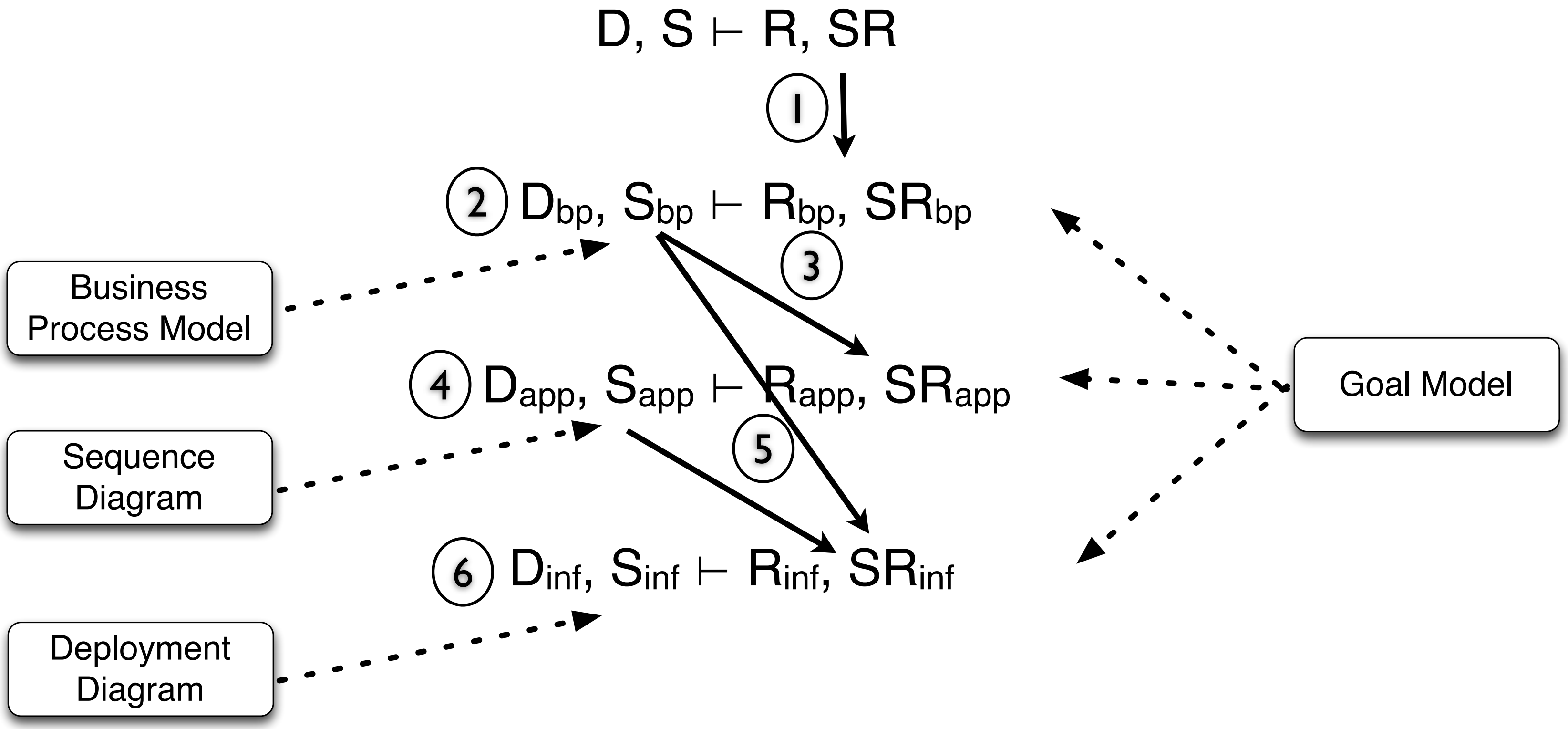
4 $D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$

5

6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$

Research Approach

- System Design Hierarchy



$D, S \vdash R, SR$

1

2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$

3

4 $D_{app}, S_{app} \vdash R_{app}, SR_{app}$

5

6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$

Business Process Model

Sequence Diagram

Deployment Diagram

Goal Model

Research Plan

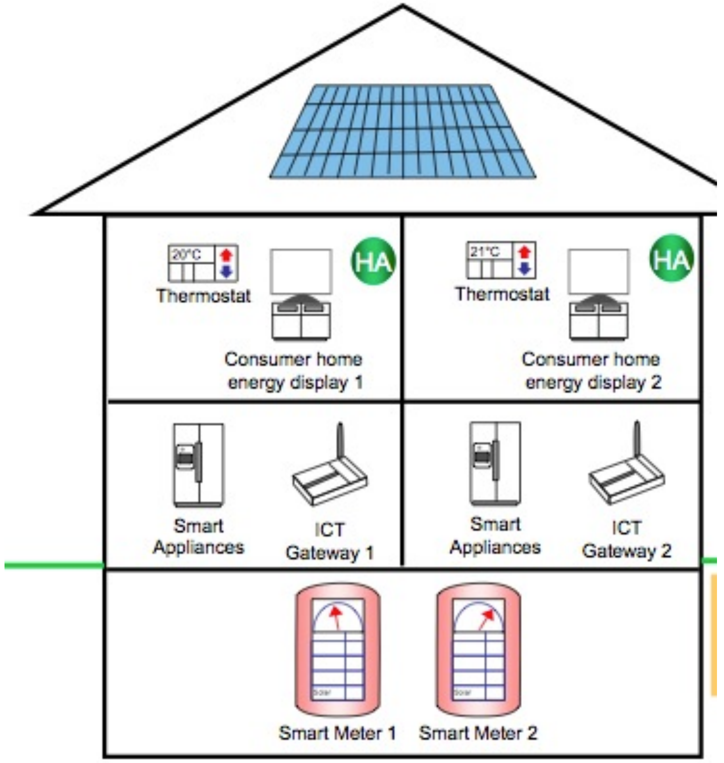
Research Questions	Research Plan
What are the interrelationships among each domain?	Investigate domain knowledge and represent it with an ontology.
How to orchestrate the security analysis and design in different domains?	Propose a methodology based on previous ontology to guide the secure STS development and evolution.
How to adapt designs to handle system changes?	
How to support real secure system development?	Develop a graphical tool to support the ontology construction and related reasoning.
What about the correctness and effectiveness of the proposed method?	Evaluate the proposed approach with a real case study.
How to derive secure design in each domain?	Investigate the way to derive security designs by exploiting the semantics of the proposed ontology.

Research Baseline

- Requirement goal model (Tropos)
- Business process model (BPMN)
- State diagram (UML)
- Deployment diagram (UML)
- Description Logic
- Attack model (Attack tree)
- Risk model (CORAS)
- Security pattern

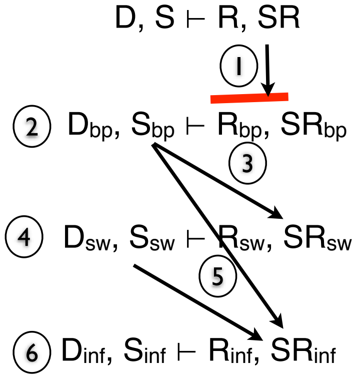
Global Design Illustration

- **Real-time pricing**: Dynamically change the price of energy to regulate customer's demands
- --- Global secure design
- --- Change management

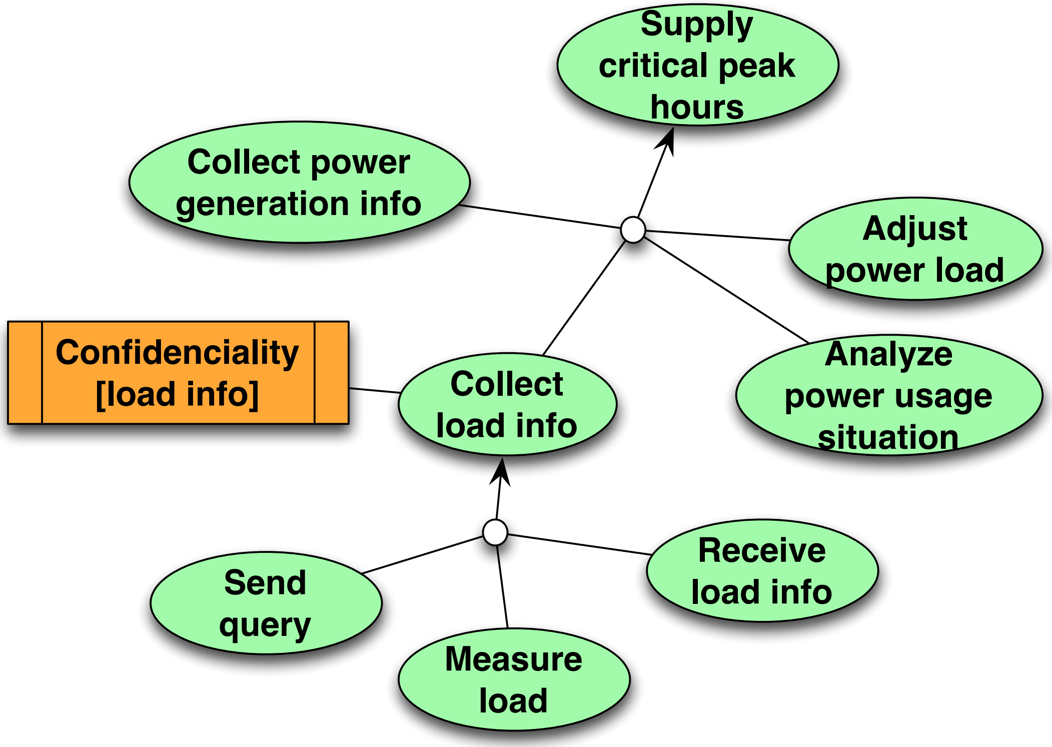


Design-Step 1

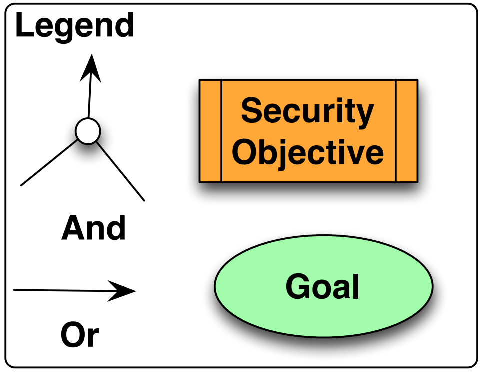
- Build System requirement model (R,SR)



$D, S \vdash R, SR$
1
2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$
3
4 $D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$
5
6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$

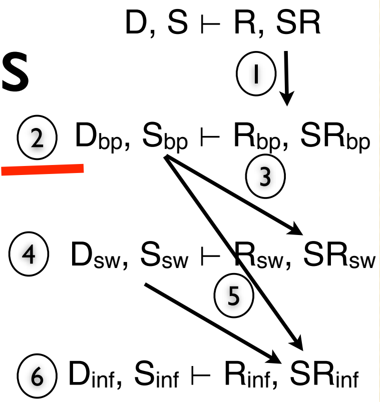


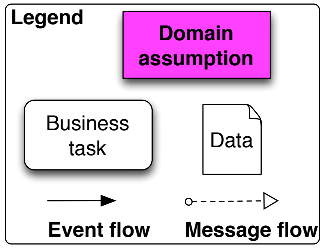
Supply critical peak hours
Collect power generation info
Adjust power load
Confidenciality [load info]
Collect load info
Analyze power usage situation
Send query
Receive load info
Measure load

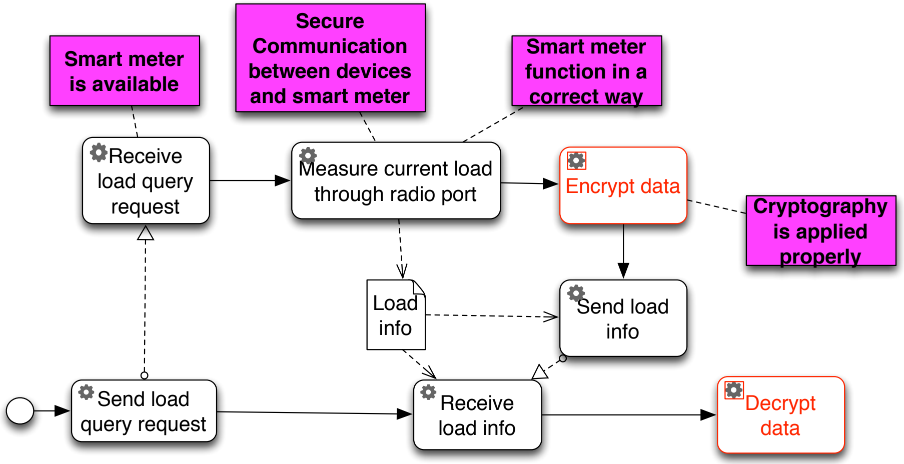


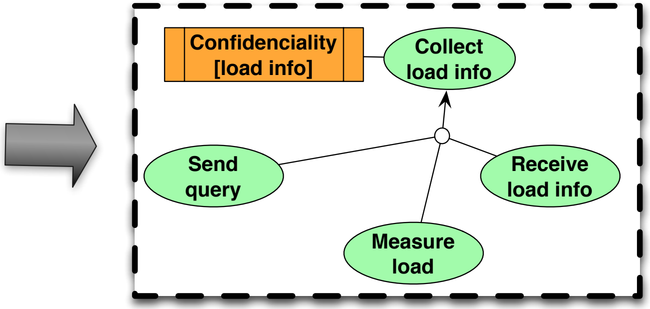
Design-Step 2

- Generate secure business process designs $(D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp})$


D, S ⊢ R, SR
1
2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$
3
4 $D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$
5
6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$



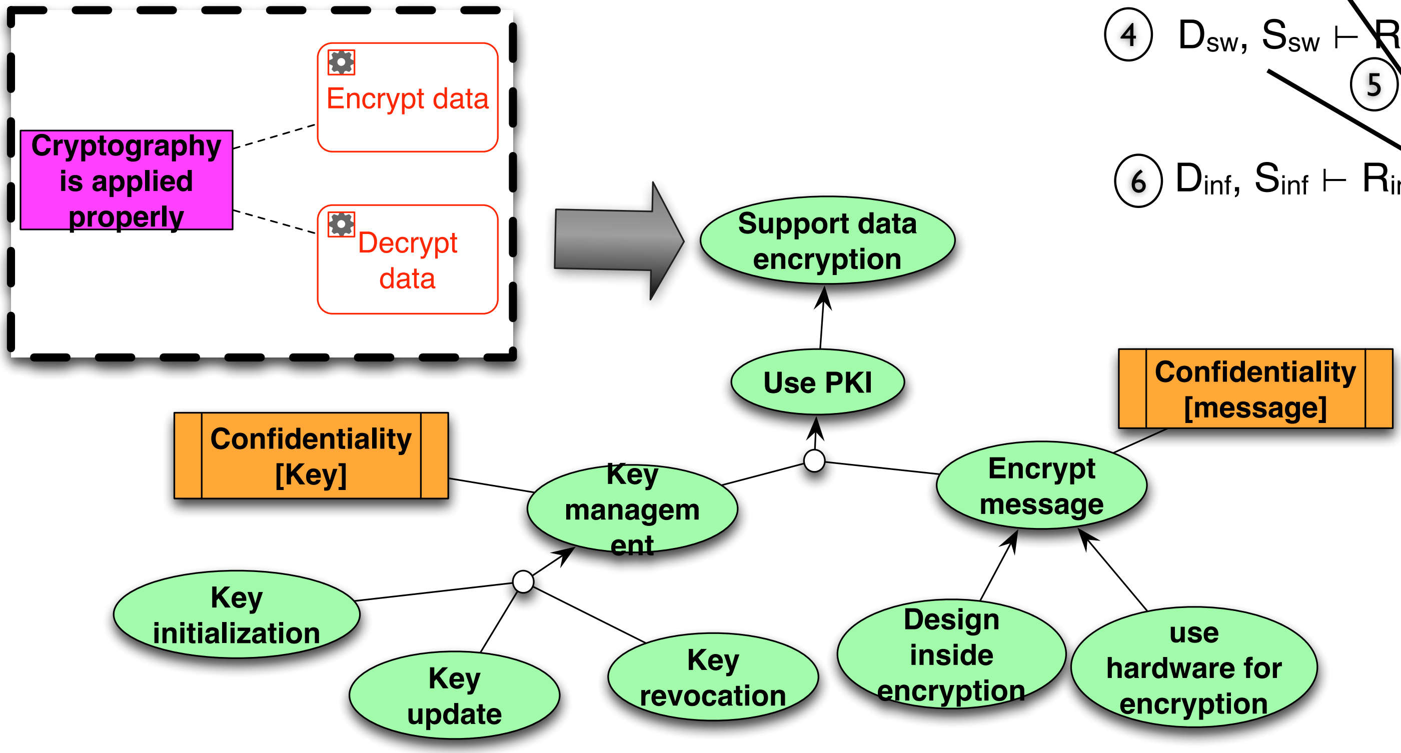

Smart meter is available
Secure Communication between devices and smart meter
Smart meter function in a correct way
Receive load query request
Measure current load through radio port
Encrypt data
Cryptography is applied properly
Load info
Send load info
Send load query request
Receive load info
Decrypt data



Design-Step 3

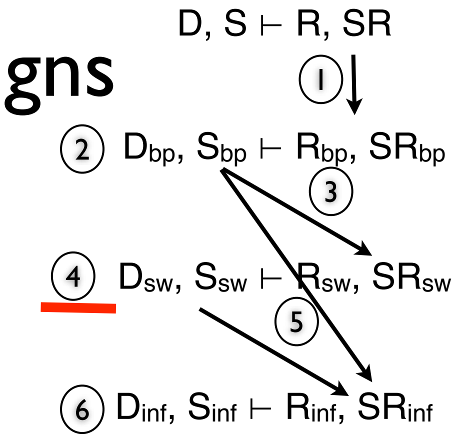
- Derive requirement goal model for software(R_{sw}, SR_{sw})

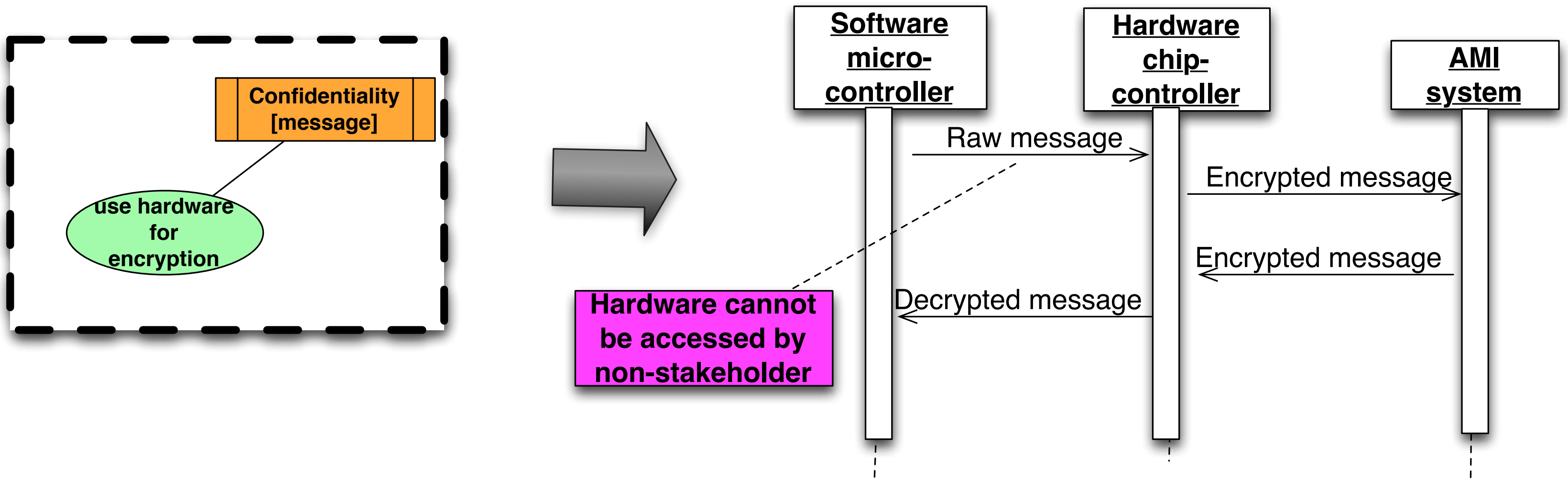
$$\begin{tikzcd}
 & D, S \vdash & R, & SR \arrow[d, "\textcircled{1}"] \\
\textcircled{2} & D_{bp}, S_{bp} \vdash \arrow[drr, "\textcircled{3}"] \arrow[ddrr] & R_{bp}, & SR_{bp} \\
\textcircled{4} & D_{sw}, S_{sw} \vdash \arrow[dr, "\textcircled{5}"] & R_{sw}, & SR_{sw} \\
\textcircled{6} & D_{inf}, S_{inf} \vdash & R_{inf}, & SR_{inf}
\end{tikzcd}$$



Design-Step 4

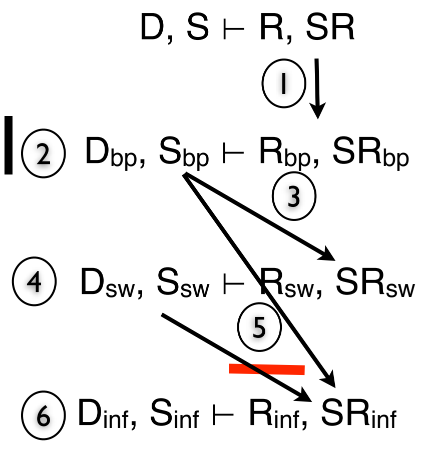
- Generate secure software designs ($D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$)


D, S ⊢ R, SR
1
2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$
3
4 $D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$
5
6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$

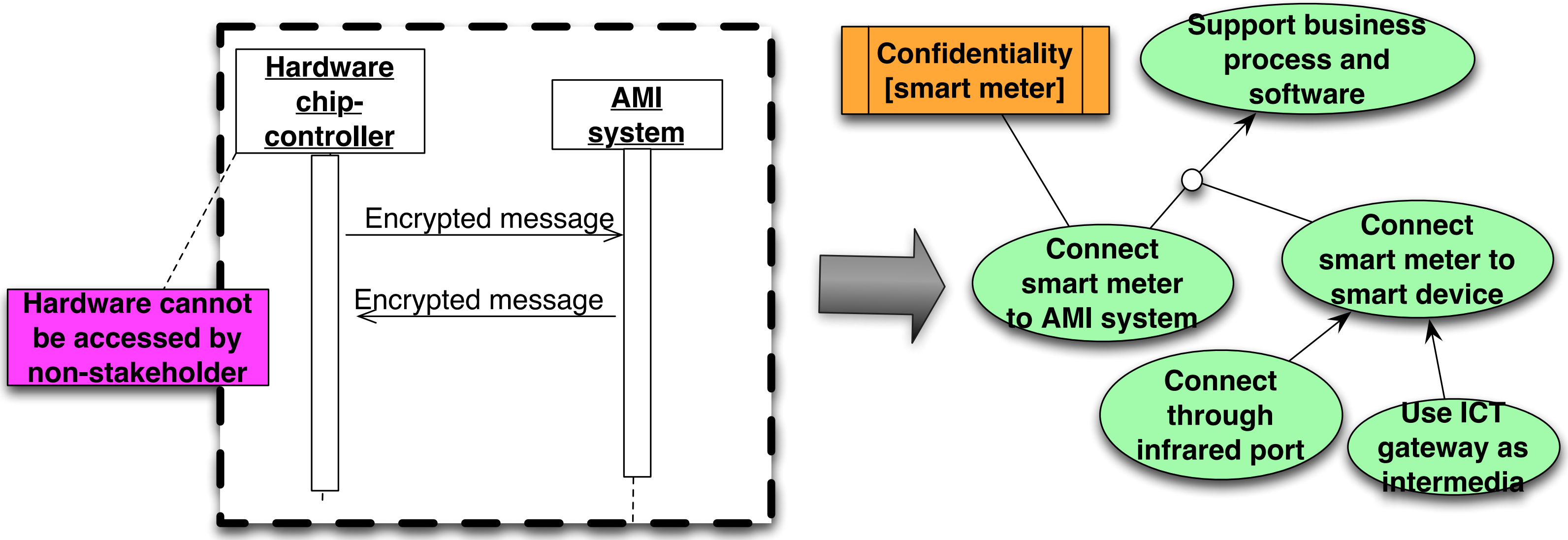

Confidentiality [message]
use hardware for encryption
Software micro-controller
Hardware chip-controller
AMI system
Raw message
Encrypted message
Encrypted message
Decrypted message
Hardware cannot be accessed by non-stakeholder

Design-Step 5

- Derive requirements goal model for infrastructure ($R_{inf,}$ SR_{inf})



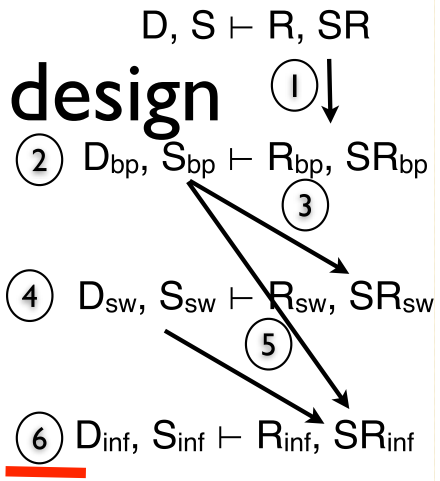
$D, S \vdash R, SR$
1
2
$D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$
3
4
$D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$
5
6
$D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$

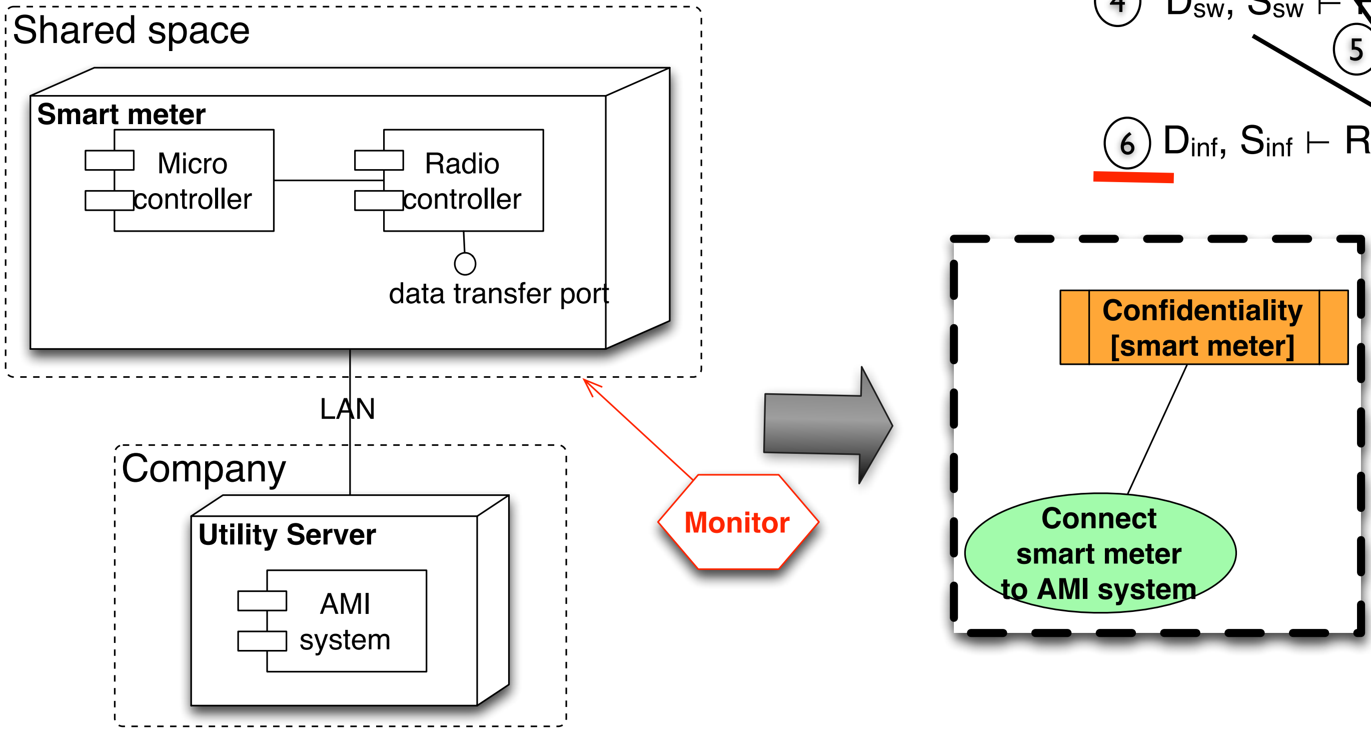


Hardware chip-controller
AMI system
Encrypted message
Encrypted message
Hardware cannot be accessed by non-stakeholder
Confidentiality [smart meter]
Support business process and software
Connect smart meter to AMI system
Connect smart meter to smart device
Connect through infrared port
Use ICT gateway as intermedia

Design-Step 6

- Generate secure infrastructure design ($D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$)


D, S ⊢ R, SR
1
2 $D_{bp}, S_{bp} \vdash R_{bp}, SR_{bp}$
3
4 $D_{sw}, S_{sw} \vdash R_{sw}, SR_{sw}$
5
6 $D_{inf}, S_{inf} \vdash R_{inf}, SR_{inf}$



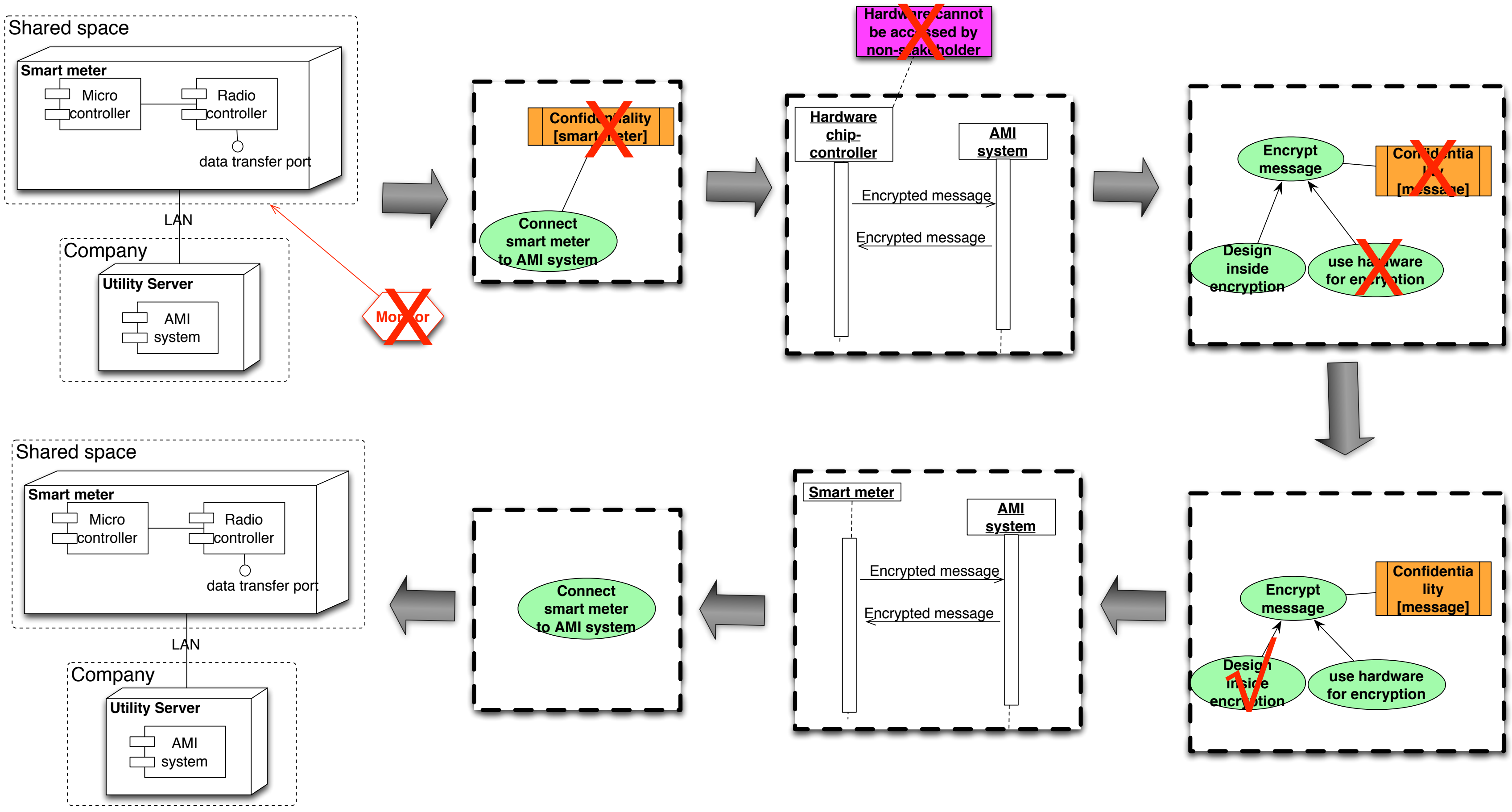
Design Changes Processes

Infrastructure Design

Infrastructure Requirement

Software Design

Software Requirement



Research Schedule

Plan	2013				2014				2015			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Develop Ontology	🟥	🟥	🟥									
Global Design Methodology			🟥	🟥	🟥							
System Evolution Process				🟥	🟥	🟥						
Develop Tool					🟥	🟥	🟥	🟥				
Case Study						🟥	🟥	🟥	🟥			
Write Thesis									🟥	🟥	🟥	🟥

Conclusion

- Propose a conceptual framework to represent interactions among different system domains.
- Investigate a methodology to globally design a secure socio-technical system, which satisfy both organizational objectives and security requirements.
- A systematic process to evolve system design to manage requested changes.
- Develop a tool to support the whole methodology.
- Evaluate the methodology with several case studies.

Thanks You!