Design Secure STS through Multi-views Security Analysis

Tong Li

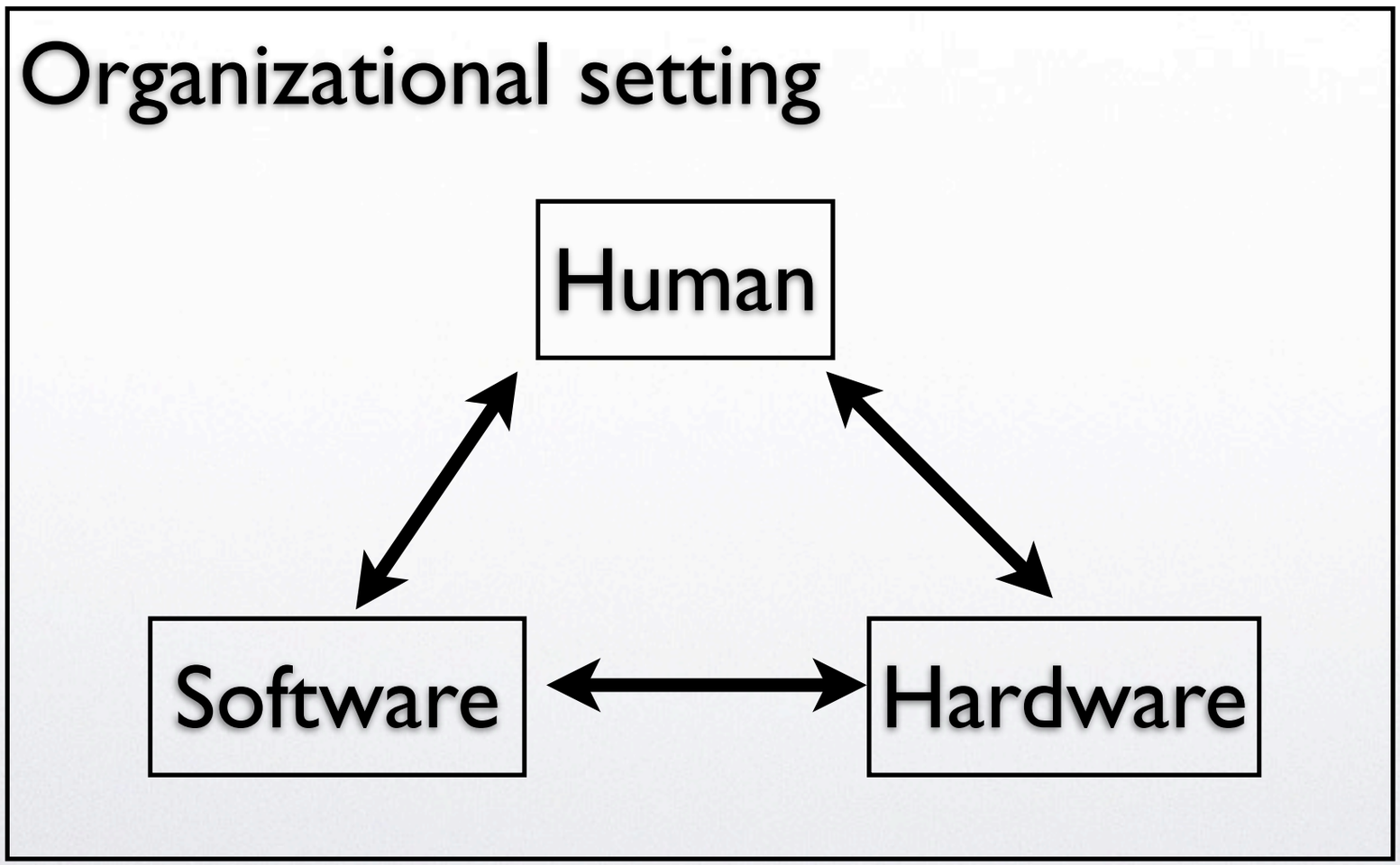
2012.11.08 @Ofek

Syllabus

- Motivation
- Research Problem
- Research Approach
- Illustration
- Related work
- Conclusion

Motivation

- Socio-Technical System



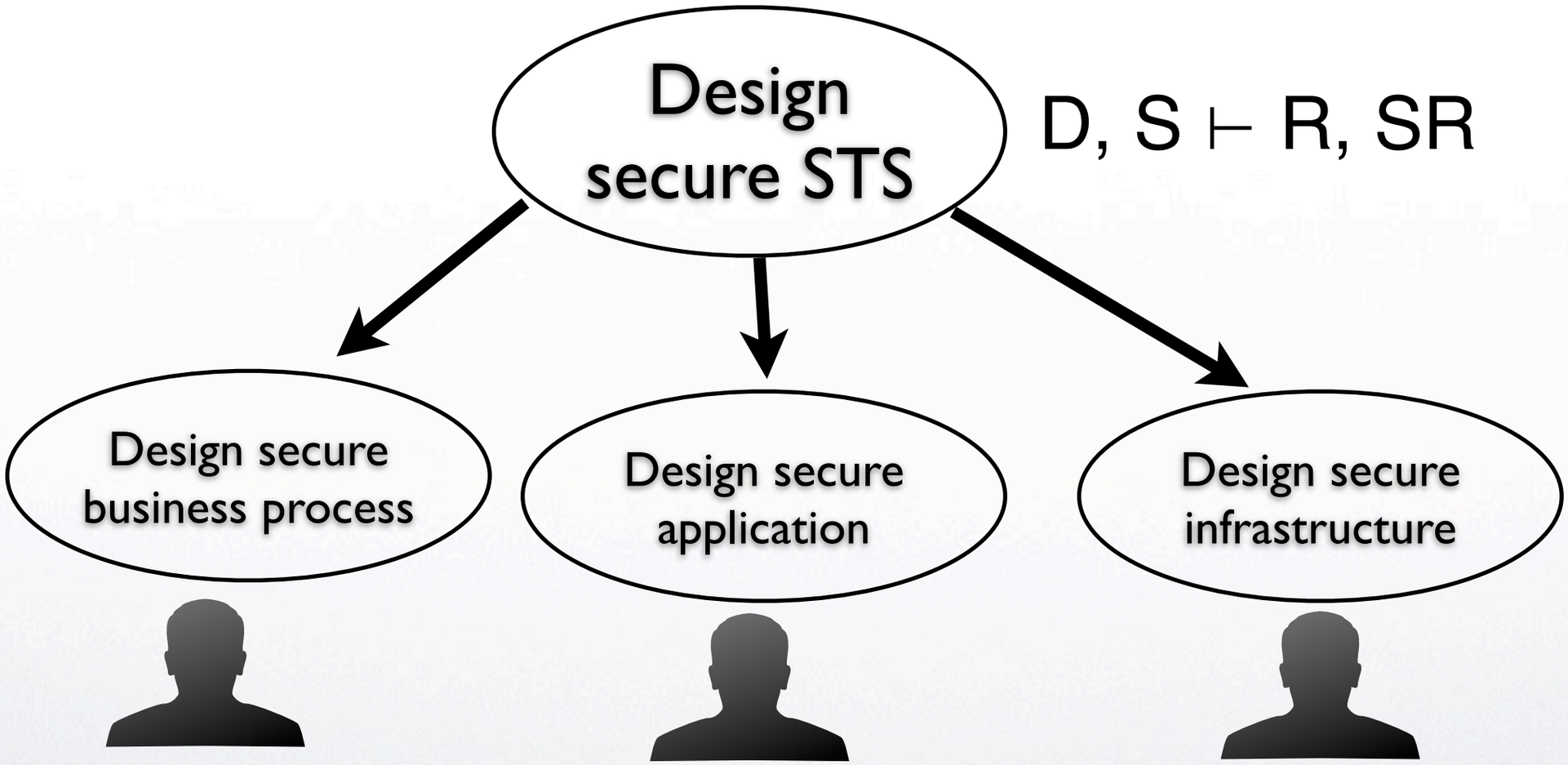
Motivation

- However...
  - a piecemeal fashion
- Case: How do you make your paper secure?
  - A: set a password to the file
  - B: use some anti-virus software
  - C: lock the computer
  - ...

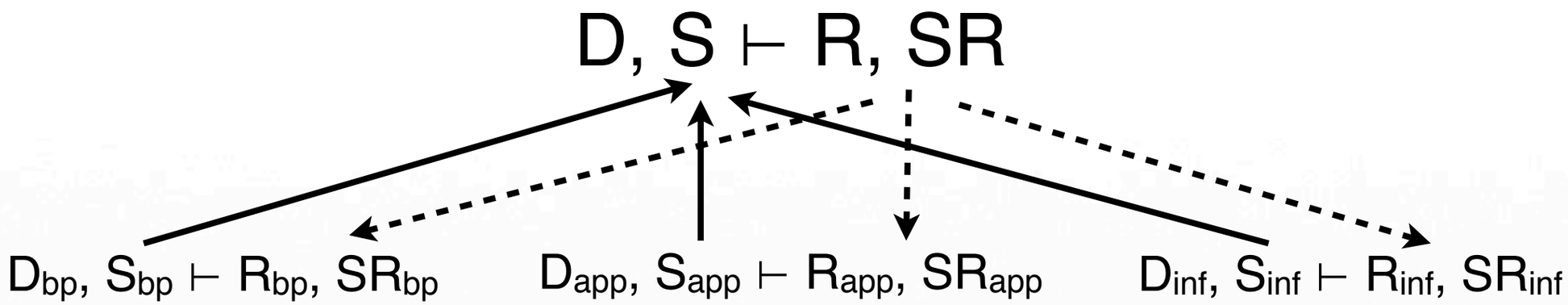
Research Problem

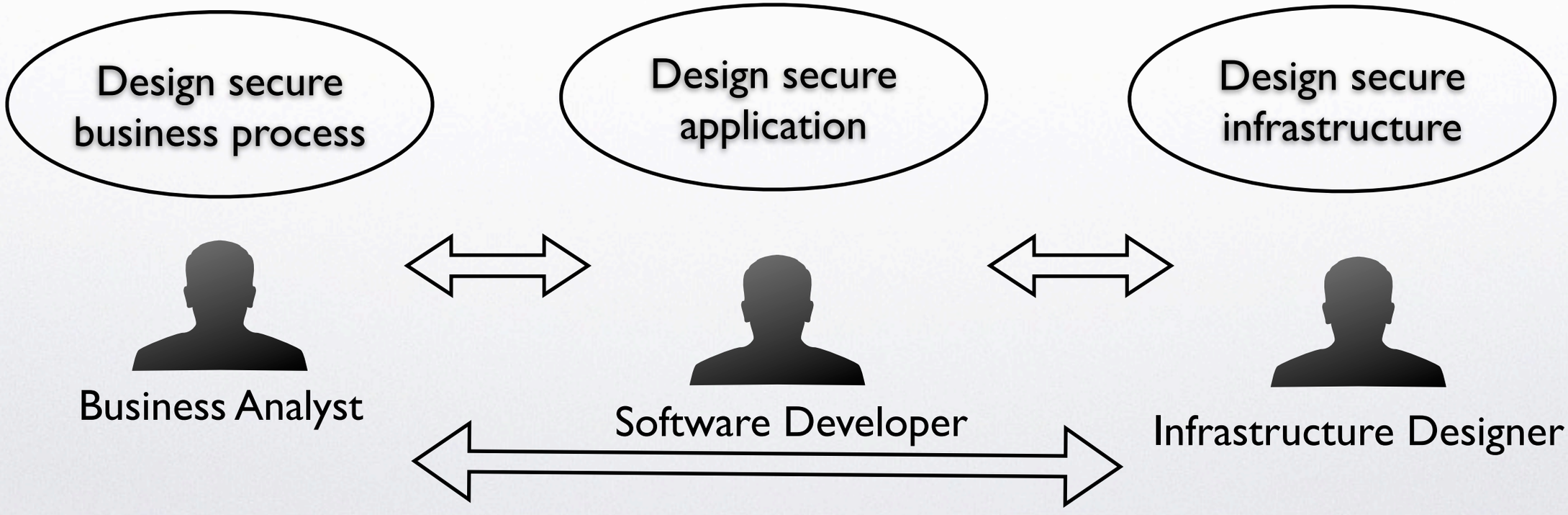
- Design secure STS through multi-views
  - Business process view
  - Application view
  - Infrastructure view

Research Problem



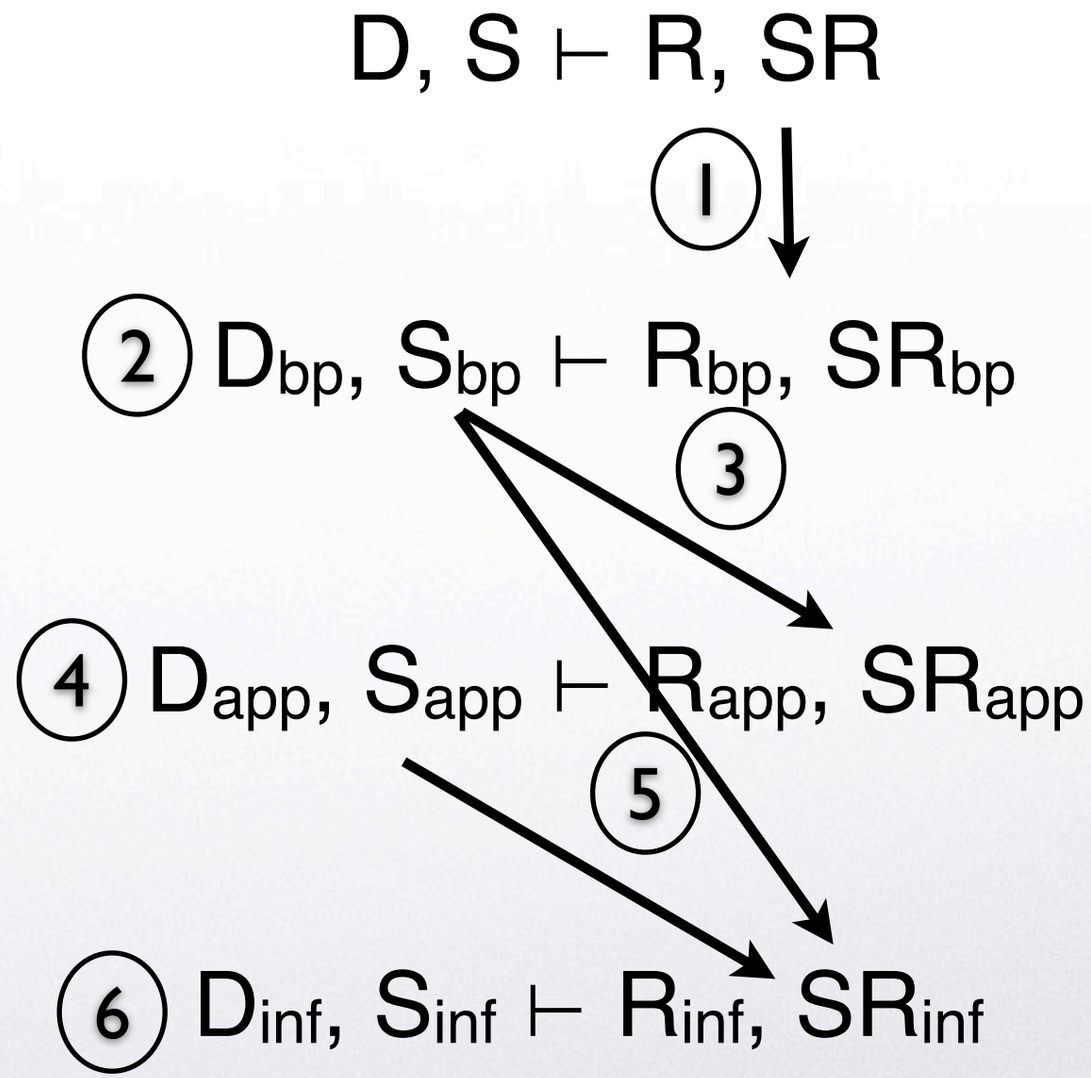
Research Problem





Research Approach

- Research structure
- Research task

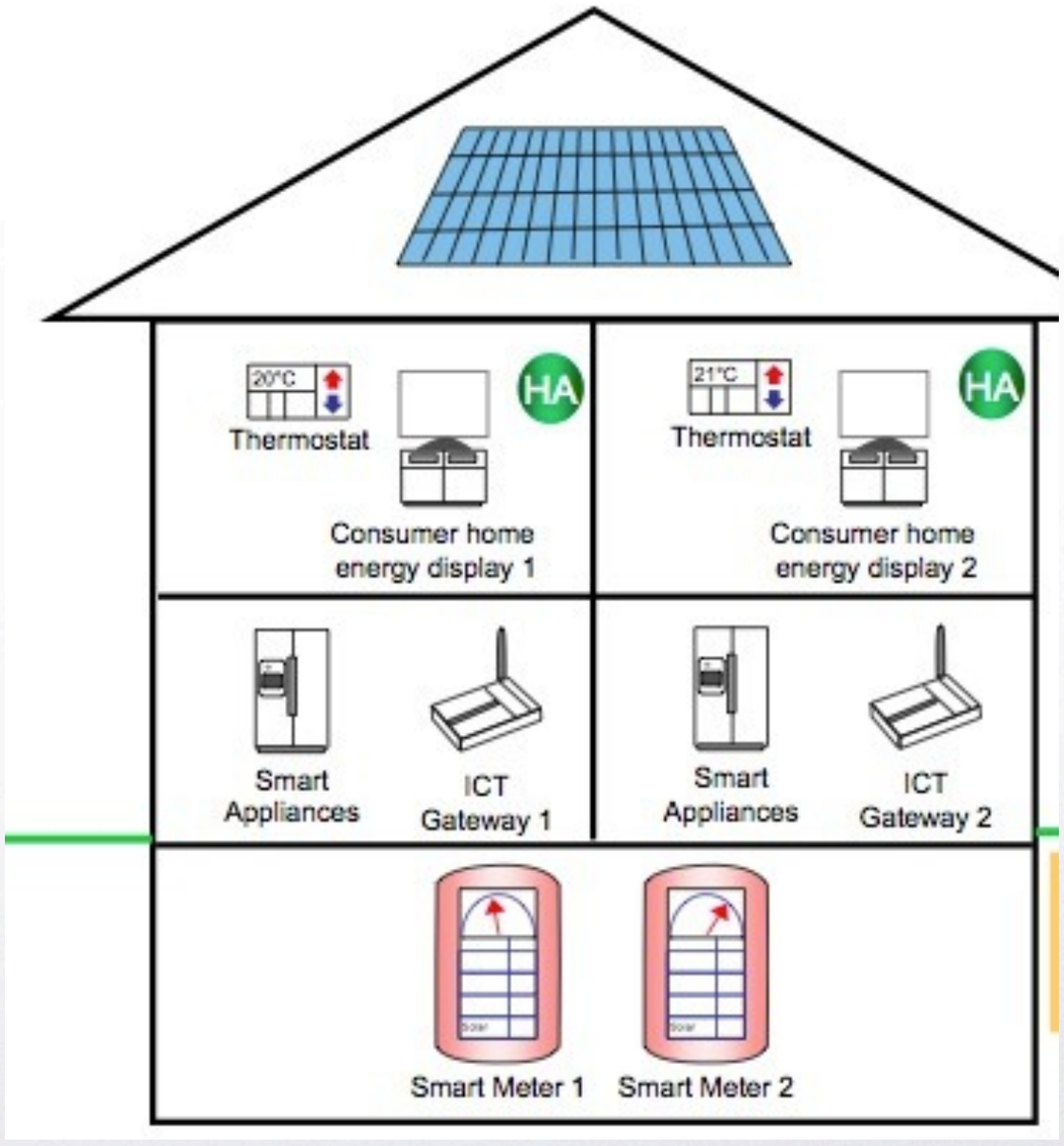


Research Approach

- Research Baseline
  - Requirement goal model (KAOS)
  - Business process model (BPMN)
  - Attack model (Attack tree)
  - Risk model (CORAS)
  - Security pattern
  - State diagram (UML)
  - Deployment diagram (UML)

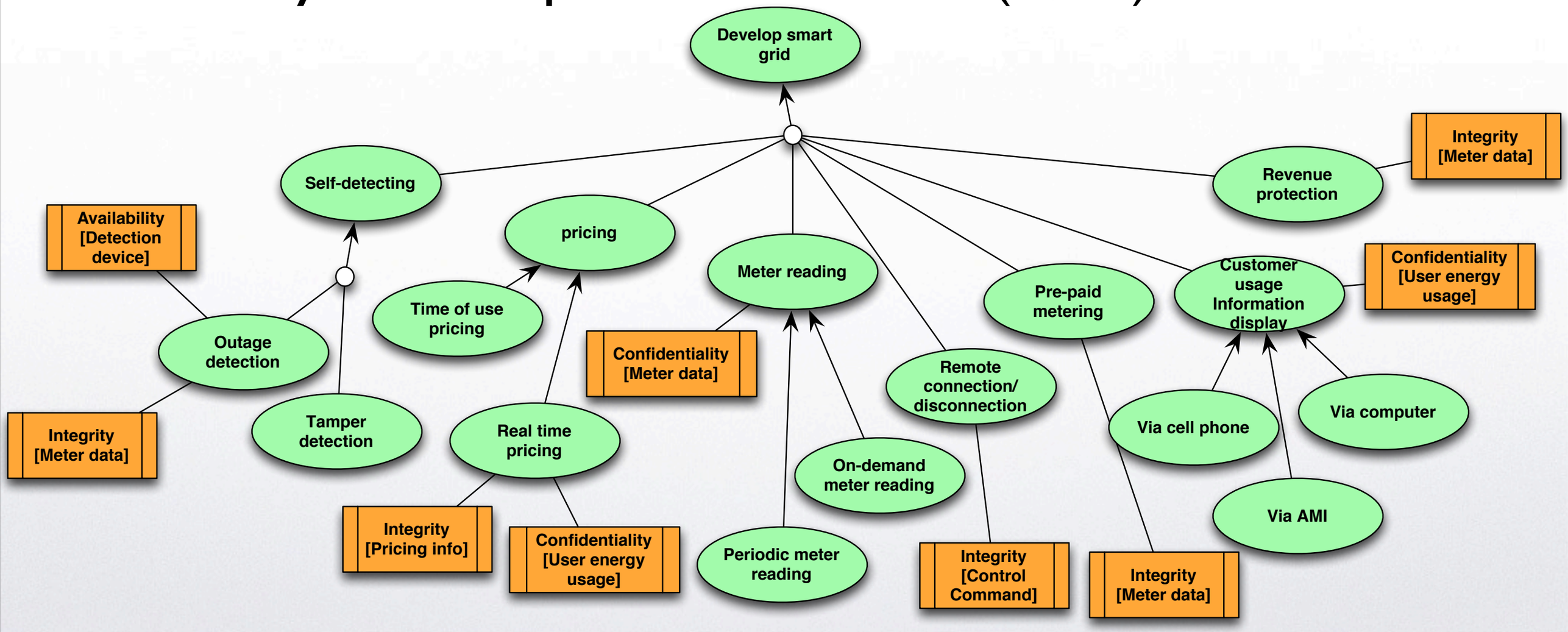
Illustration

- Smart Grid
  - Traditional power grid enhanced by ICT
- Two-way communication through smart meters

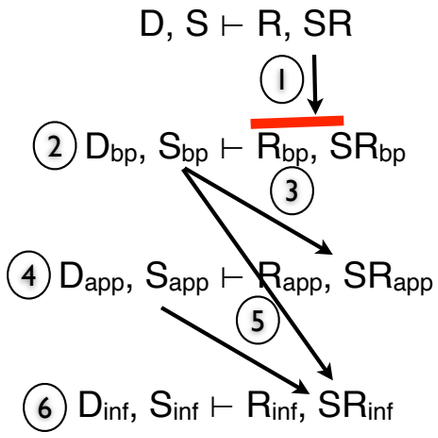


Illustration

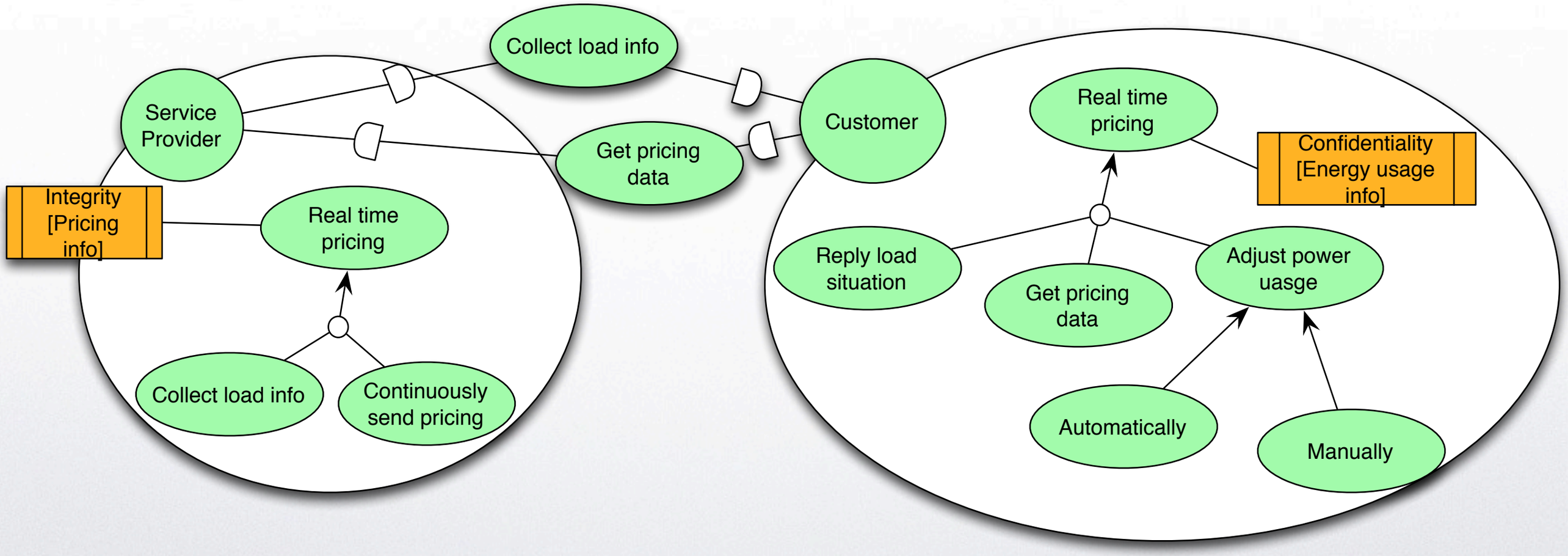
- System requirement model (R,SR)



Illustration

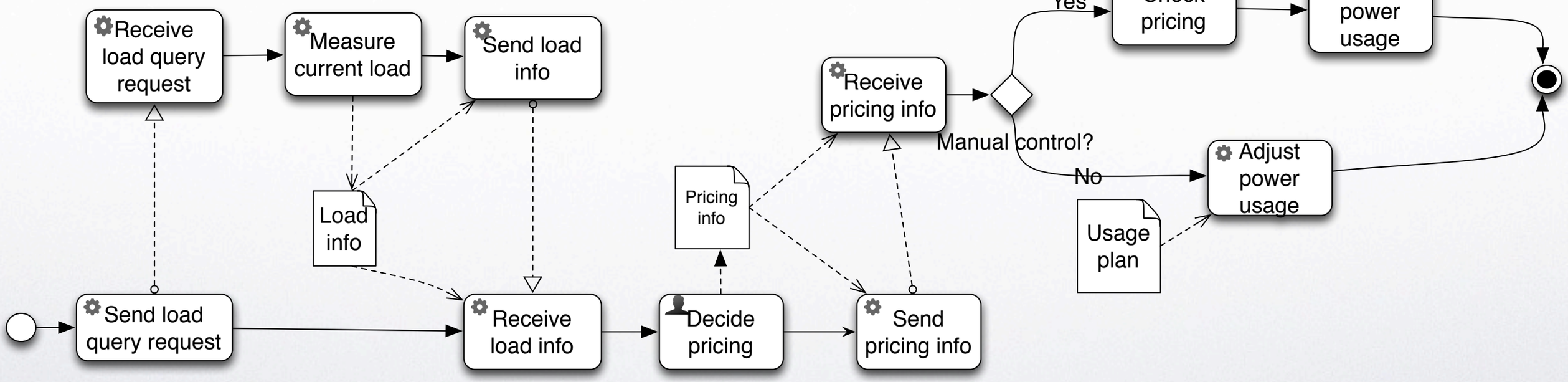


- System requirement model (R,SR)

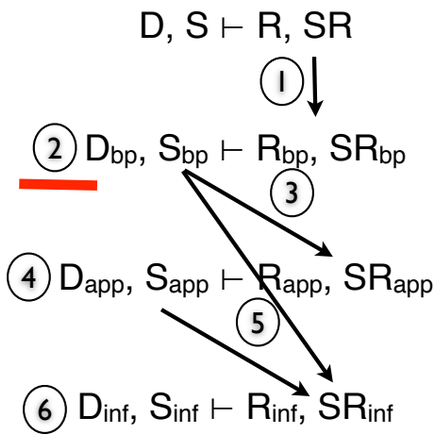


Illustration

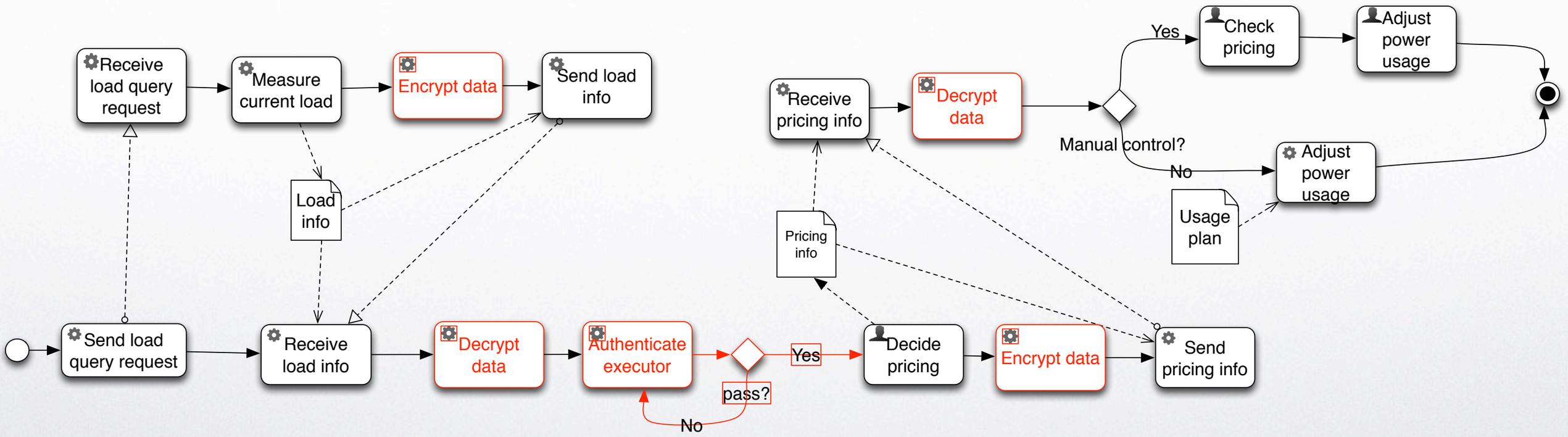
- Business process model ($D_{bp}, S_{bp} \vdash R_{bp}$)



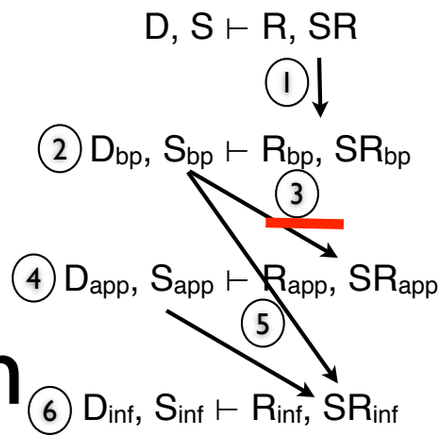
Illustration



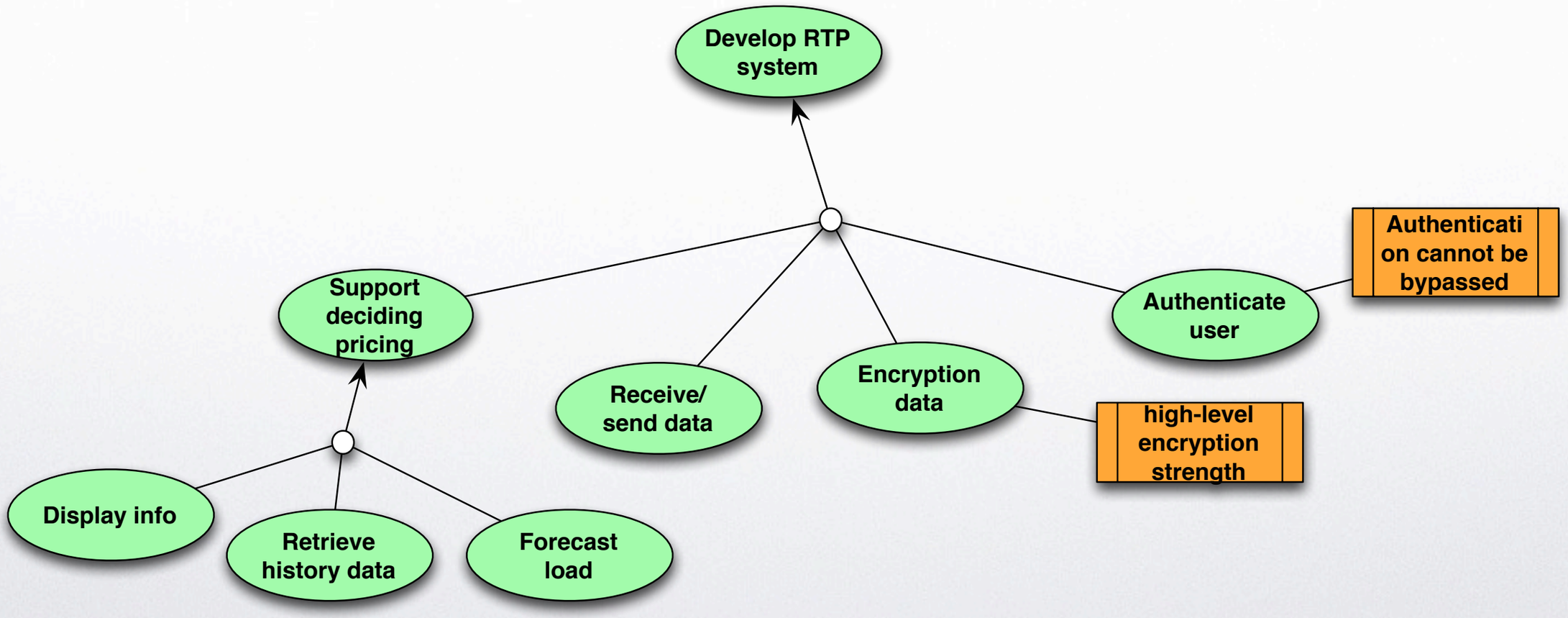
- Generate security solution for BP ($D_{bp}, S_{bp} \vdash R_{bp}, RS_{bp}$)



Illustration

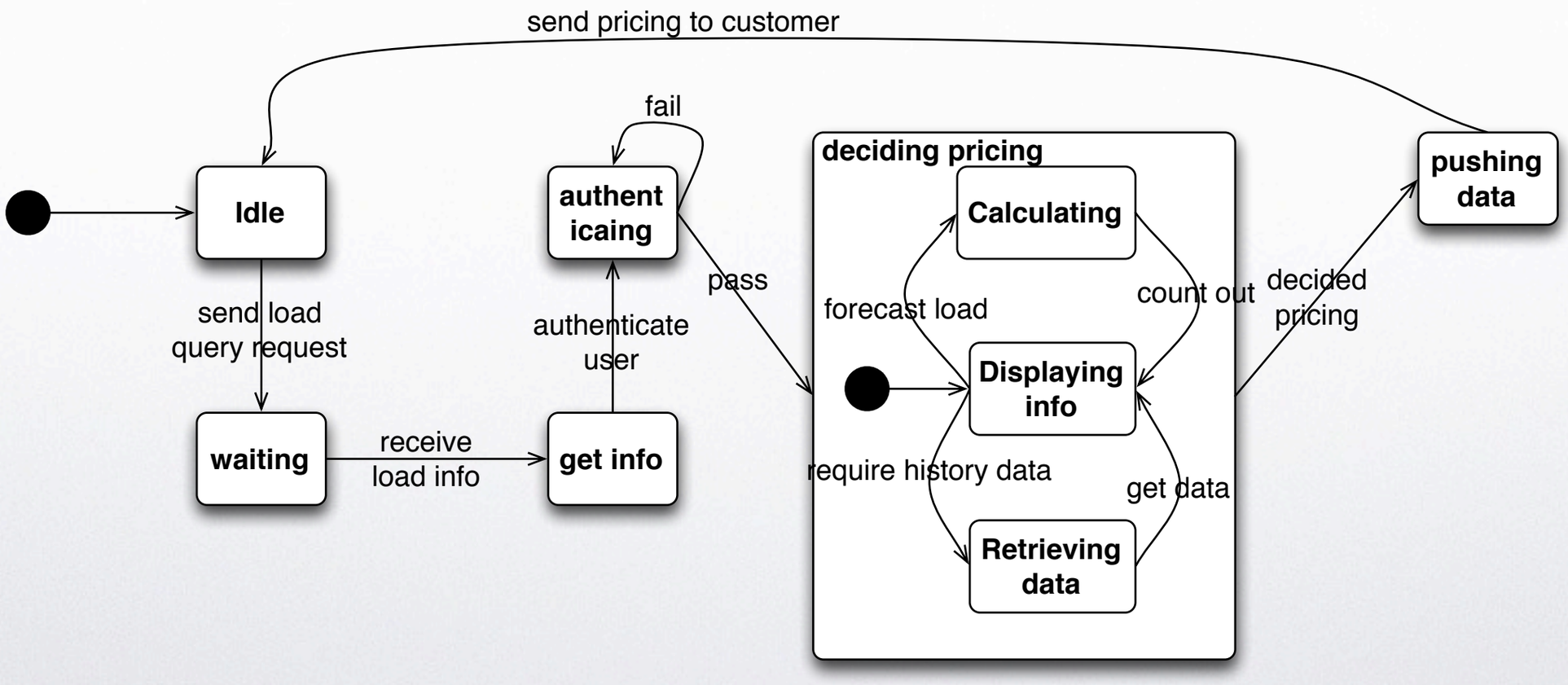


- Requirement goal model for application (R_{app}, RS_{app})

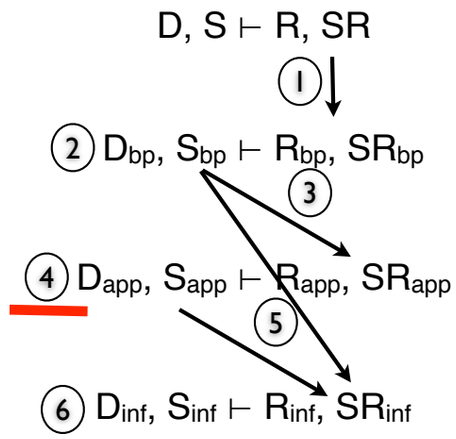


Illustration

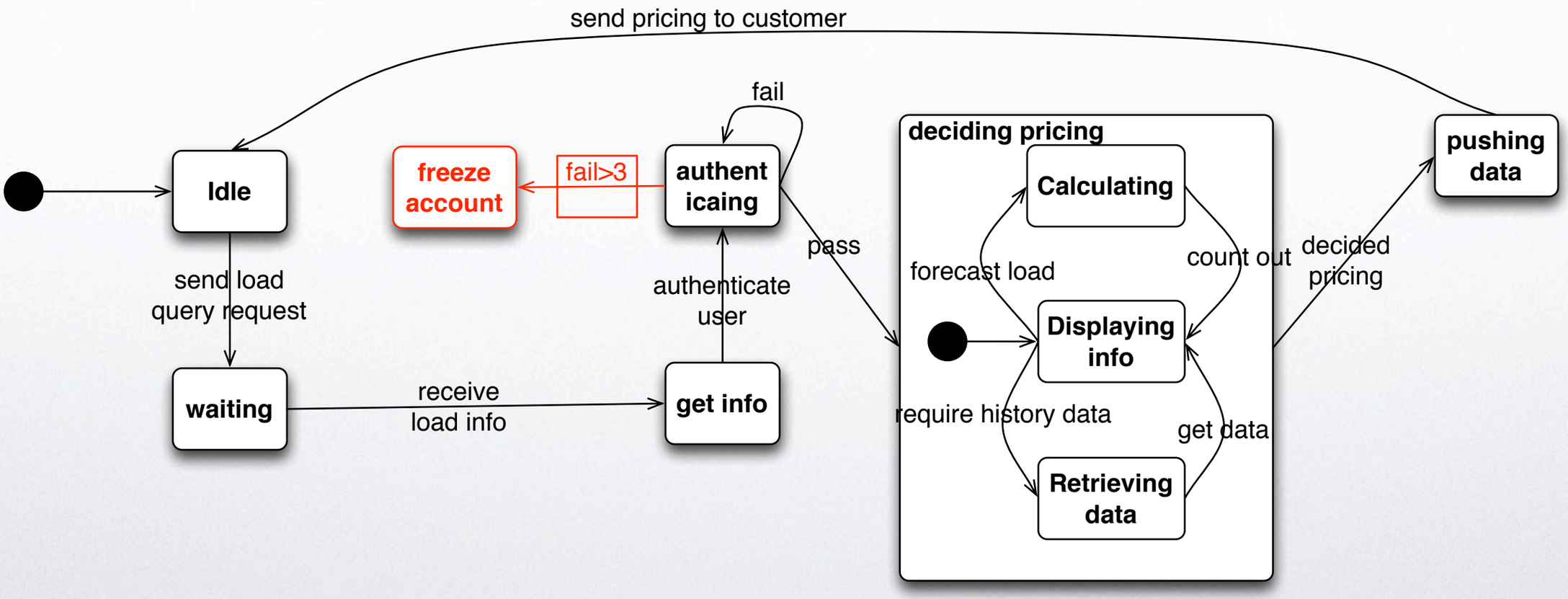
- Generate state diagram for application design ($D_{app}, S_{app} \vdash R_{app}$)



Illustration



- Generate state diagram for application design ($D_{app}, S_{app} \vdash R_{app}, RS_{app}$)



Research Steps

- Given a socio-technical system and a set of security requirements, design through a systematic process a security solution.
- Given a set of organizational objectives and security requirements, design a secure socio-technical system that fulfills organizational objectives and security requirements.
- Given a secure socio-technical system and some required changes, derive a new system that accommodates the changes, and continues to meet organizational objectives and security requirements.

Related work

- Misuse/abuse case, Abuse frame, Anti-goal
- i* based security analysis(Elahi, Liu, Mayer)
- UMLsec, SecureUML
- Secure Tropos (Mouratidis, Zannone)
- Kruchten, P. Architectural blueprints: The ”4+1” view model of software architecture.

Conclusion

- Security should be considered from multi-view to provide an all-round security solution.
- Design secure STS through multi-view, which consists of business process, application and infrastructure.

Thank you!

Questions?