A Refinement Planning Sheet

Shin NAKAJIMA
National Institute of Informatics
Tokyo, Japan

Talk Overview

- Backgrounds -- DSF
- Sketch before Event-B/RODIN
- A Refinement Planning Sheet
- Conclusions

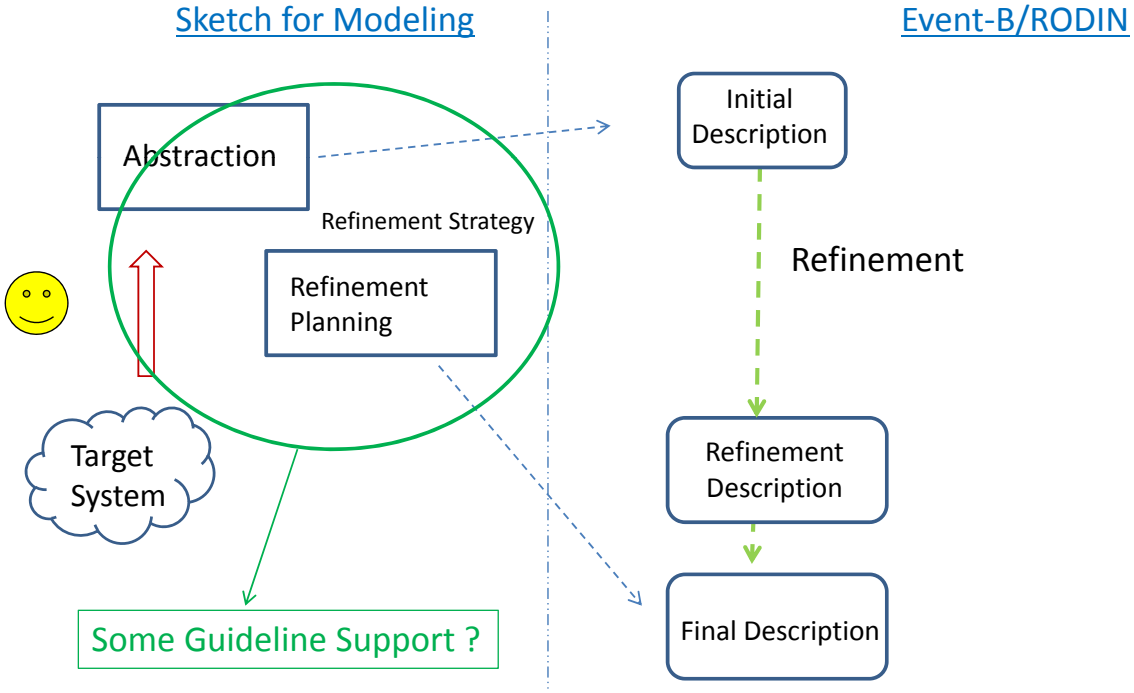
Backgrounds

- Dependable Software Forum (DSF)
  - Formed in December 2009 (until March 2012)
  - Members – major IT companies + academia
    - NTT-Data, Fujitsu, Hitachi, NEC , and Toshiba
    - National Institute of Informatics (NII) – Shin NAKAJIMA
  - Joint Research Group – collaboration of competitors
    - For use in early stages of Enterprise Software Development
    - Event-B, VDM++, and SPIN

Event-B in DSF

- A Series of Seminar on Event-B/RODIN
  - From May to July : 8 lectures with lab. work, 20 hours
  - About 20 engineers from 4 member companies
  - Lecturer – Hirokazu YATSU (an expert in formal methods)
- Some Findings
  - OK : Event-B descriptions (set-theoretic notation)
  - NG : Proof with RODIN -> further training needed
  - Essential Problem : Modeling (or Sketch before Event-B)
    (1) Identifying Events, (2) Refinement Planning

Sketch before Event-B/RODIN



Our Proposal

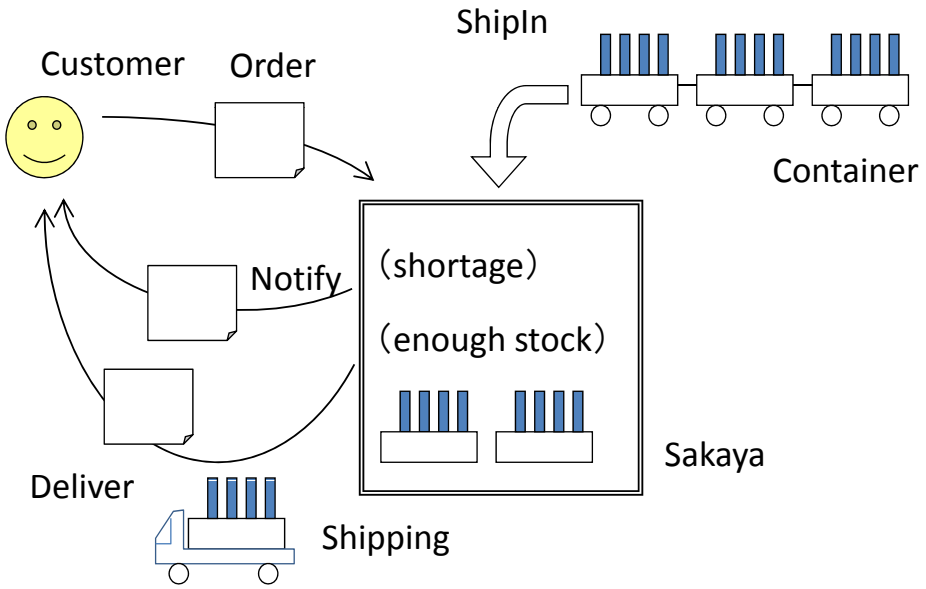
(1) Identifying Events

- Problem : How we find events in problem sketches
- Approach : Joint Action Diagram in Catalysis
- Reason : (familiar) Object-oriented Modeling

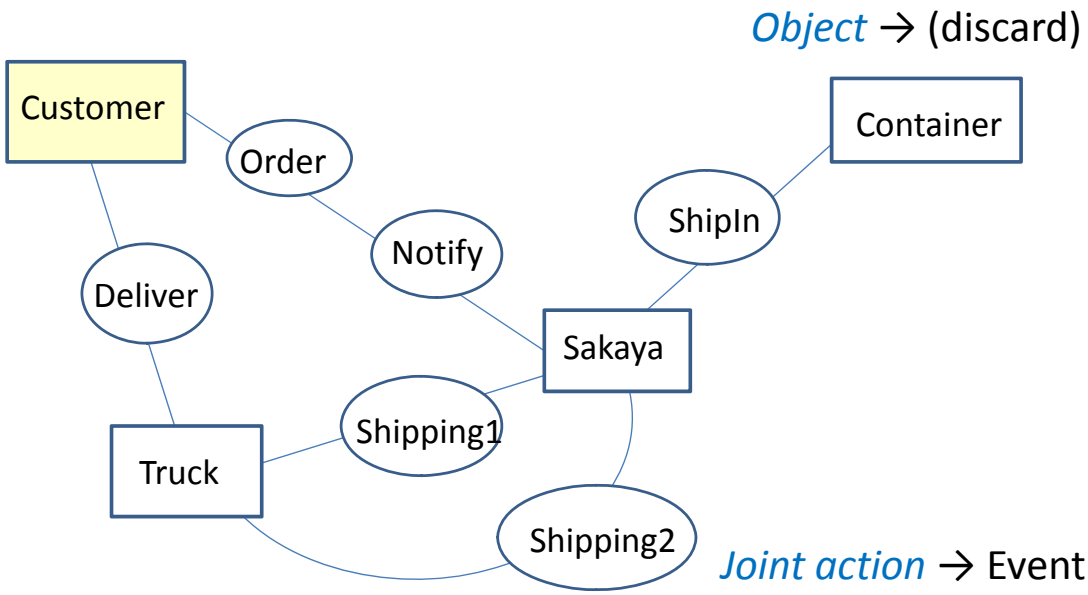
(2) Refinement Planning

- Problem : How we decide to conduct refinement
- Approach : Refinement Planning Sheet
- Reason : Birds-eye's view on the whole Refinement Process

Example: Sake Warehouse



Catalysis Joint Action



Second Problem

- Refinement Planning
  - In which order are events formally defined and proved?
  - No trial-and-error in refinement process
- Various Considerations
  - Initial Machine (Events) … easy to understand
  - Refinement Proof … automated as much as possible

Refinement Planning Sheet

Contexts Machines

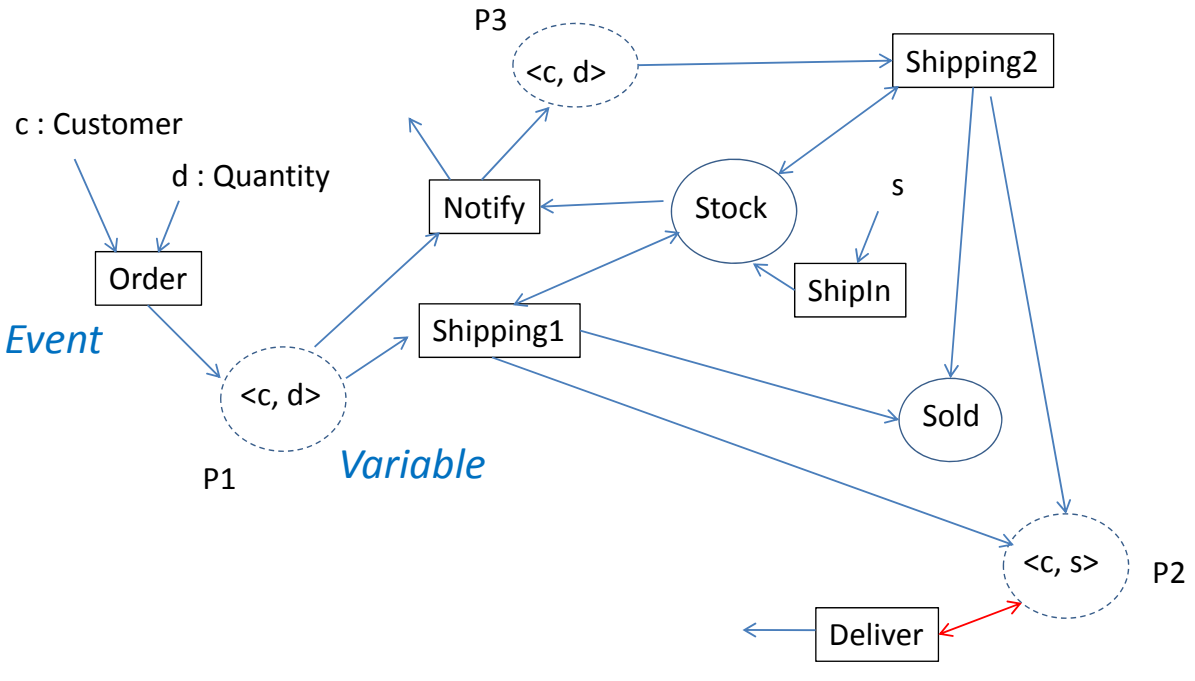
Step	Sets, Constants	Variables	Events
1	Sake S ⊆ Sake Customer Quantity	P ∈Customer x Quantity	Order ShipIn
2	NewSake	Stock ∪Sold ⊆S Stock ∩ Sold = {} P2 ∈Customer x Quantity	Order Shipping ShipIn Deliver
3		P1 ∈Customer x Quantity P3 ∈Customer x Quantity P1 ∪ P3 ⊆ P	Order Shipping1 Shipping2 Notify

Ready to Construct Event-B Descriptions using RODIN

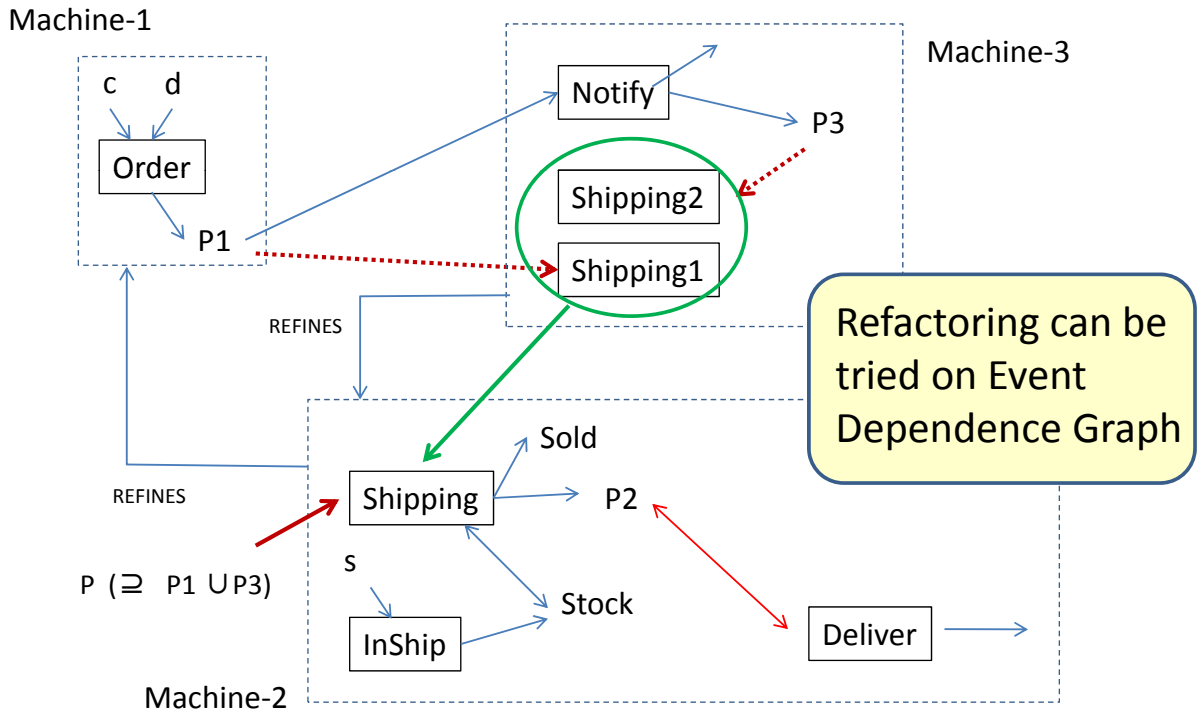
Bridge the Gap

- Gap
  - Joint Action → (candidate) Events
  - Refinement Planning → States, Event Dependency
- Auxiliary Sketches
  - Dataflow between States
  - Event Dependency Graph

Dataflow : Events and Variables



Event Dependence Graph



Final Sheet

Contexts | Machines

Step	Sets, Constants	Variables	Events
1	Sake S ⊆ Sake Customer Quantity	P ∈Customer x Quantity	Order ShipIn
2	NewSake	Stock ∪Sold ⊆S Stock ∩ Sold = {} P2 ∈Customer x Quantity	Order Shipping ShipIn Deliver
3		P1 ∈Customer x Quantity P3 ∈Customer x Quantity P1 ∪ P3 ⊆ P	Order Shipping1 Shipping2 Notify

A Possible Plug-in generates Event-B Skelton from Sheet

Conclusions

- Current Activities in DSF
  - Accumulating Idioms for writing Event-B descriptions
  - Making Guidelines including Refinement Planning Sheet
  - Web-site to make the activities public (November 2010)
- Next Step
  - Using Event-B in an Industrial Project planned in 2011

- Suggestions on DSF Project !!
- Future Collaboration !?