Formal Analysis of Risks in Business Processes

March 3rd, 2011
@Second Romanian-Japanese
Algebraic Specification Workshop

Shusaku Iida

Presentation plan

- ■ Backgrounds.
  - ✓ Risks in business processes.
  - ✓ What are the problems?
  - ✓ Goal of our project.
- ■ A formal model of business processes.
- ■ Analysis techniques.
- ■ Conclusion and future works.

Where are we now?

- Backgrounds.
    - ✓ Risks in business processes.
    - ✓ What are the problems?
    - ✓ Goal of our project.
- A formal spec of business processes.
- Analysis techniques.
- Conclusion and future works.

What is "business process"

- A business process is a set of activities in companies, public institutions, medical institution, and so on.
- These activities are partially ordered.
- Examples: whole sale, ticket reservation, security check, permission for business trip, and so on.

Business process modeling

- Designing a business process is called business process modeling.
- There are two important aspects:
  - ✓ (effectiveness) optimizing the business process, and
  - ✓ (safety) avoiding risks that are involved in it.

Risks and businesses

- A business can be observed as a translation from risks to a value.
- "Risk appetite" means how much risks are we willing to accept.
- More risks more gain. No risk no gain. This is basic rule for profit organizations.
- What should be avoided is an unintended risk.

Understanding risk

- If all the persons working in a company cannot be trusted then anything can happen.
- If you cannot trust anyone then you cannot do anything.
- What we can do is to decide how much and what kind of risks we can take.

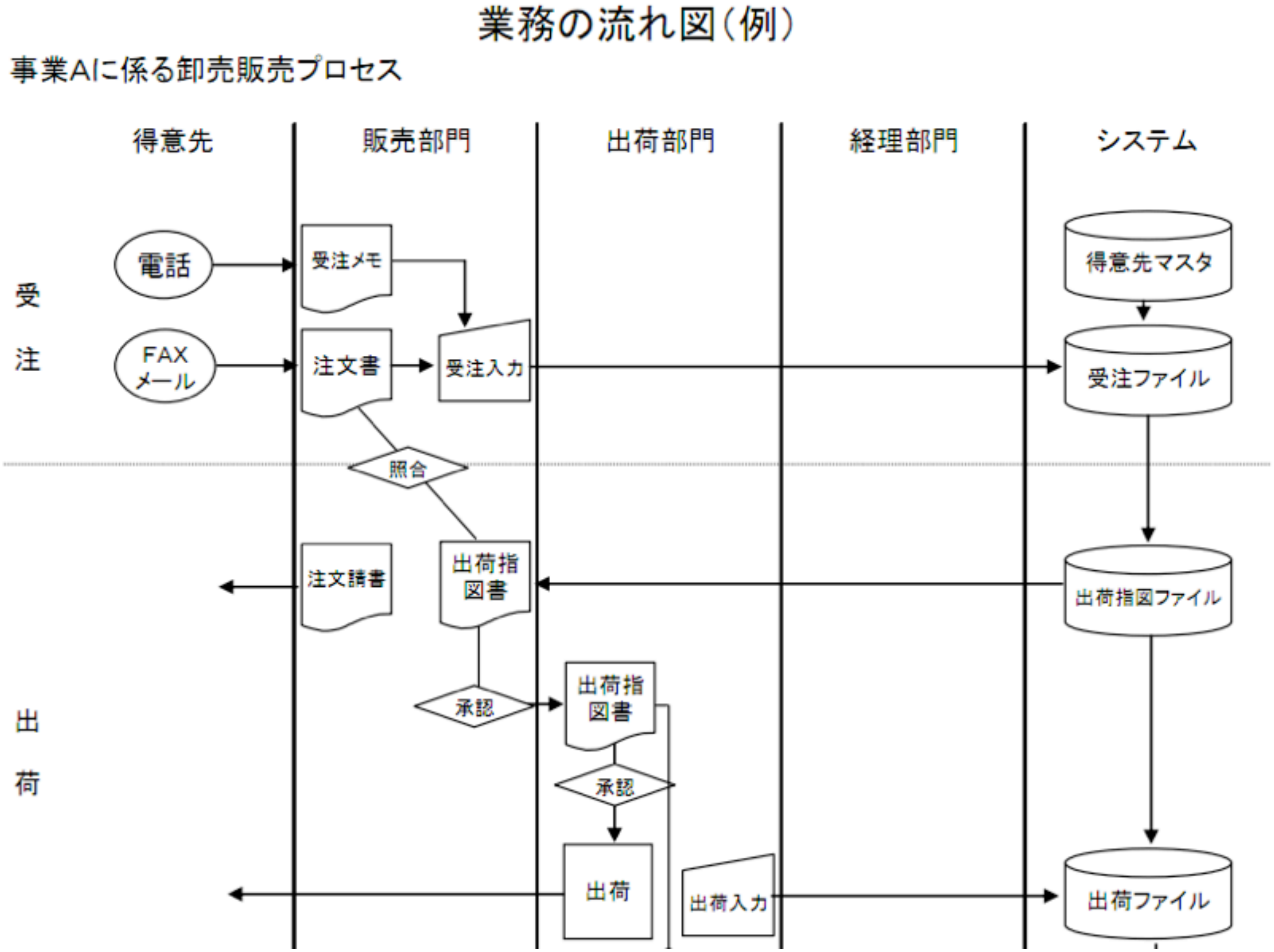
Disasters

- Sumitomo Corp. 1996.
  - ✓ Illegal copper trade by "Mr. Copper".
  - ✓ Sumitomo got 2.8 billion dollars damage.
- Countless numbers of such examples.
- Investors have much interest in safety aspect than before.
  - ✓ For example, SOX.

SOX

- Japanese version of SOX (Sarbanes-Oxley Act)
- All the public companies in Japan should follow.
- Requires several types of documents including flowchart like business process specifications.
- Based on these documents, public accountants express their opinions.

Business process spec.



- Financial Services Agency Japan.

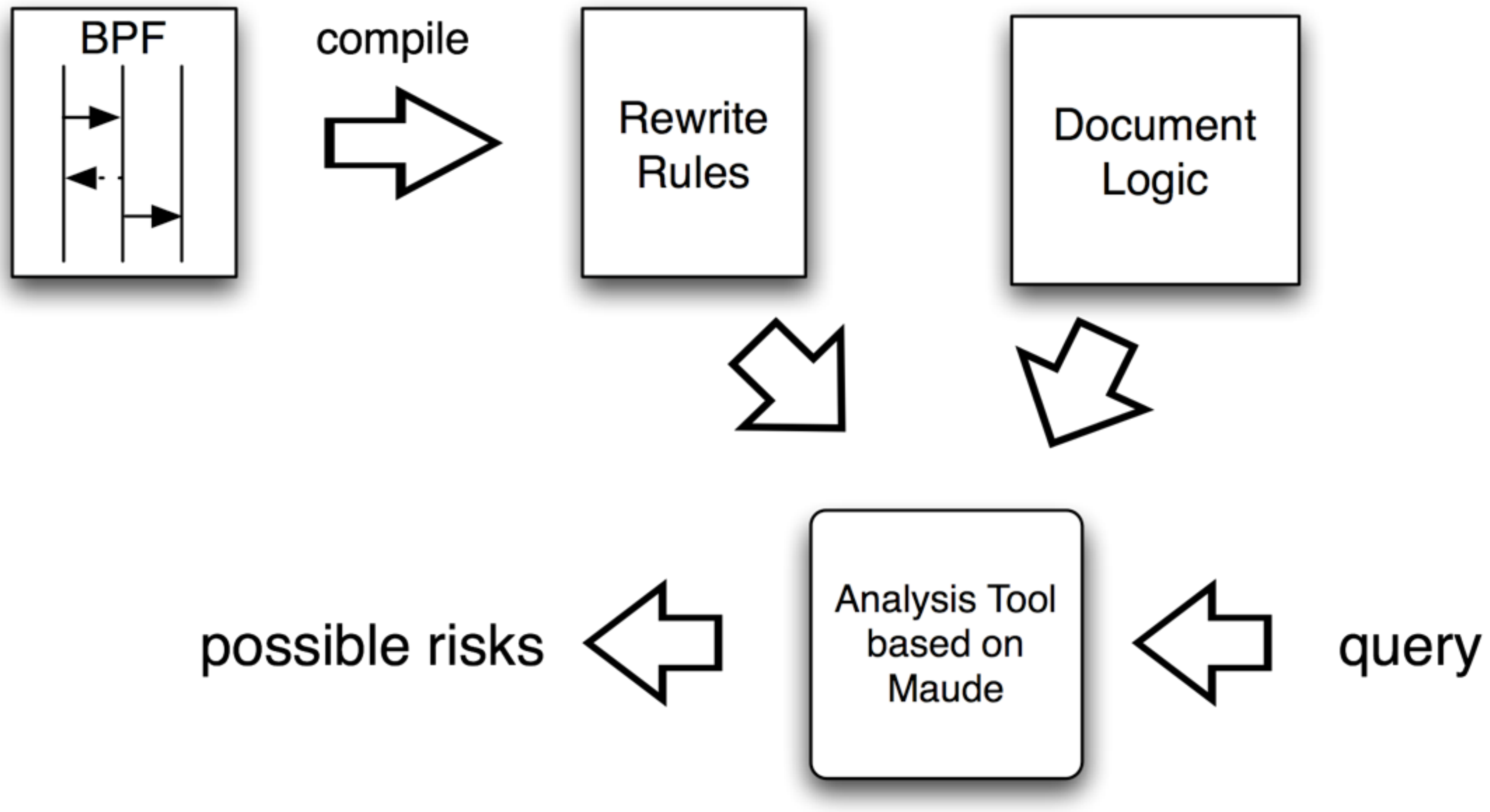
What are the problems?

- Some important information are missing.
  - ✓ What kind of risks they are going to take, and which are not.
- It is quite hard to find out a risk hiding in the business process.
- What does it mean “check” or “approve”?
  - ✓ They seems to be unspoken

World of business processes

- In many cases, several instances of a business process are running concurrently.
- However, this perspective is not commonly understood.
  - ✓ Almost no support tools consider this perspective.
- We define three perspectives:
  - ✓ micro view (considers only an instance of a BP),
  - ✓ macro view (considers several instances of a BP),
  - ✓ enterprise view (considers several instances of several BPs).

Goal


BPF
compile
Rewrite Rules
Document Logic
Analysis Tool based on Maude
possible risks
query

What we found

- We found a serious risk when we consider macro view for the example given by Financial Services Agency Japan.
- Even it seems to be OK when we only consider micro view.

- to be appear in Journal of Research and Practice in Information Technology.

Where are we now?

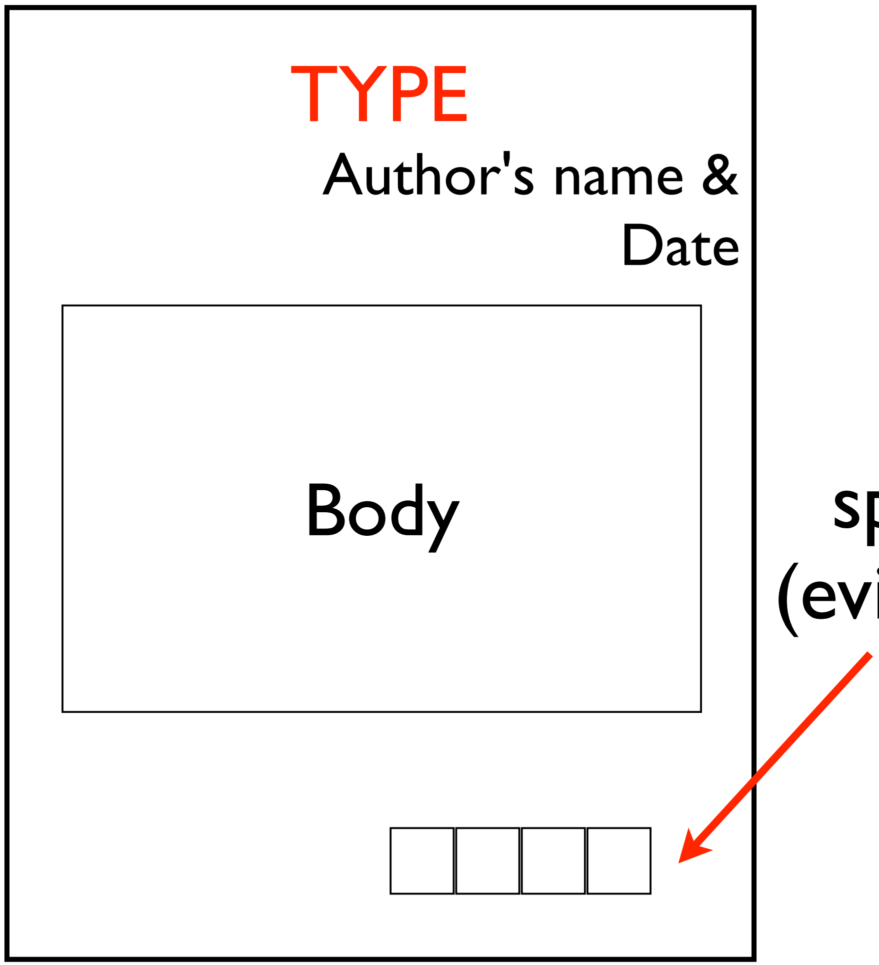
- Backgrounds.
  - ✓ Risks in business processes.
  - ✓ What are the problems?
  - ✓ Goal of our project.
- A formal spec of business processes.
- Analysis techniques.
- Conclusion and future works.

Document Logic

- We focus only on the flow of documents to formalize a business process.
- Documents can be created, sent, checked, approved, and forged.
- Document logic is a framework consists of:
  - ✓ data which are documents, divisions, and so on,
  - ✓ rules which define operations on documents such as create, sent, check, approve, and so on.

Business Documents

typical Japanese business documents



TYPE

Author's name & Date

Body

space for seals (evidence history)

Document

- A document has a type and an evidence history.
- An evidence history is a list of signatures or seals.

$$doc : DocType \times Bool \times SessionId \times EvidenceHistory \rightarrow Doc$$

- The second arity Bool is used to represent authenticity of the document (meta information).
- SessionID is used to identify the session in macro view.

Division

- A division is a location where activities taken place.
- A document's location is a pair of a document and a division which shows the location where the document currently is.

$$in : Doc \times Div \rightarrow DocLoc$$

- A cabinet is a set of document's locations.

Strand

- A message is one of the following types: I/O message, create message, check and approve message, and attacker message.
- A strand is a list of messages with a mark representing the current position.

$$\_[\_ \mid \_] : Div \times MsgList \times MsgList \to Strand$$

- A bar "|" is called the current position and it divides a message list into two: already invoked messages and to be invoked messages.

Trust

- We have to distinguish a undtrusted division from an trustful one.
- We restrict our analysis only to the cases which illegal activities are bounded with certain number. We call the number illegal activity bound.

State

- A state of a business process is a 4-tuple

$$(S, C, U, n)$$

where S is a set of strand, C is a cabinet, U is an untrusted division, n is illegal activity bounds.

Rules

- A business activity is represented as rewrite rule:

$$SP \rightarrow SP'$$

which *SP* and *SP’* are state patterns.

- A state pattern is a state which has variables in its representation.

Example

- If the next message of a strand is *check(t_1, t_2)* and we have both doc(t1, b, ...) and doc(t2, b, ...) are in the same division and both document's authenticity are the same, then the check will pass.

$$
\begin{aligned}
&((e[\ ML_1 \mid check(t_1,t_2)\,;ML_2\ ]\ S),\ (in(doc(t_1,b,i,H_1),v)\ in(doc(t_2,b,i,H_2),v)\ C)\ U,\ n)\\
\to&((e[\ ML_1\ ;check(t_1,t_2) \mid ML_2\ ]\ S),\ (in(doc(t_1,b,i,(ch(t_2)H_1)),e)\\
&(in(doc(t_2,b,i,H_2),e)\ C),\ U,\ n).
\end{aligned}
$$

Document Logic

- A document logic is a triple:

$$(\Sigma, A, R)$$

where $\sum$ is the set of function symbols, A consists of equations used only as equational attributes, R is a set of rules we define.

Attack

- We assume quite simple attacks:
- forging a document, and
- illegal use of a document:
  - ✓ using a document which doesn't belong to proper session, or
  - ✓ using a document when it shouldn't be used.
- An attack can be happen at anytime in anyplace except if it doesn't belongs to untrusted division.

Where are we now?

- ■ Backgrounds.
  - ✓ Risks in business processes.
  - ✓ What are the problems?
  - ✓ Goal of our project.
- ■ A formal spec of business processes.
- ■ Analysis techniques.
- ■ Conclusion and future works.

Situation

- An attacker is represented as a strand.
- We don’t know how many attackers are there.
- There are many kind of unintended risks.
  - ✓ Expertise know many of them but maybe not all of them.

Levels of Analysis

- Execution.
- Reachability analysis using forward execution.
- Reachability analysis using backward execution.

Forward Reachability Analysis

- We give an initial state and an unintended state and search all the reachable states from the initial state to see if we get to the unintended state.

Pros & Cons

- ■ Pros:
  - ✓ Less computational cost compare to backward reachability analysis.
- ■ Cons:
  - ✓ We have to specify a concrete initial state. But, how do we know that?

Backward Reachability Analysis

- Make the direction of all the rules other way round.
- We give a pattern of a final state and by using narrowing technique to see if it reaches to an initial state.

Pros & Cons

- Pros:
  - ✓ You don’t have to know about final states, for example, how many attackers are there.
- Cons:
  - ✓ Requires much computational power compare to forward reachability analysis. (How much is it? Well...)

Where are we now?

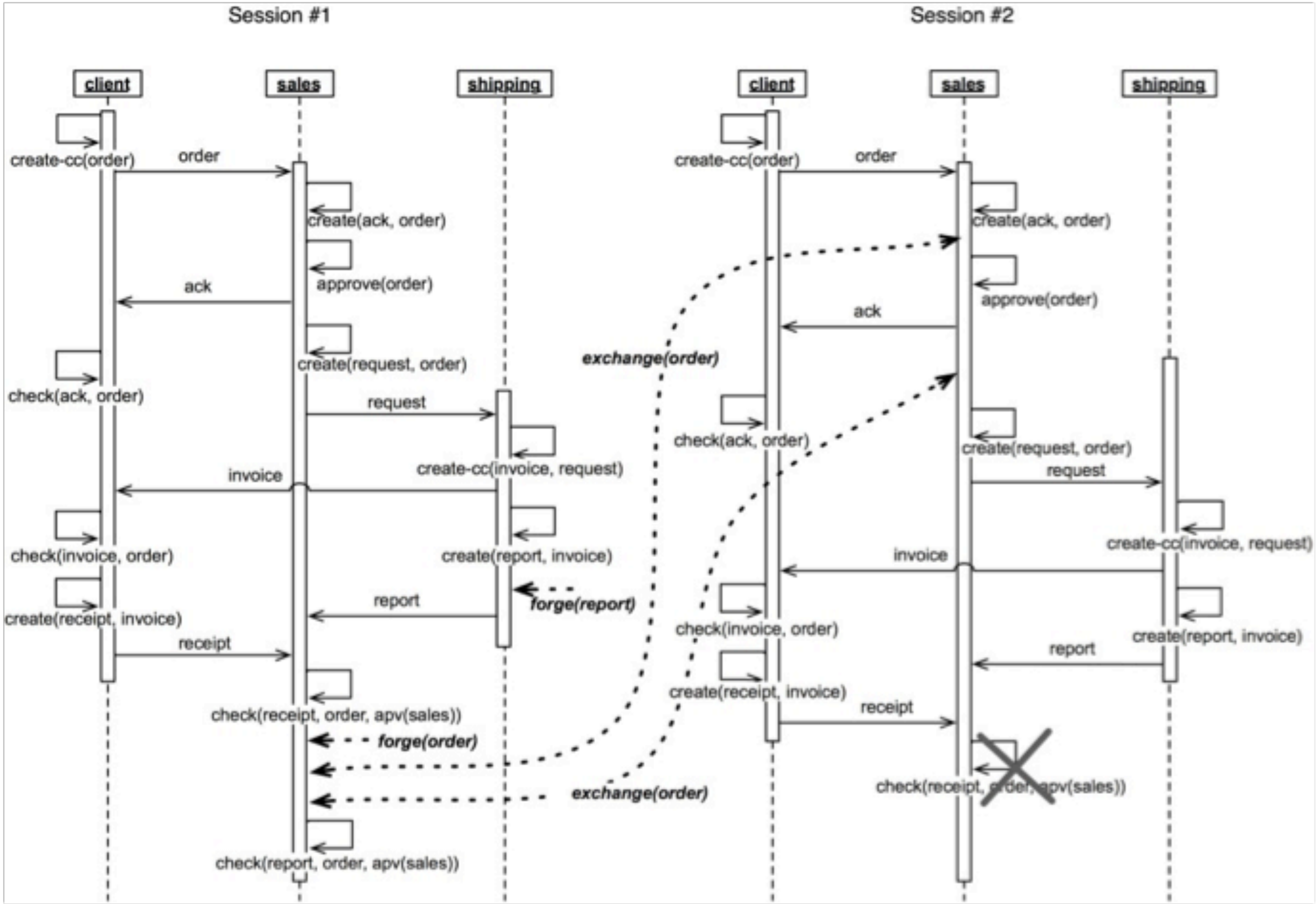
- Backgrounds.
  - ✓ Risks in business processes.
  - ✓ What are the problems?
  - ✓ Goal of our project.
- A formal spec of business processes.
- Analysis techniques.
- Conclusion and future works.

Example

- Using backward reachability analysis.
- “Is there a case for which the sales division finally has a forged report that is checked with order?”

$$in(doc(report, false, (ch(order)H)), sales)$$

- Other part of the state is just represented by variables.


Session #1
Session #2
client
sales
shipping
create-cc(order)
order
create(ack, order)
approve(order)
ack
create(request, order)
check(ack, order)
request
create-cc(invoice, request)
invoice
check(invoice, order)
create(report, invoice)
create(receipt, invoice)
report
forge(report)
receipt
check(receipt, order, apv(sales))
forge(order)
exchange(order)
check(report, order, apv(sales))
exchange(order)
client
sales
shipping
create-cc(order)
order
create(ack, order)
approve(order)
ack
check(ack, order)
create(request, order)
request
create-cc(invoice, request)
invoice
check(invoice, order)
create(report, invoice)
report
create(receipt, invoice)
receipt
check(receipt, order, apv(sales))

Discussions

- Although we adopt extremely simple model to formalize business processes, we still can learn something about business processes and risks.
- What we have done is analysis not verification. So, when we got a result, we always go back to the real world and check if it looks OK.
- Can we verify that there is no unintended risk by CafeOBJ?

Conclusion

- If we want to discuss about risks in business, we have to know the true characters of risks.
- Without a precise definition of business processes and risks, it is quite difficult.
- Operations like check and approve have different meanings in organization to organization.
  - ✓ This means we are using the same words to talk each other with the different meaning.

Conclusion

- It is important to clarify how we can deal with such a fragile world.
- We have to know that not only critical software systems are facing a crisis, but also, many social fundamentals like companies, medical services, laws, and so on, are facing a crisis.
- Domain analysis is an important area.

Future works