Questions on refinement and security analysis

December 2, 2005

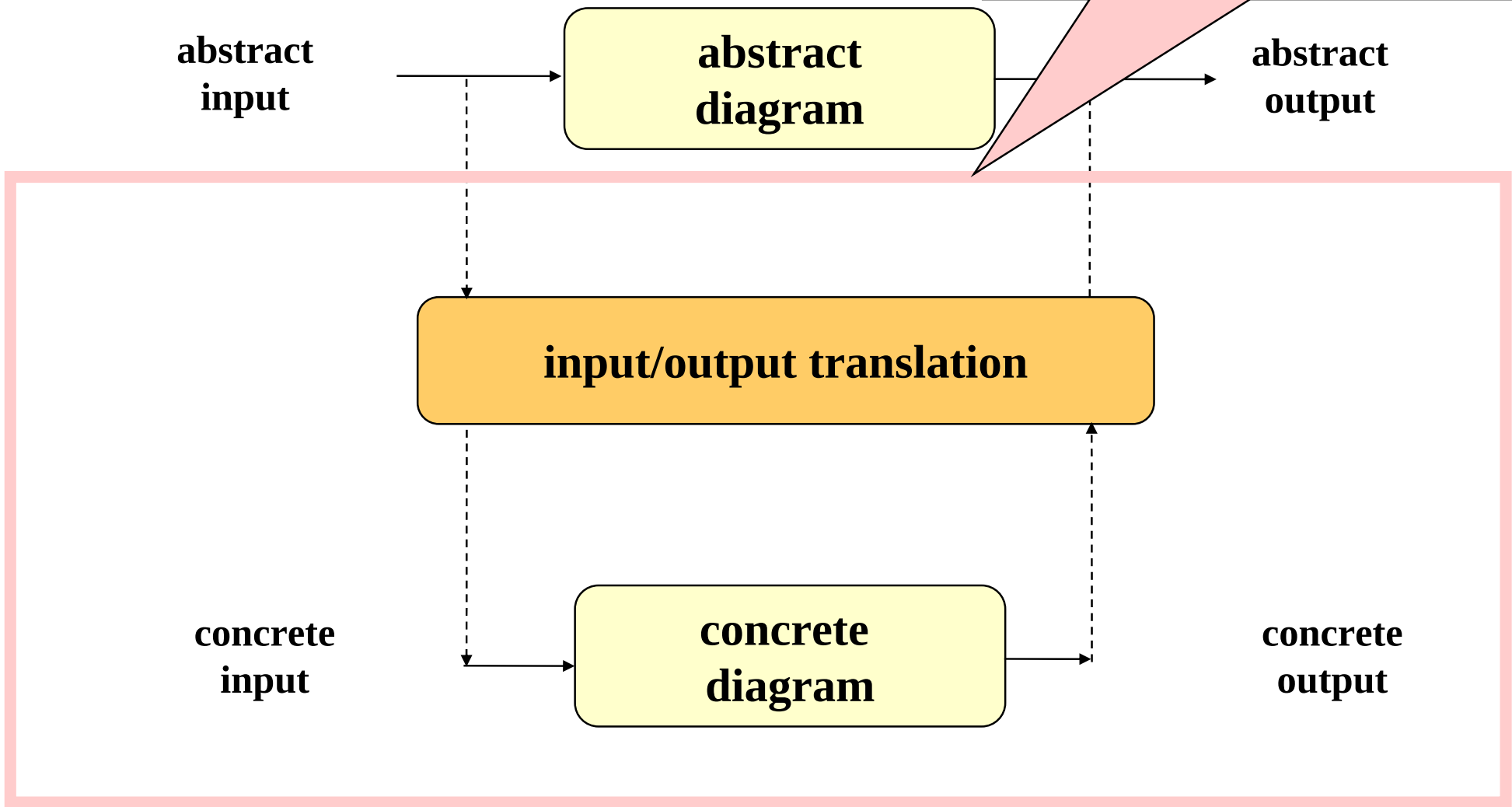
Øystein Haugen **Ketil Stølen**

Refinement: Summary of questions

- How to prove property refinement?
  - inconclusive traces
  - negative traces
  - new example
  - supplementing and narrowing by drawing sequence diagram
- Difference between alt and xalt
- Summary of the advanced forms
- Refinement of sequence diagrams by state machines

Interface refinement

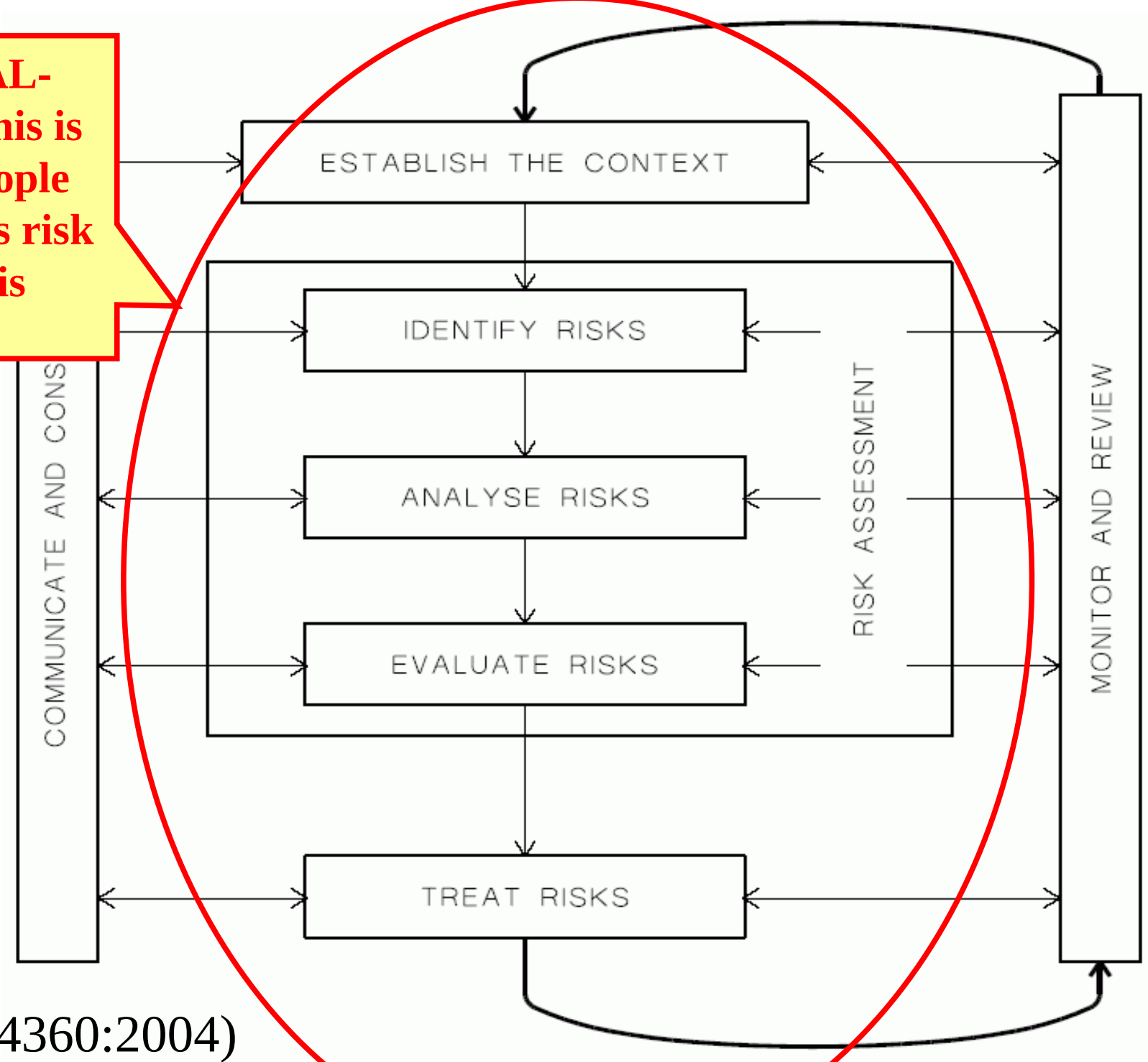
Requirement: Composition of concrete diagram and translation is a property refinement of abstract diagram



Security Analysis: Summary of Questions

- Explain the different elements
- What should we focus on in particular?
- Why is risk analysis useful?
- What characterises a weak analysis (antipatterns)?

In REAL-LIFE: This is what people refer to as risk anaysis



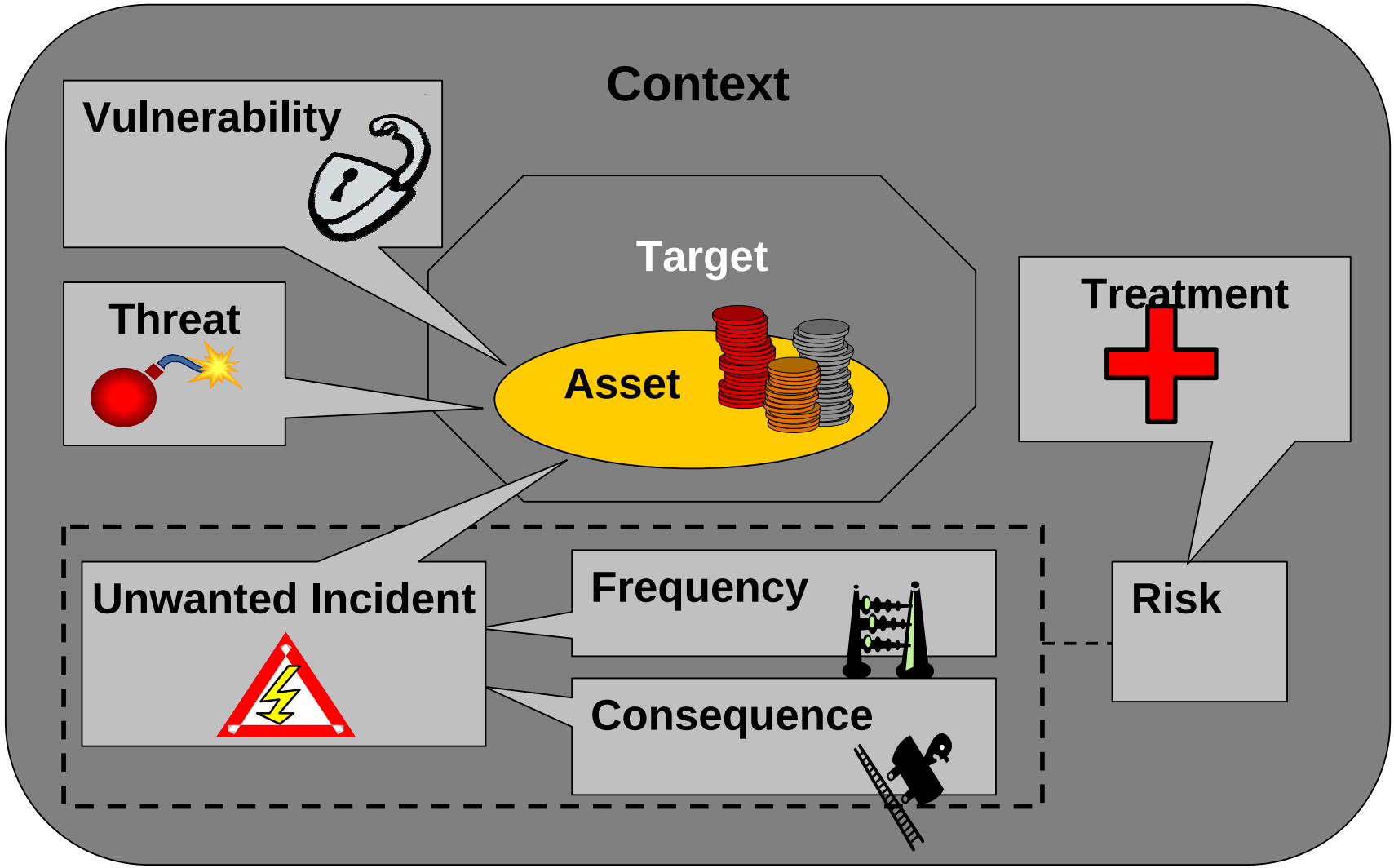
(AS/NZS 4360:2004)

Defensive versus operational

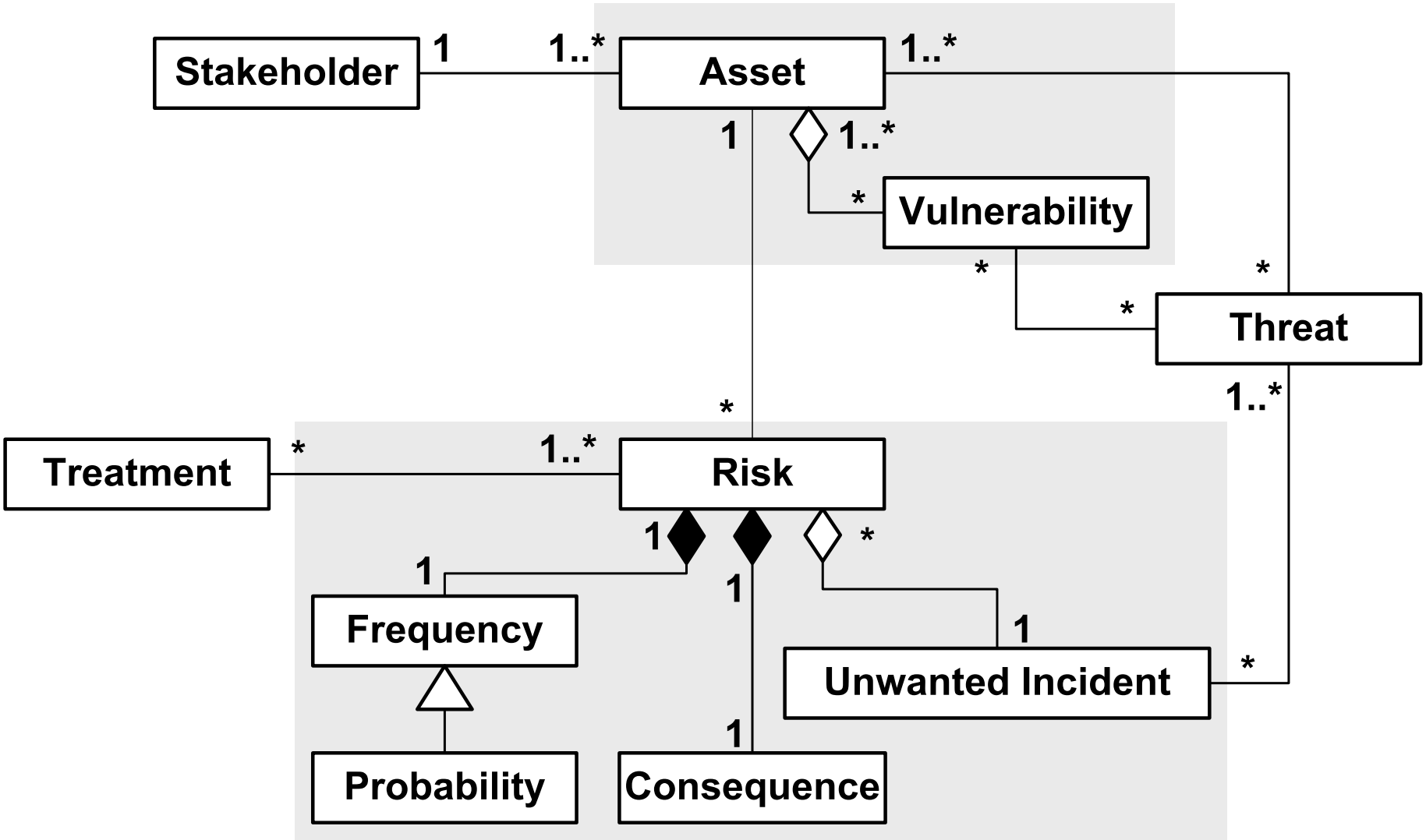
- **Defensive risk analysis – focus on defending the value of existing assets**
  - **Security**
  - **Safety**
  - **Reliability**

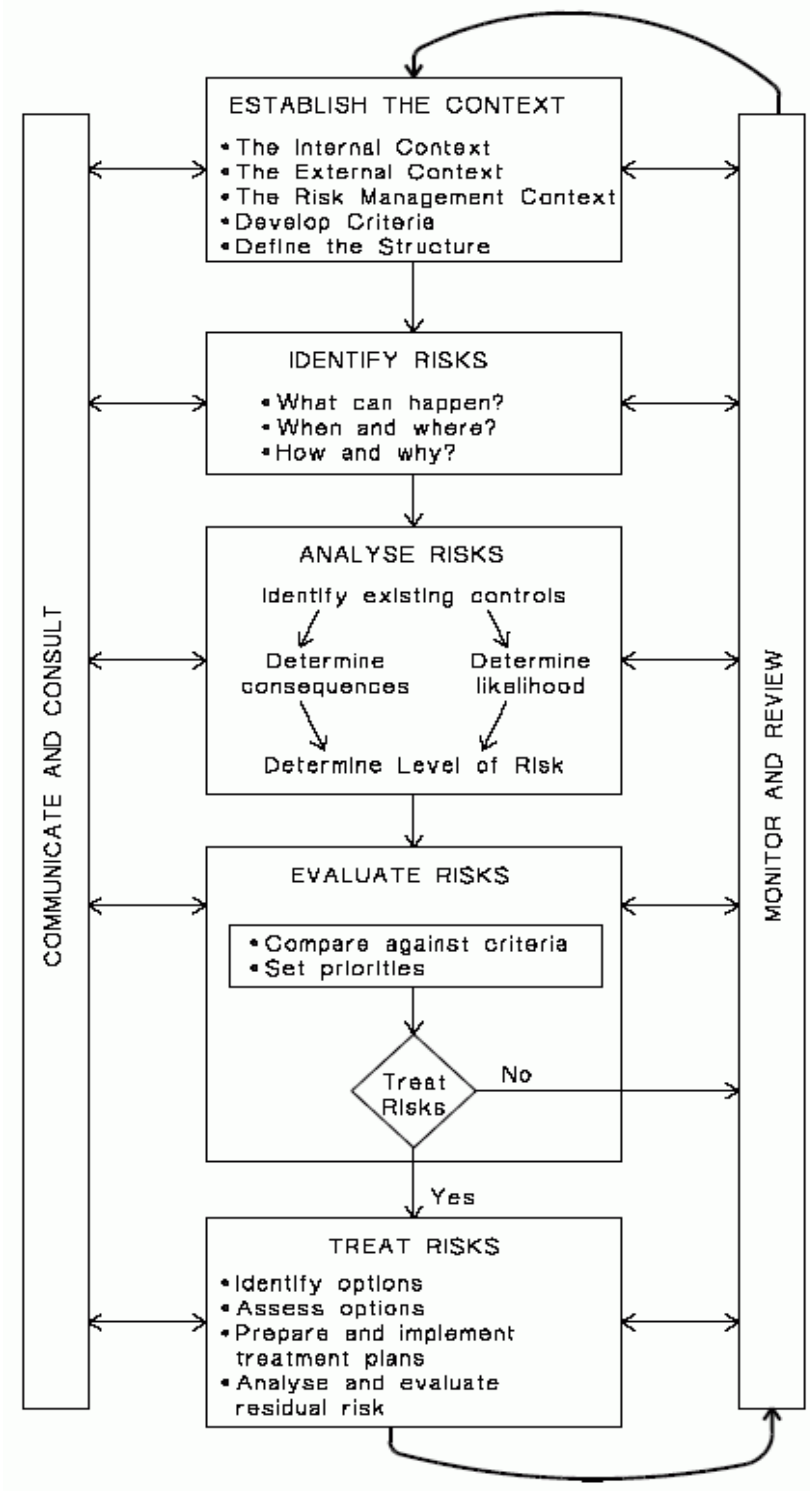
- **Operational risk analysis – focus on developing new assets or increasing the valuse of existing assets**
  - **Earn money on the stock exchange**
  - **Gambling**

Elements of a risk analysis



Conceptual model for risk analysis





(AS/NZS 4360:2004)

Øystein Haugen **Ketil Stølen**

CORAS Modelling: Summary of Questions

- The CORAS style versus the style in the questionaires
- Example of threat scenarios

Fault Trees: Summary of Questions

- Are fault trees important?
- How to use fault trees to calculate probability?
- Fault tree from risk analysis in Drop 2

Quantitative frequency estimation for fault trees

- A minimal cut set is a minimal set of basic events that are sufficient to cause the root event happening
- The minimal cut sets for the fault tree to the right are {1}, {2,5}, {2,3,4}
- If all events are independent then the probability of a least cut set is equal to the product of the probabilities for its basic events
- For a fault tree with n minimal cut sets with probabilities p_1, p_2, … p_n the probability for the root event is:

$$1-((1-p_1)*(1-p_2)*\ldots*(1-p_n))$$