Threat modeling and fault tree analysis

November 18, 2005

Øystein Haugen **Ketil Stølen**

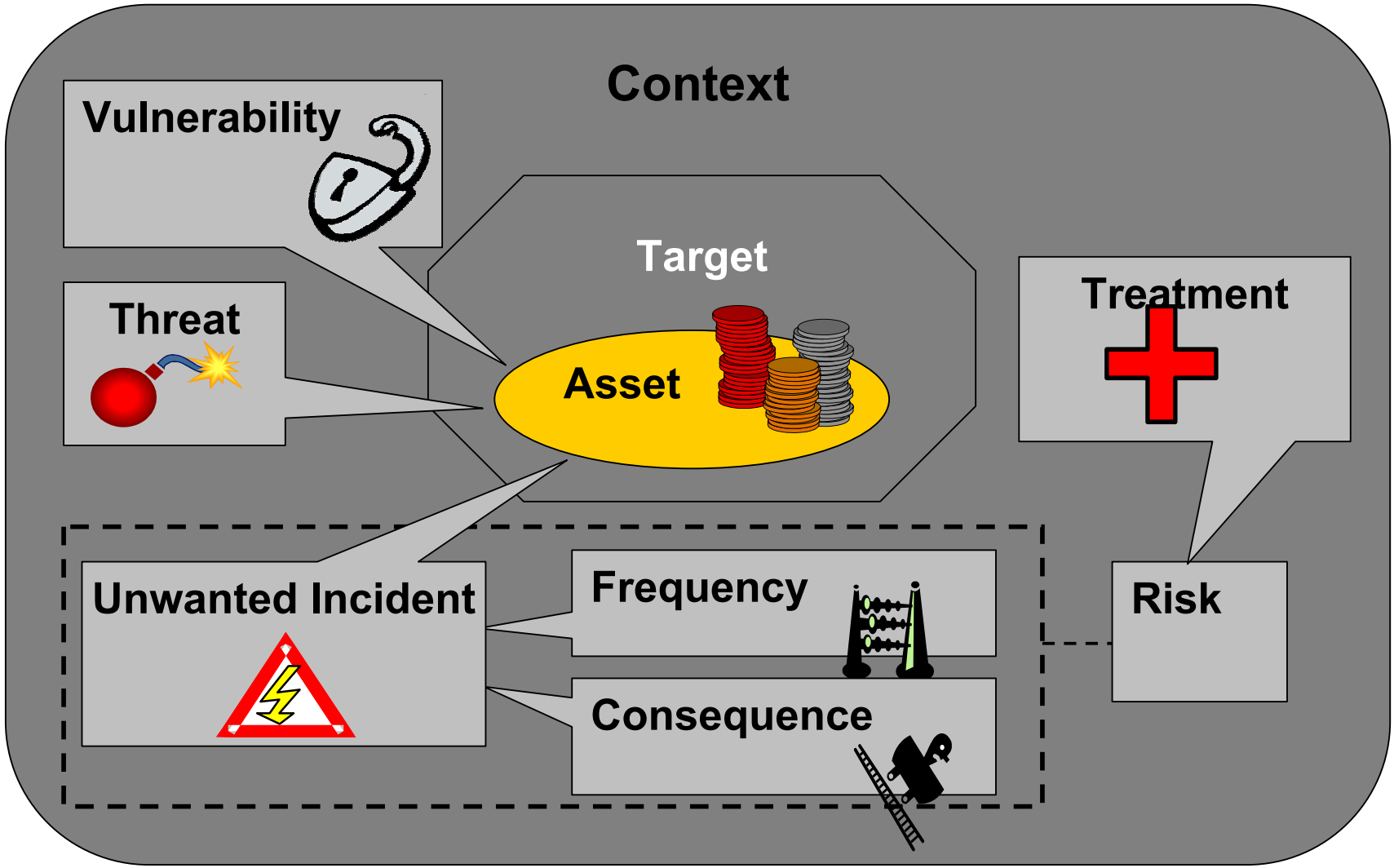
PART I:

Threat Modeling

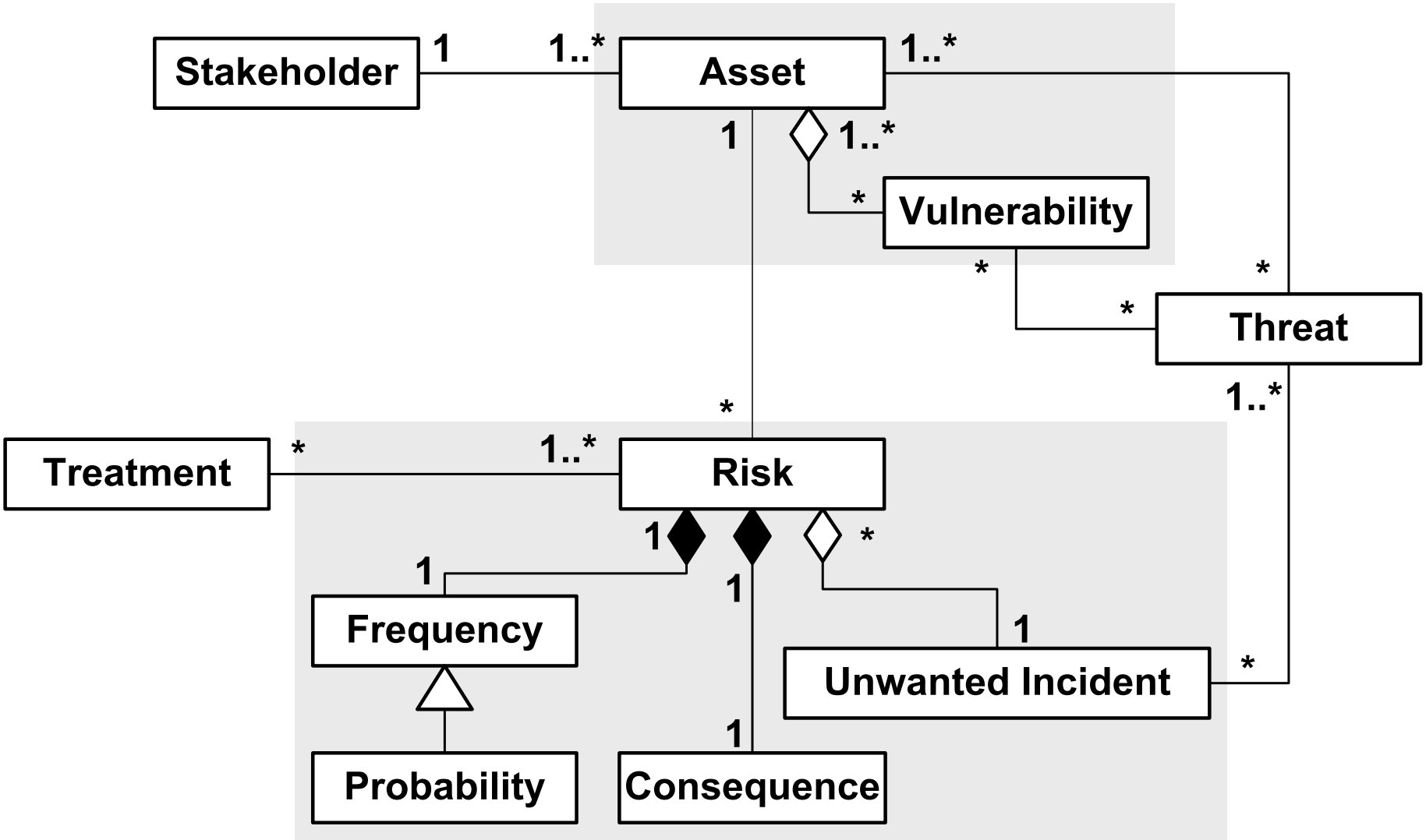
Exercise in the CORAS language

- The exercise is about the threat modeling using the CORAS threat modeling language
- This first part addresses common modeling tasks during a risk analysis
- The second part considers various ways of modeling the same situation and your task is to prioritize between them and choose the way you think is best!

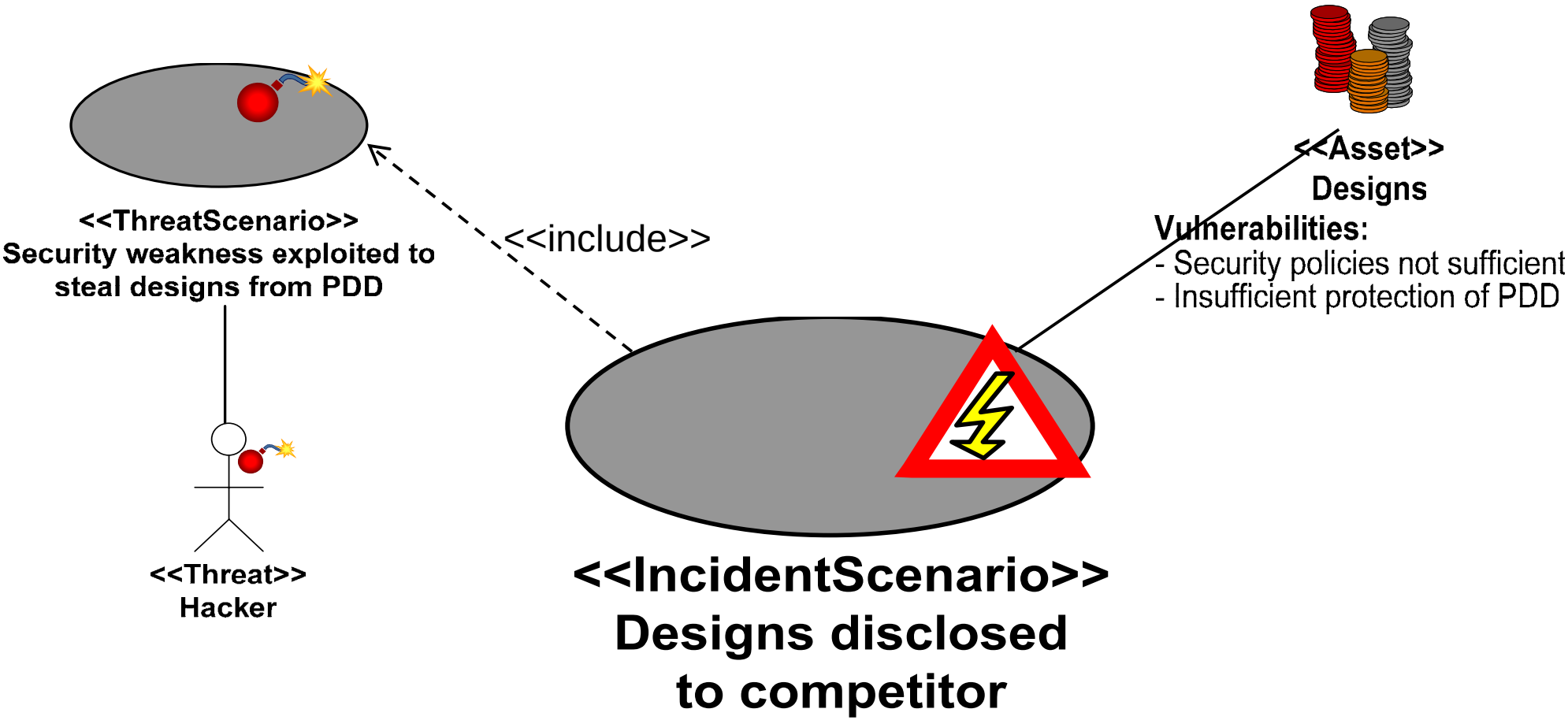
Elements of risk analysis



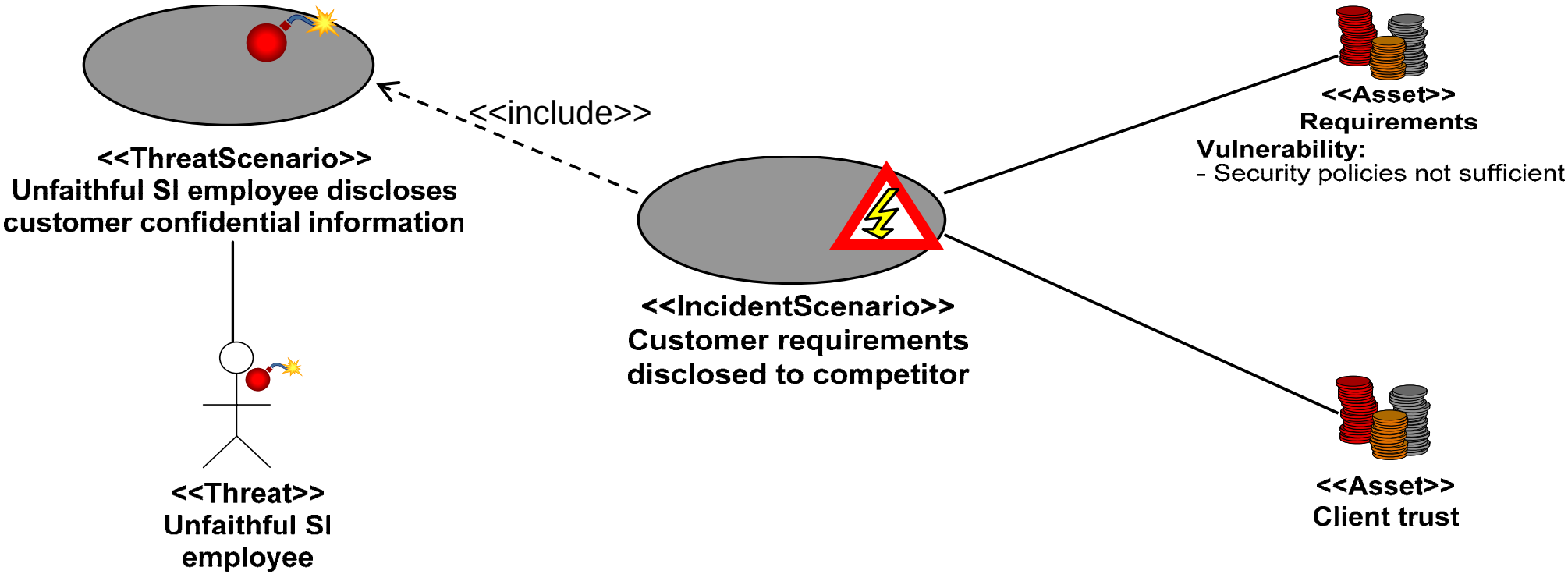
Conceptual model for risk analysis



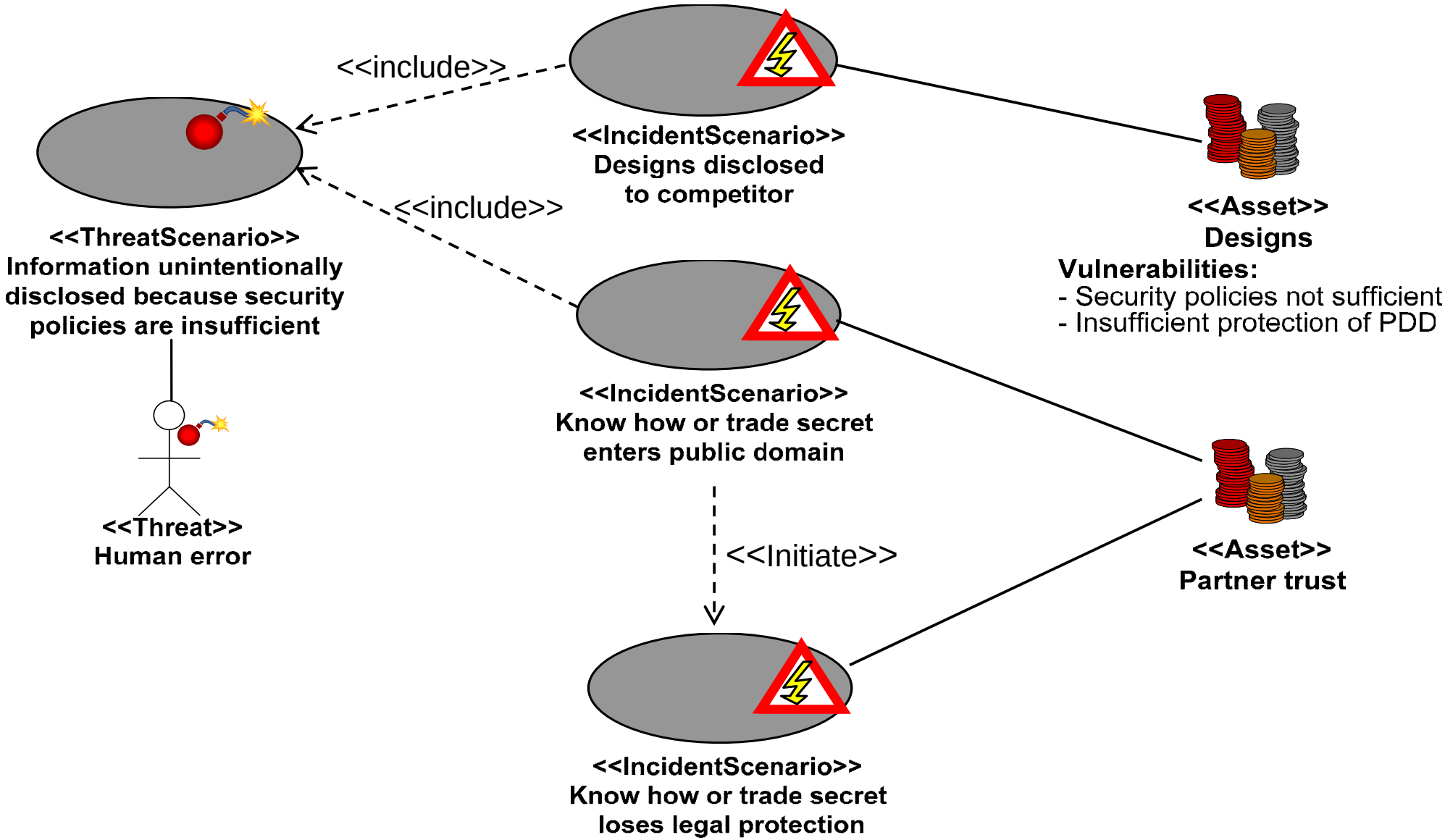
Threat modeling



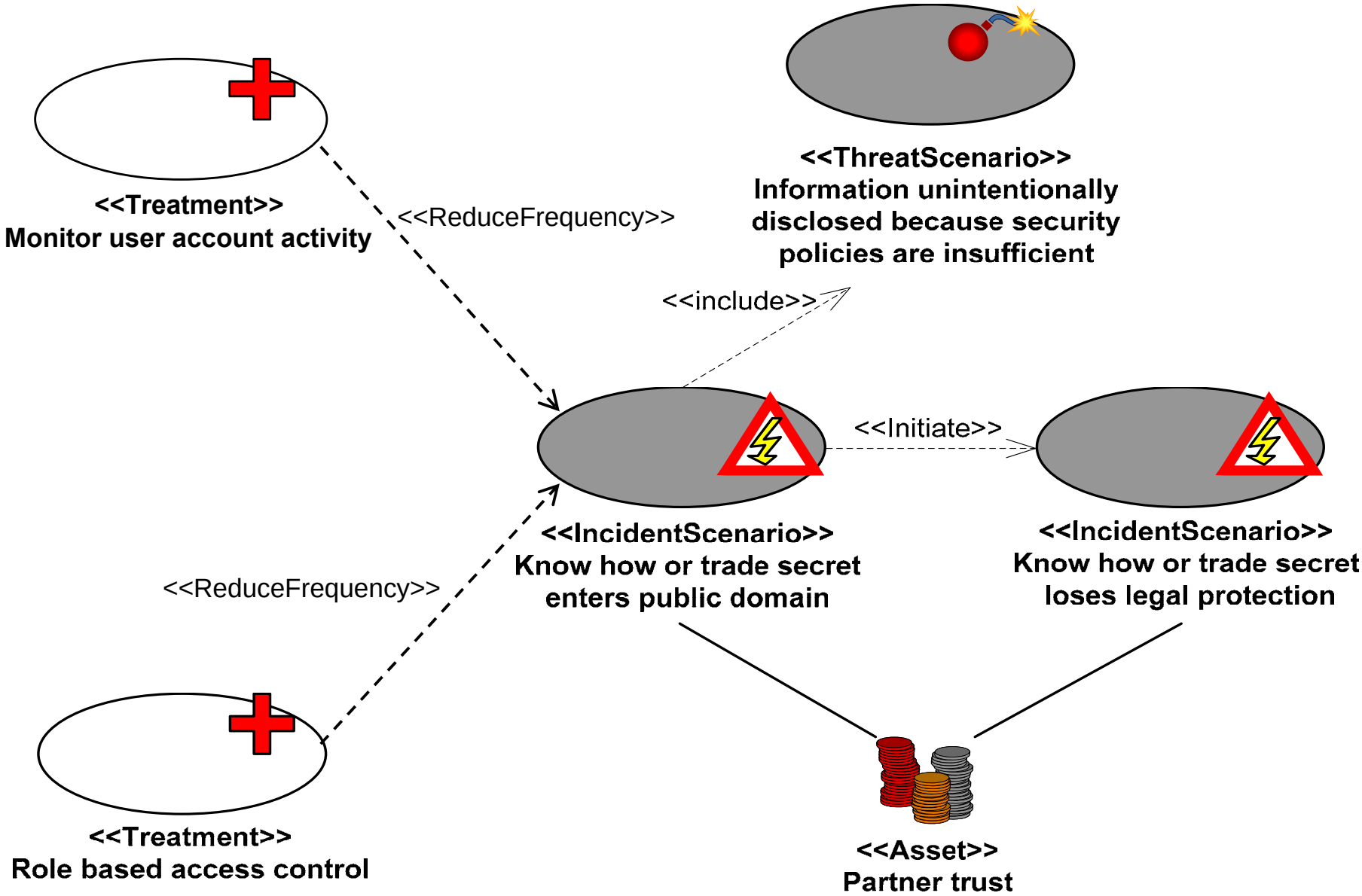
Threat modeling



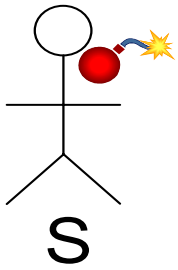
Threat modeling



Treatment

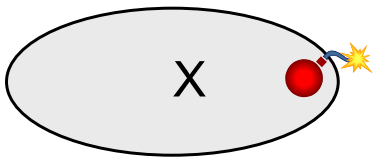

<<Treatment>>
Monitor user account activity
<<ReduceFrequency>>
<<ThreatScenario>>
Information unintentionally disclosed because security policies are insufficient
<<include>>
<<Initiate>>
<<IncidentScenario>>
Know how or trade secret enters public domain
<<IncidentScenario>>
Know how or trade secret loses legal protection
<<ReduceFrequency>>
<<Treatment>>
Role based access control
<<Asset>>
Partner trust

Threat, vulnerability and threat scenario



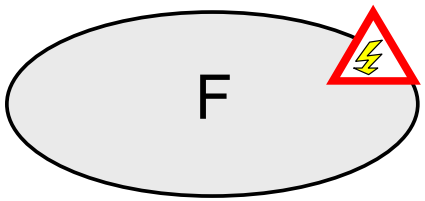
- **Threat: someone/something that intentionally or non-intentionally can cause an event that may harm an asset**

- **Vulnerability: a weakness or a lack that a threat can exploit**

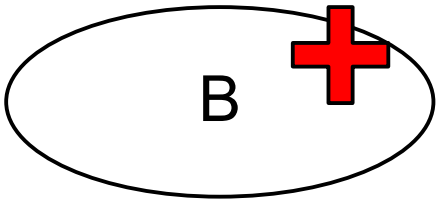


- **Threat scenario: sequence of events corresponding to a threat exploiting vulnerabilities**

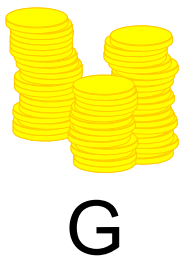
Incident scenario, treatment and asset



- **Incident scenario: sequence of events leading to an unwanted incident**



- **Treatment scenario: a description of the actions made to reduce a risk**



- **Asset: something of value which needs to be protected.**

Exercise in the CORAS language

- Useful for you, for me and for further research
- We will present the correct answers later in the lecture
- Filled in forms will be copied and handed back during the lecture
- Furthermore:
  - This is anonymous
  - You have to remember your number to get your form back
  - IMPORTANT TO GUESS IF YOU DON'T KNOW THE ANSWER

- NOTE: The pointed arrow should be understood as "<<initiate>>"

- You have 20 minutes to complete the form!

PART II:

Fault Tree Analysis (FTA)

Assigning risk values

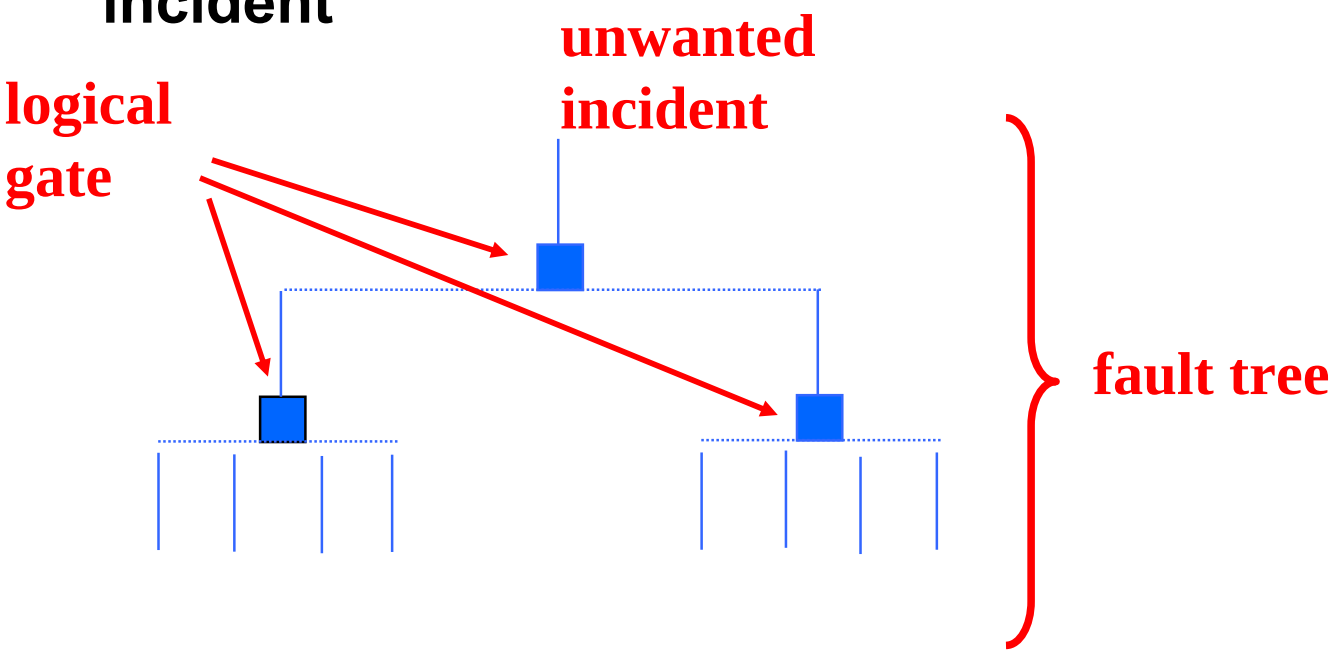
- Objective: Assign risk values to unwanted incidents
- The risk value is a function of consequence and frequency
  - Frequency: how often the identified incident is expected to occur
  - Consequence: the loss of value the unwanted incident may cause for a given asset each time it occurs
- The risk value is used later in the process to
  - Decide whether a risk needs to be treated
  - Prioritize risks
  - Choose treatment strategy

Frequency analysis

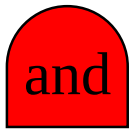
- Objective: To analyze and evaluate the frequency of an unwanted incident
- The frequency we are interested in will typically be at the enterprise level
- This frequency is often determined from frequencies at a lower level — e.g., technical level
- Frequency may be measured quantitatively or qualitatively
- Frequency is estimated from
  - historical data
  - simulations
  - expert judgments
- Fault tree analysis is a usual technique for estimating frequencies

Fault tree analysis

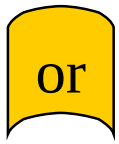
- When we have identified an unwanted incident we would like to know under what circumstances and with what frequency it may occur
- A fault tree analysis is a means to identify circumstances causing an unwanted incident



The elements of a fault tree

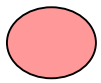


AND gate: all input events required to cause the output event

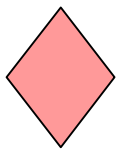


OR gate: one input event is sufficient to cause the output event

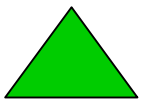
event: output from a logical gate



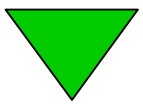
basic event: event that is not decomposed further



unfinished event: event that has not been traced back to its cause; taken as input but its cause may be unknown



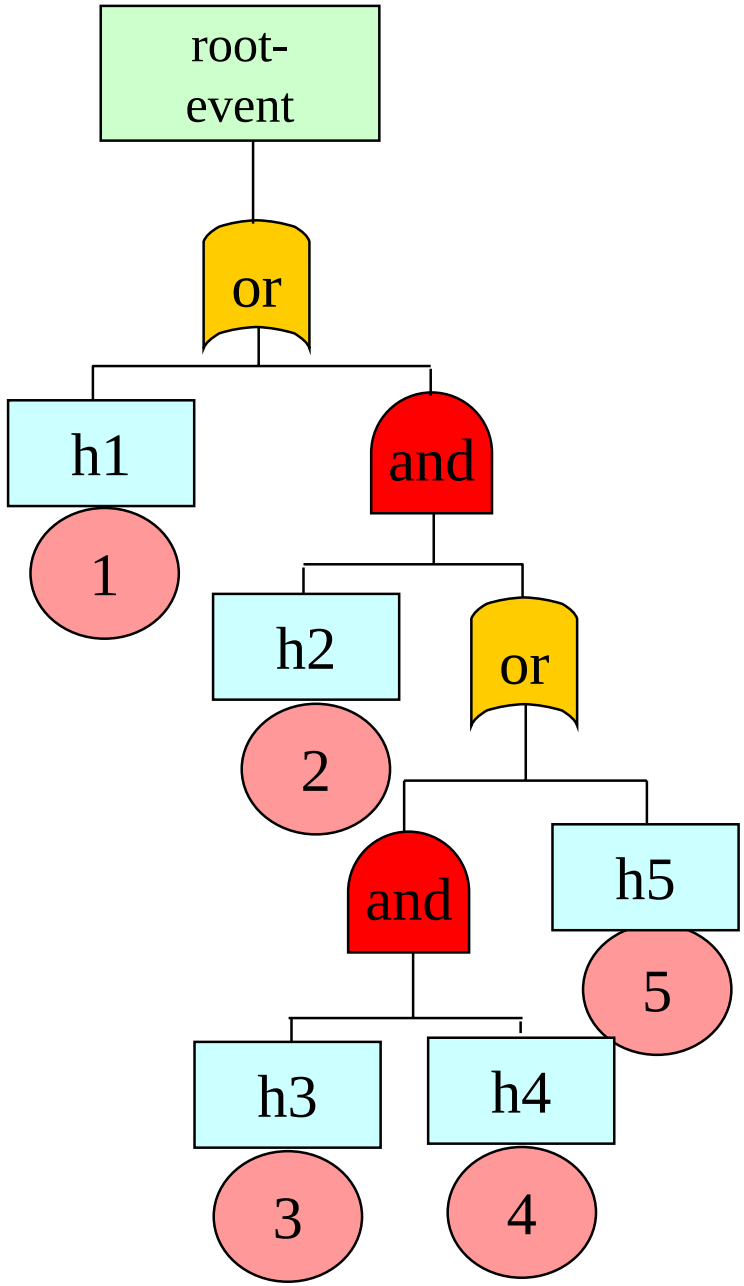
continuation in another tree:



continuation of another tree:

Different steps in a fault tree analysis

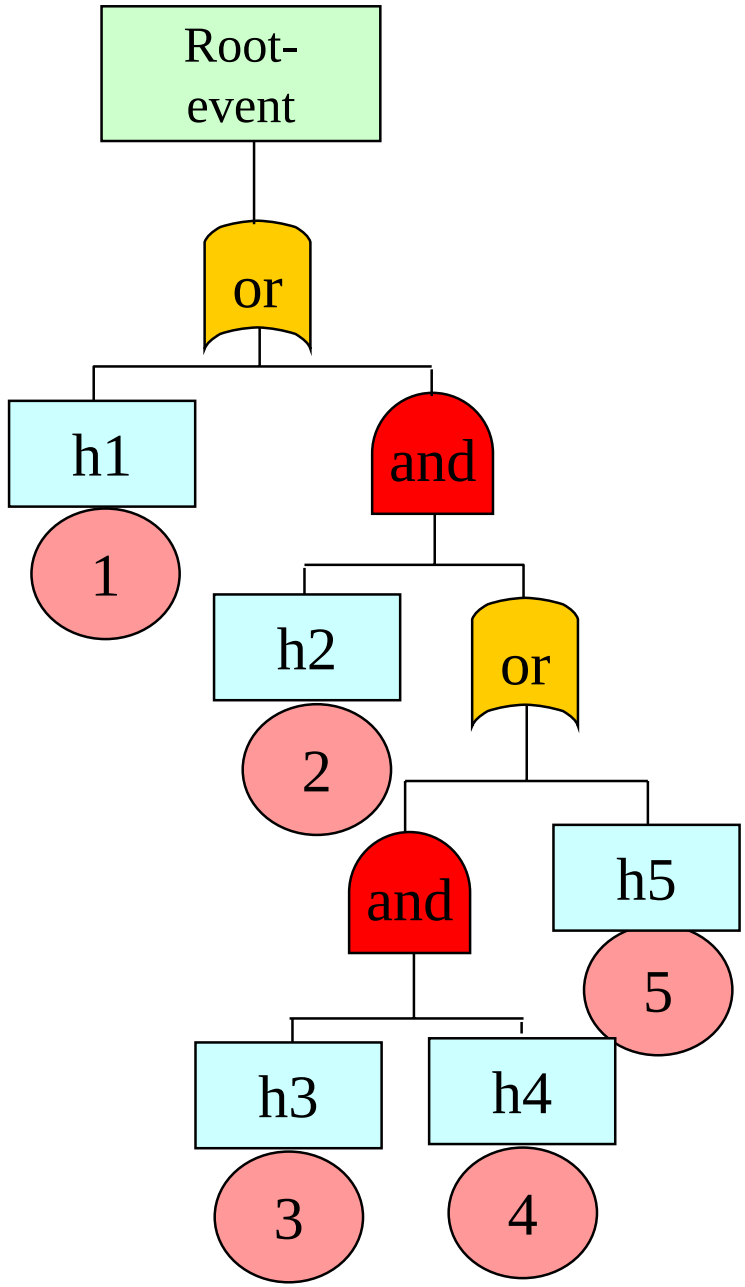
- **STEP 1: Identification of root event**
  - In a security analysis this is typically an unwanted incident at the enterprise level
- **STEP 2: Construction of a fault tree**
  - Root event is placed at the top
  - It is thereafter decomposed into a set of more specialized events
  - These (causing events) are connected to the top event through a logical gate
  - The rest of the tree is constructed accordingly by treating each causing event in the same way as we treated the root event above until the desired level of granularity has been reached
- **STEP 3: Identification of minimal cut sets**
- **STEP 4: Qualitative or quantitative analysis of the fault tree**



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:

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



Strengths and weaknesses of fault trees and fault tree analysis

- **Positive**
  - Fault trees gives a good overview of the relation between unwanted incidents
  - Fault trees are easy to understand and use
  - Fault trees are useful for structuring and organizing unwanted incidents
  - Fault tree analysis is a simple method for finding the probability of an unwanted incident
- **Negative**
  - Fault trees give only a static picture of possible fault combinations
  - Fault trees are difficult to use for testing and maintenance
  - The validity of fault tree analysis depends on that the basic events are independent
  - Fault tree analysis is less useful for qualitative values
  - Requires deep knowledge of the system