

# A contract-oriented view on threat modelling

Ketil Stølen  
SINTEF ICT and University of Oslo

Joint work with  
Gyrd Brændeland, Heidi Dahl, Olav Ligaarden

FLACOS  
Malta, November 27, 2008

# Motivation

- How to modularize threat modelling
- How to deal with mutual dependencies in threat modeling of complex systems
- We need a notion of contract at the abstraction level of threat models

# Problem of risk analysis

- Systems
  - are complex
  - mutually dependent
  - cross national borders
  - are continuously updated
- You never have full access to all documentation
- And, if you had, there would just be too much of it

# There is only one way forward

- **We need a reductionistic approach to risk analysis**
  - Decomposing analyses into smaller parts
  - Composing (already completed) analyses into an overall risk picture
- Methodological reductionism is the idea that developing an understanding of a complex system's constituent parts (and their interactions) is the best way to develop an understanding of the system as a whole

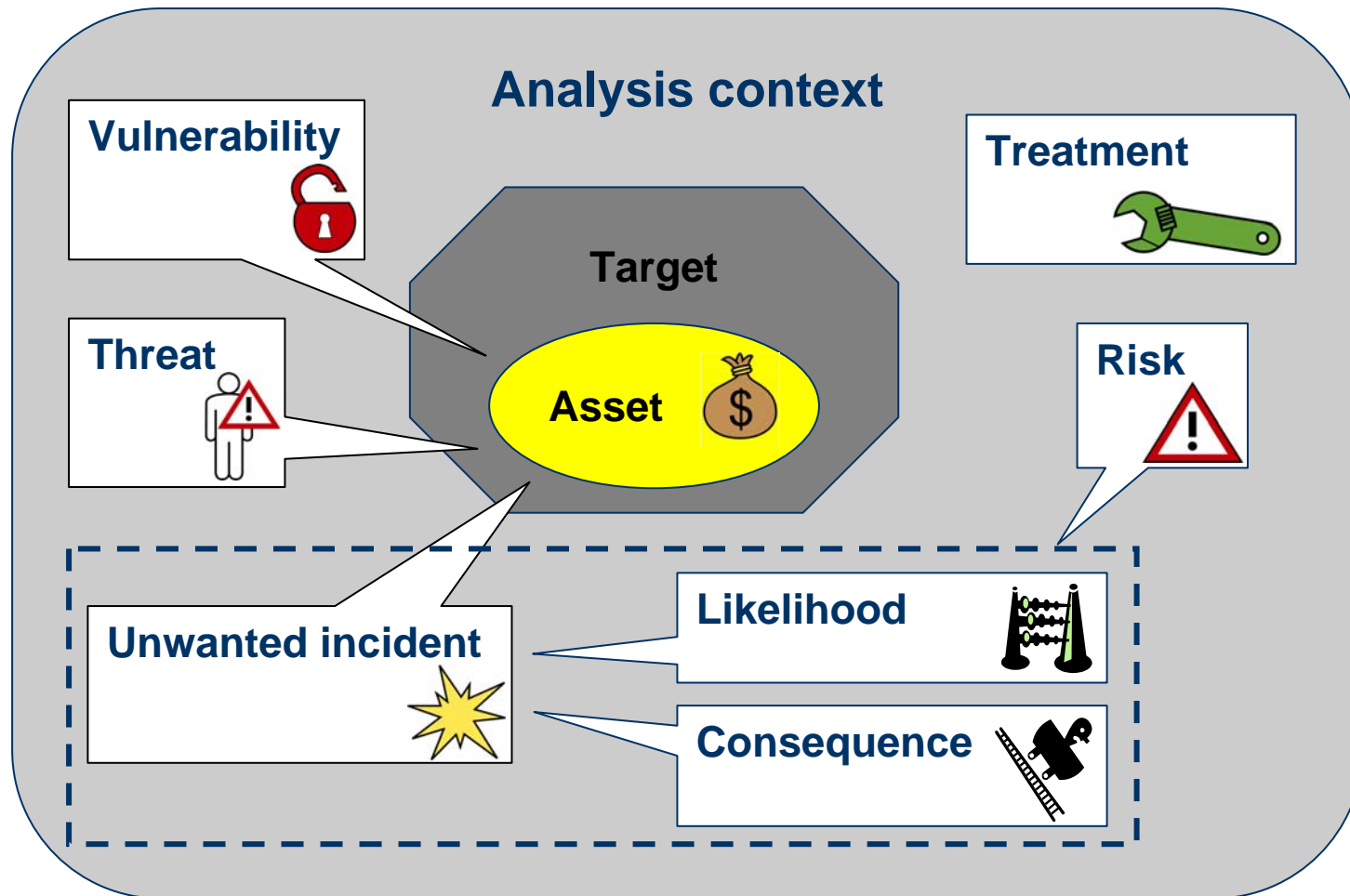
# Reductionistic approach to the modeling of threat scenarios

- I will illustrate the approach on CORAS
- CORAS is
  - a method for model-driven security risk analysis
  - a graphical language
    - for structured brainstorming and analysis
    - semantics defined as schematic translation of diagrams into English
  - a tool
- You may do likewise with your favorite threat scenario modeling language – (or your favorite risk table)

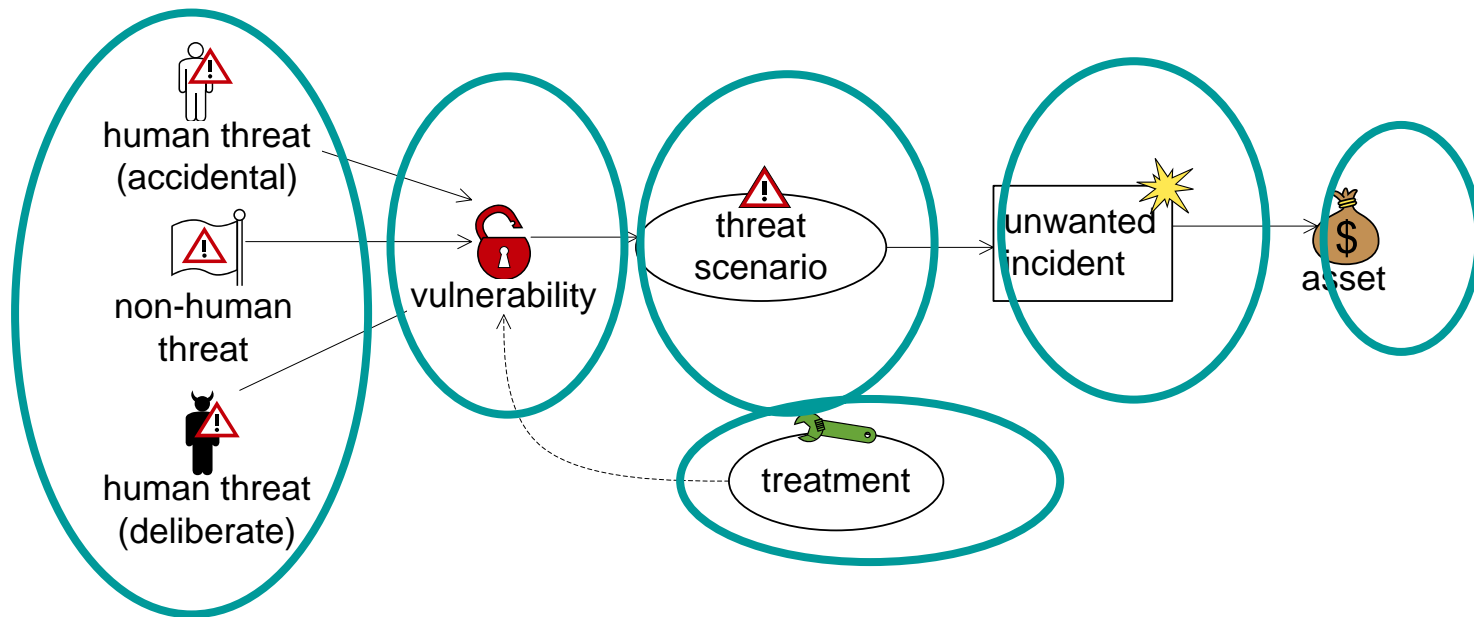
# Approach

- Extend the graphical CORAS language to cope with context dependencies
  - We refer to the extended language as **Dependent CORAS**
- Update the semantics of the CORAS language to deal with context dependencies
- Define rules to reason about context dependencies
- Define rules for simplifying composed scenarios

# One Step Back: What is Security Risk Analysis?

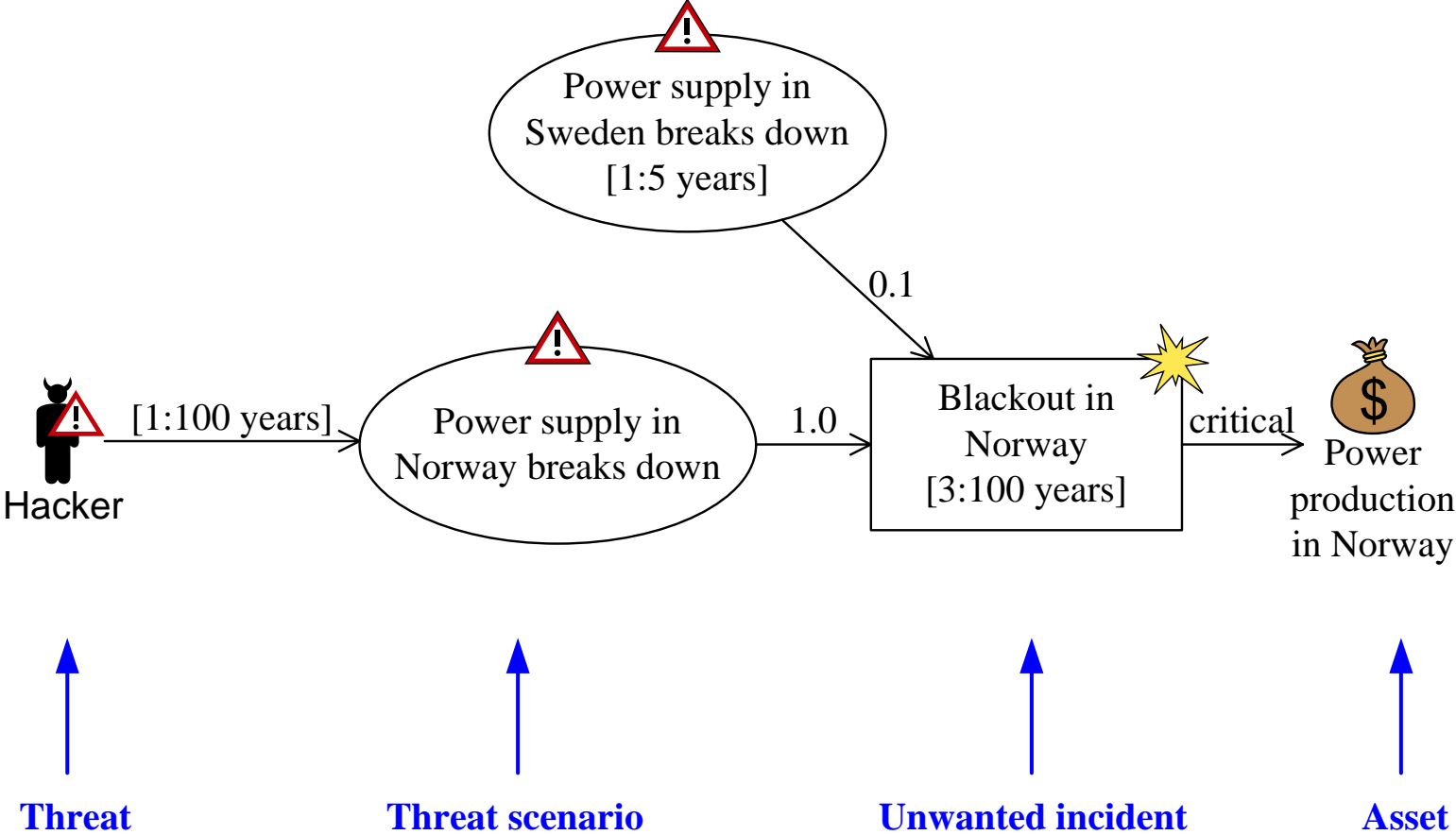


# The CORAS security risk modeling language





# Threat Diagram



# Semantics: Translation into English

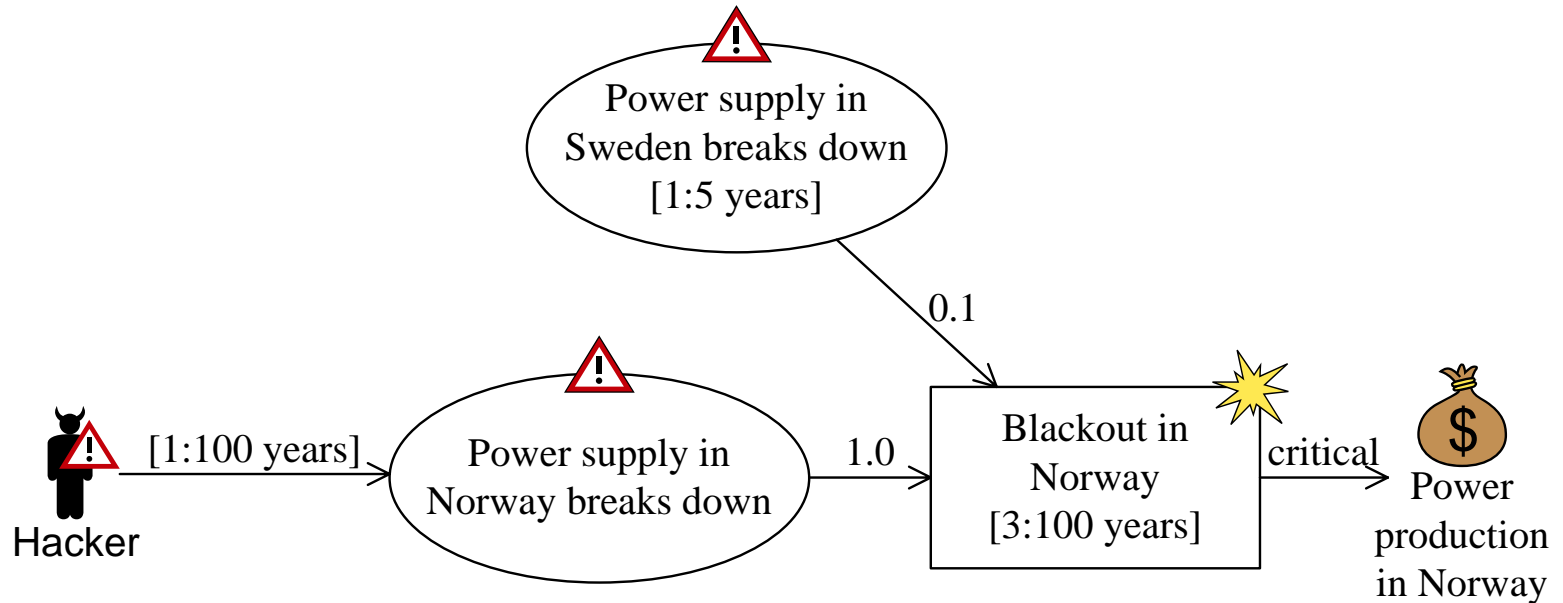
## ■ Vertices

- "Hacker" is a deliberate threat.
- Threat scenario "Power supply in Norway breaks down" occurs with undefined likelihood.
- Threat scenario "Power supply in Sweden breaks down" occurs with likelihood "1:5 years".
- Unwanted incident "Blackout in Norway" occurs with likelihood "3:100 years".
- "Power production in Norway" is an asset.

## ■ Relations

- Hacker initiates "Power supply in Norway breaks down" with likelihood "1:100" years.
- "Power supply in Norway breaks down" leads to "Blackout in Norway" with conditional likelihood "1.0".
- "Power supply in Sweden breaks down" leads to "Blackout in Norway" with conditional likelihood "0.1".
- "Power supply in Norway breaks down" impacts "Power production in Norway" with consequence "critical".

# Checking Likelihoods

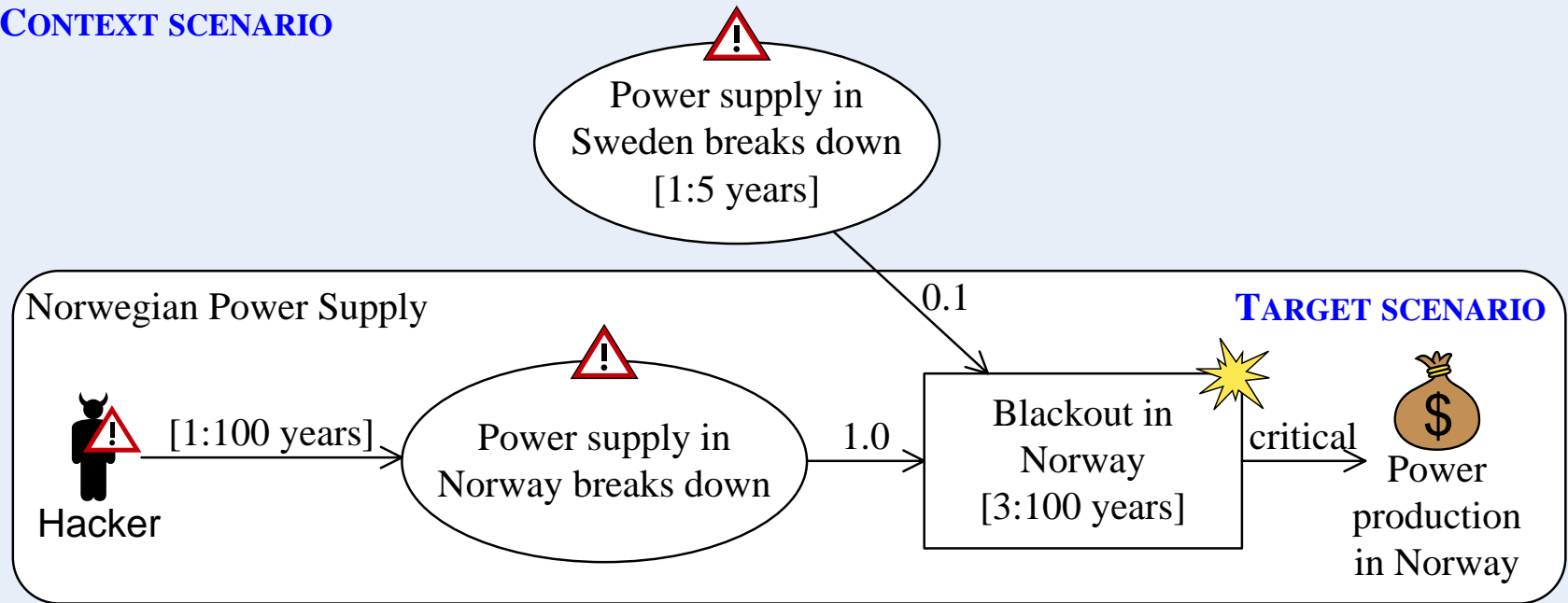


$$[1:5 \text{ years}] * 0.1 = [1:50 \text{ years}]$$

$$[1:100 \text{ years}] + [1:50 \text{ years}] = [3:100 \text{ years}]$$

# Dependent Diagram

## CONTEXT SCENARIO



# Semantics of Dependent Diagram

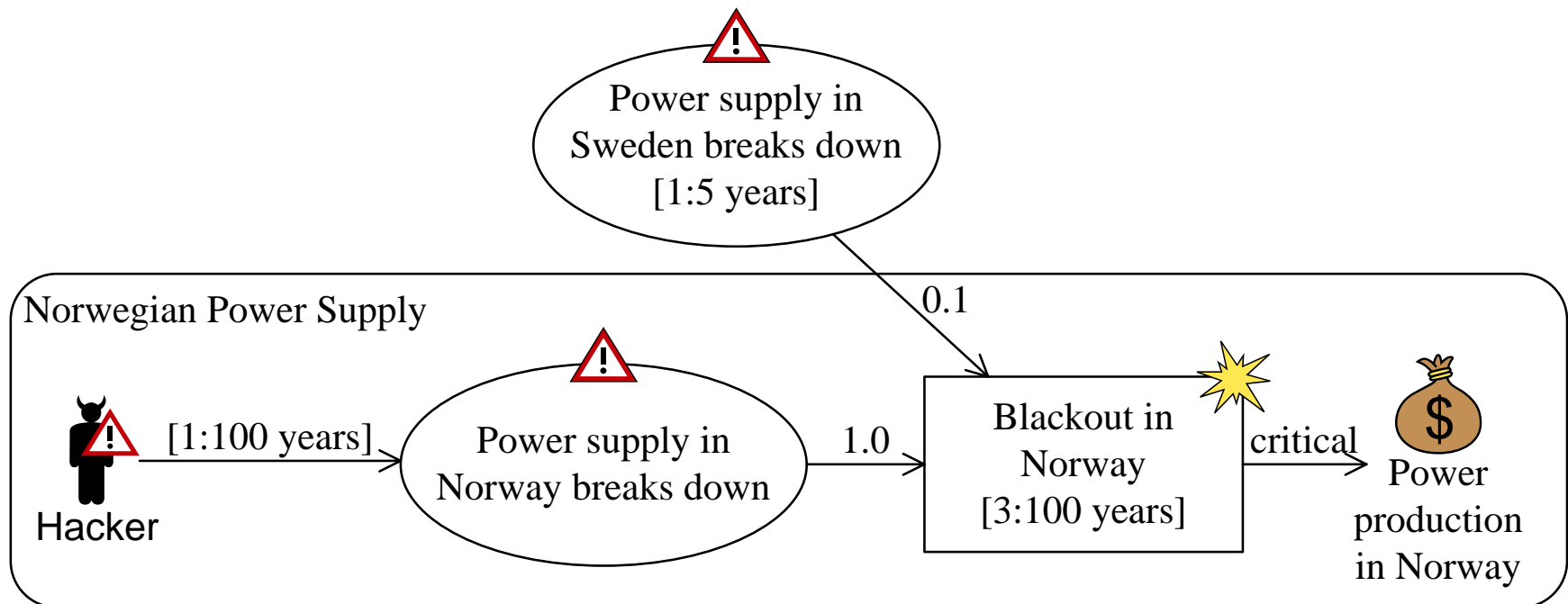
■  $[[C \triangleright T]] :=$

$[[T]]$

assuming

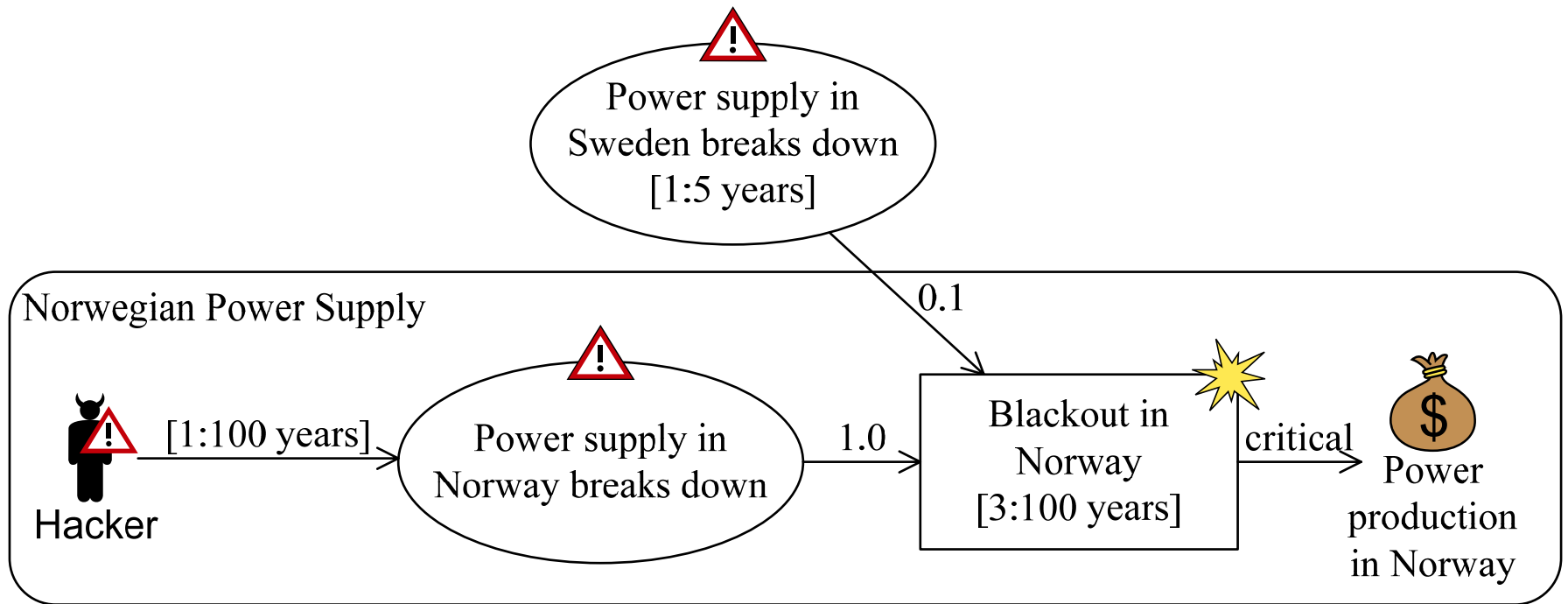
$[[C]]$

to the extent there are explicit dependencies



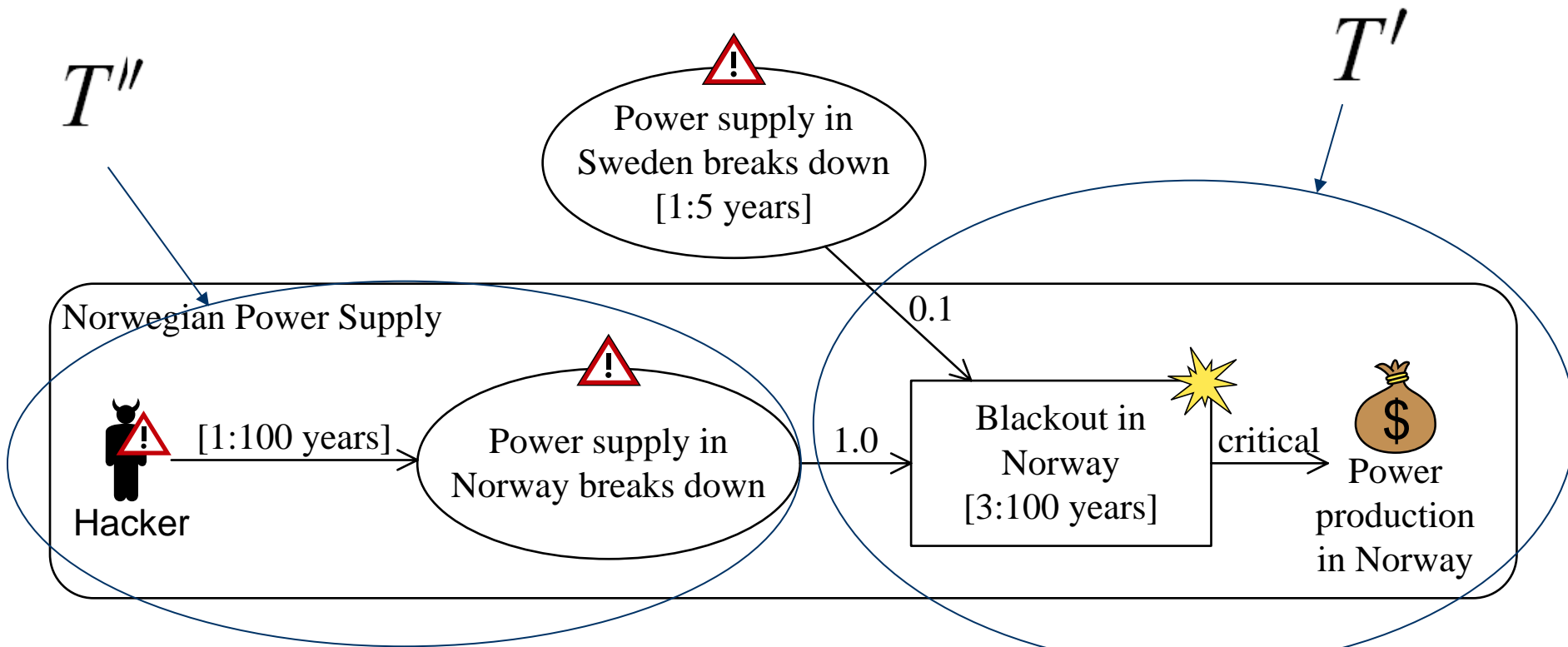
# Independence of Context

$C \nleftrightarrow T$  : T is independent of C if there are no paths from C to T



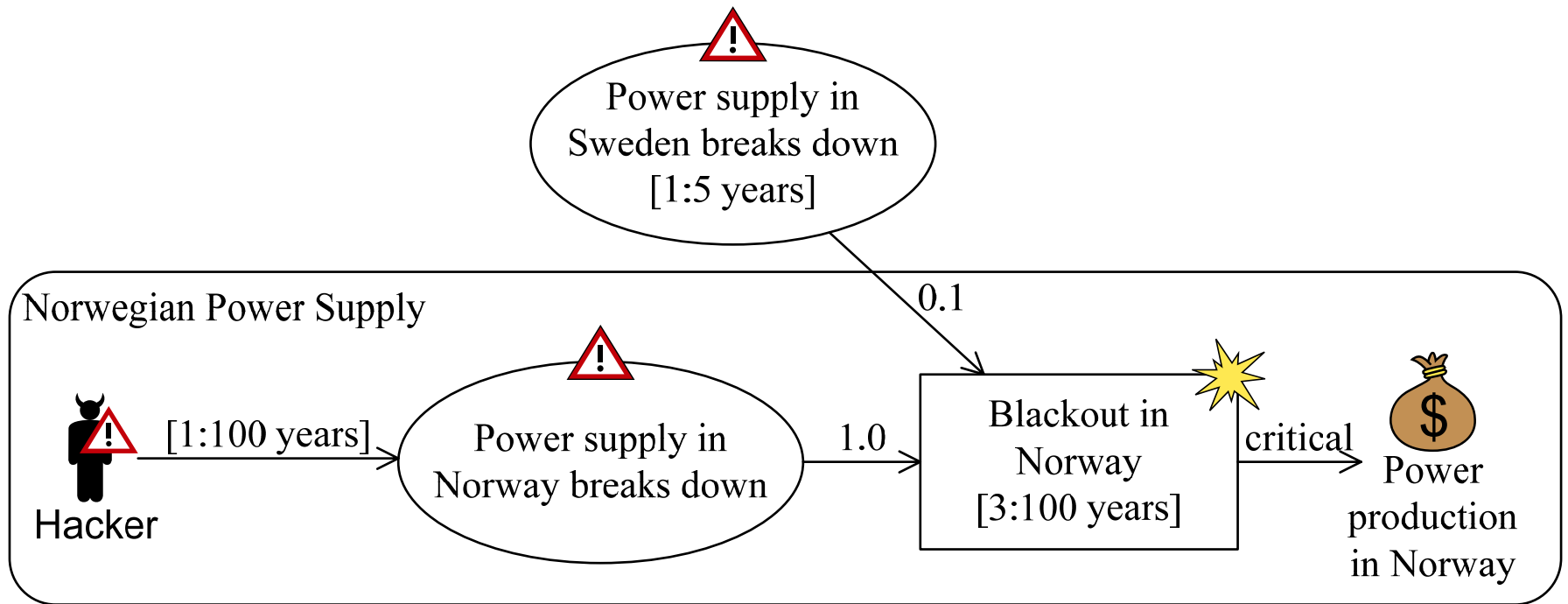
# Rule of Independence

$$\frac{C \triangleright T \quad C \ddagger T'' \quad T' \ddagger T''}{\triangleright T''}$$



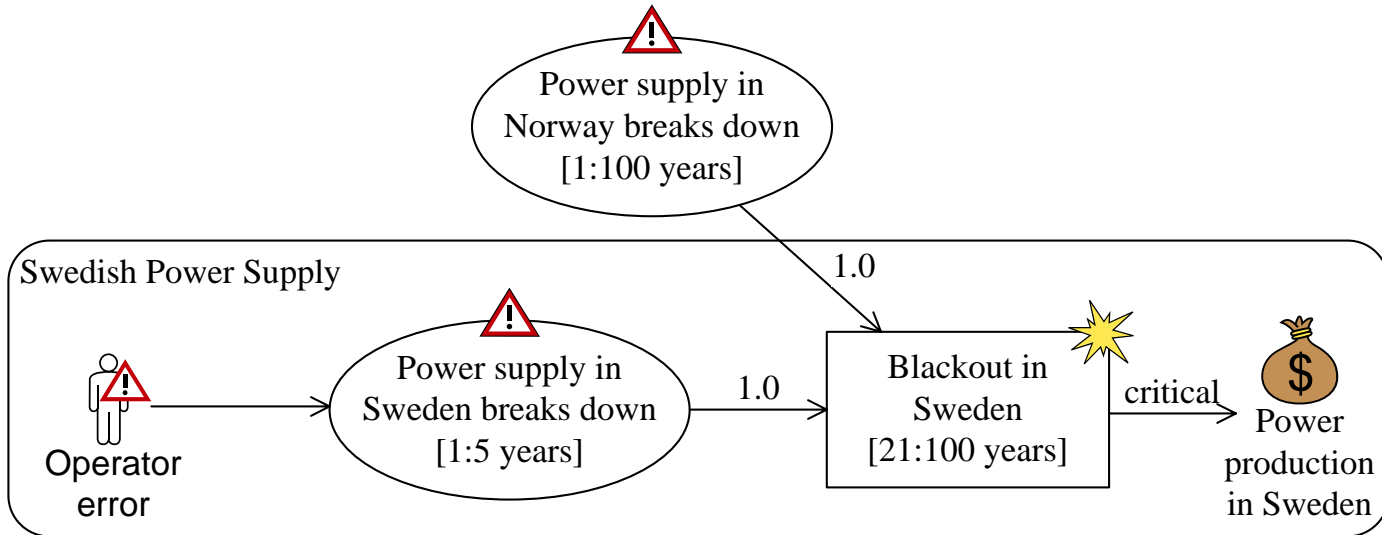
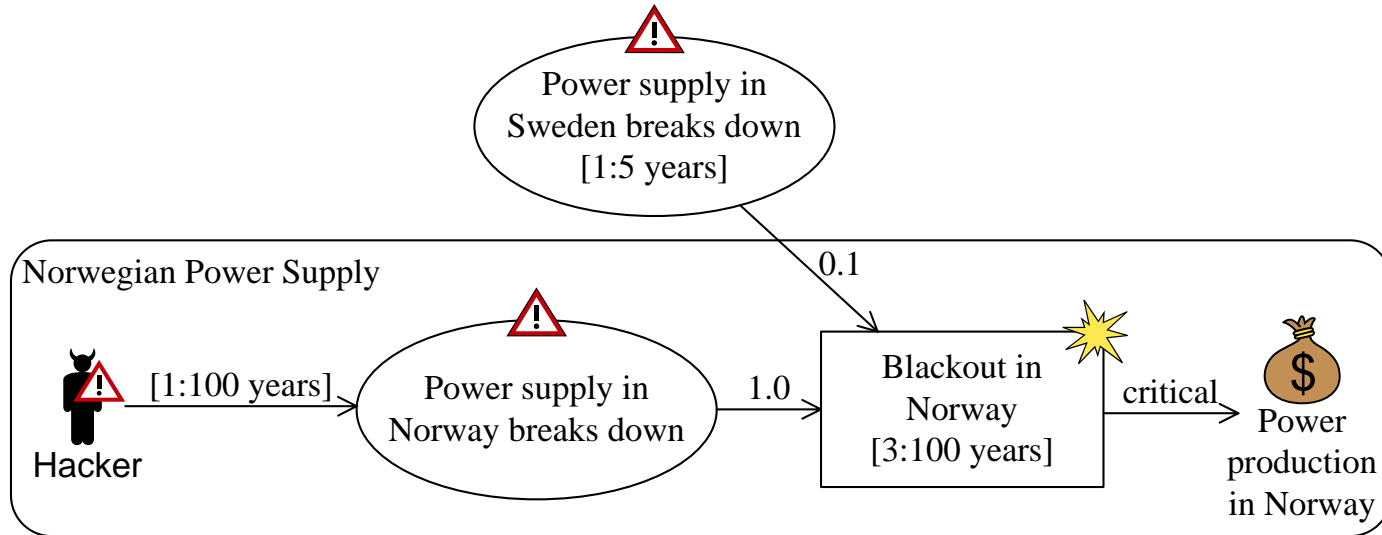
# Modus Ponens

$$\frac{C \triangleright T \quad \triangleright C}{\triangleright T}$$

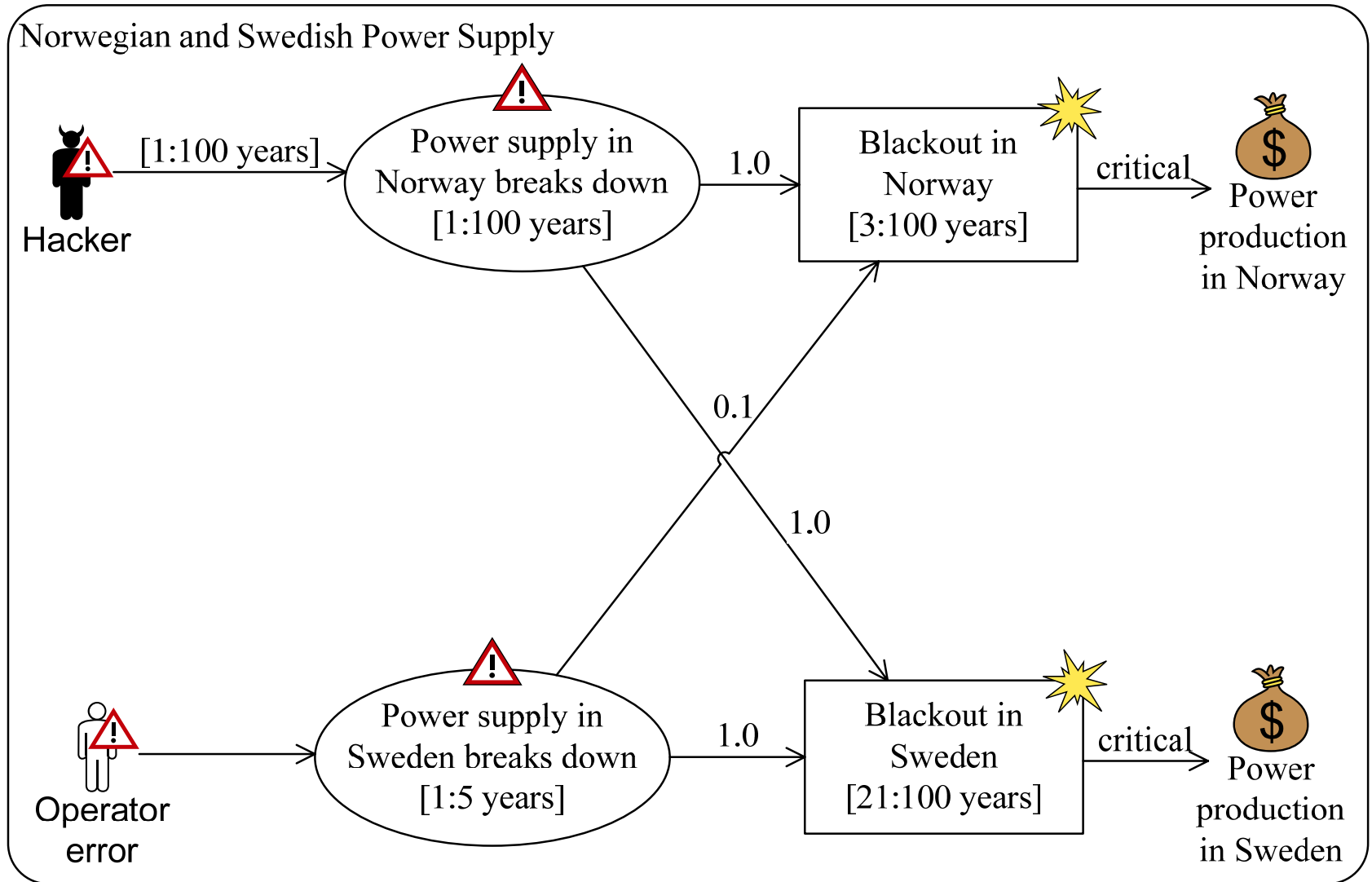




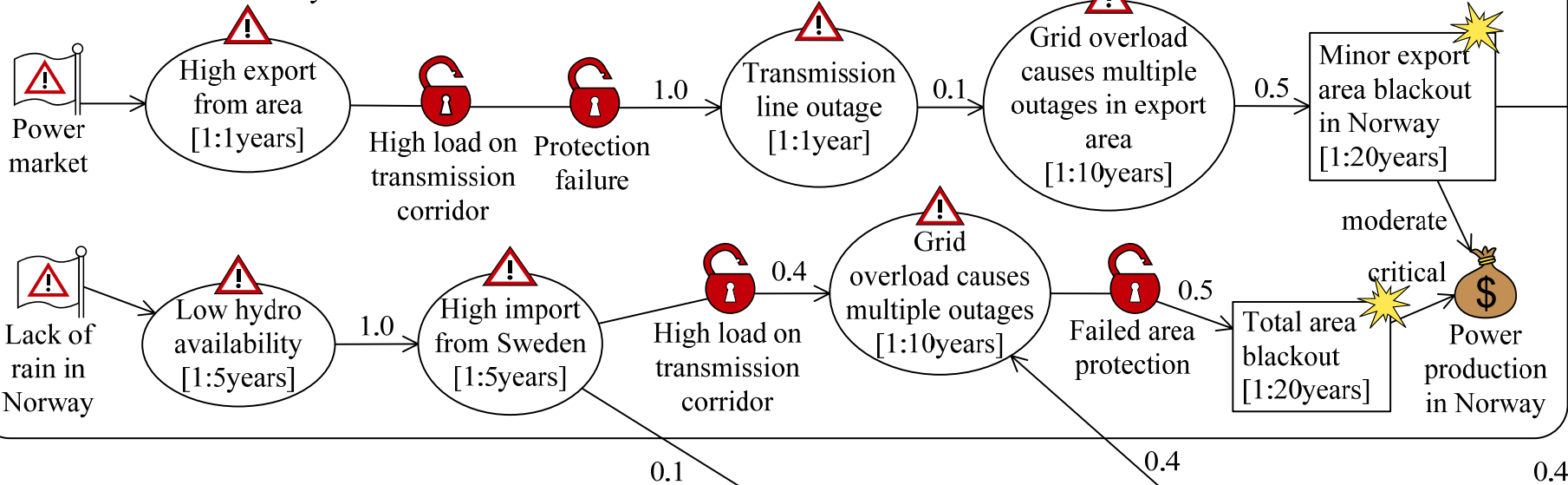
# Applying the Deduction Rules



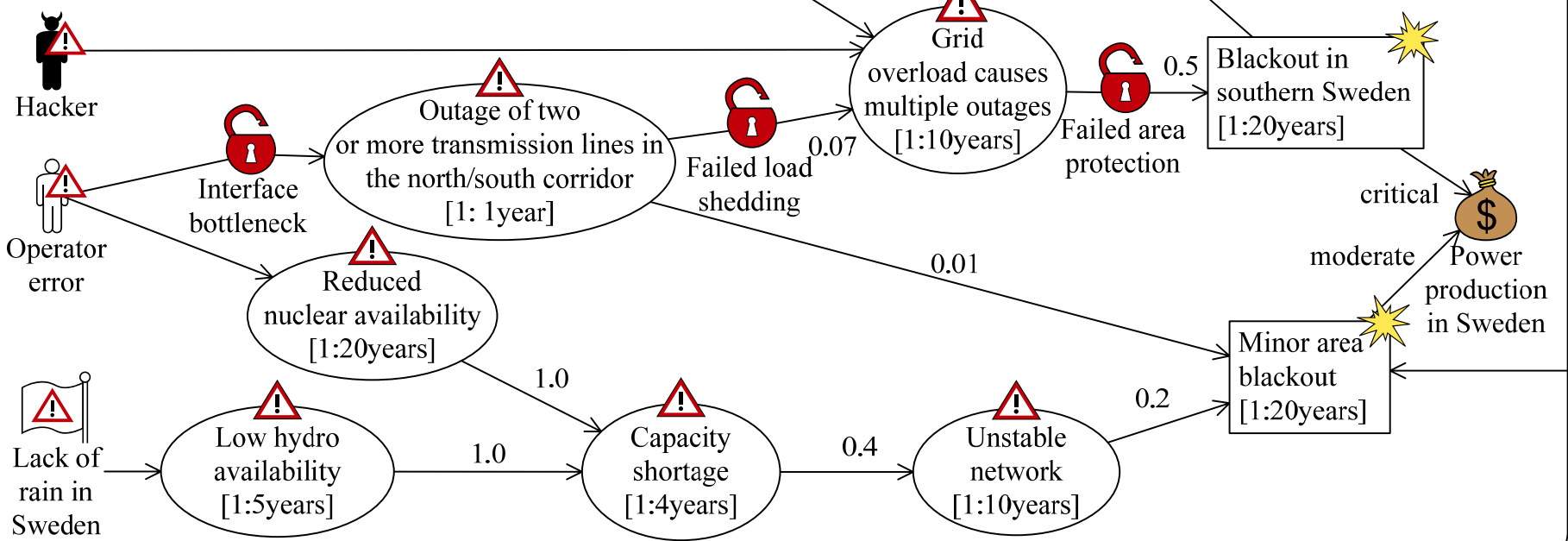
# The Combined Diagram



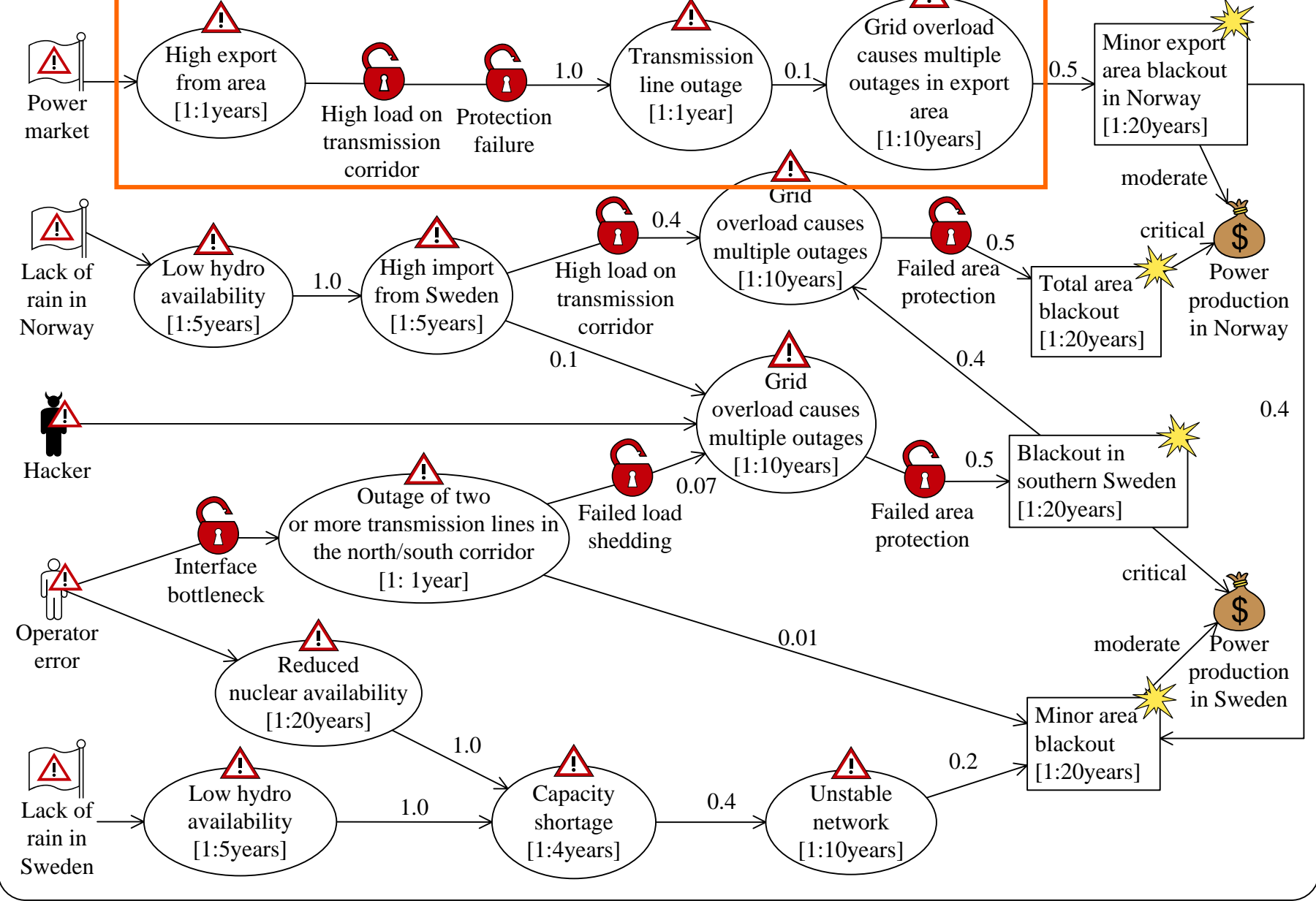
### Blackout in southern Norway



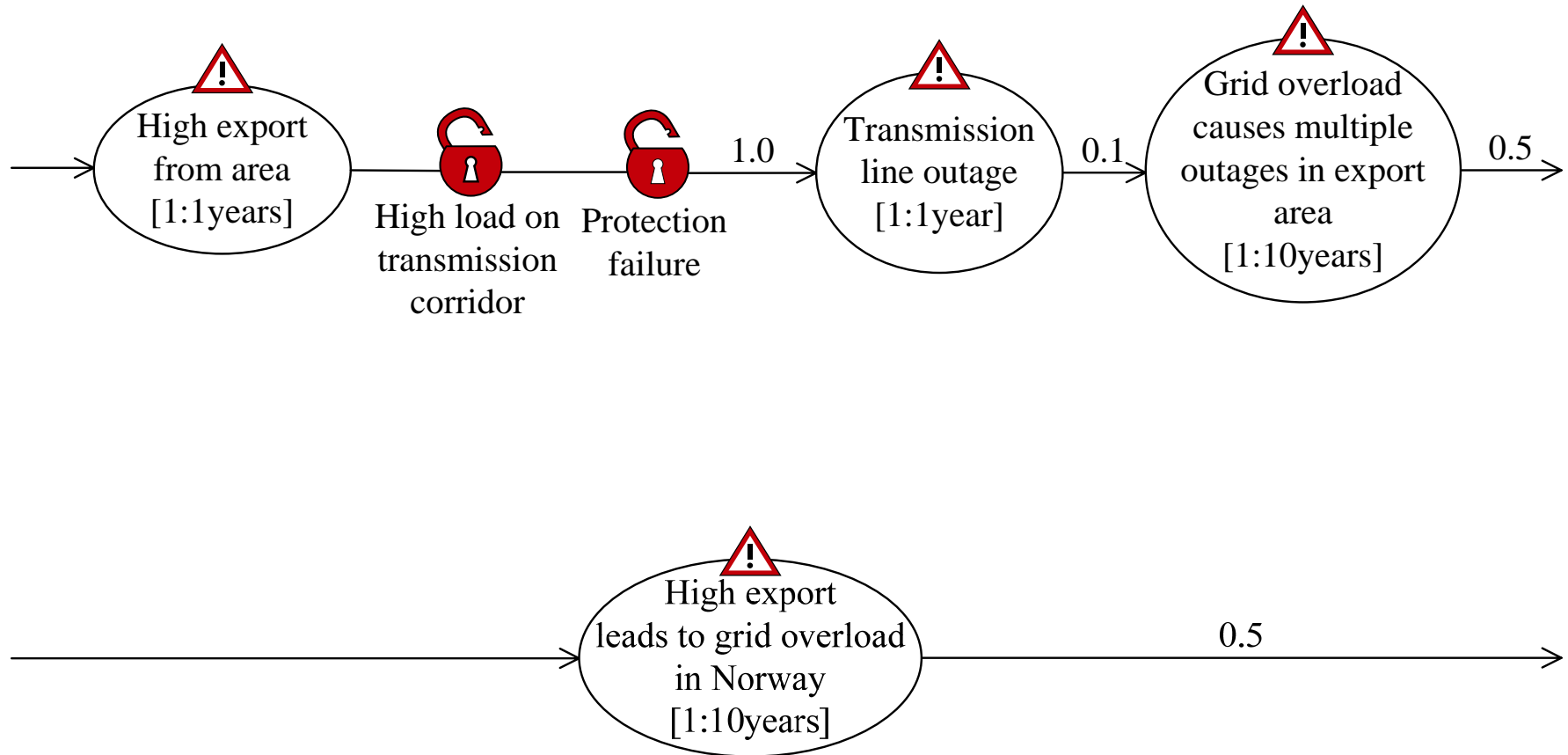
### Blackout in southern Sweden



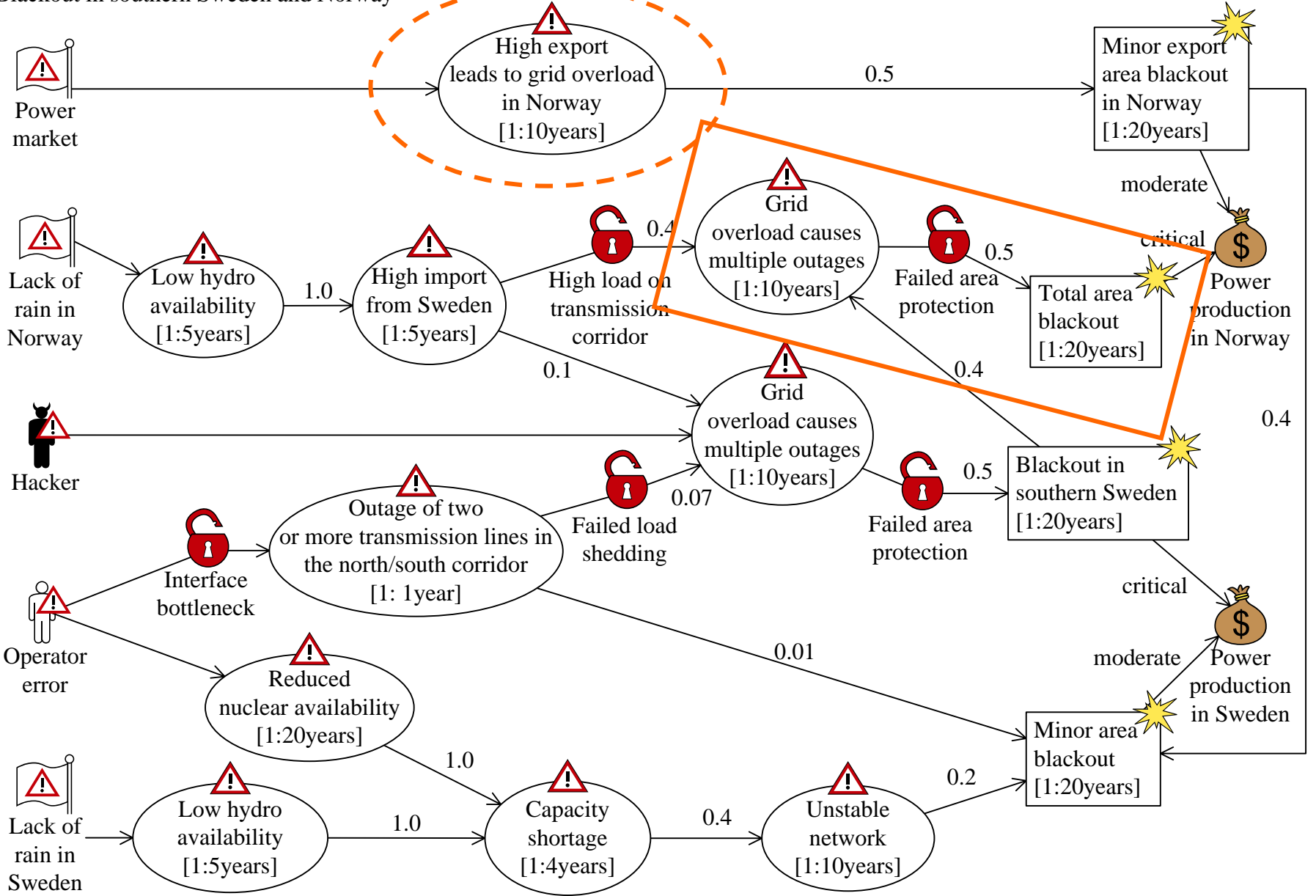
Blackout in southern Sweden and Norway



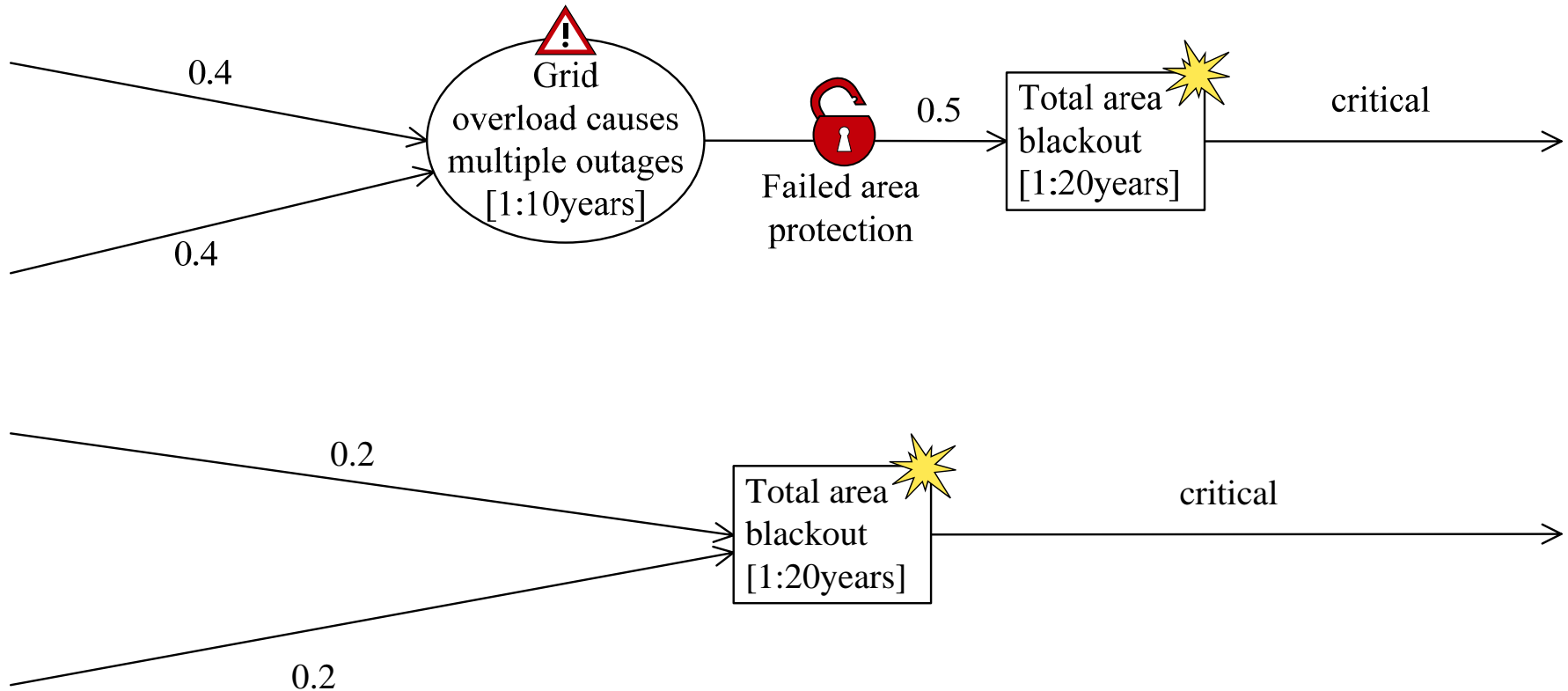
# Horizontal Composition



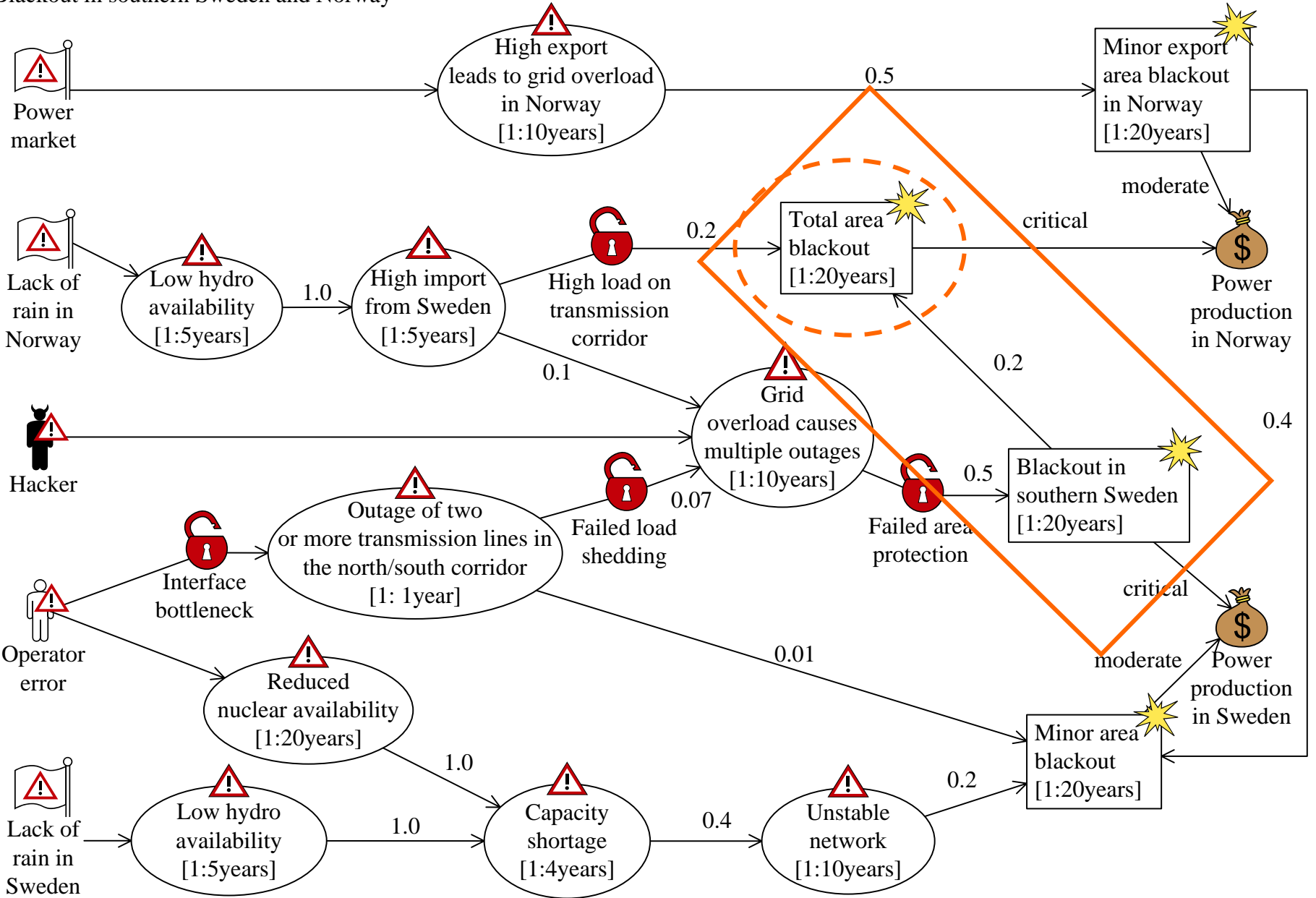
# Blackout in southern Sweden and Norway



# Horizontal Composition

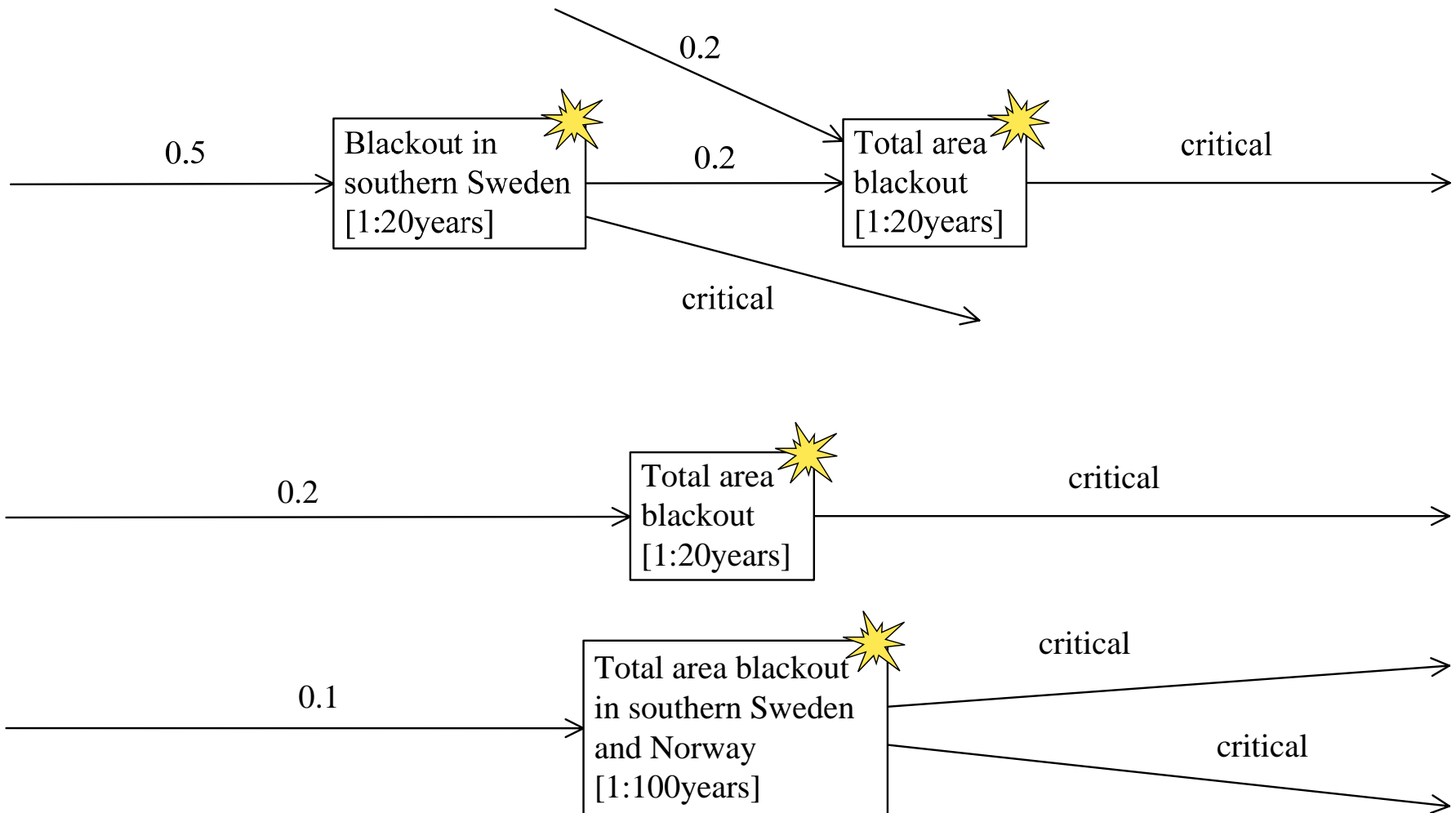


# Blackout in southern Sweden and Norway

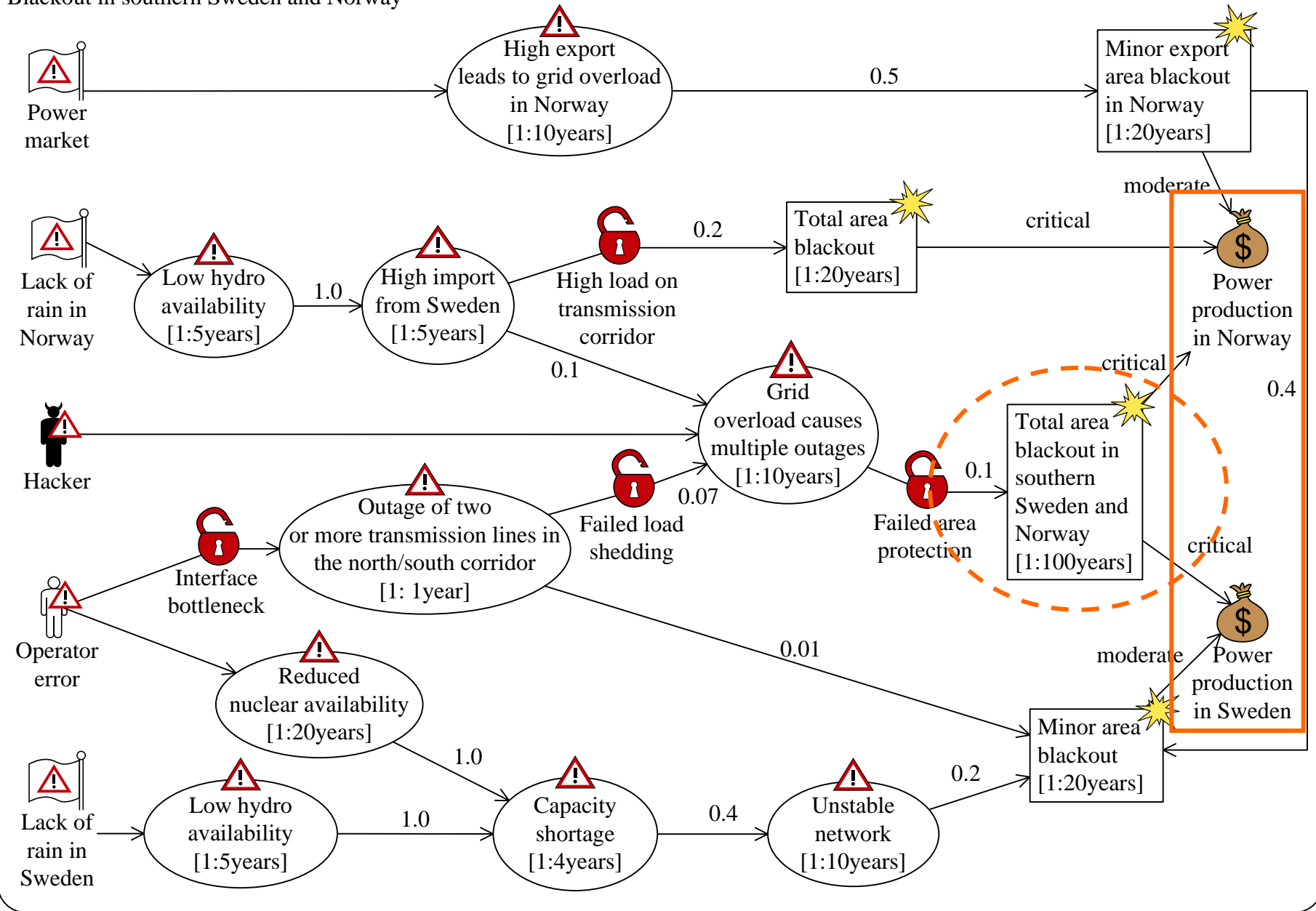




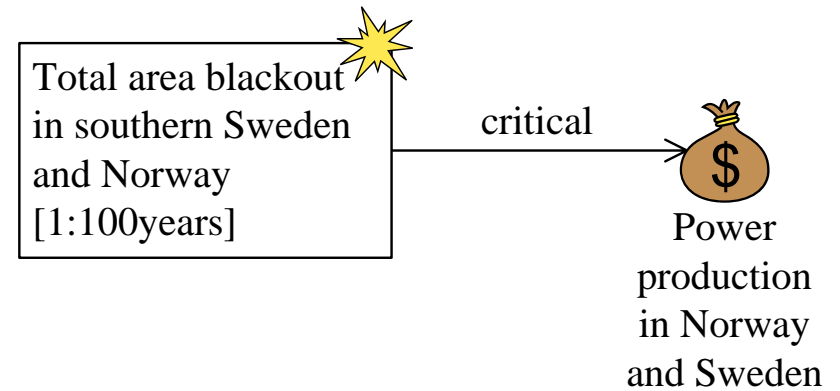
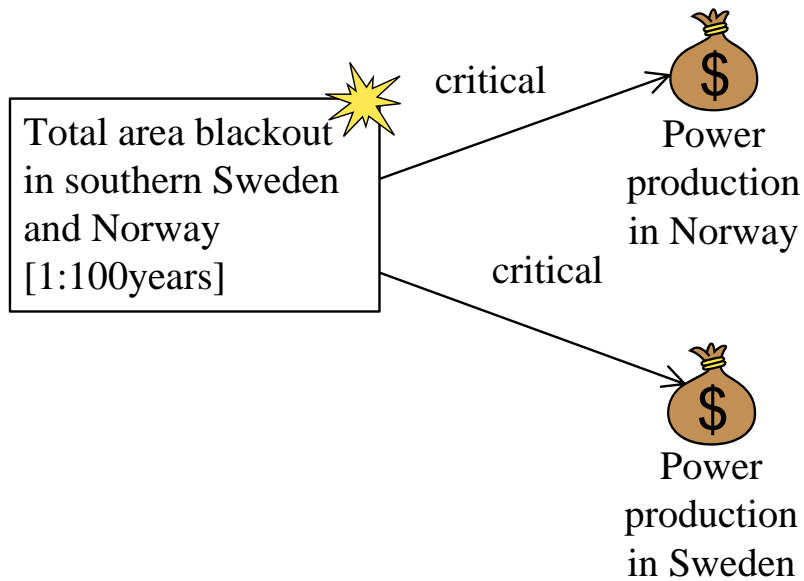
# Horizontal Composition



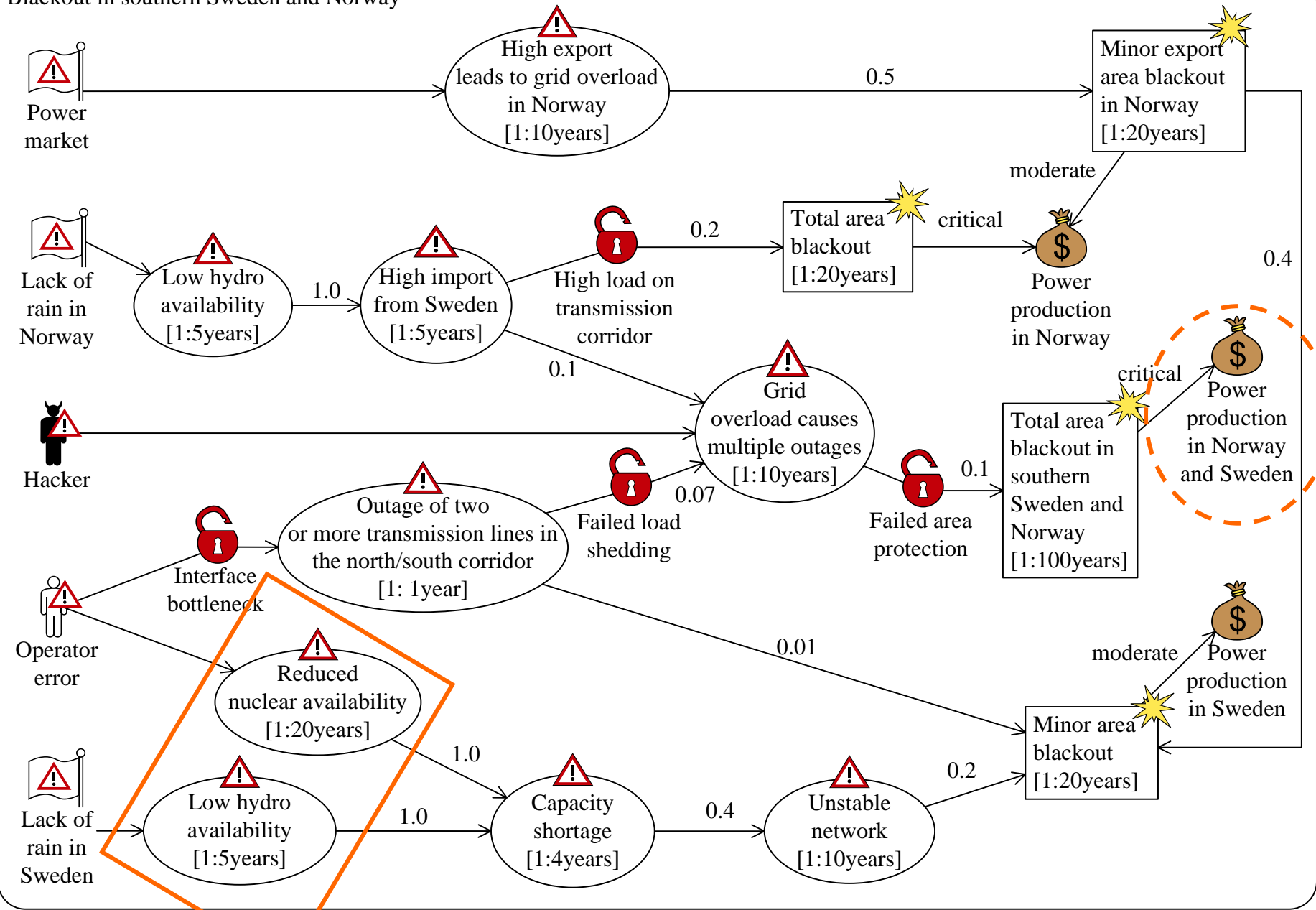
# Blackout in southern Sweden and Norway



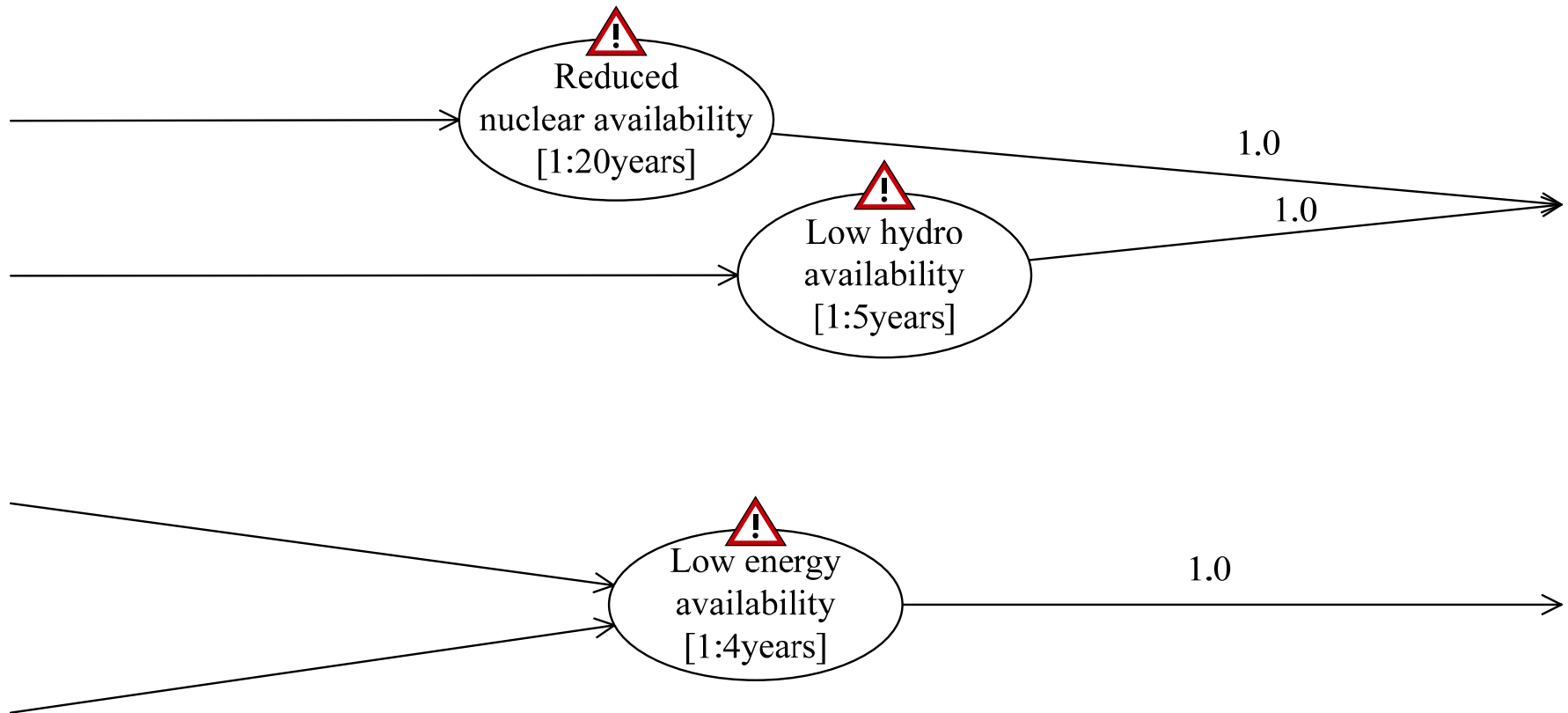
# Asset Composition



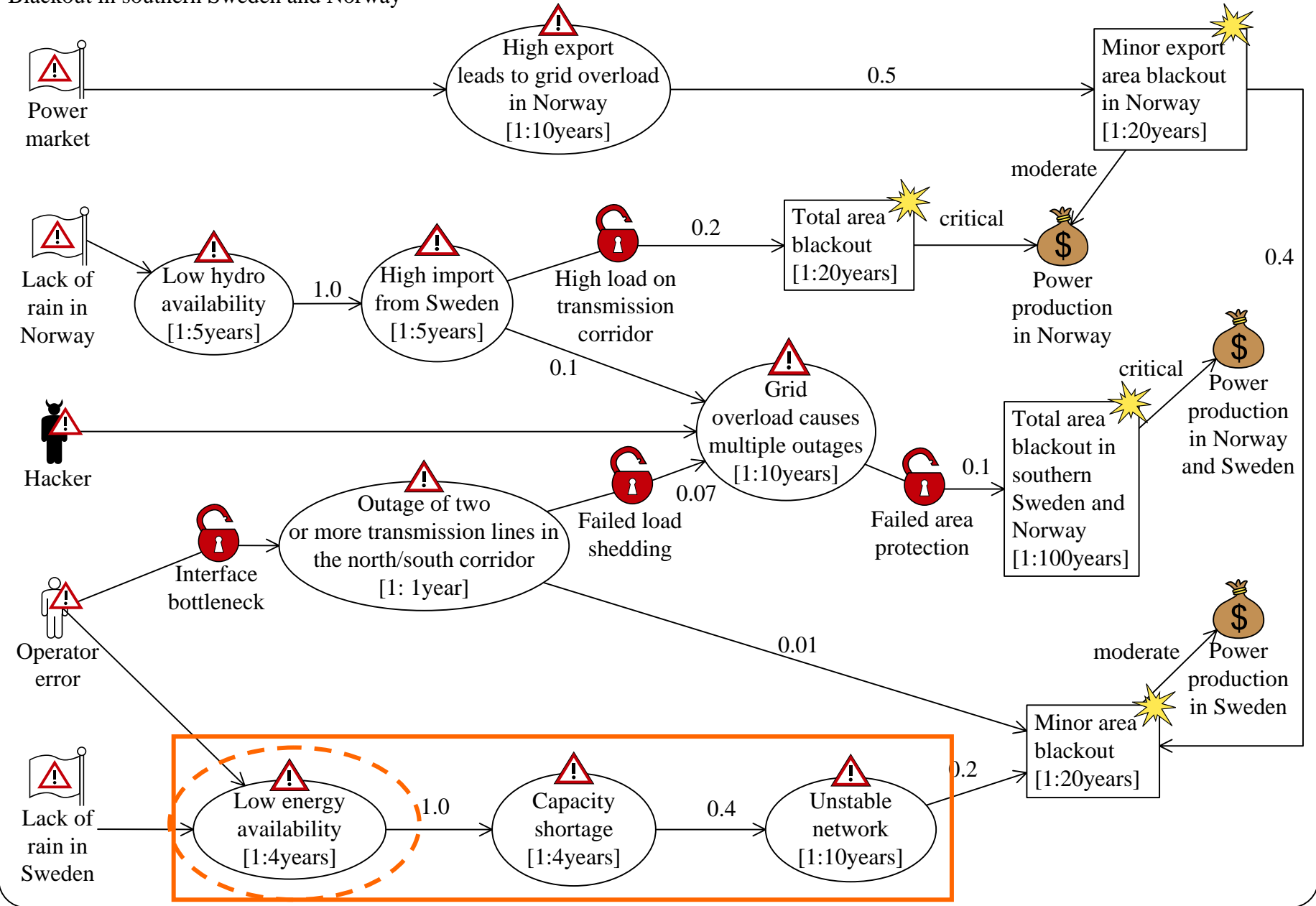
# Blackout in southern Sweden and Norway



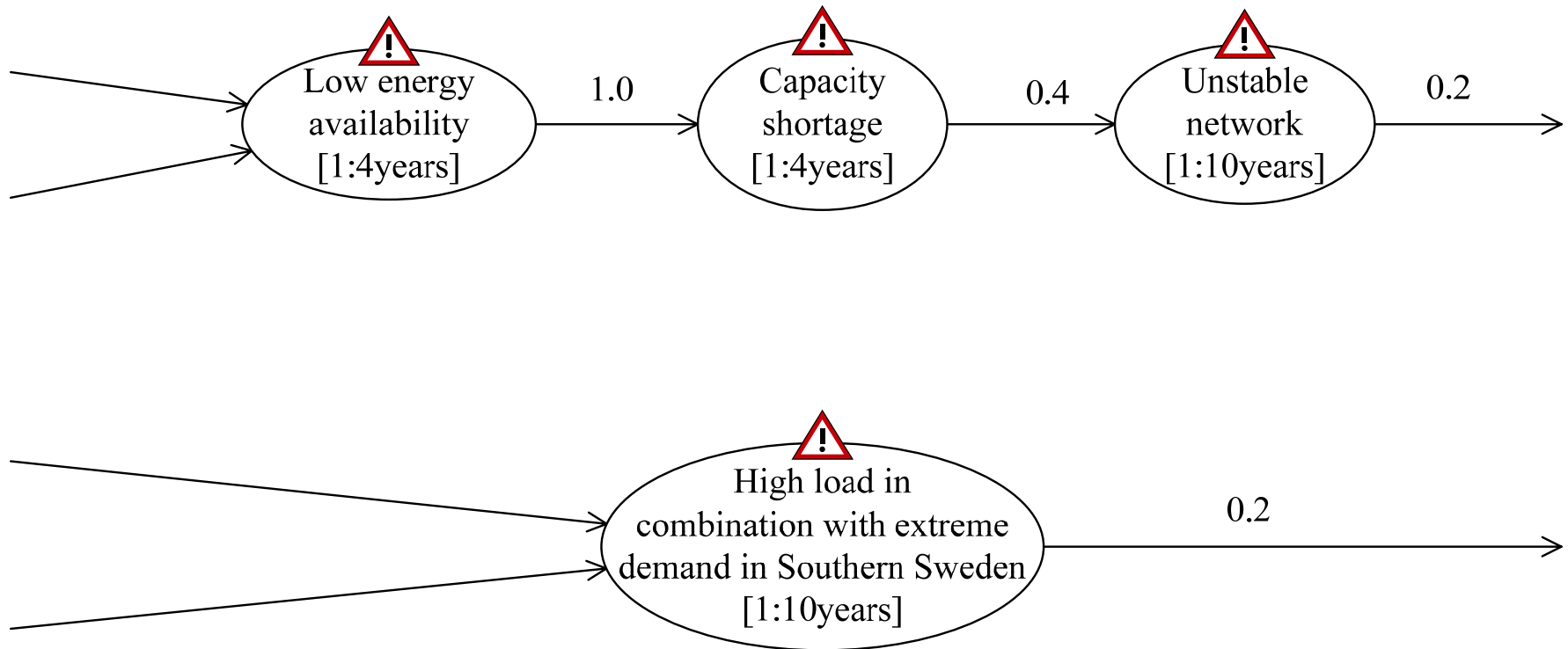
# Vertical Composition



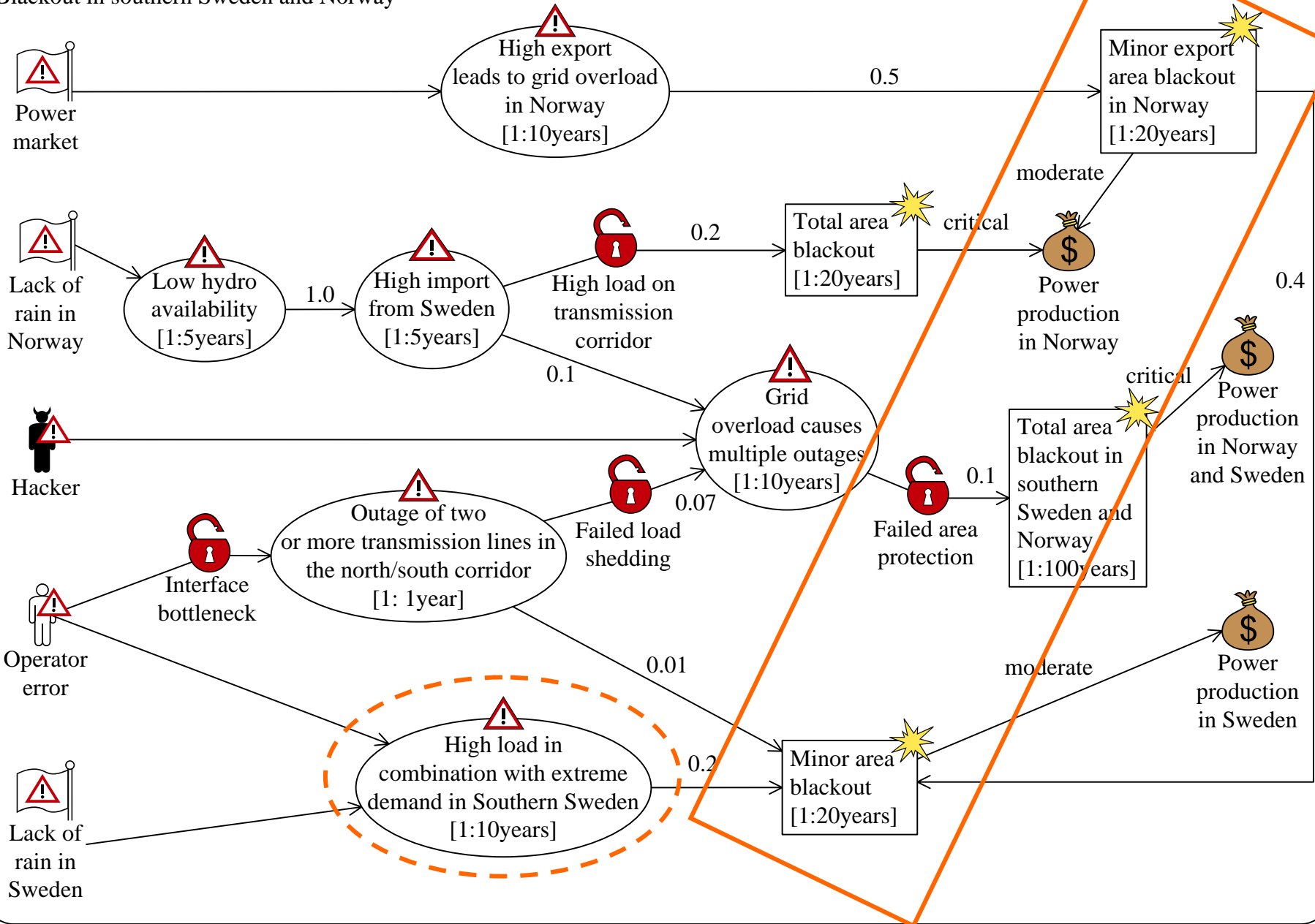
# Blackout in southern Sweden and Norway



# Horizontal Composition

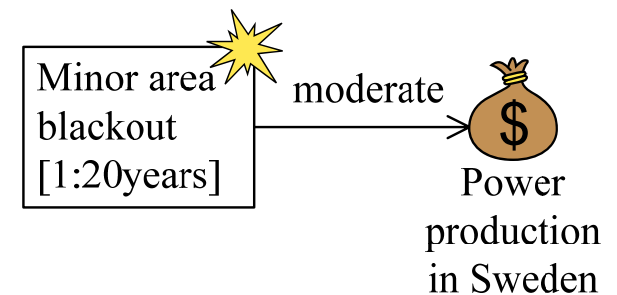
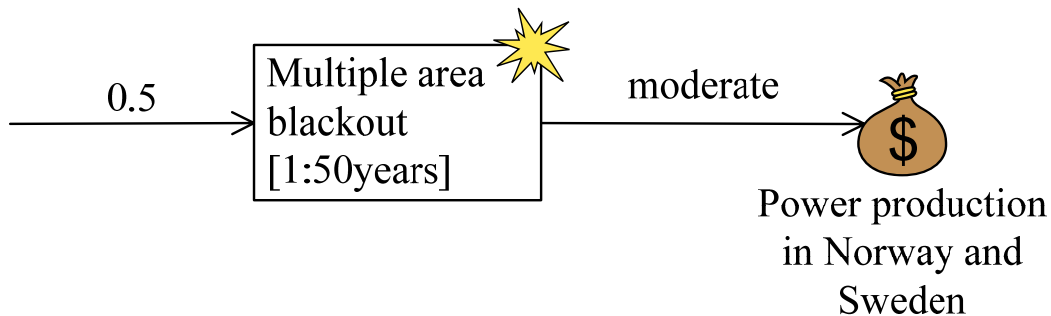
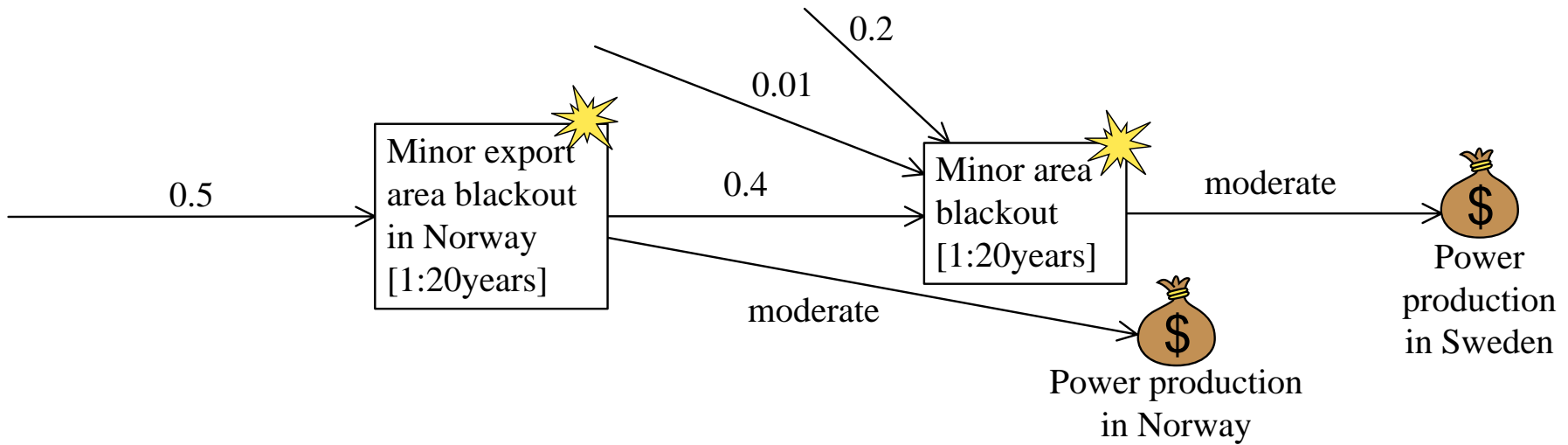


# Blackout in southern Sweden and Norway

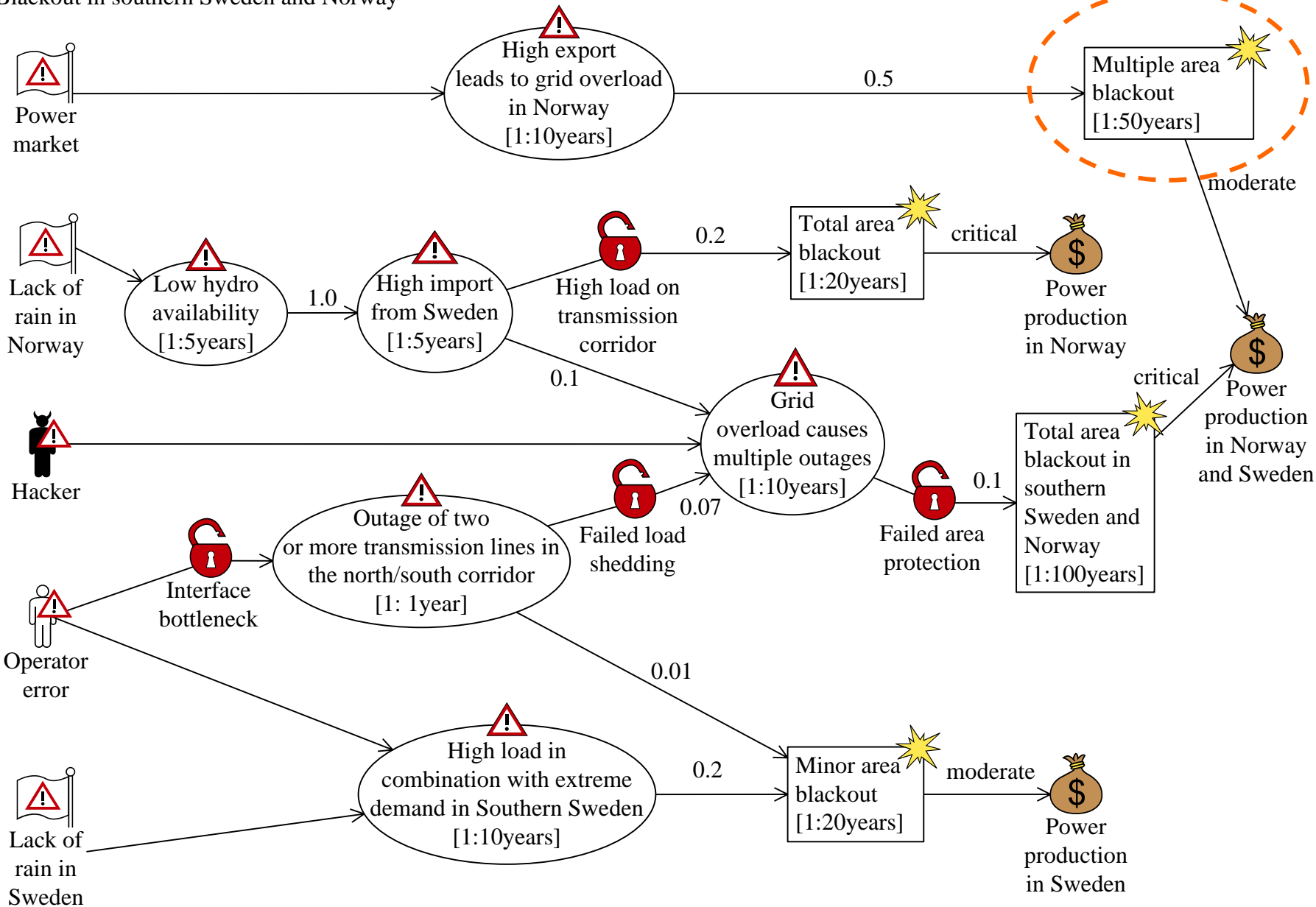




# Horizontal & Asset Composition



# Blackout in southern Sweden and Norway



# Conclusions

We have

- argued the need for a reductionistic approach to risk analysis
- outlined a generic strategy to facilitate modular threat modelling
- illustrated the generic strategy on the CORAS language

# Resources: <http://coras.sourceforge.net/>

## ■ Downloads

- The CORAS diagram editor
- The CORAS icons (Visio stencil, PNG, SVG)

## ■ Publications:

- Folker den Braber, Ida Hogganvik, Mass Soldal Lund, Ketil Stølen, and Fredrik Vraalsen. **Model-based security analysis in seven steps – a guided tour to the CORAS method.** BT Technology Journal, 25(1): 101 – 117, 2007.
- Ida Hogganvik. **A graphical approach to security risk analysis.** PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo, 2007.
- Gyrd Brændeland, Heidi E.I. Dahl, Iselin Engan, Ketil Stølen. **Using dependent CORAS diagrams to analyse mutual dependency.** To appear in Proc. 2nd International Workshop on Critical Information Infrastructure Security (CRITIS'2007).

# Questions?

**Ketil Stølen**  
**SINTEF ICT and University of Oslo**

[Ketil.Stolen@sintef.no](mailto:Ketil.Stolen@sintef.no)