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

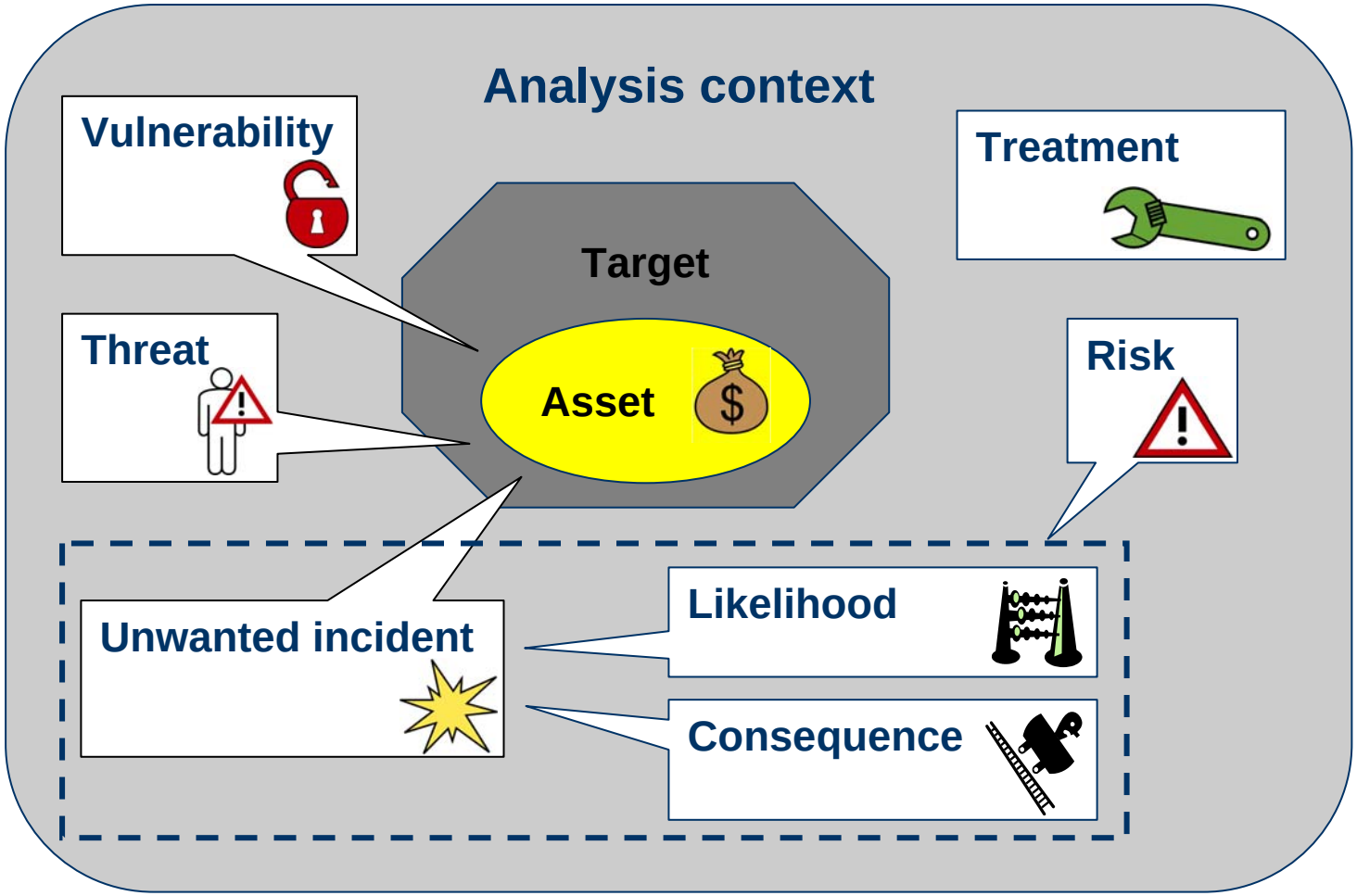
Reductionistic approach to the modeling of threat scenarios

- 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)

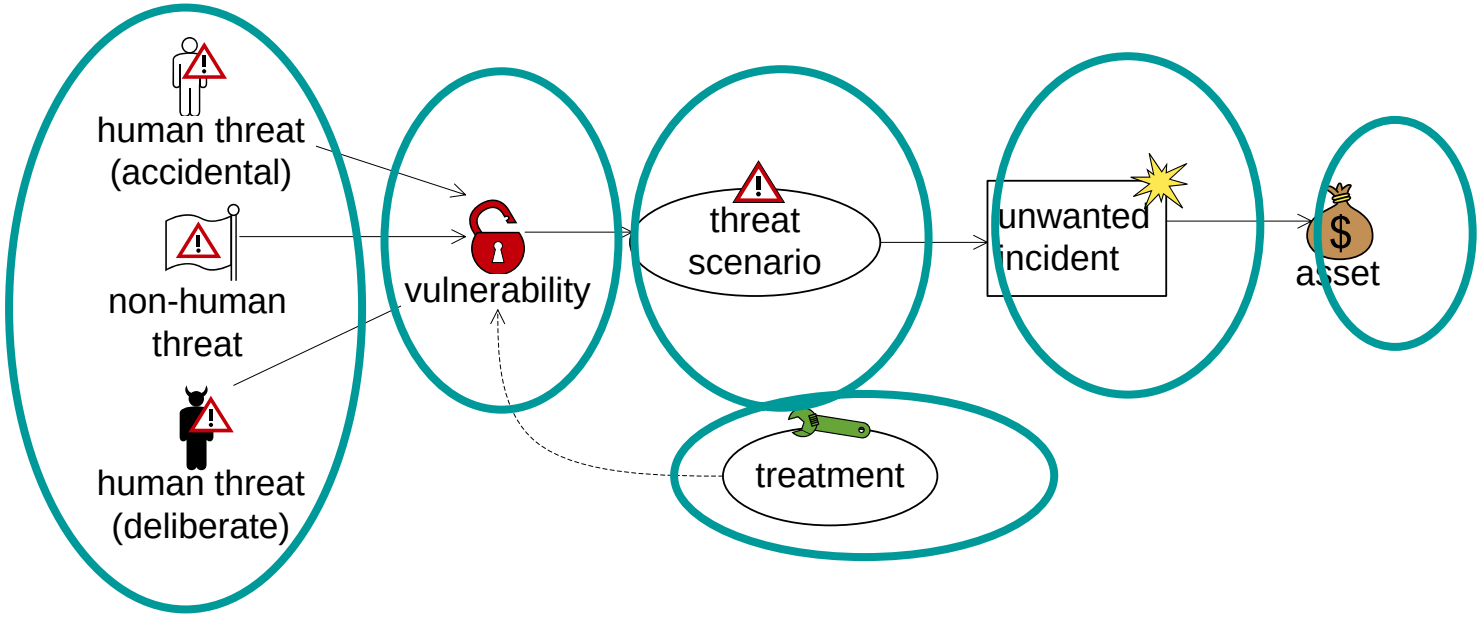
Approach

- 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

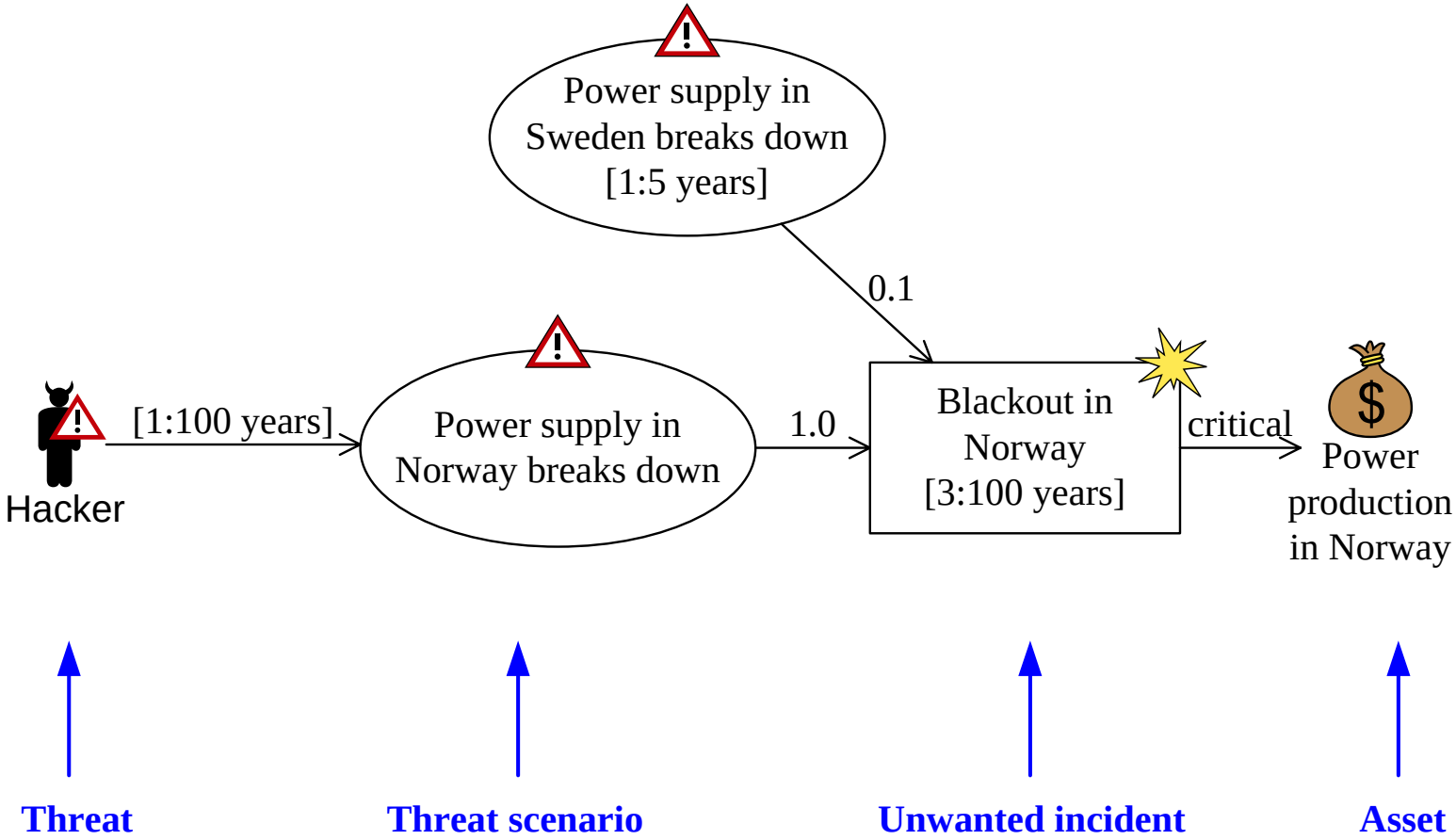
One Step Back:
What is Security Risk Analysis?



The CORAS security risk modeling language



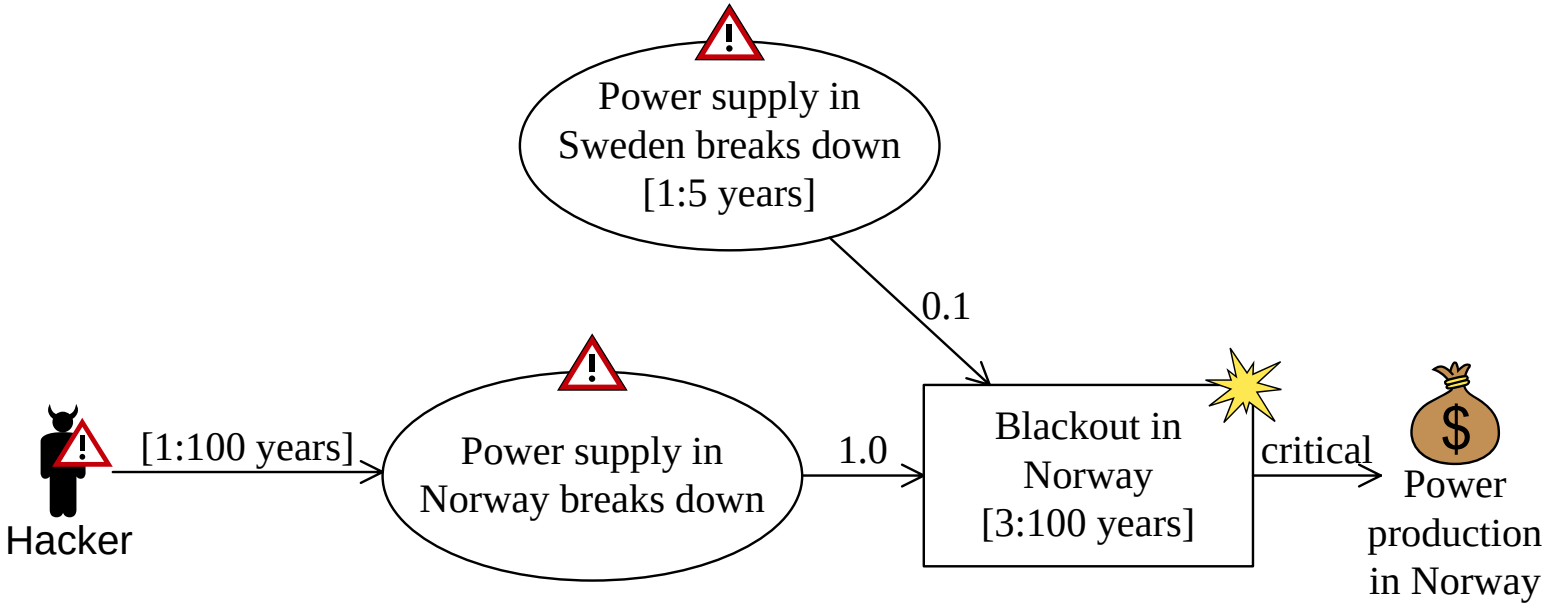
Threat Diagram



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”.

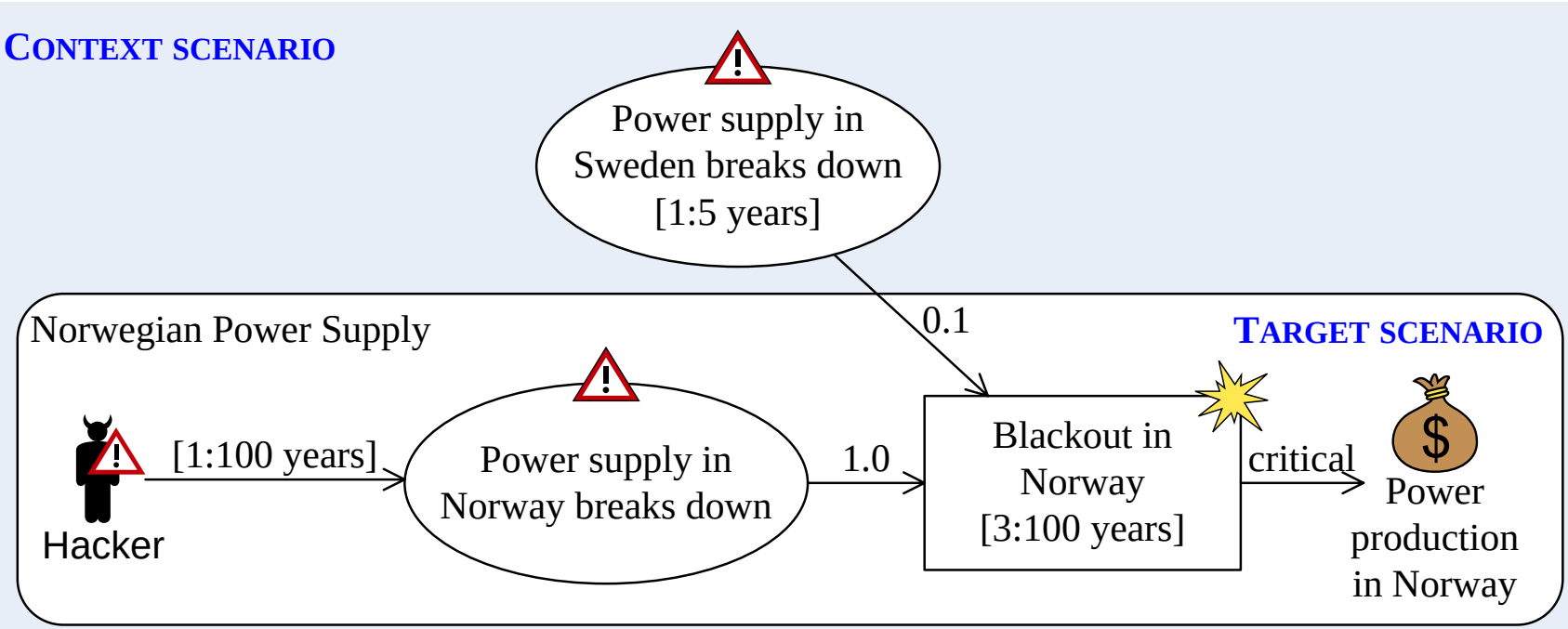
Checking Likelihoods



[1:5 years] * 0.1 = [1:50 years]

[1:100 years] + [1:50 years] = [3:100 years]

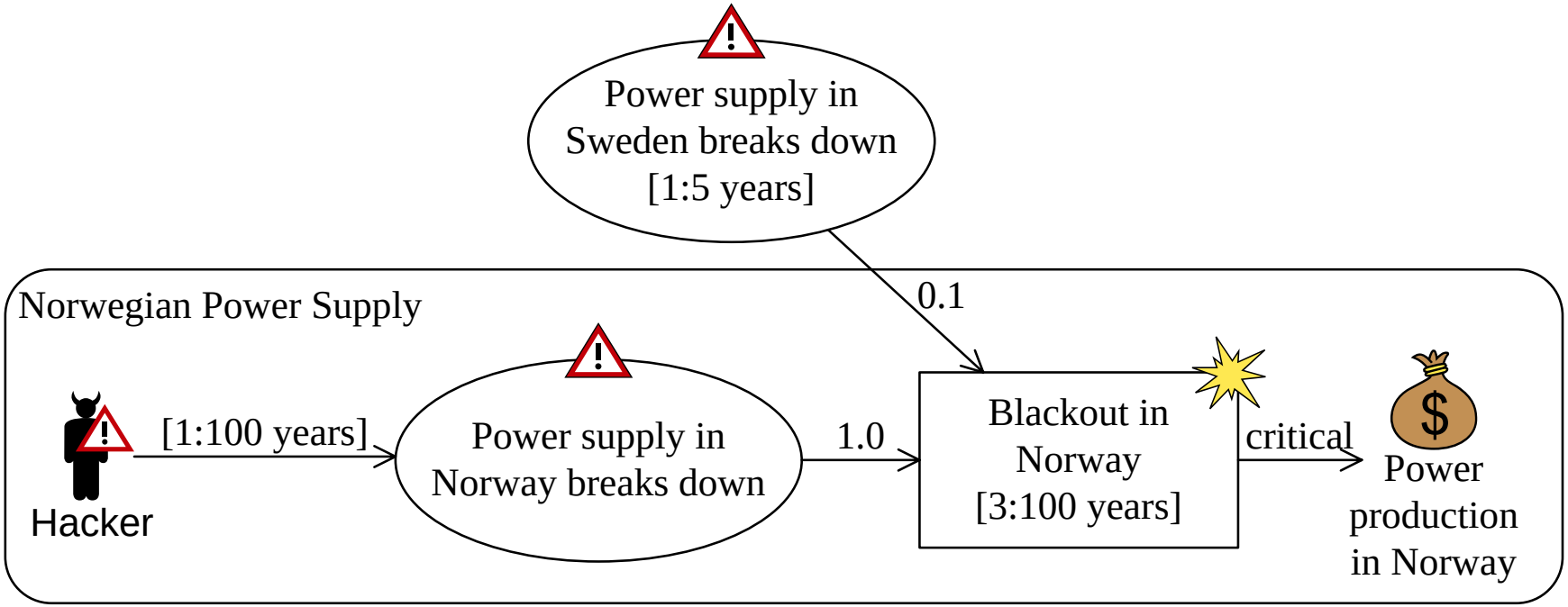
Dependent Diagram



Semantics of Dependent Diagram

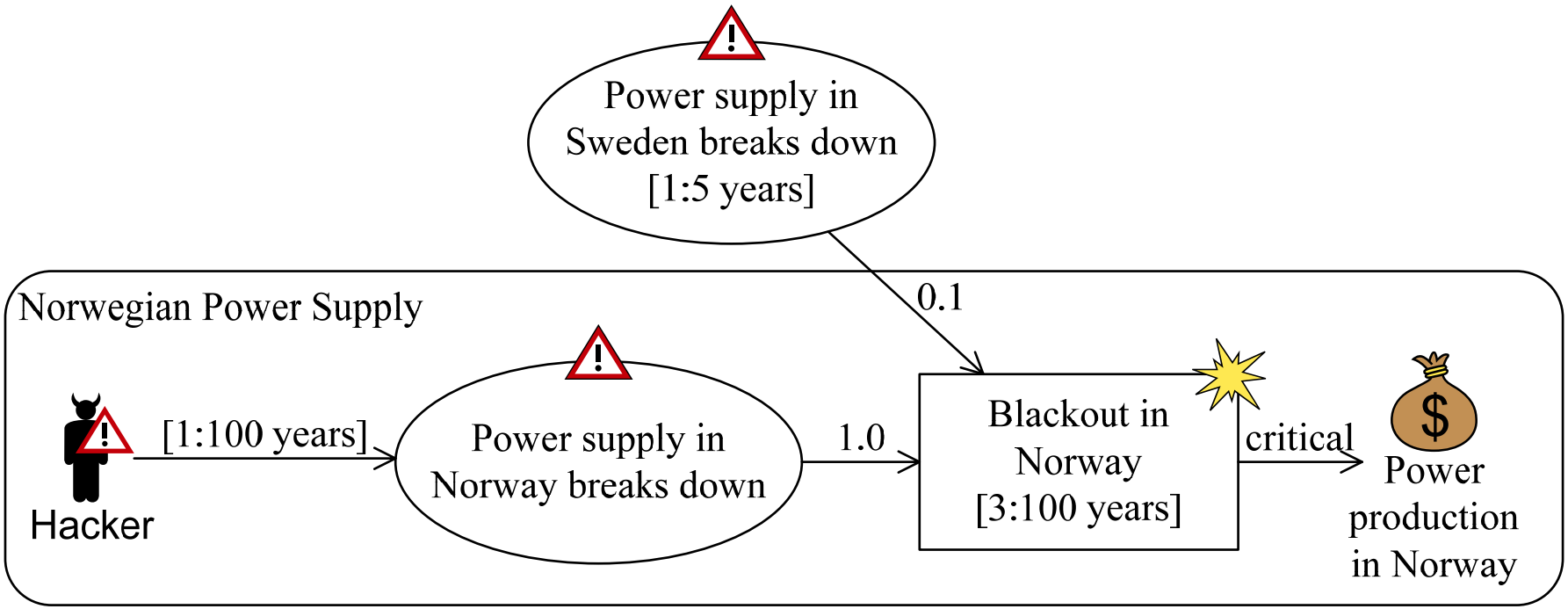
- $[[C \triangleright T]]$:=

  [[T]]
  assuming
  [[C]]
  to the extent there are explicit dependencies



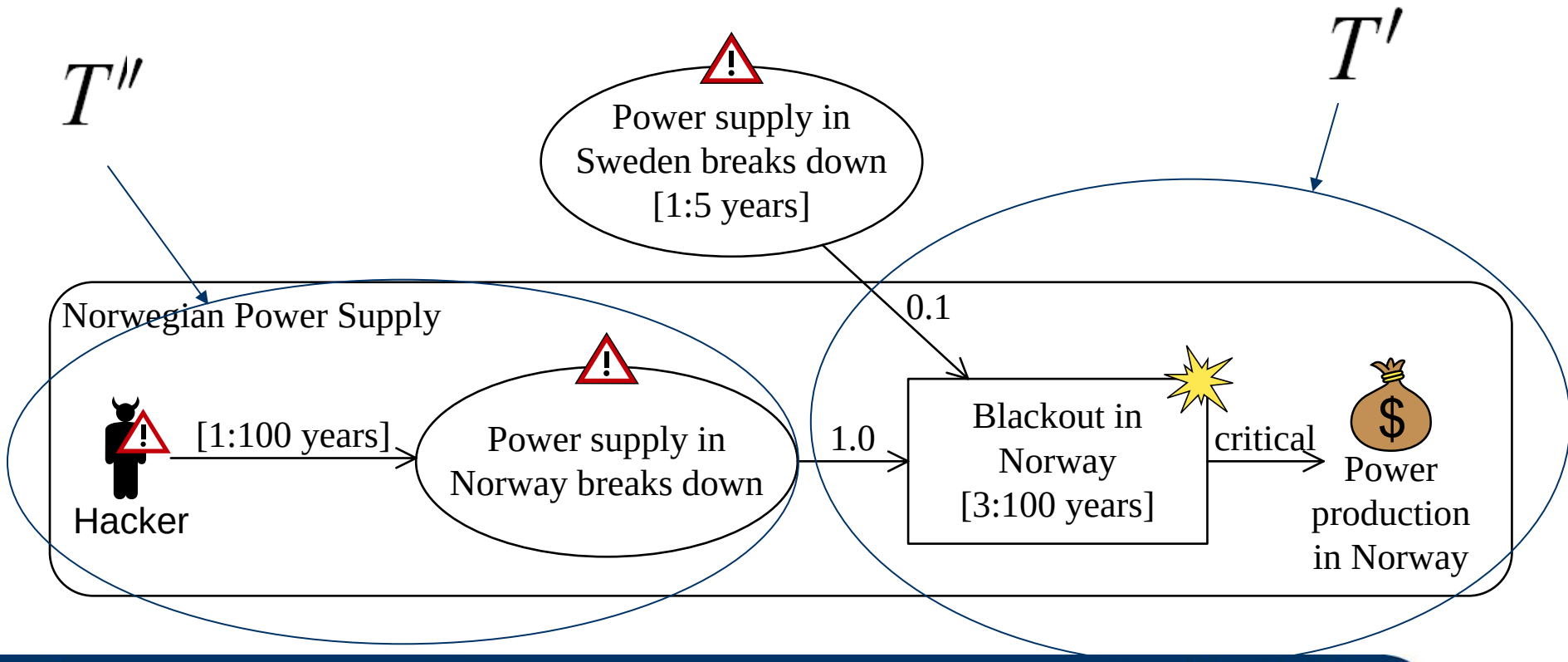
Independence of Context

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



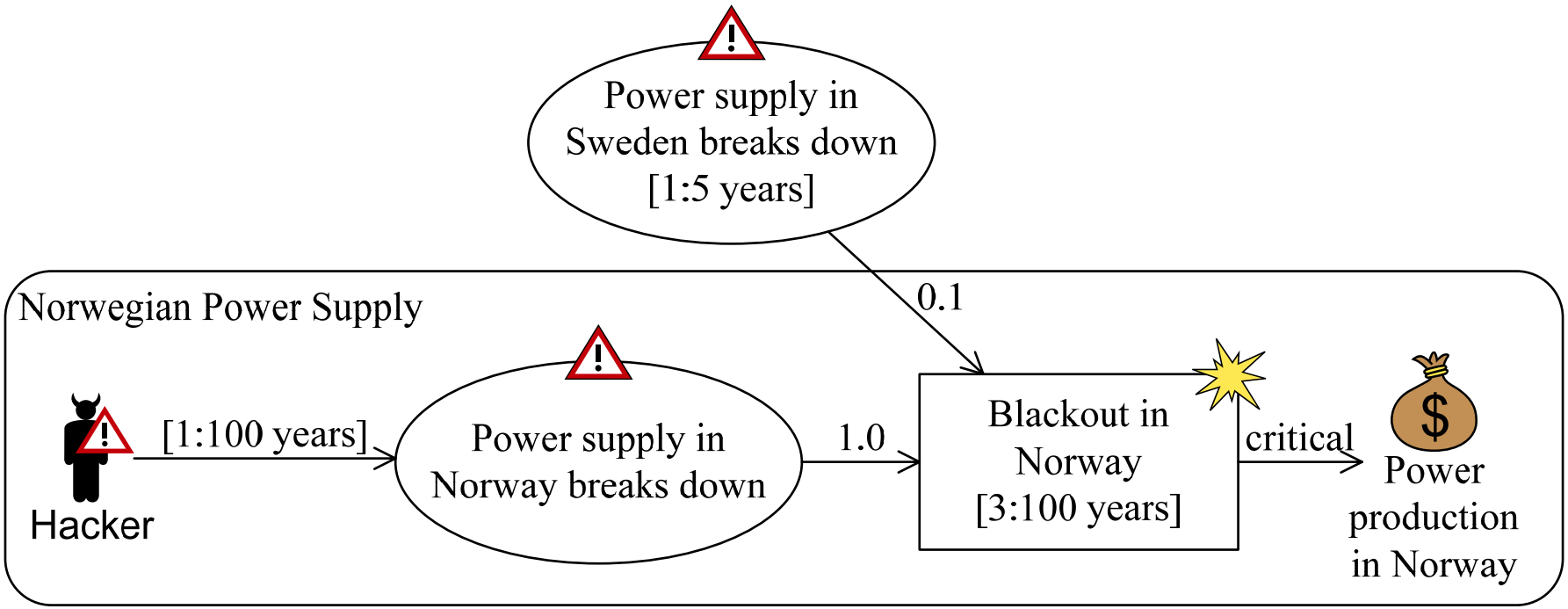
Rule of Independence

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

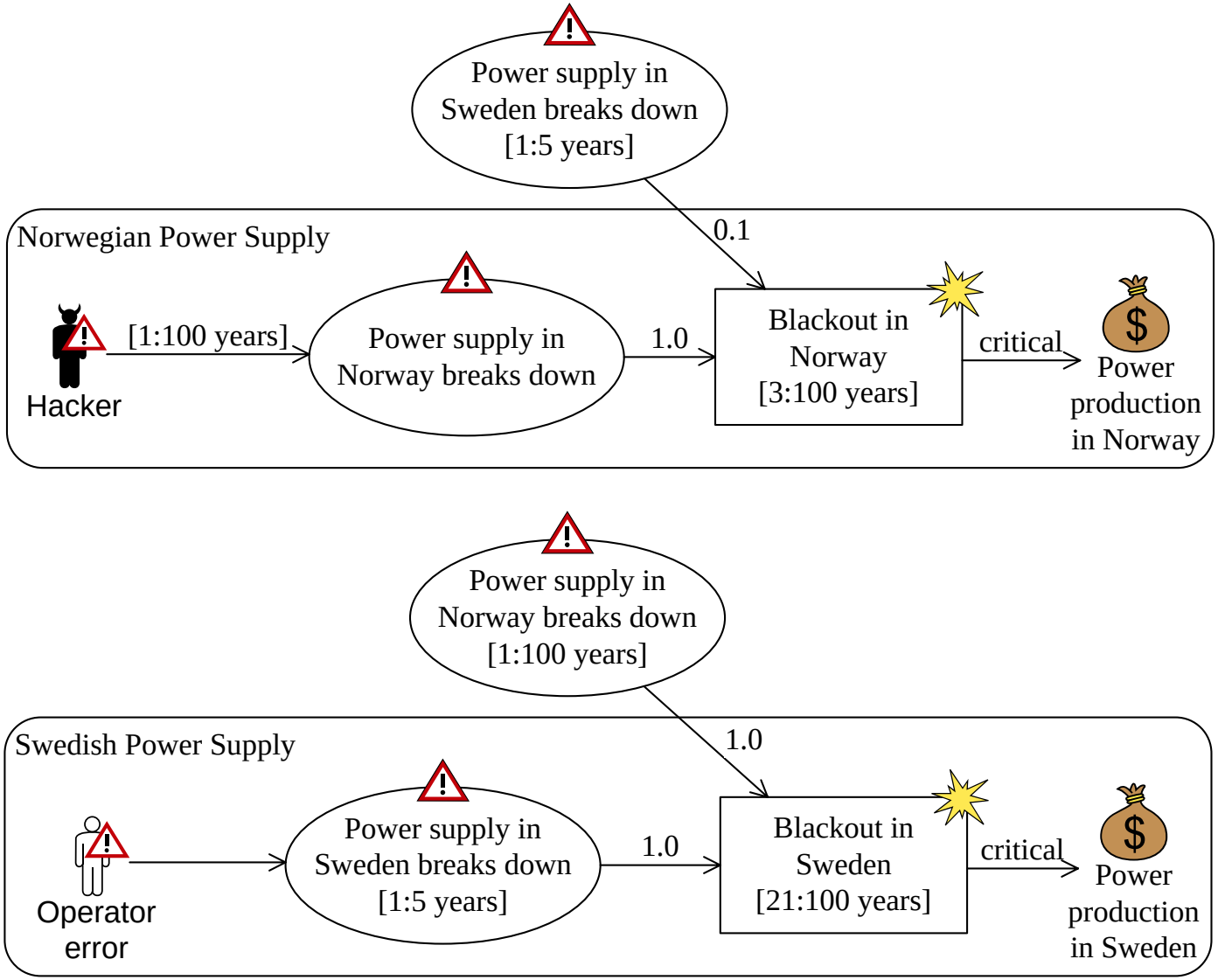


Modus Ponens

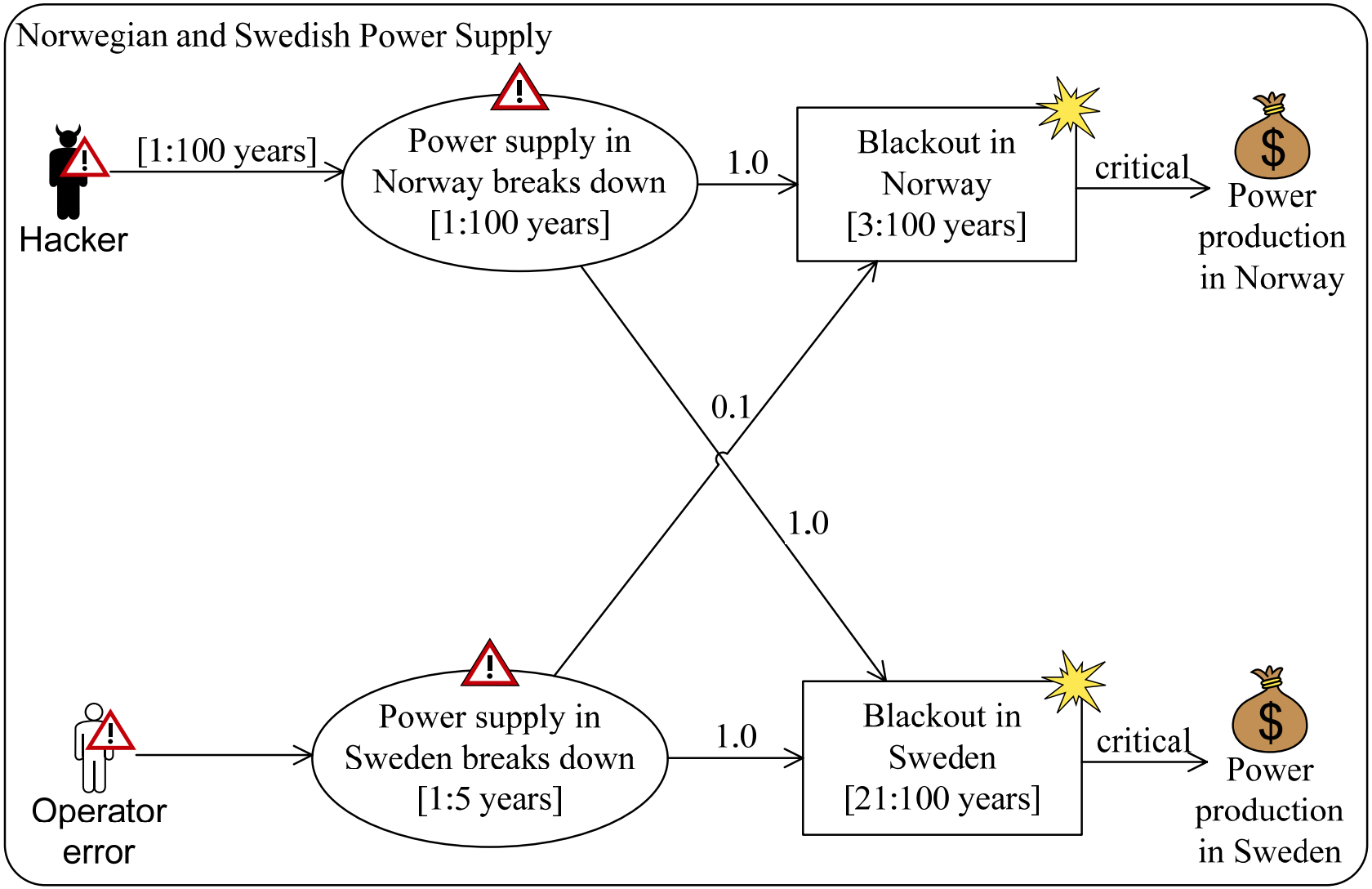
$$\frac{C \triangleright T \quad \triangleright C}{\triangleright T}$$

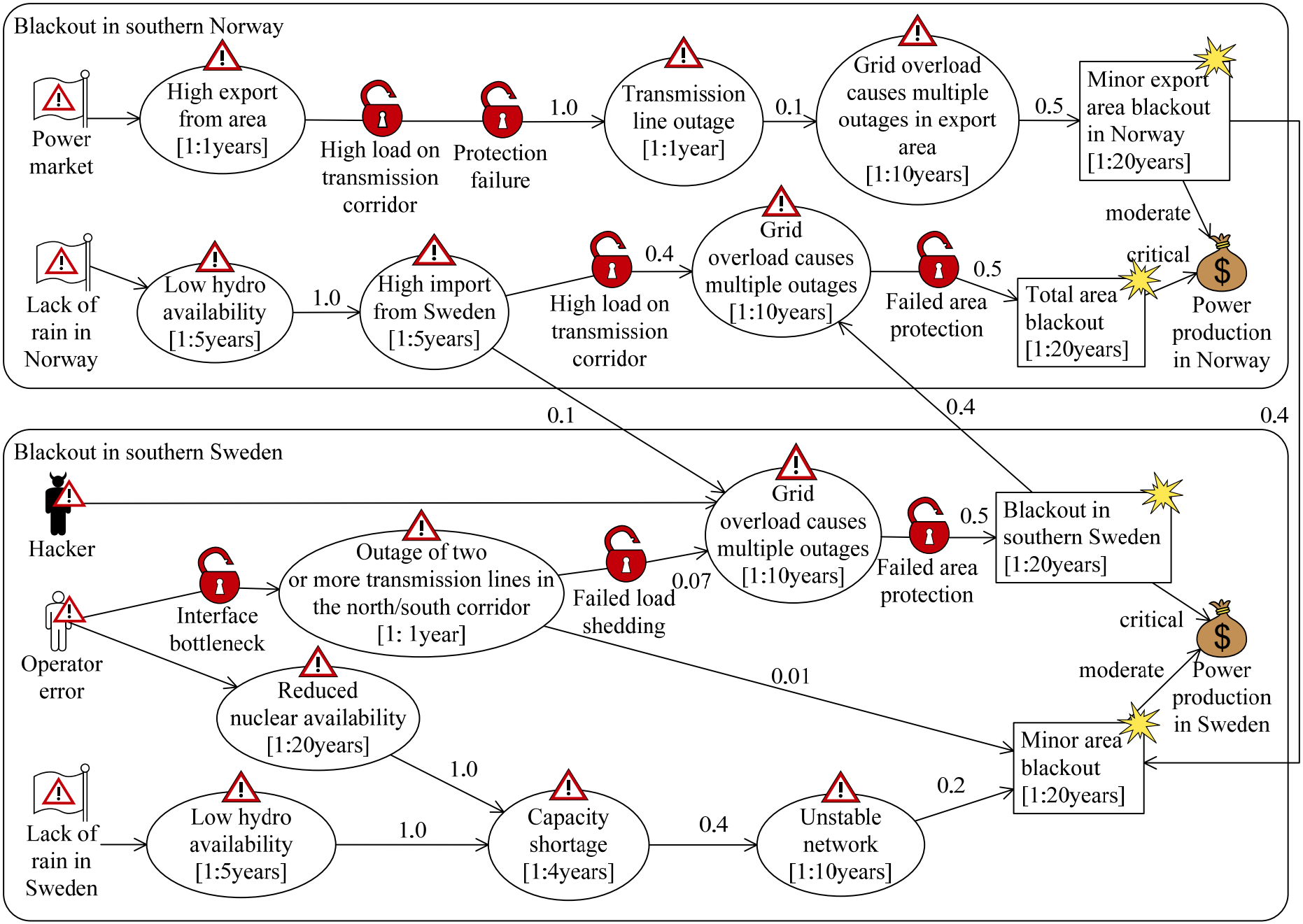


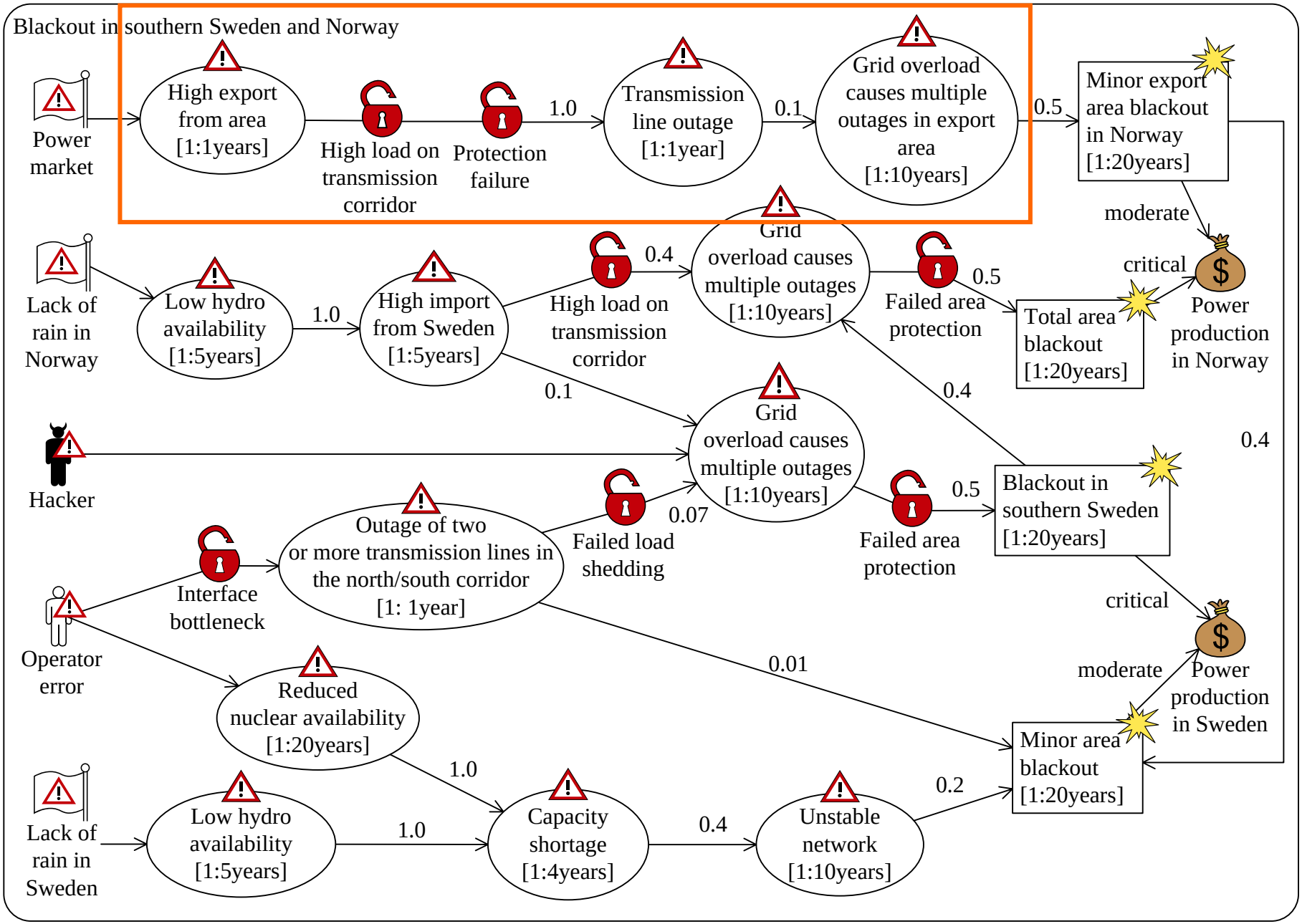
Applying the Deduction Rules



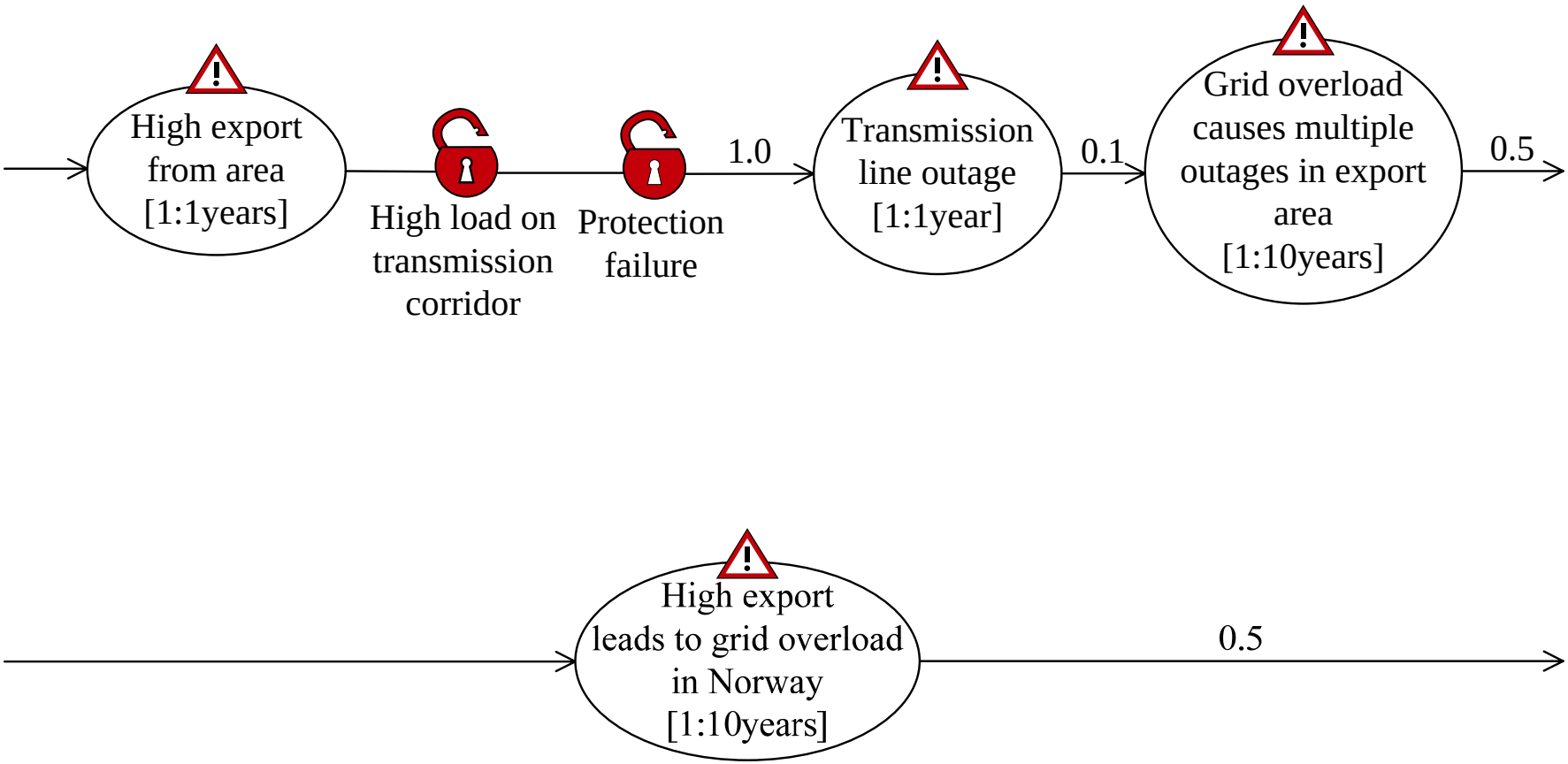
The Combined Diagram

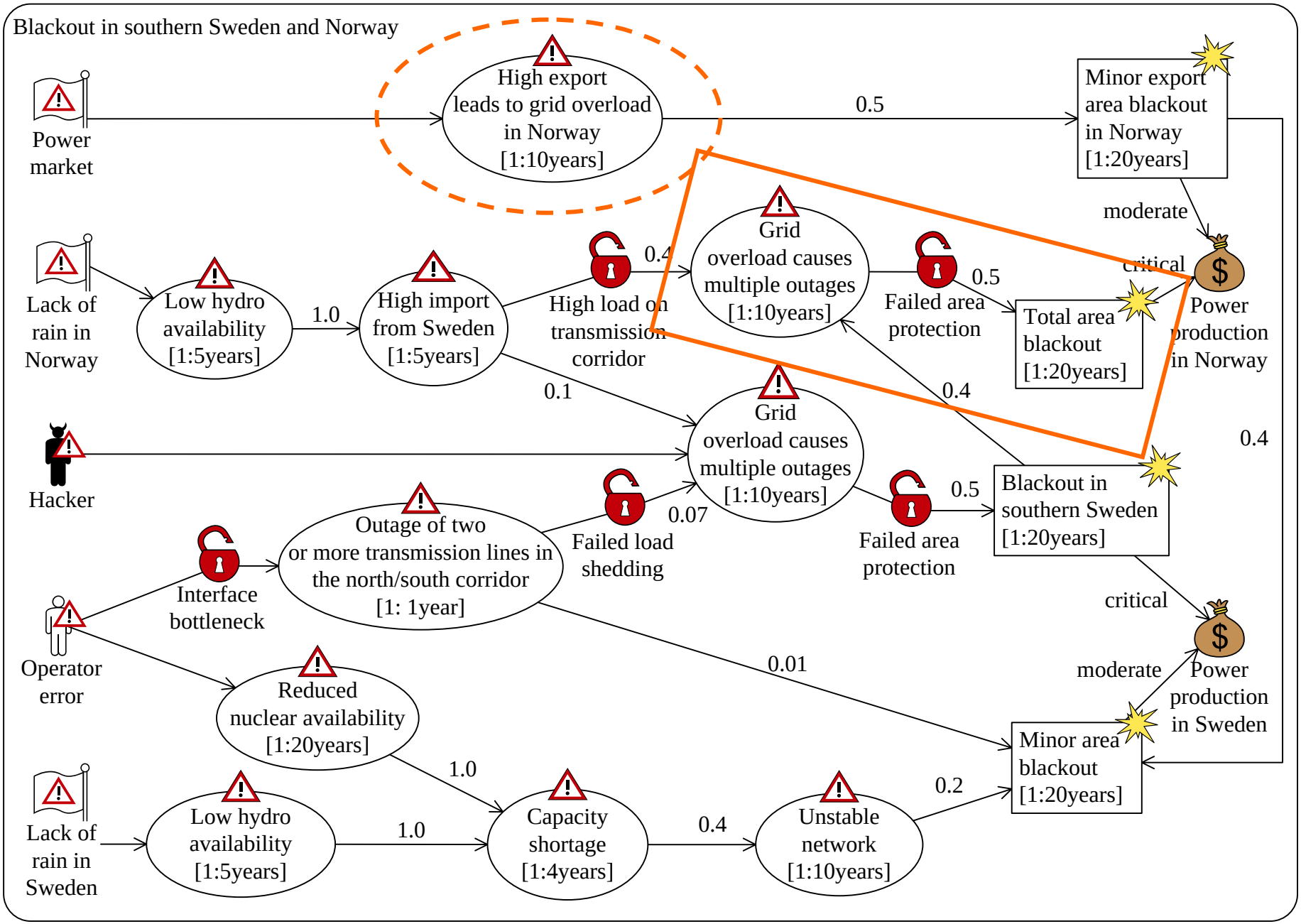



Blackout in southern Norway
Power market
High export from area [1:1years]
High load on transmission corridor
Protection failure
1.0
Transmission line outage [1:1year]
0.1
Grid overload causes multiple outages in export area [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
critical
$
Power production in Norway
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.4
Grid overload causes multiple outages [1:10years]
Failed area protection
0.5
Total area blackout [1:20years]
0.1
0.4
0.4
Blackout in southern Sweden
Hacker
Operator error
Interface bottleneck
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Grid overload causes multiple outages [1:10years]
Failed area protection
0.5
Blackout in southern Sweden [1:20years]
critical
moderate
$
Power production in Sweden
0.01
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
1.0
0.4
Unstable network [1:10years]
0.2

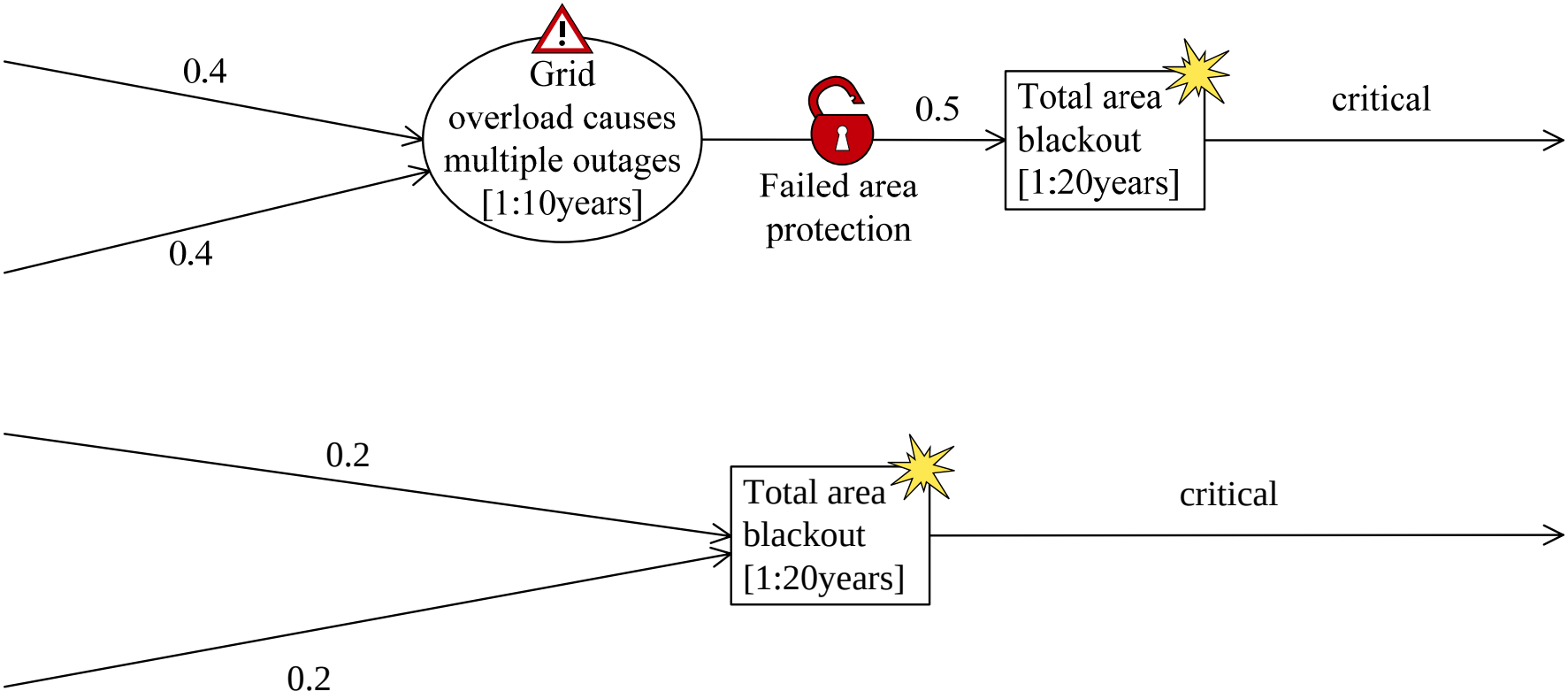

Blackout in southern Sweden and Norway
Power market
High export from area [1:1years]
High load on transmission corridor
Protection failure
1.0
Transmission line outage [1:1year]
0.1
Grid overload causes multiple outages in export area [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
critical
$
Power production in Norway
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
0.4
High load on transmission corridor
Grid overload causes multiple outages [1:10years]
0.5
Failed area protection
Total area blackout [1:20years]
0.1
0.4
Hacker
Grid overload causes multiple outages [1:10years]
0.5
Failed area protection
Blackout in southern Sweden [1:20years]
0.4
Outage of two or more transmission lines in the north/south corridor [1: 1year]
0.07
Failed load shedding
Interface bottleneck
Operator error
critical
moderate
Power production in Sweden
0.01
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
1.0
0.2
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]

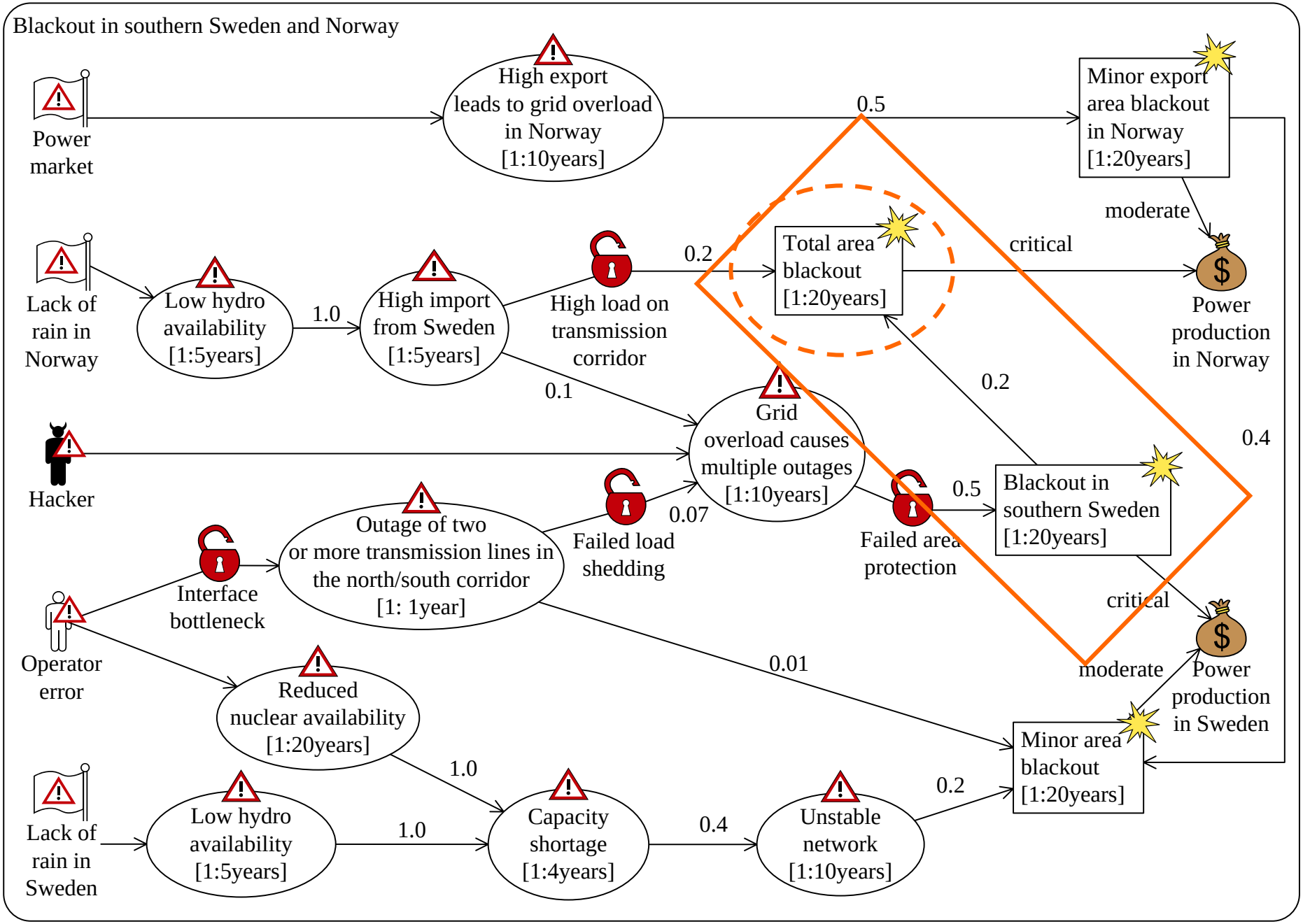
Horizontal Composition



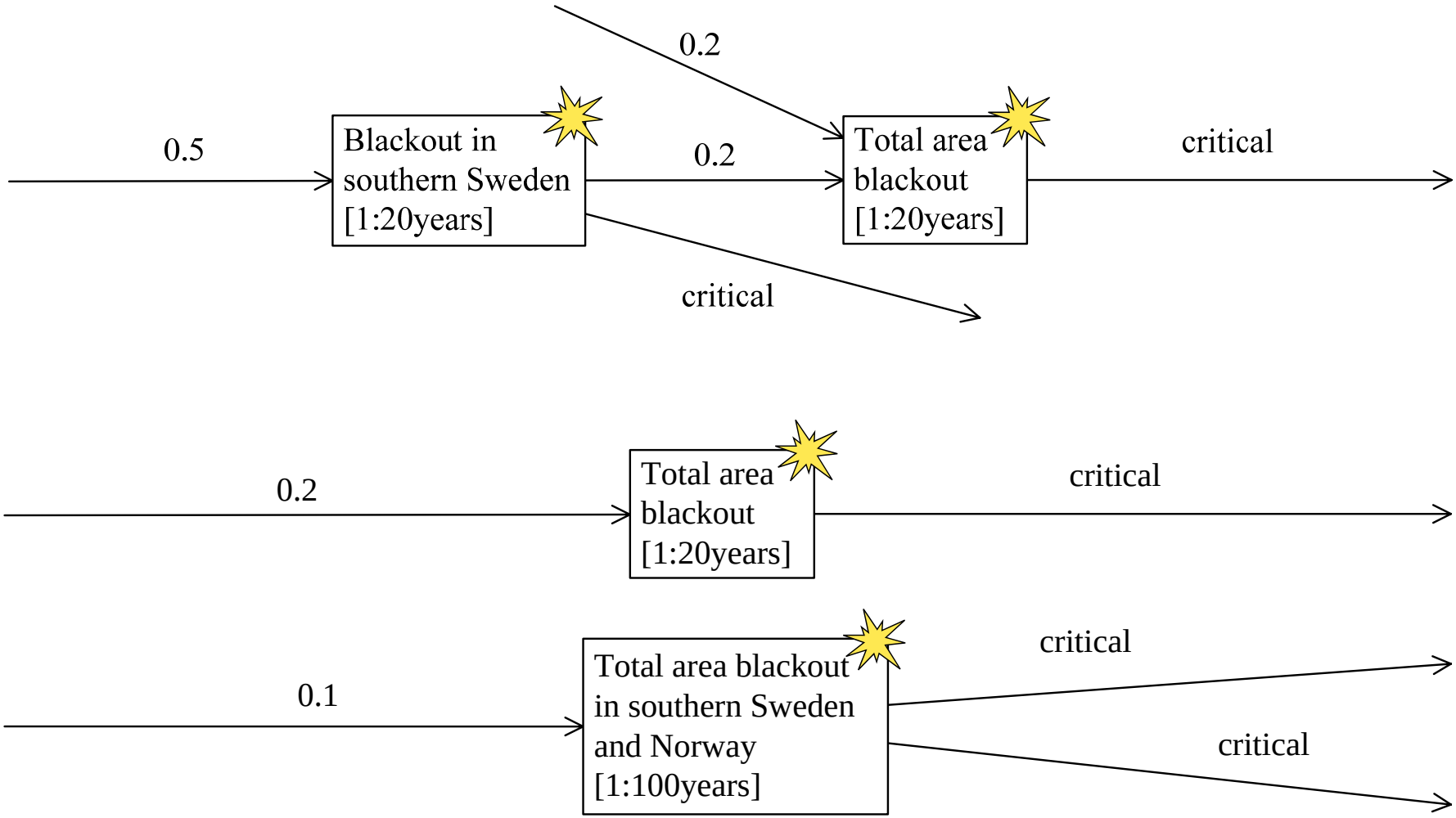

Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
critical
Power production in Norway
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
0.4
High load on transmission corridor
Grid overload causes multiple outages [1:10years]
Failed area protection
0.5
Total area blackout [1:20years]
0.1
0.4
Hacker
Grid overload causes multiple outages [1:10years]
0.4
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Failed area protection
0.5
Blackout in southern Sweden [1:20years]
Interface bottleneck
critical
Operator error
0.01
moderate
Power production in Sweden
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
1.0
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]
0.2

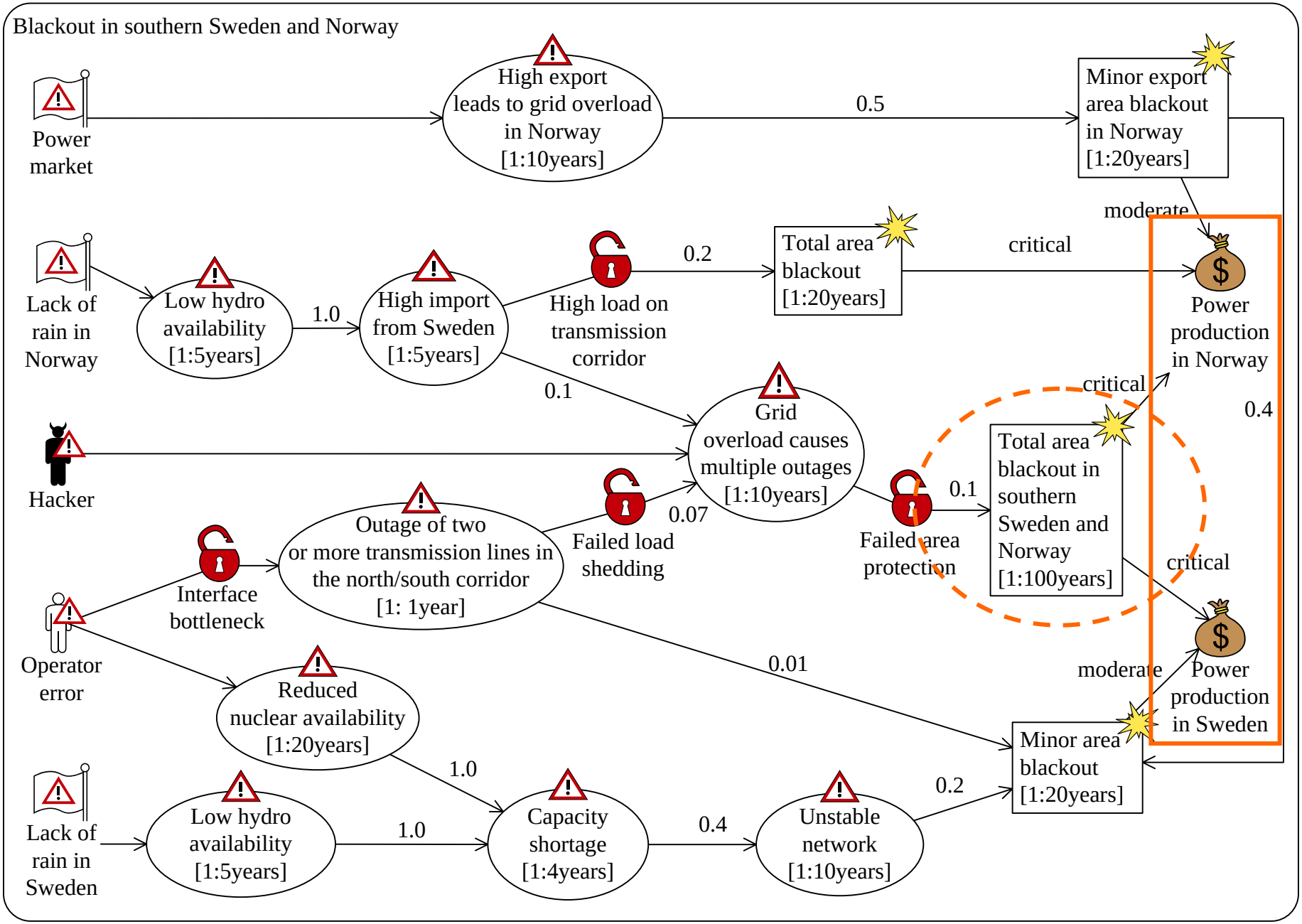
Horizontal Composition



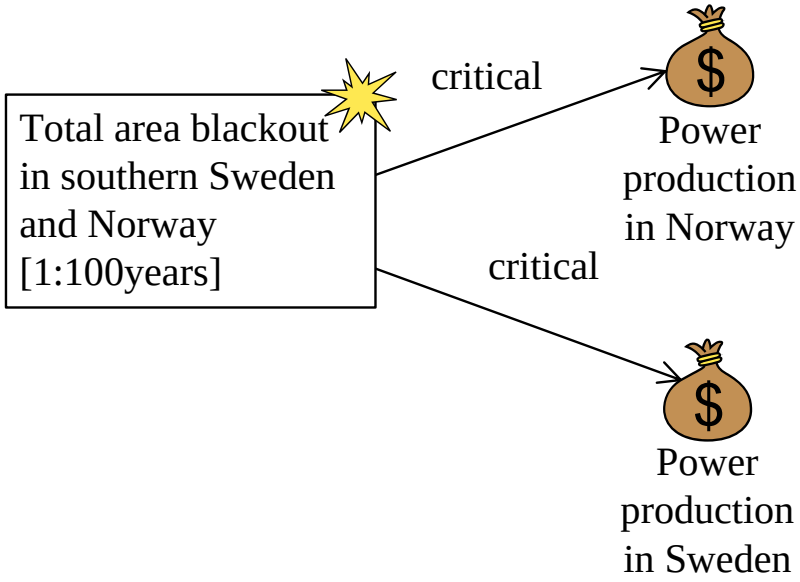

Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
Power production in Norway
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
0.1
Grid overload causes multiple outages [1:10years]
0.2
0.4
Hacker
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Failed area protection
0.5
Blackout in southern Sweden [1:20years]
Interface bottleneck
critical
Operator error
0.01
moderate
Power production in Sweden
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
1.0
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]
0.2

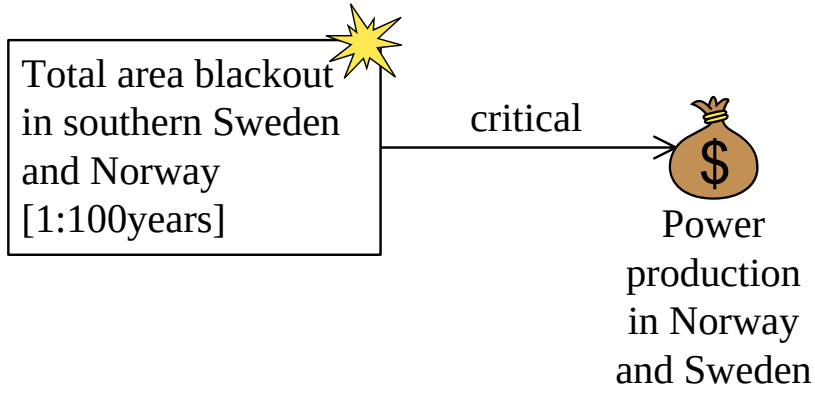
Horizontal Composition

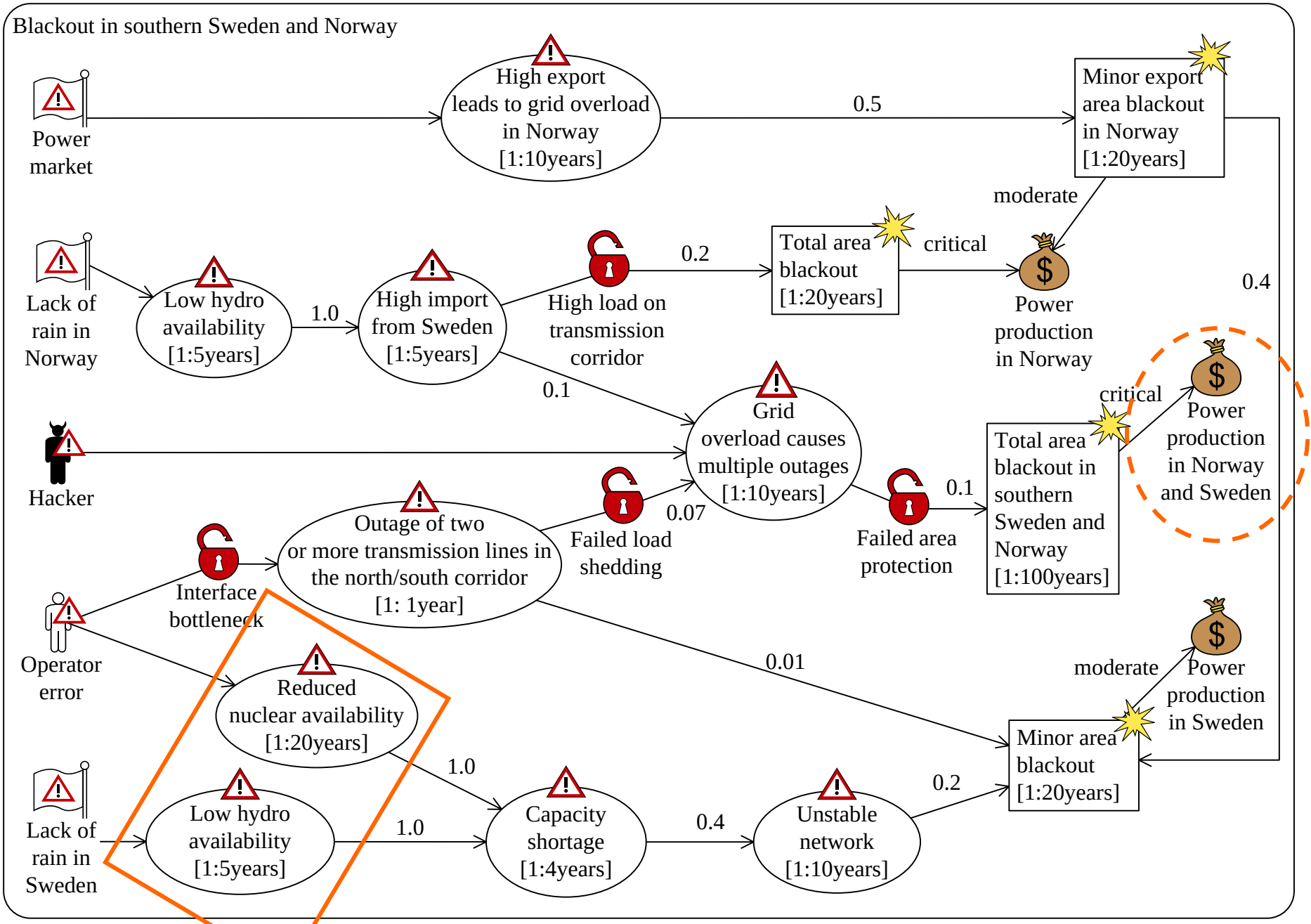



Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
Power production in Norway
0.4
0.1
Hacker
Grid overload causes multiple outages [1:10years]
critical
Total area blackout in southern Sweden and Norway [1:100years]
0.1
Failed area protection
Failed load shedding
0.07
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Interface bottleneck
Operator error
critical
Power production in Sweden
moderate
0.01
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
1.0
0.2
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]

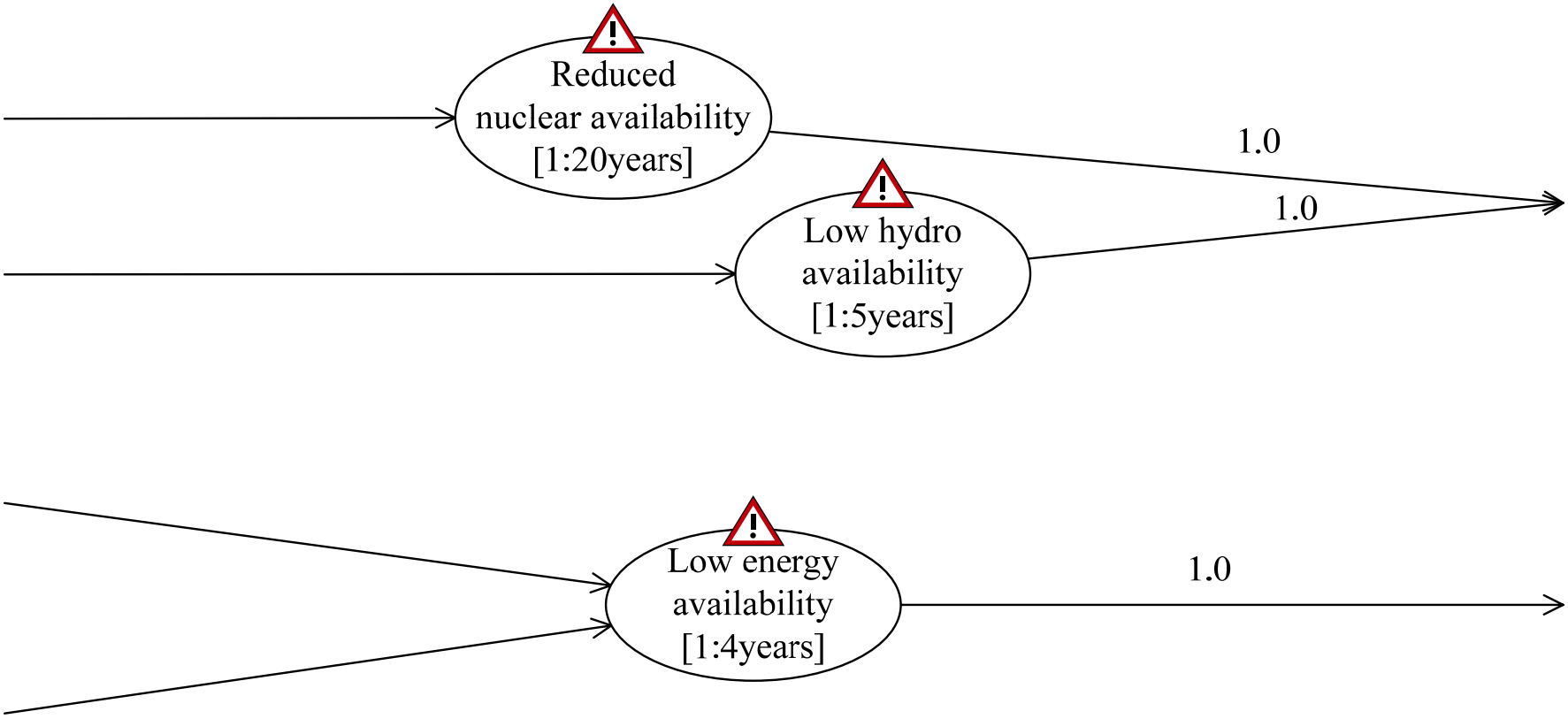
Asset Composition

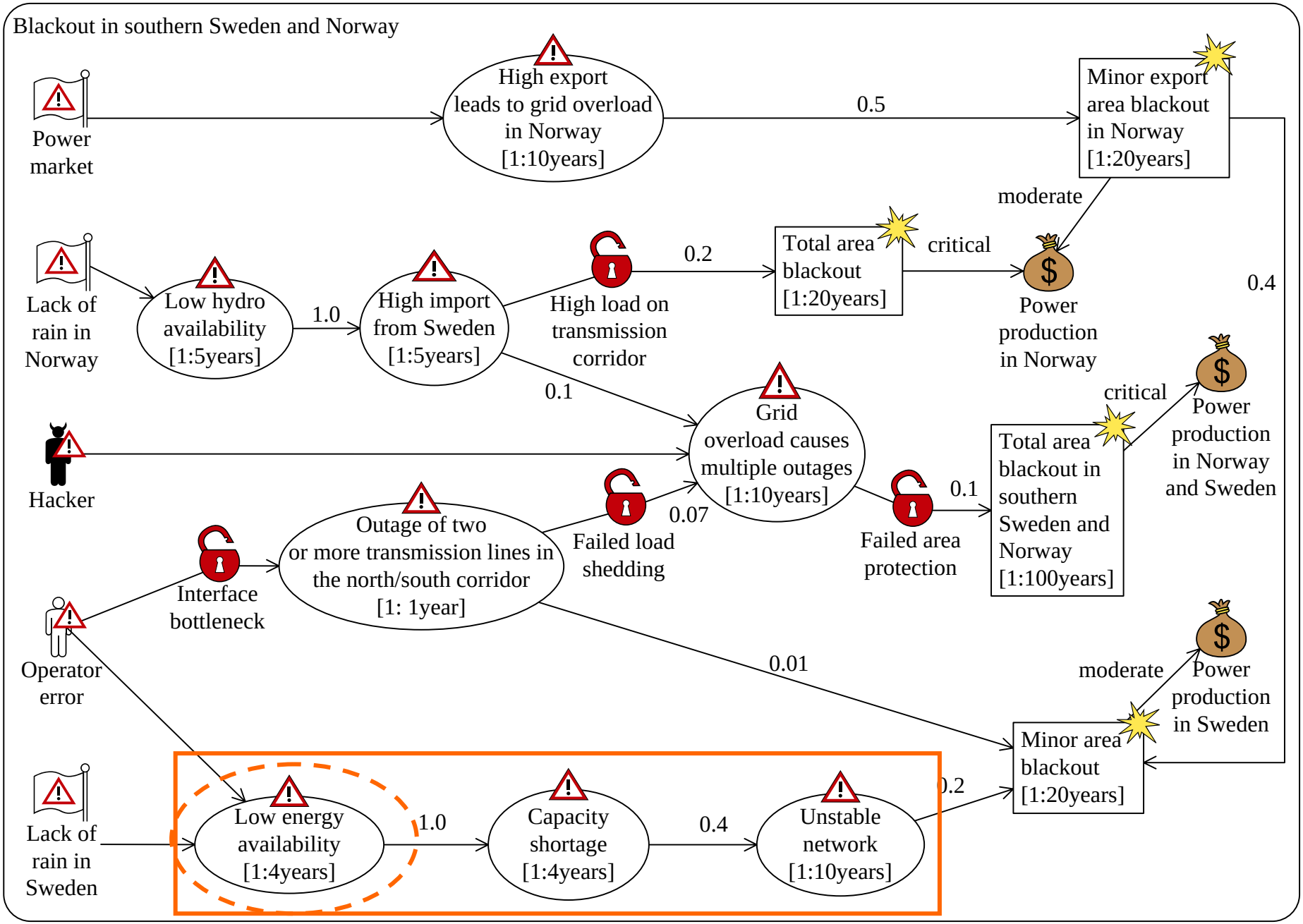




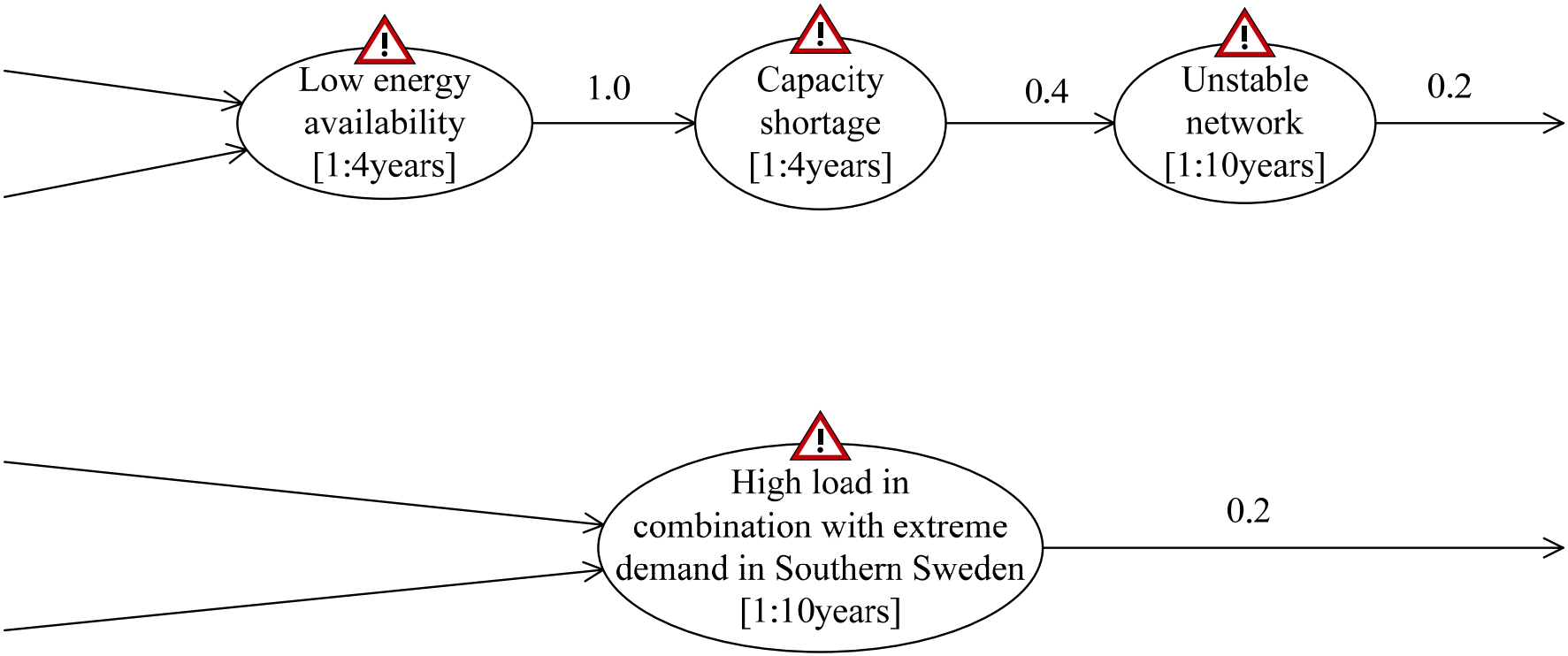

Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
Power production in Norway
0.4
0.1
Grid overload causes multiple outages [1:10years]
critical
Power production in Norway and Sweden
Hacker
Total area blackout in southern Sweden and Norway [1:100years]
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Failed area protection
0.1
Interface bottleneck
Operator error
0.01
moderate
Power production in Sweden
Reduced nuclear availability [1:20years]
Minor area blackout [1:20years]
1.0
Lack of rain in Sweden
Low hydro availability [1:5years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]
0.2

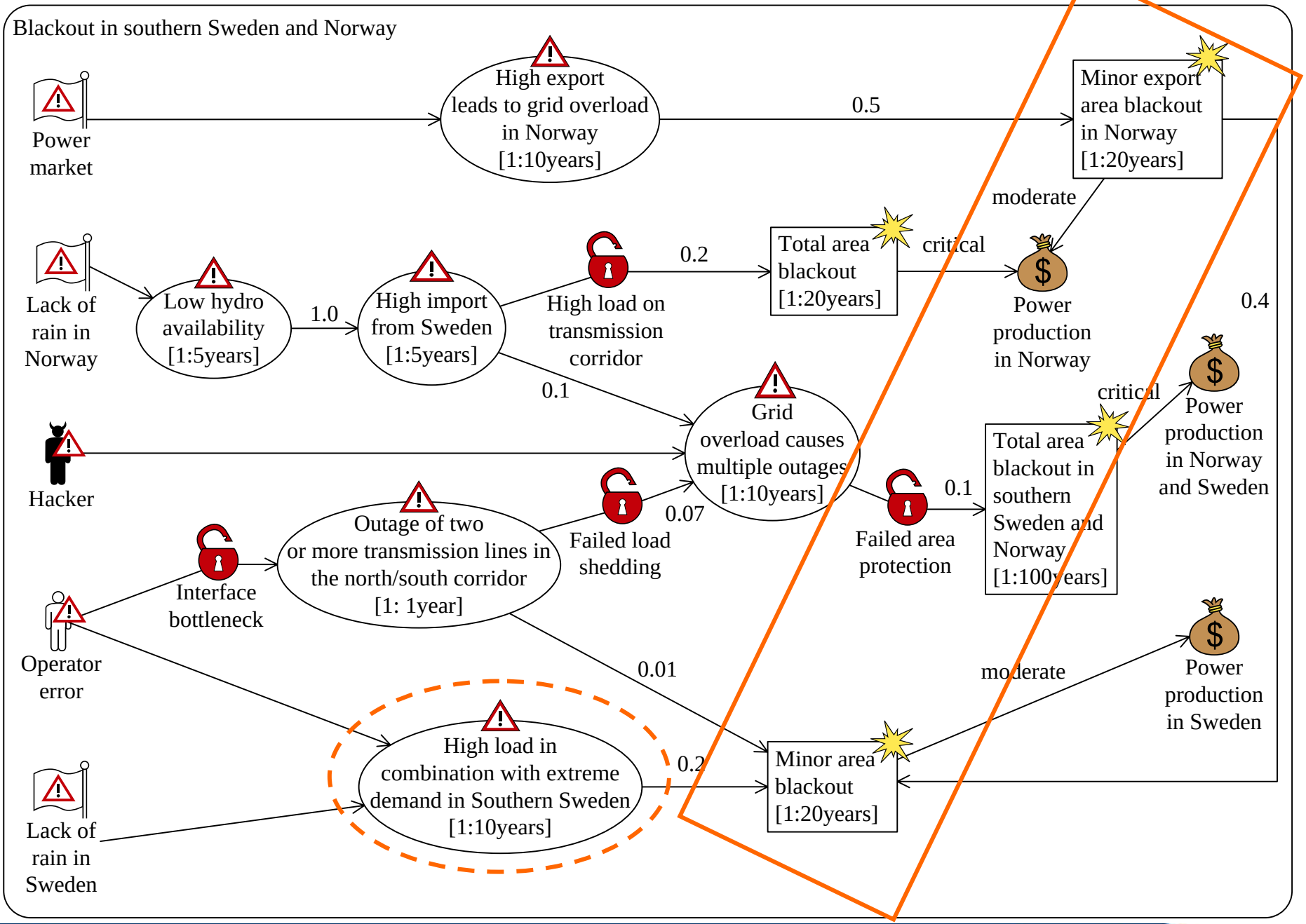
Vertical Composition



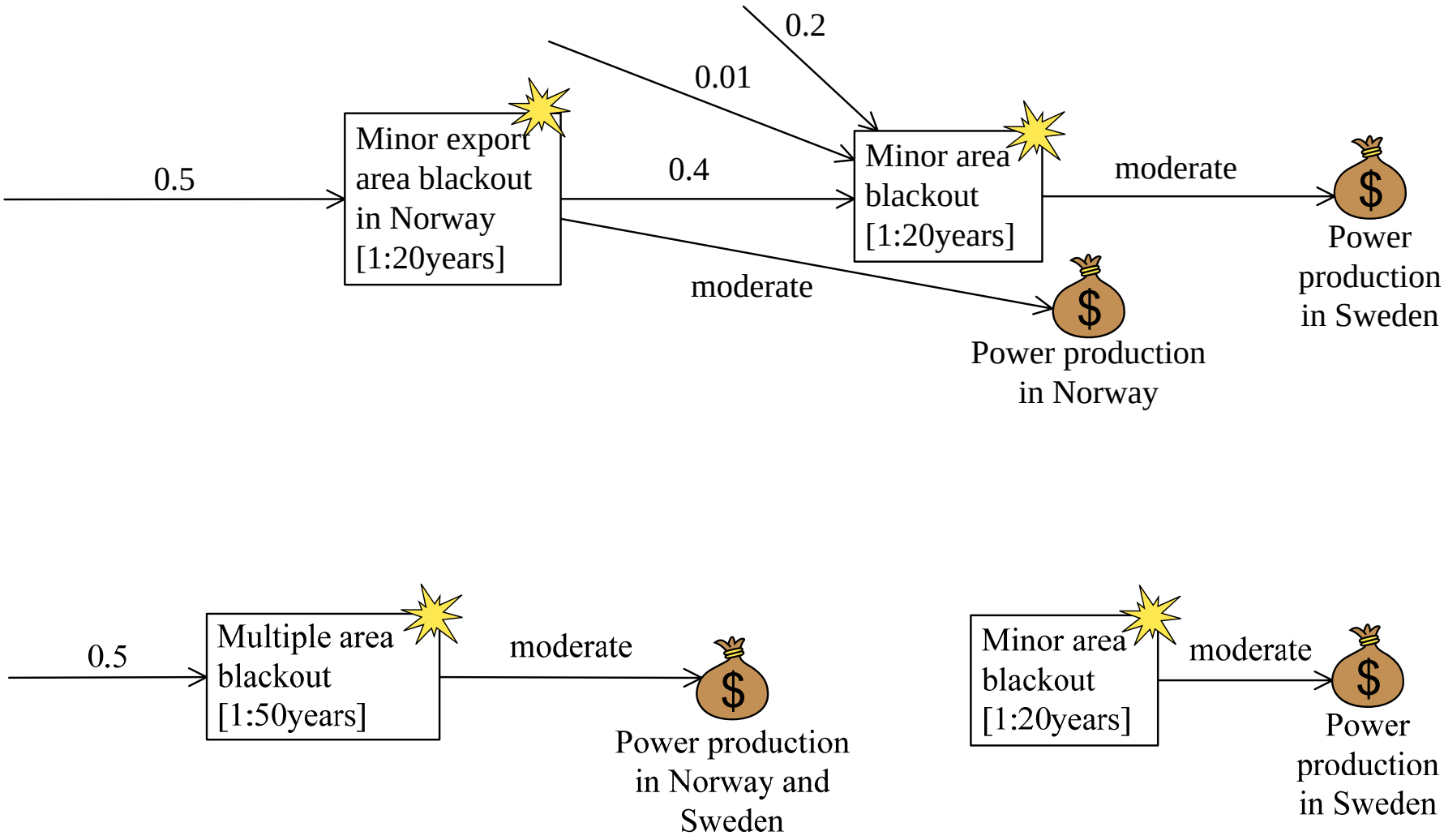

Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
Power production in Norway
0.4
0.1
Hacker
Grid overload causes multiple outages [1:10years]
critical
Power production in Norway and Sweden
Total area blackout in southern Sweden and Norway [1:100years]
0.1
Failed area protection
0.07
Failed load shedding
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Interface bottleneck
Operator error
0.01
moderate
Power production in Sweden
Minor area blackout [1:20years]
0.2
Lack of rain in Sweden
Low energy availability [1:4years]
1.0
Capacity shortage [1:4years]
0.4
Unstable network [1:10years]

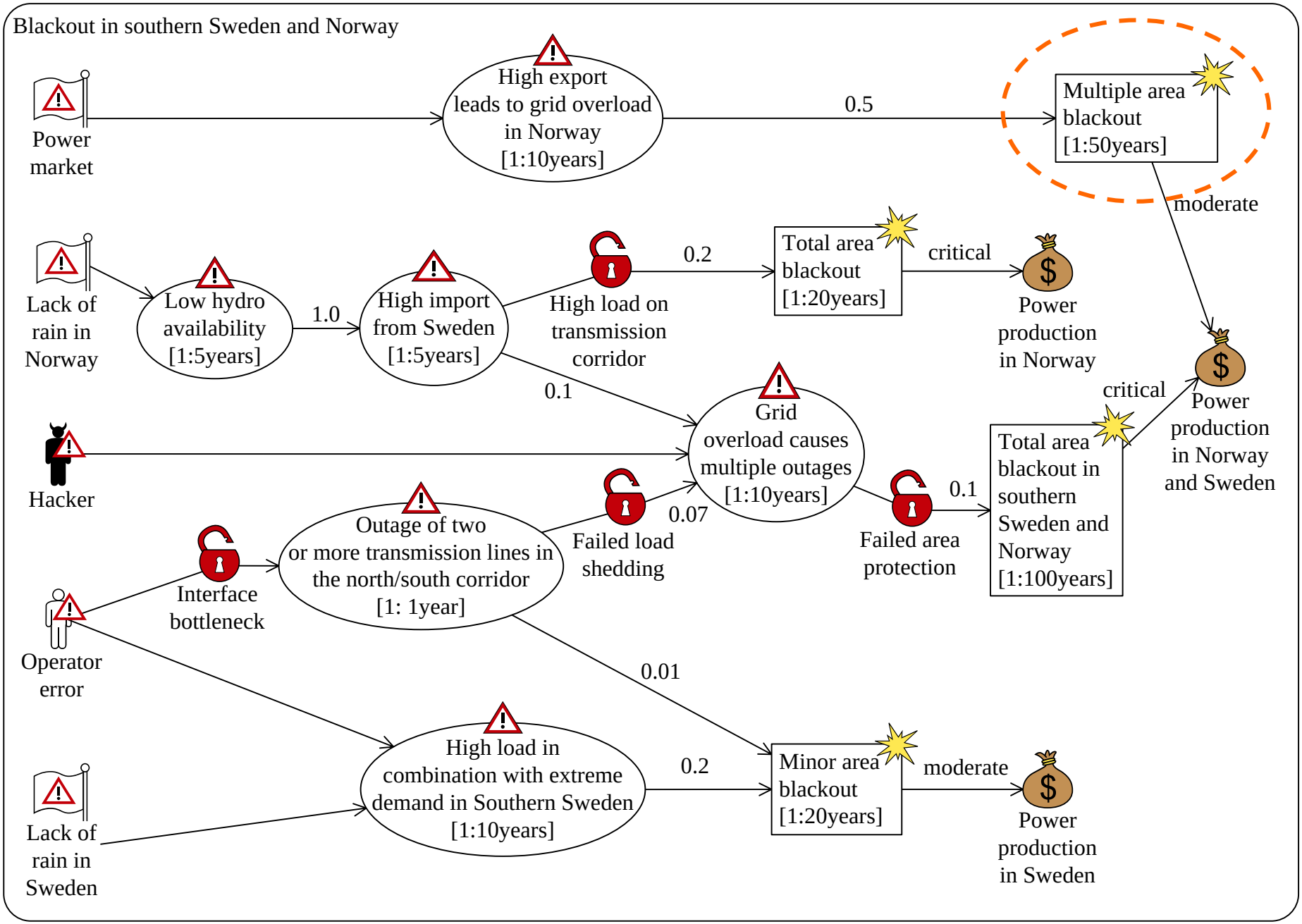
Horizontal Composition




Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Minor export area blackout in Norway [1:20years]
moderate
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
Power production in Norway
0.4
0.1
Grid overload causes multiple outages [1:10years]
critical
Power production in Norway and Sweden
Hacker
Total area blackout in southern Sweden and Norway [1:100years]
0.1
Failed area protection
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Interface bottleneck
Operator error
0.01
moderate
Power production in Sweden
High load in combination with extreme demand in Southern Sweden [1:10years]
0.2
Minor area blackout [1:20years]
Lack of rain in Sweden

Horizontal & Asset Composition




Blackout in southern Sweden and Norway
Power market
High export leads to grid overload in Norway [1:10years]
0.5
Multiple area blackout [1:50years]
moderate
Lack of rain in Norway
Low hydro availability [1:5years]
1.0
High import from Sweden [1:5years]
High load on transmission corridor
0.2
Total area blackout [1:20years]
critical
Power production in Norway
0.1
Hacker
Grid overload causes multiple outages [1:10years]
critical
Power production in Norway and Sweden
Total area blackout in southern Sweden and Norway [1:100years]
0.1
Failed area protection
Outage of two or more transmission lines in the north/south corridor [1: 1year]
Failed load shedding
0.07
Interface bottleneck
Operator error
0.01
High load in combination with extreme demand in Southern Sweden [1:10years]
0.2
Minor area blackout [1:20years]
moderate
Lack of rain in Sweden
Power production in Sweden

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