



Solution to exercises

17 October, 2008



Answers to questionnaire

- Correct: Selecting true for the wine-red alternatives, false for the blue

1a b c d e f g h i

- Types of assets:
- Information
 - Documents (e.g. contracts)
 - Data base
- Software
- Physical
 - Hardware
 - Communication equipment
- Services (e.g. computational services)
- Personnel
- The reputation and image of an organization



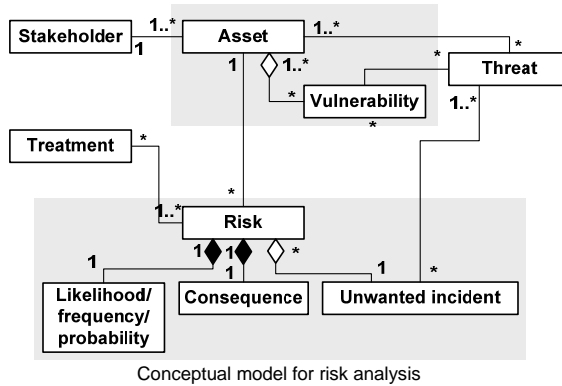


Answers to questionnaire

Correct:

- True for the wine-red alternatives ■
- False for the blue alternatives ■

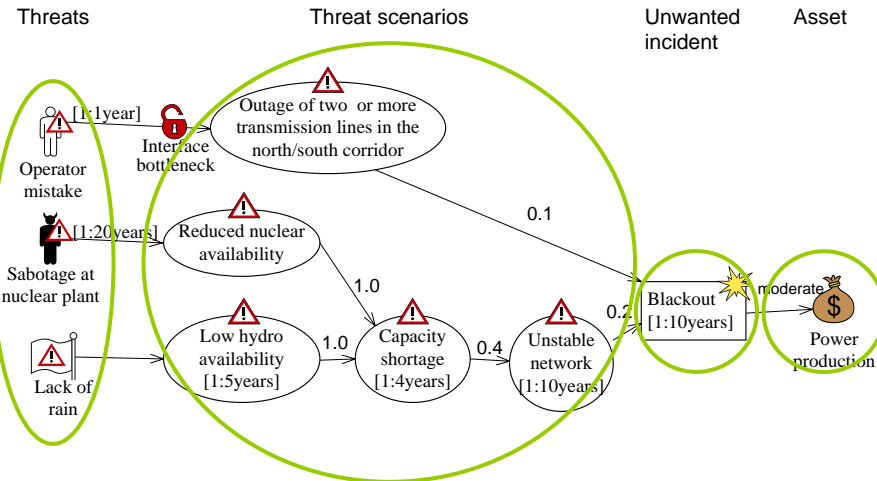
1a	b	c	d	e	f	g	h	i
2a	b	c	d					
3a	b	c						
4a	b	c	d	e	f	g	h	
5a	b	c	d	e	f	g		
6a	b	c	d	e				
7a	b	c	d					
8a	b	c						
9a	b	c	d					
10a	b	c	d					
11a	b	c						
12a	b	c						
13a	b	c	d					
14a	b	c	d	e				



INF 5150



Exercise 1: Syntax of threat diagrams - vertices



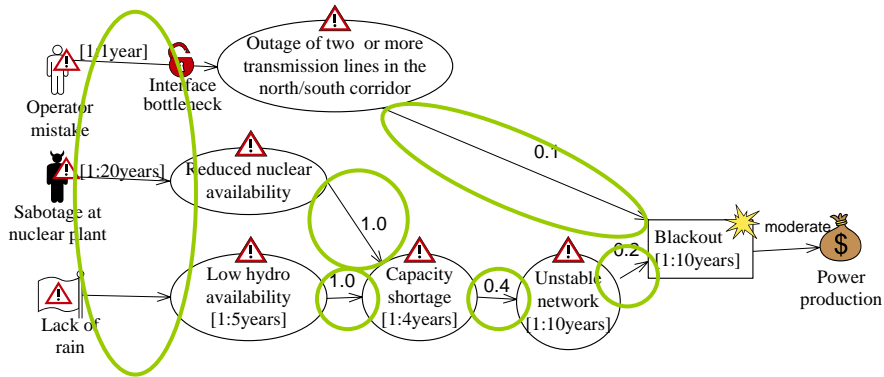
INF 5150



Exercise 2: Syntax of threat diagrams - relations

Initiate relations

Leads-to relations



Exercise 3: Translation – vertices

- 'Operator mistake' is an accidental threat.
- Threat scenario 'Outage of two or more transmission lines in the north/south corridor' occurs with undefined likelihood.
- 'Sabotage at nuclear plant' is a deliberate threat.
- Threat scenario 'Reduced nuclear availability' occurs with undefined likelihood.
- 'Lack of rain' is a non-human threat.
- Threat scenario 'Low hydro availability' occurs with likelihood '1:5 years'.
- Threat scenario 'Capacity shortage' occurs with likelihood '1:4 years'.
- Threat scenario 'Unstable network' occurs with likelihood '1:10 years'.
- Unwanted incident 'Blackout' occurs with likelihood '1:10 years'.
- 'Power production' is an asset.



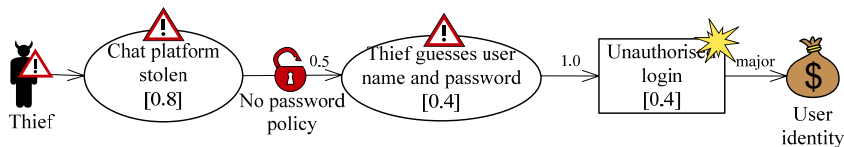
Exercise 3: Translation – relations

- 'Operator mistake' exploits vulnerability 'Interface bottleneck' to initiate 'Outage of two or more transmission lines in the north/south corridor' with likelihood '1:1 year'.
- 'Outage of two or more transmission lines in the north/south corridor' leads to 'Blackout' with conditional likelihood '0.1'.
- 'Sabotage at nuclear plant' initiates 'Reduced nuclear availability' with likelihood '1:20 years'.
- 'Reduced nuclear availability' leads to 'Capacity shortage' with conditional likelihood '1.0'.
- 'Lack of rain' initiates 'Low hydro availability' with undefined likelihood.
- 'Low hydro availability' leads to 'Capacity shortage' with conditional likelihood '1.0'.
- 'Capacity shortage' leads to 'Unstable network' with conditional likelihood '0.4'.
- 'Unstable network' leads to 'Minor area blackout' with conditional likelihood '0.2'.
- 'Minor area blackout' impacts 'Power production' with consequence 'moderate'.



Exercise 4: threat modeling

- Threats towards a chat service



- An unauthorised login may harm the asset 'User identity'
 - if the thief sends spam, offensive messages and the like under the stolen id, the credibility of the id gets compromised
 - if it is employed as id for many different services, then access to the 'User identity' may provide access to these
 - suggestions?

