Dokumentasjon av risiko på en måte som folk forstår

Folker den Braber

Abelia-seminar

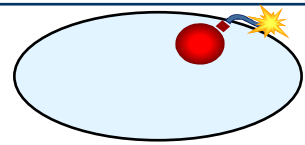
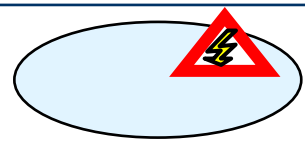
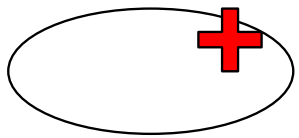
24. november 2005

Eksempel: et risikoanalysescenario

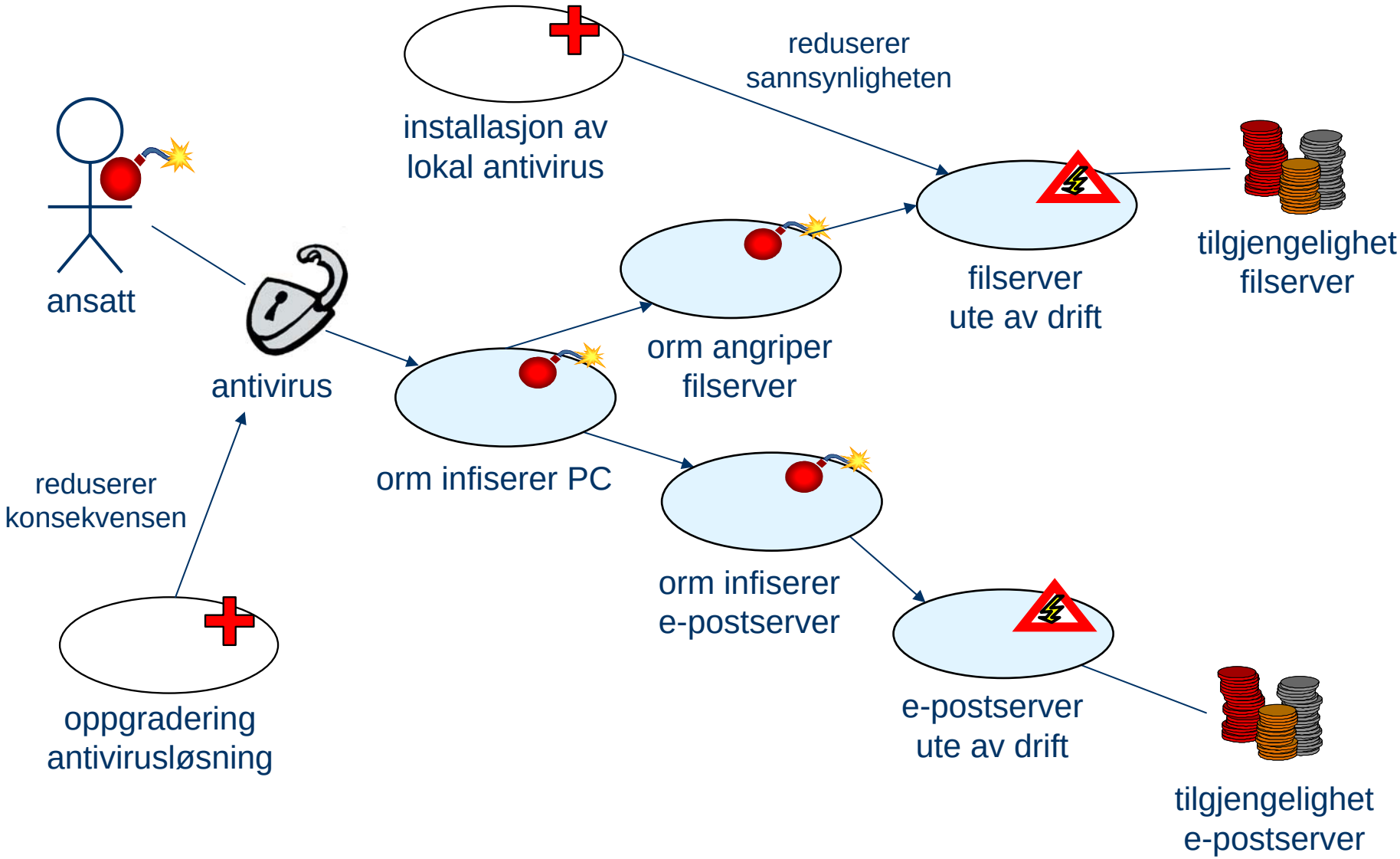
- En ansatt i et stort firma infiserer ved et uhell firmaets nettverk med en orm som angriper e-postserveren og som gjør det umulig å sende og motta e-post resten av dagen. Den ansattes pc ble infisert pga. en utilstrekkelig antivirusløsning.

ansatt	Trussel (threat)
orm angriper e-postserver	Trussel scenario (threat scenario):
tilgjengelighet e-postserver	Aktivum (asset)
e-postserver ute av drift	Hendelse (incident):
orm infiserer pc	Trussel scenario (threat scenario):
utilstrekkelig antivirusløsning	Mangel/svakhet (vulnerability):

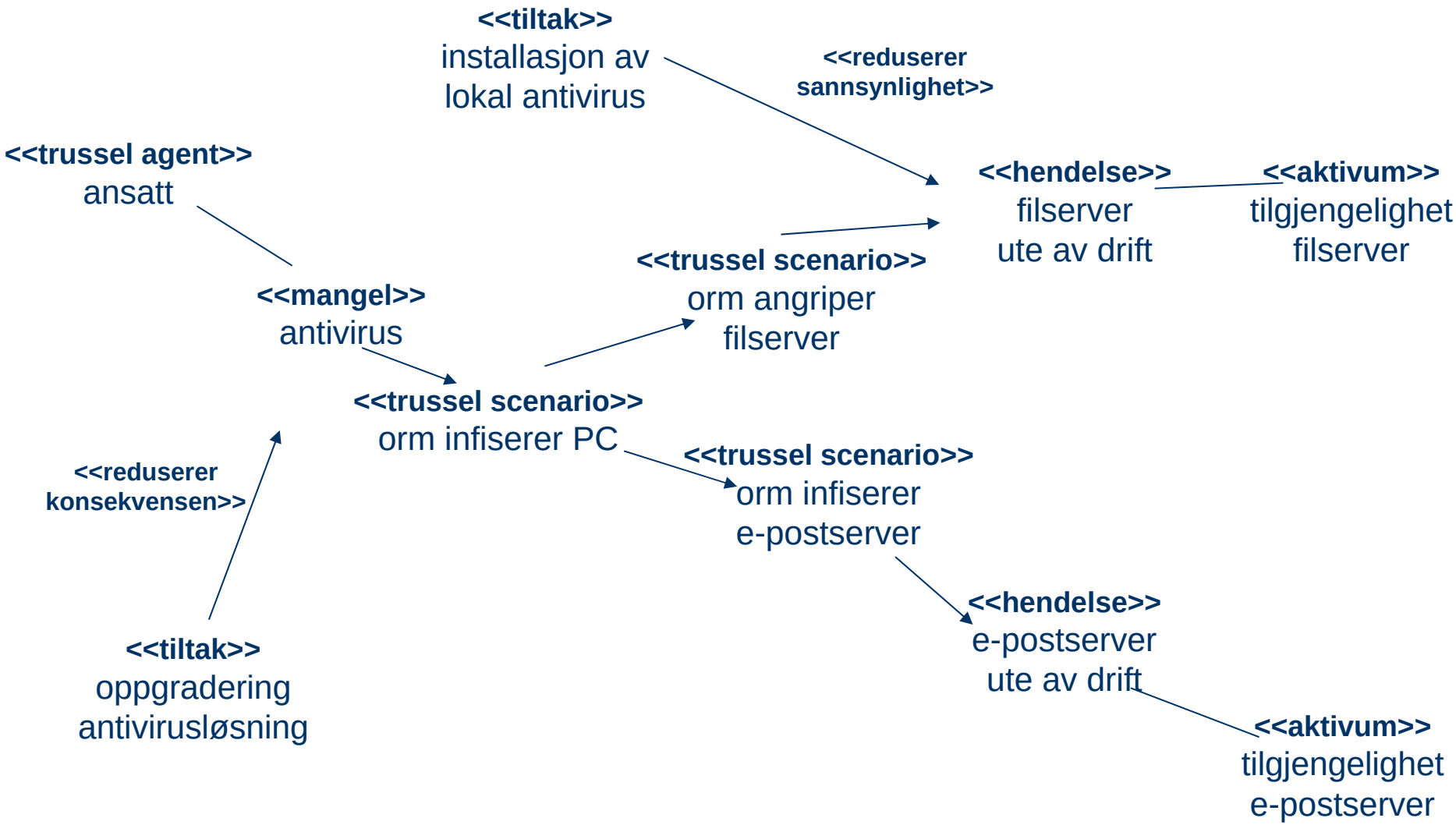
Grafisk modellering

Tilgjengelighet e-postserver	**Aktivum**	**Asset**	
Ansatt	**Trussel**	**Threat**	
E-postserver angripes av orm	**Trussel scenario**	**Threat scenario**	
E-postserver ute av drift	**Hendelse**	**Incident**	
Utilstrekkelig antivirusløsning	**Mangel**	**Vulnerability**	
Oppgradering antivirusløsning	**Tiltak**	**Treatment**	

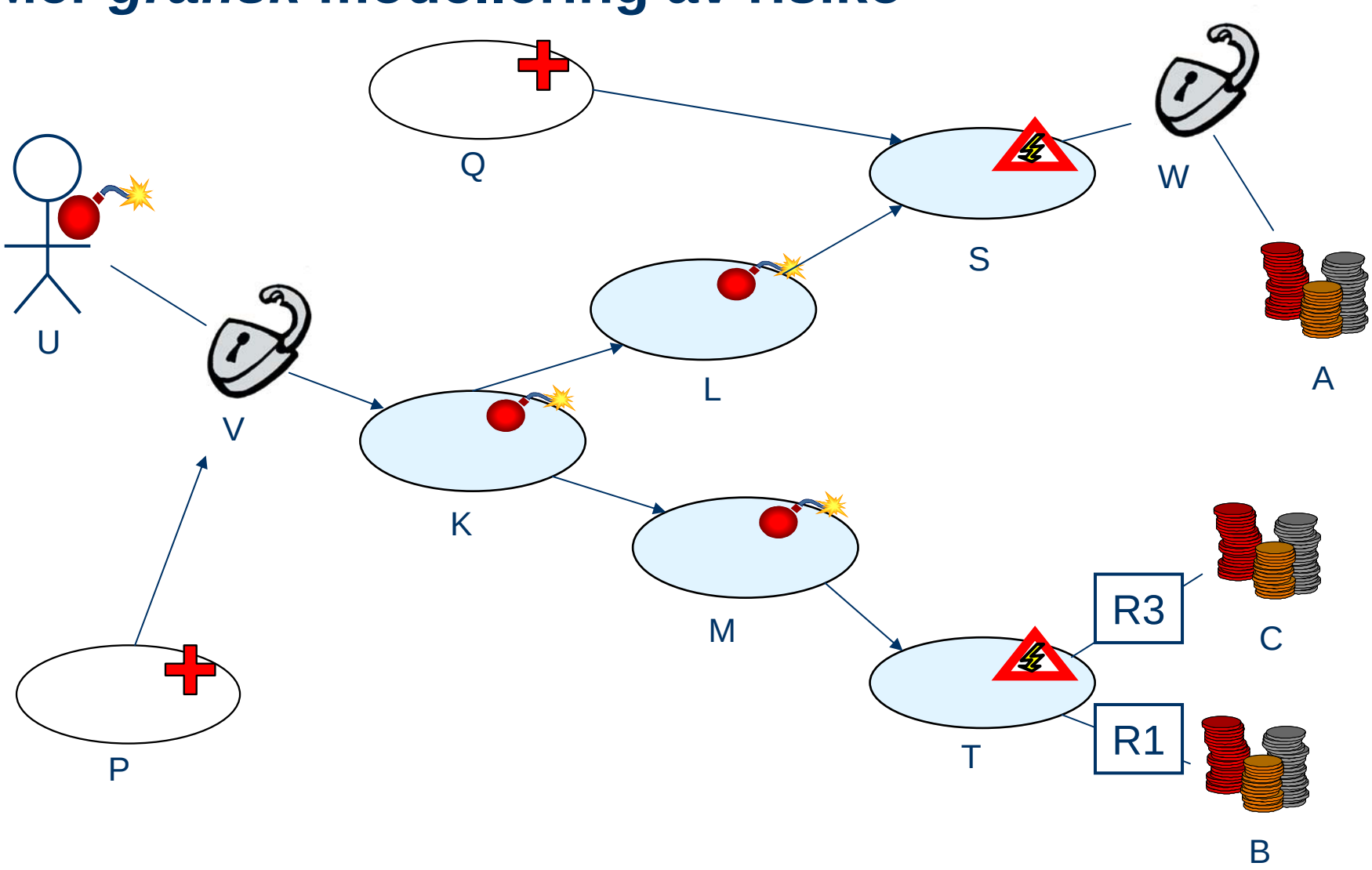
Eksempel: et *grafisk* risikoanalysescenario I



Eksempel: et *grafisk* risikoanalysescenario II



Mer *grafisk* modellering av risiko



Konklusjon

- Presis modellering reduserer faren for misforståelser
- Presis modellering legger til rette for konsistenssjekking
- Presise modeller står på egne bein
- Grafiske ikoner leses raskere enn tekst
- Grafiske ikoner gjør risikoanalyseresultater tilgjengelig for flere (uerfarne) involverte
- Grafiske risikoscenarier er lettere å bearbeide og dermed også lettere å vedlikeholde
- Grafisk risikodokumentasjon er:
  utvetydig, rask, vedlikeholdbar, automatiserbar og vakker!

Referanser

- **UML Profile for QoS and Fault Tolerance**
  Document - ptc/04-09-01
  (http://www.omg.org)

- Ida Hogganvik, Ketil Stølen.
  On the Comprehension of Security Risk Scenarios.
  In Proc. 13th International Workshop on Program Comprehension (IWPC 2005),
  pages 115-124, IEEE Computer Society, 2005.