Model-based analysis of security and trust using CORAS

Overview of CORAS

Folker den Braber

4. november 2005

Overview

- Background and motivation
- Model-based risk analysis
- Risk analysis of security, trust and legal issues
- Risk analysis process
- CORAS modelling language for security risk analysis
- Tool support

CORAS background

- Research and technological development project under the Information Society Technologies (IST) Programme
- January 2001 -> July 2003
- 11 partners from 4 European countries

- Goal: Develop an improved methodology for precise, unambiguous, and efficient risk analysis of security critical IT systems

Usage of CORAS

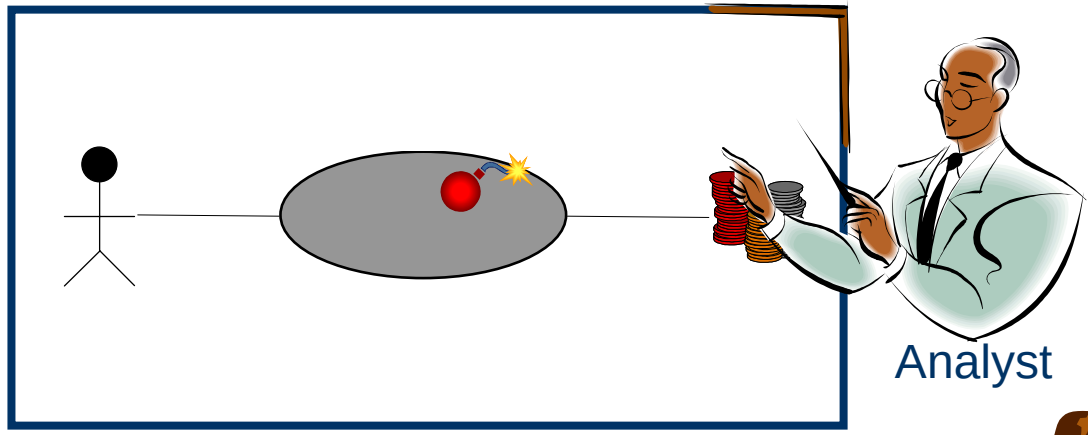
- The CORAS methodology and tools have been utilised in a wide variety of settings
- 7 field trials during the CORAS project
  - E-Commerce and tele-medicine IT systems
- Risk analysis in industrial and EU projects
  - Authentication in mobile services
  - Electronic document handling
  - Mobile access to information systems
  - Analysis of trust and legal issues in virtual organisations

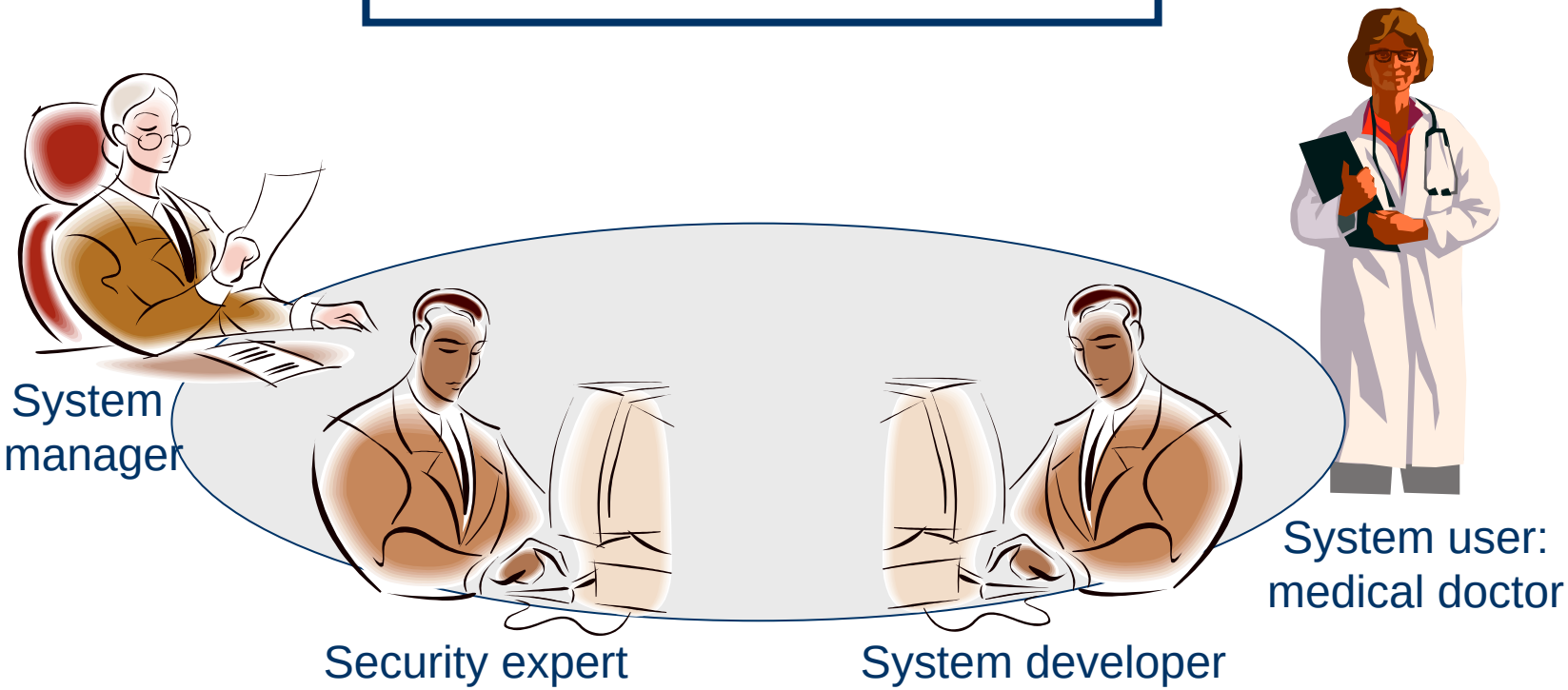
Risk analysis – what is it?

- Determining what can happen, why and how
- Systematic use of available information to determine the level of risk
- Prioritisation by comparing the level of risk against predetermined criteria
- Selection and implementation of appropriate options for dealing with risk

IT-security is more than technology

- From a technical standpoint, security solutions are available – but what good is security if no one can use the systems?
  - For example, the Secure Electronic Transaction (SET) proved to be too complicated to use
- Security requires more than technical understanding
- Security problems are often of non-technical origin
- A sound security evaluation requires a uniform description of the system as a whole
  - how it is used, the surrounding organisation, etc.

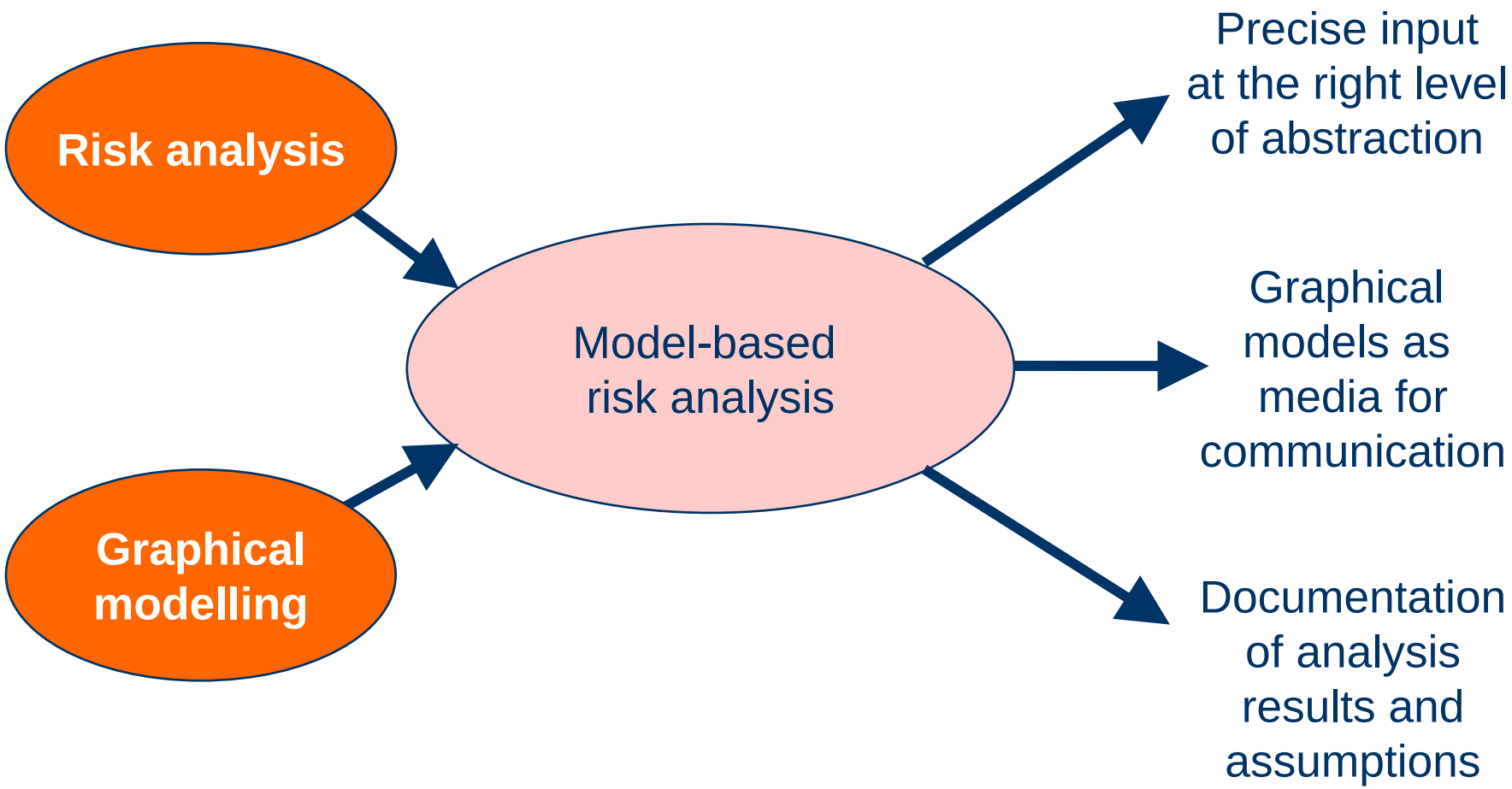

Analyst


System manager
Security expert
System developer
System user: medical doctor

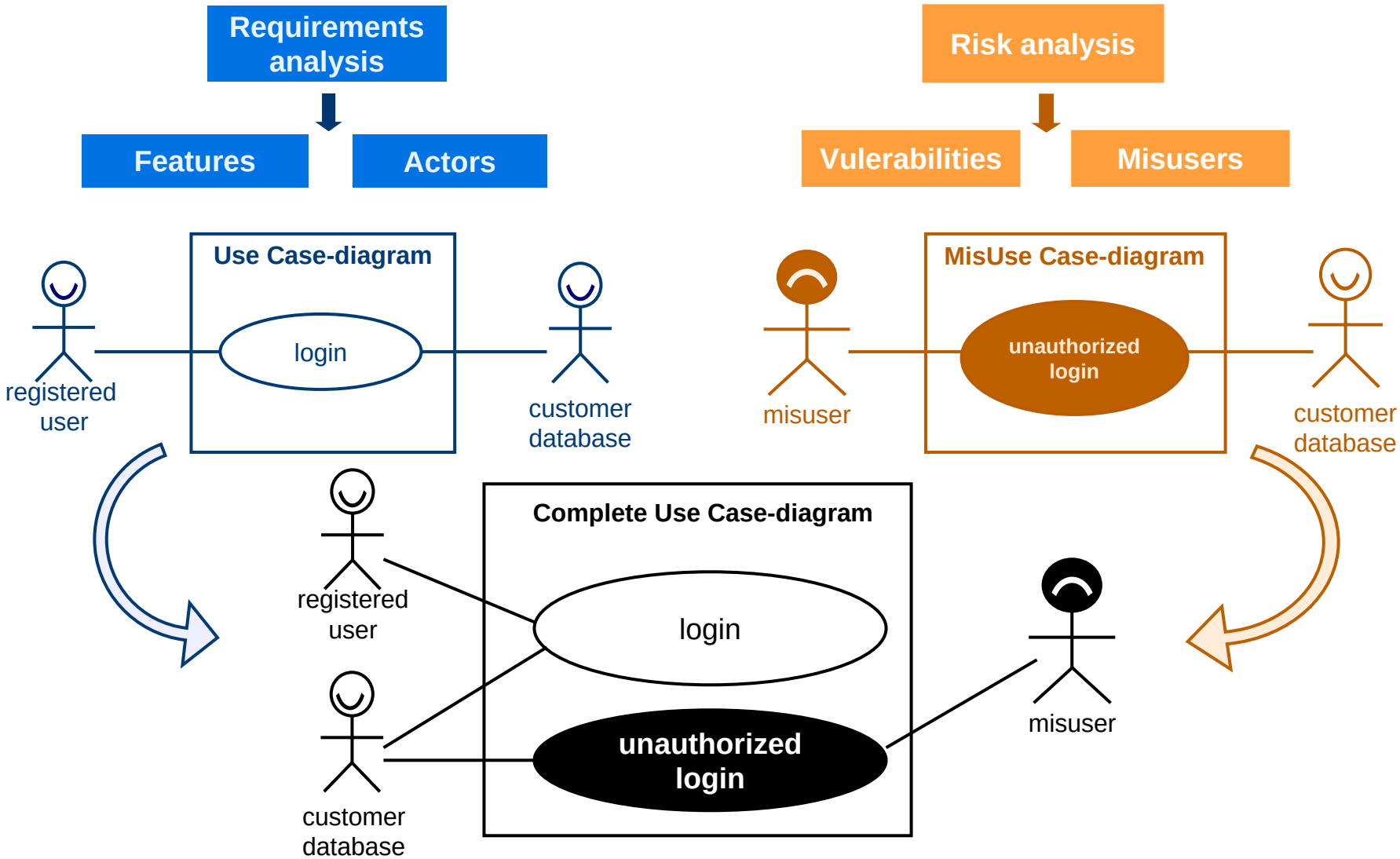
IT-security – part of system development

- Security is traditionally added as an “afterthought”
  - Solutions often reactive rather than proactive
  - Security issues often solved in isolation
  - Costly redesign
  - Security not completely integrated
- Requirements analysis and risk analysis are two sides of the same coin and should be integrated
  - Focus on desired and undesired behaviour, respectively

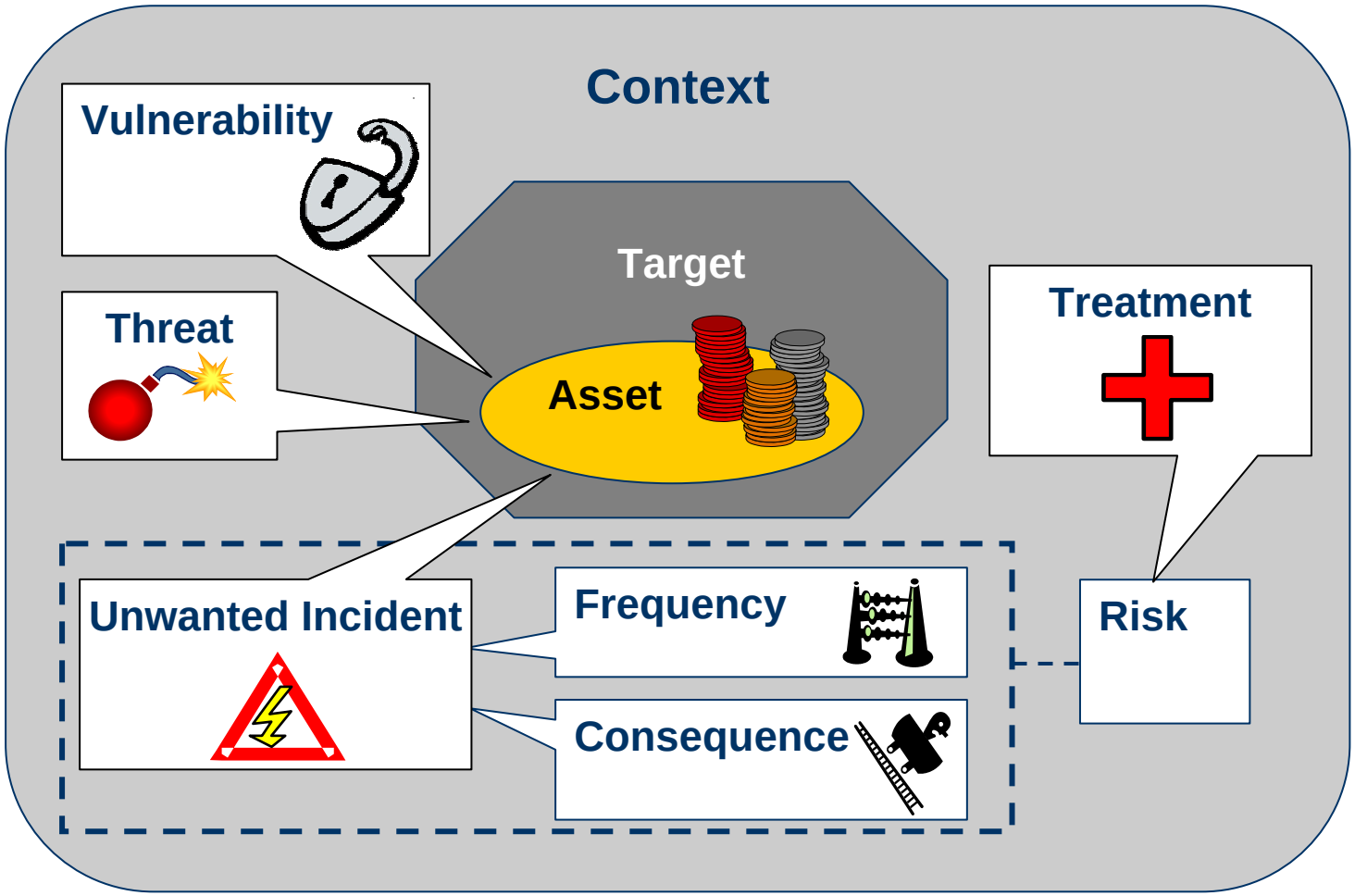
Model-based risk analysis



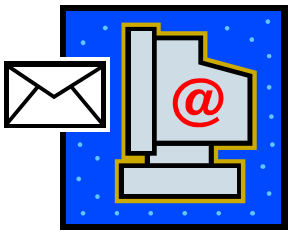
Model-based risk analysis



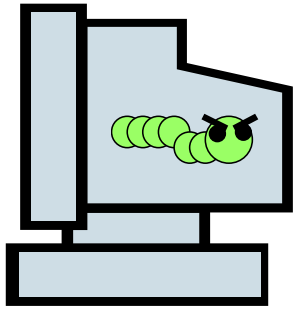
Elements of risk analysis



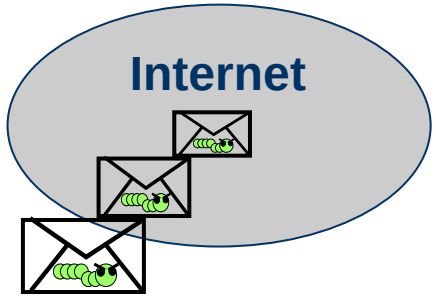
Terms

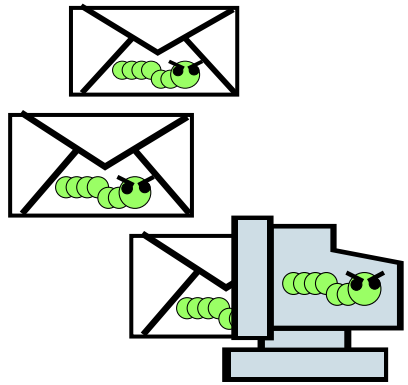


Computer running Outlook



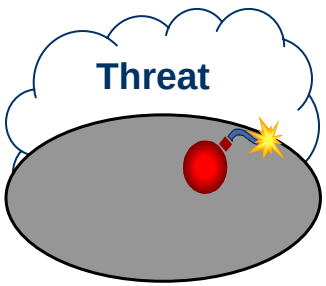
Infected PC

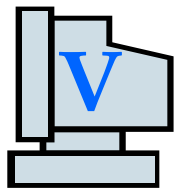




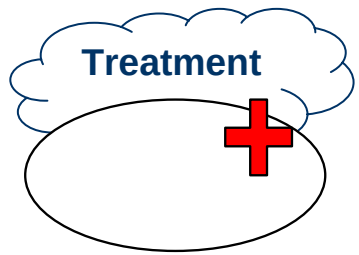
- Infected twice per year
- Infected mail send to all contacts

Worm



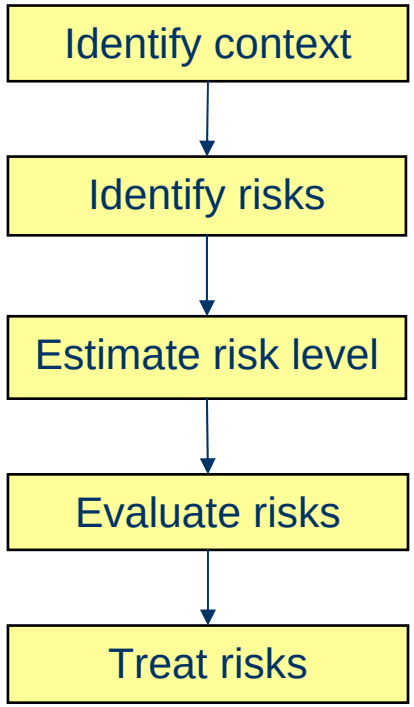


Install virus scanner

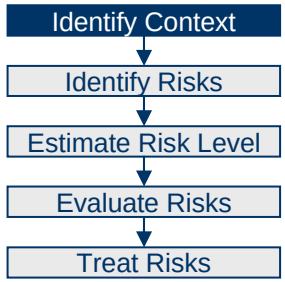


CORAS methodology

- Risk management process based on AS/NZS 4360
- Provides *process* and *guidelines* for risk analysis

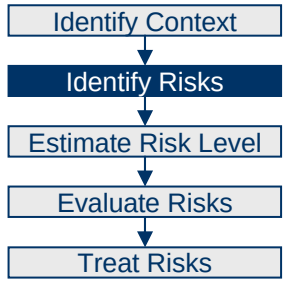


Context identification



- Characterise target of analysis
  - What is the focus and scope of the analysis?
- Identify and value assets
  - Asset-driven risk analysis process
  - Business oriented, e.g. availability of services generating revenue
- Specify risk acceptance criteria
  - There will always be risks, but what losses can the client tolerate?
  - Similar to requirements in system development

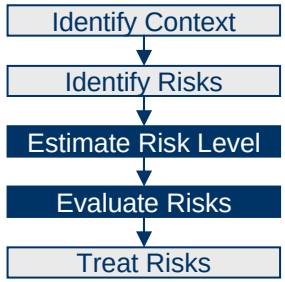
Risk identification



- Identify threats to assets through structured brainstorming
  - Hazard and Operability analysis (HazOp)
  - Involving system owners, users, developers, domain experts, risk analysis experts, etc. (typically 5-7 people)
- Identify vulnerabilities of assets
  - Questionnaires and checklists

Equipment physical security
- Is equipment properly physically protected against unauthorised access to data or loss of data?
- Are power supplies handled in a manner that prevents loss of data and ensures availability?
- …

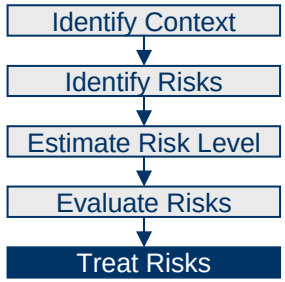
Risk evaluation



- We cannot completely eliminate all risks
- Determine which risks need treatment
  - We need to know how serious they are so we can prioritise

- Risk level is determined based on analysis of the frequency and consequence of the unwanted incident
  - Quantitative values: e.g., loss of 1M€, 25% chance per year
  - Qualitative values: e.g., high, medium, low

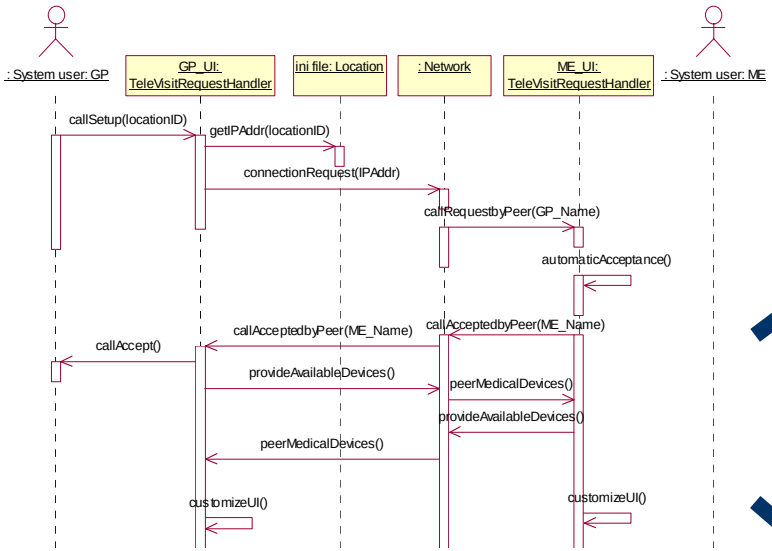
Risk treatment

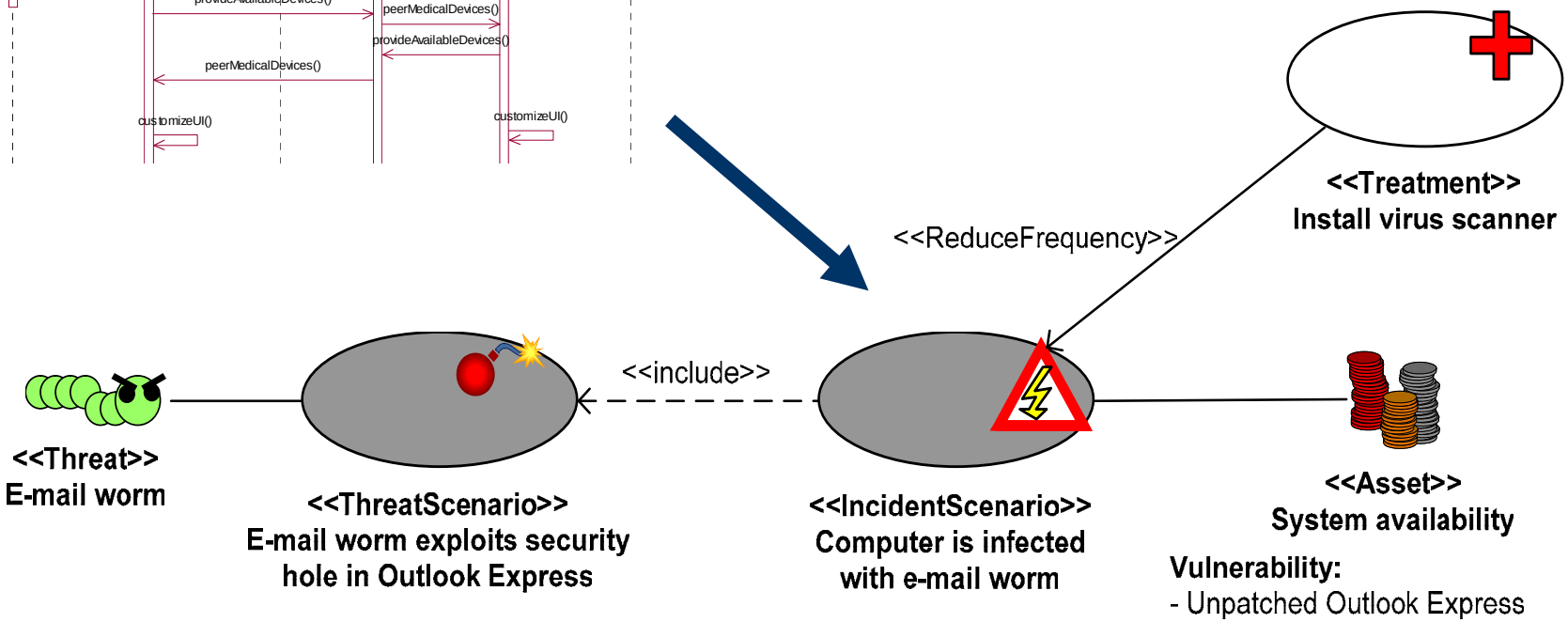


- Identify treatments for unaccepted risks
- Evaluate and prioritise different treatments

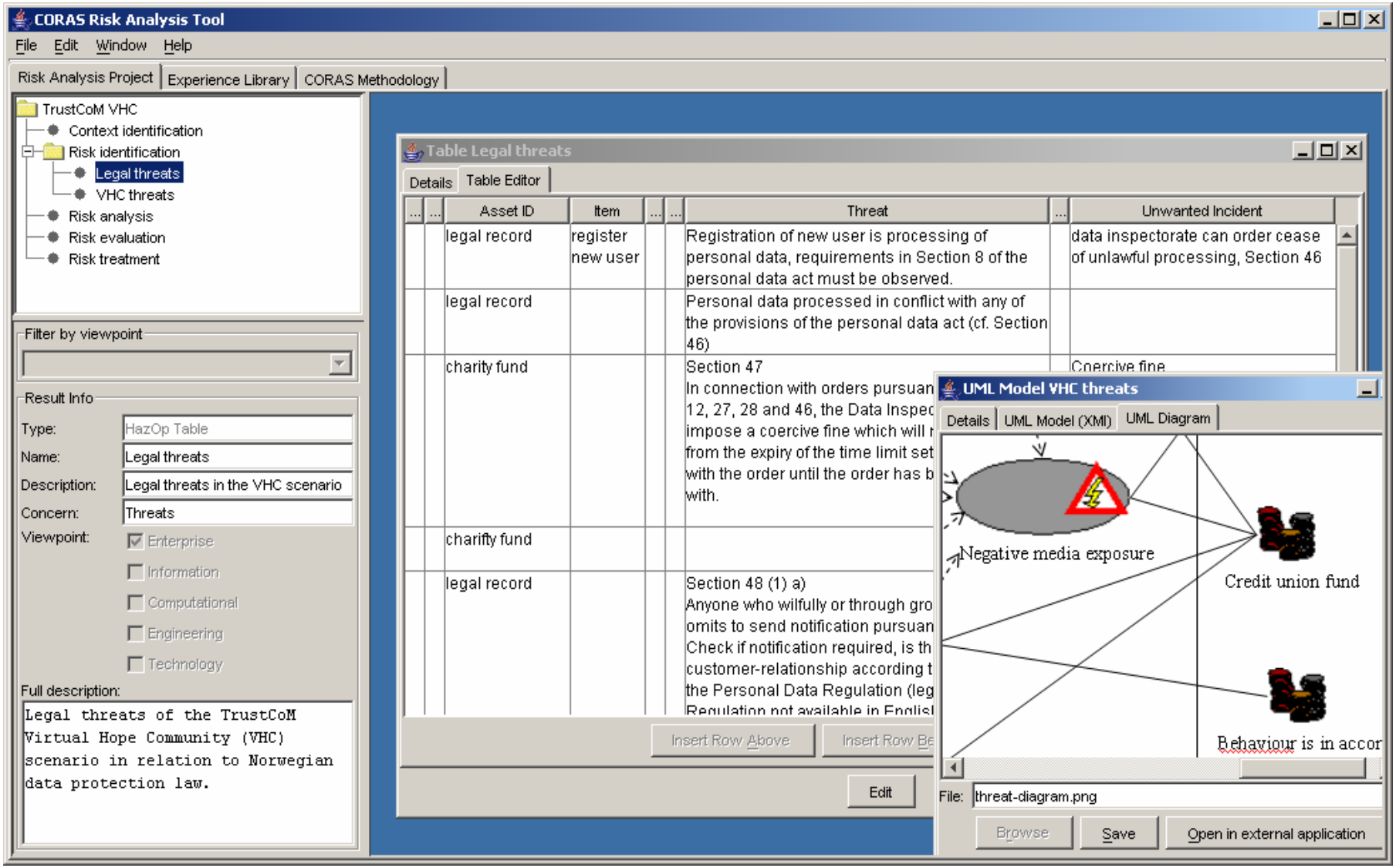
Graphical models

HazOp ID	Asset ID	Guideword	Attribute	Scenario





CORAS risk analysis tool



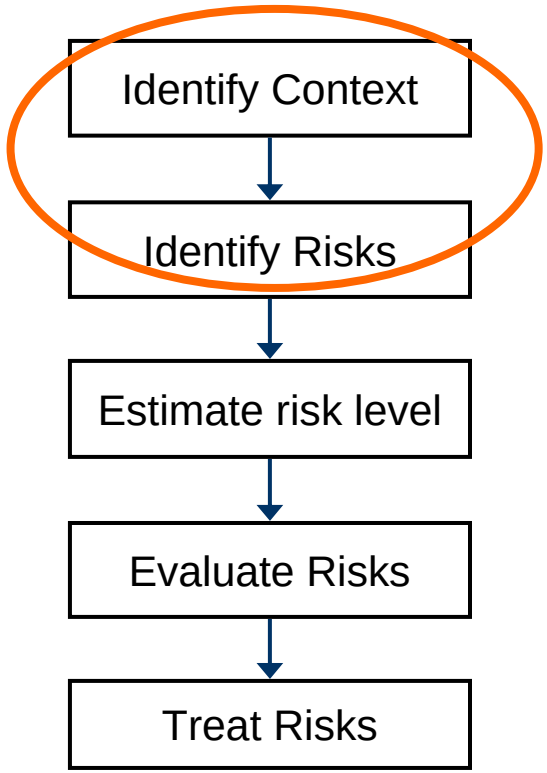
Context & Threat Identification

Model-based analysis of security and trust using CORAS

4. november 2005

Overview

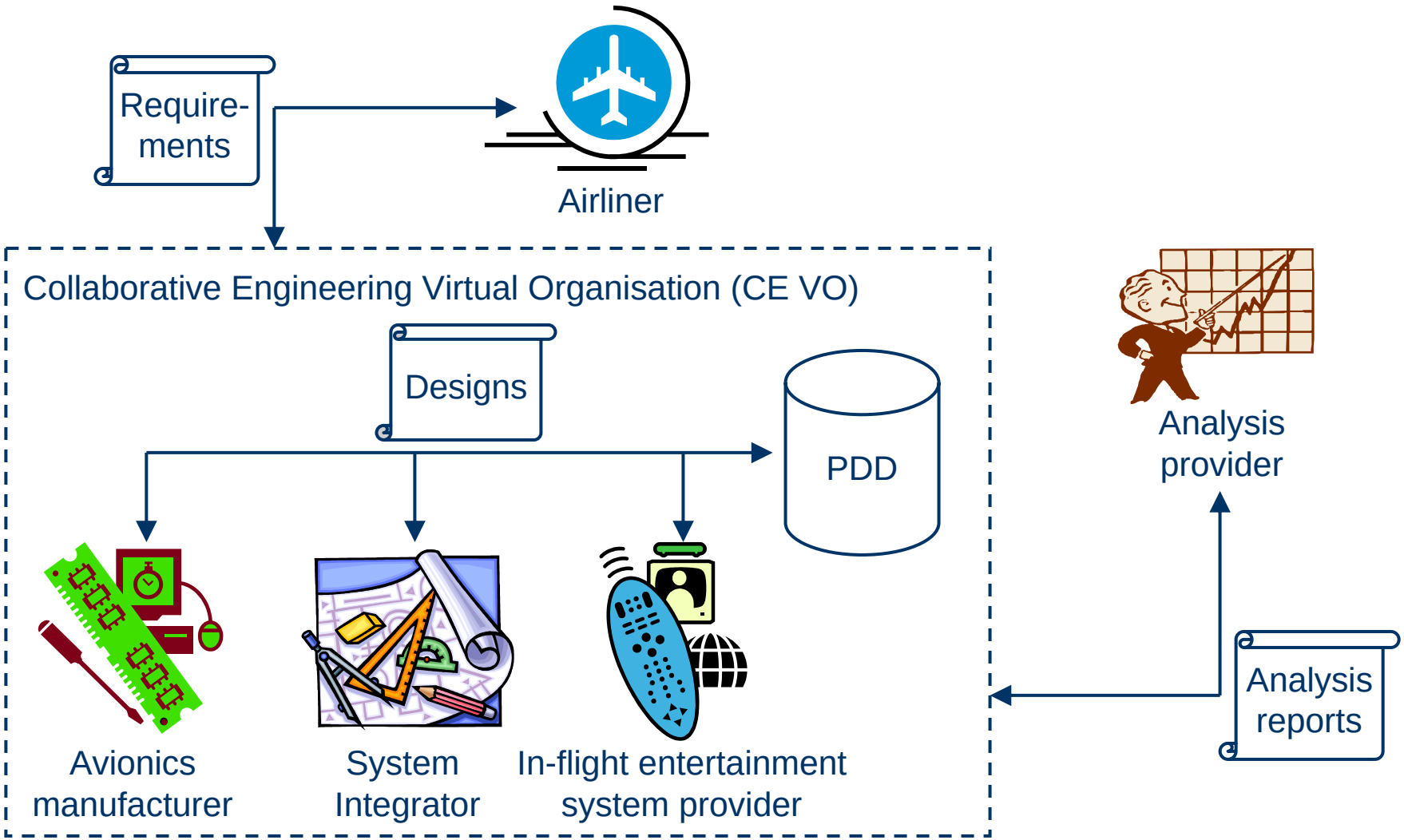
- Case
- Context
  - Risk management context
  - Risk acceptance
  - Target of Evaluation
  - Stakeholders
  - Assets
- Threats
  - Threat identification
  - Threat modelling
  - Vulnerabilities



Case: Collaborative Engineering in a Virtual Organisation

- The case is an excerpt of a risk analysis carried out in the TrustCoM project
- The focus is on Intellectual Property Rights (IPR) and legal aspects
- Three organisations are collaborating in a virtual organisation (VO)
  - The goal of the VO is to design a new business jet for an airliner
  - The analysis is carried out for one of the participants in the VO, who wants to assess the risks of the project

Case: Collaborative Engineering in a Virtual Organisation

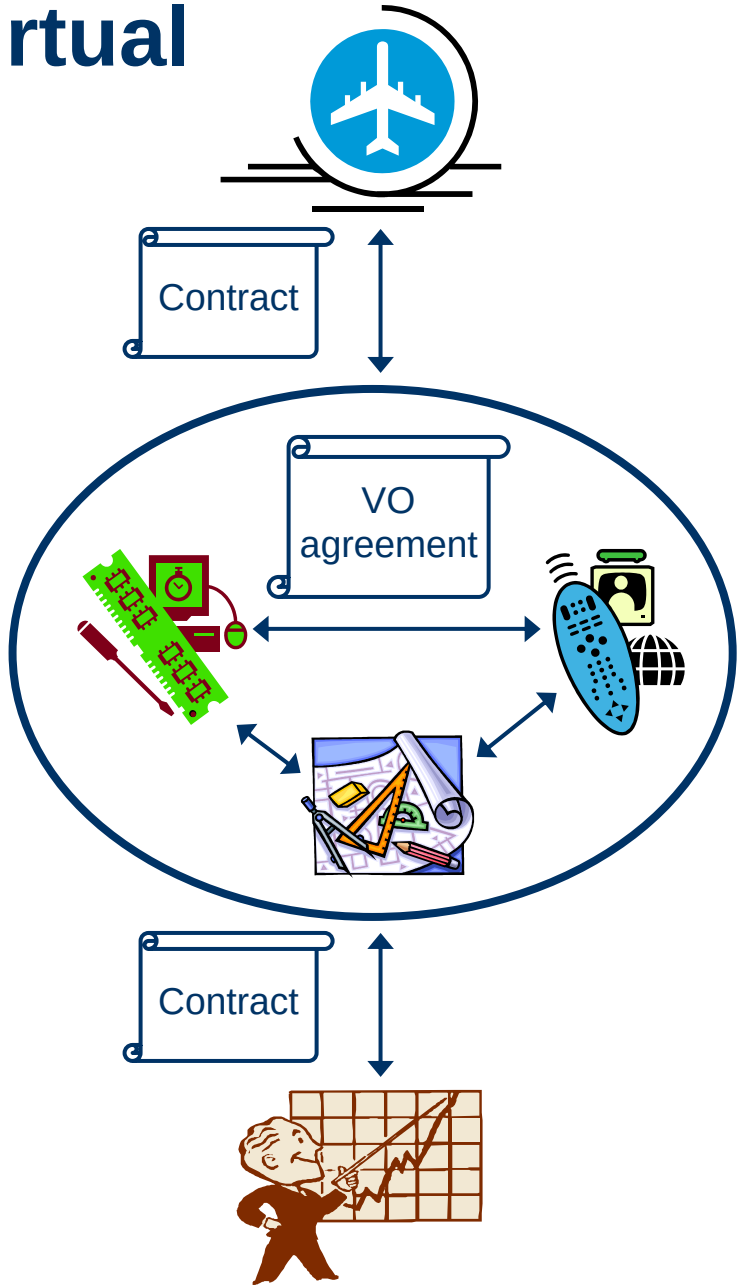


Case: Collaborative Engineering in a Virtual Organisation

- The Collaborative Engineering Virtual Organisation (CE VO) has three partners
  - System Integrator (SI)
  - Avionics manufacturer
  - In-flight entertainment system provider
- The customer of CE VO is an airliner who will build and operate the aircraft
- The System Integrator orders a risk analysis of the project before the work is started

What is special about a virtual organisation?

- Ad hoc, temporal
- Not hierarchical
  - Governed by contracts
- Legal status
  - Not necessarily a legal person
  - Who owns IPR produced by the VO?
- Co-operation
  - External interface
  - Sharing of information
  - Trust among the partners



Context identification

Identify Context

Identify Risks

Risk management context

Target of evaluation

Assets

- In the context identification we must address a number of important questions
  - For whom is this risk analysis carried out?
  - For what purpose do we make this analysis?
  - What do we want to protect?
  - What is the scope?
  - Which risk level are we willing to accept?
- Activities
  - Risk management context
  - Target of evaluation
  - Assets

Context identification

Identify Context

Identify Risks

Risk management context

Target of evaluation

Assets

- The purpose of context identification is to establish and document all the assumptions of the analysis
- The context includes the methods used, level of abstraction and detail, the focus, etc.
- This is important in order to
  - know in which domain the analysis results will be valid
  - use the resources available in the most efficient way

Risk management context

- The risk management context documentation describes meta-information about the analysis
  - Process information: how and when was the analysis preformed and who participated
  - Risk acceptance criteria
  - Definition of domain and range of values

Risk management context: risk acceptance criteria

- Risk acceptance criteria formalise what level of risk we will accept
- The criteria are defined by the means of risk level, frequency value or consequence value

Criteria ID	Description
C1	If “Risk level” is equal to “Low” then “Accept the risk”
C2	If “Risk level” is equal to “Moderate” then “Monitor the risk”
C3	If “Risk level” is greater than or equal to “Major” then “Treat the risk”

Risk management context: values

- The value definitions that we will need are
  - asset values
  - frequency values
  - consequence values
  - risk levels
- In this case study we used qualitative value domains
  - e.g., examples and/or ranges in (loss of) monetary value or ranges in probability
- Quantitative values may also be used, based on historical and statistical data
  - e.g., concrete numbers for (loss of) monetary value or probability on a continuous scale

Risk management context: values

Identify Context

Identify Risks

Risk management context

Target of evaluation

Assets

- Values recorded in value definition table

Value type	Values	**Description**
Asset	Very Low, Low, Medium, High, Very High	Very Low: ~10 K€ Low: Analysis report. Customer requirements. ~100 K€ Medium: 3D model. ~1 M€ High: Complete subsystem design. ~10 M€ Very High: Complete aircraft design. Upgrade contract. Aircraft. ~100 M€
Frequency	Rare, Unlikely, Possible, Likely, Certain	Rare: Less than once per ten years. Unlikely: Less than once a year. Possible: About once a year. Likely: 2-5 times a year. Certain: More than 5 times a year.
Consequence	Insignificant, Minor, Moderate, Major, Catastrophic	Insignificant: No impact on business. Minor delays. Minor: Loss of profits. Lost project phases. Moderate: Loss of project/client. Major: Loss of business sector. Close department. Catastrophic: Out of business.

Risk management context: values

Identify Context

Identify Risks

Risk management context

Target of evaluation

Assets

- Risk levels are defined in a matrix in the case of qualitative values
- Or in the case of quantitative value as a function from frequency and consequence values to risk level
  - e.g. *Risk level = Frequency value * Consequence value*

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Low	Low	Low	Moderate	Major
	Unlikely	Low	Low	Moderate	Major	Major
	Possible	Low	Moderate	Major	Major	Extreme
	Likely	Moderate	Major	Major	Extreme	Extreme
	Certain	Moderate	Major	Extreme	Extreme	Extreme

Target of Evaluation

- The Target of Evaluation (ToE) is the part of the system to be analysed
- It is important to have a clear picture of what should be analysed and what falls outside scope
  - Know in which context the analysis is valid
  - Efficient use of resources
- ToE is described using UML models and text (usually a subset of the system documentation)

Target of Evaluation

Identify Context

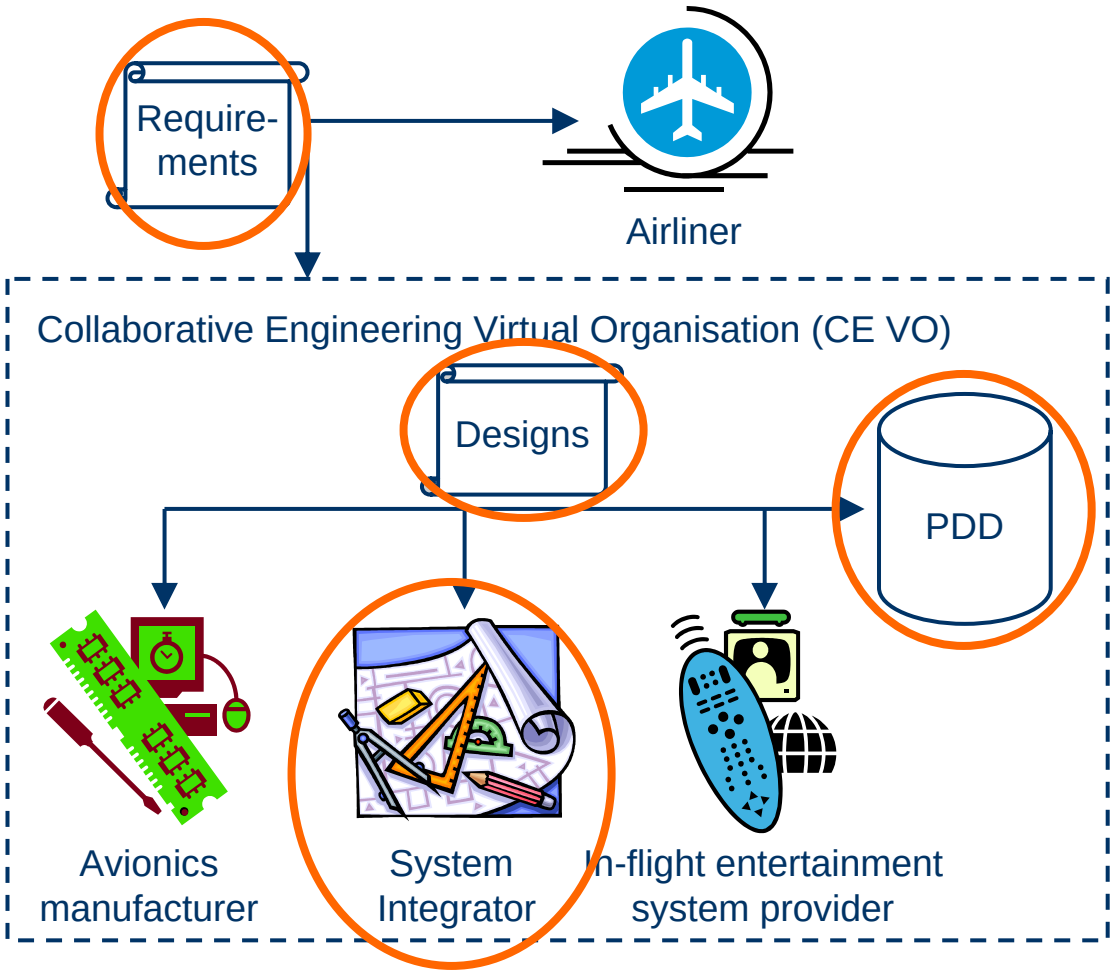
Identify Risks

Risk management context

Target of evaluation

Assets

- We define target as
  - System Integrator
  - Designs
  - Client information
  - Product Design Database
- We focus on loss of intellectual property
  - Industrial espionage
  - Confidentiality



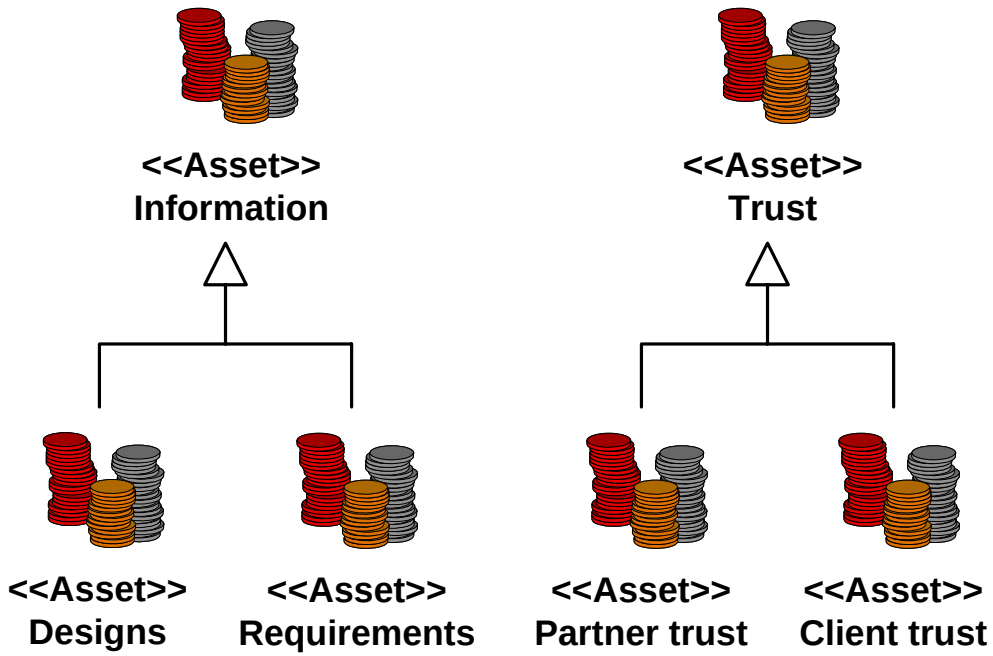
Assets

- Assets are the parts or features of the target that have value and that we want to protect
- The value of an asset is assigned by the stakeholder who has interests in the asset
- Assets are the basis for the rest of the analysis

Asset ID	Description	Asset category	Asset value
Designs	SI's share in the designs of the passenger aircraft	Information	Very high
Requirements	The requirements of the VO's customer	Information	High
Partner trust	The VO partners' trust in SI	Other	High
Client trust	The client/customer's trust in SI	Other	Very high

Asset diagram

- Assets are modelled in asset diagrams
- Provide structure and show relations between assets



Risk identification

Identify Context
Identify Risks
Estimate risk level

Threats
Vulnerabilities
Unwanted incidents

- Risk identification is about identifying the *unwanted incidents* that constitutes risks to the identified assets
- To do this we need to answer the questions
  - What or who may threaten the assets?
  - How will the threat act?
  - What are the weaknesses or vulnerabilities of the system that the threat might exploit?
  - What (bad things) will happen if a threat exploits a vulnerability?

Identify Context

Identify Risks

Estimate risk level

Threats

Vulnerabilities

Unwanted incidents

Risk identification

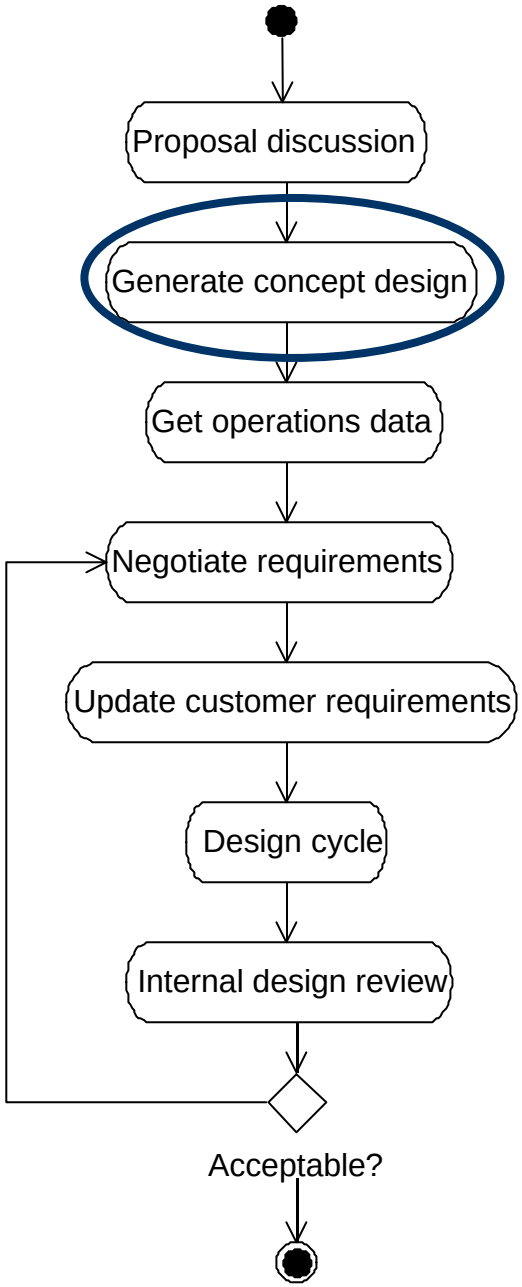
- Activities of risk identification
  - Threat identification
  - Identification of vulnerabilities
  - Identification of unwanted incidents

Threat identification

Identify Context
Identify Risks
Estimate risk level

Threats
Vulnerabilities
Unwanted incidents

- Threat identification was carried out by going through business processes, formalised in UML activity diagrams
- For each activity, the participants brainstormed about possible threats and threat scenarios
  - Possibly with help from guidewords, checklists, etc.
- The participants were
  - Risk analysis leader
  - Risk analysis secretary
  - Target owner
  - Experts on security and legal and socio-economic issues



Identify Context

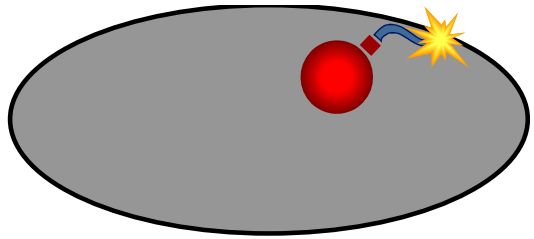
Identify Risks

Estimate risk level

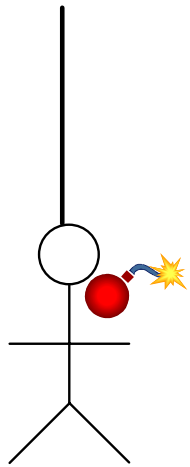
Threats

Vulnerabilities

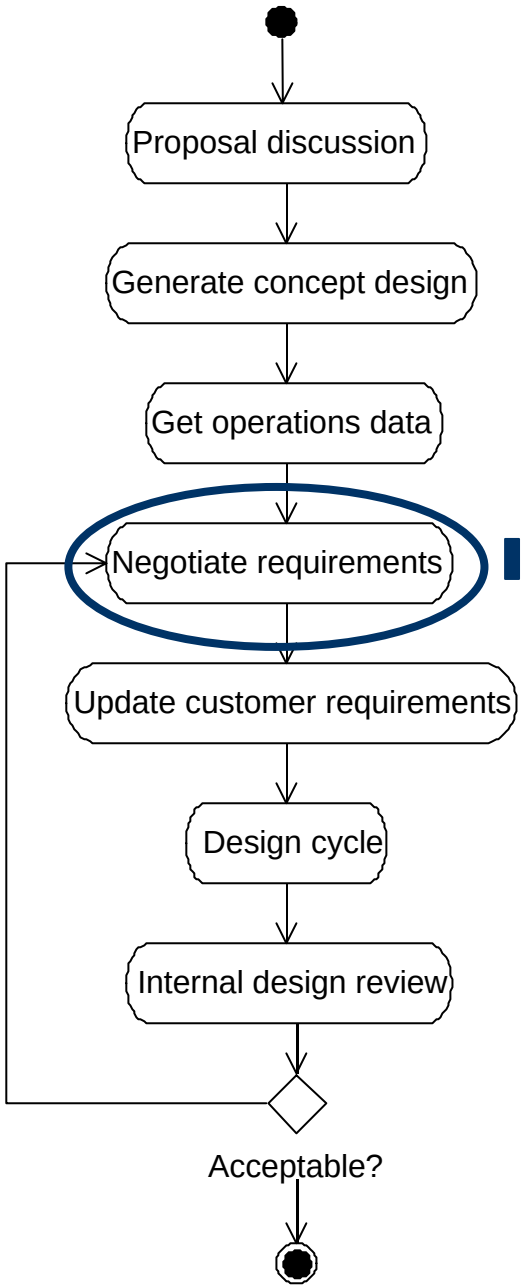
Unwanted incidents



<<ThreatScenario>>
Security weakness exploited to steal designs from PDD



<<Threat>>
Hacker



Identify Context

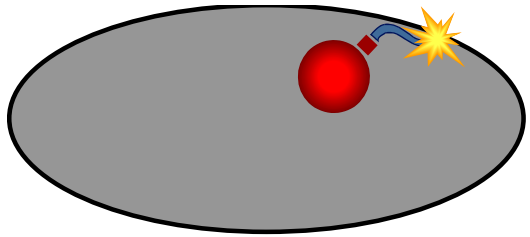
Identify Risks

Estimate risk level

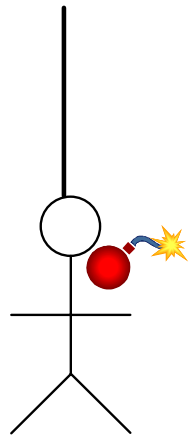
Threats

Vulnerabilities

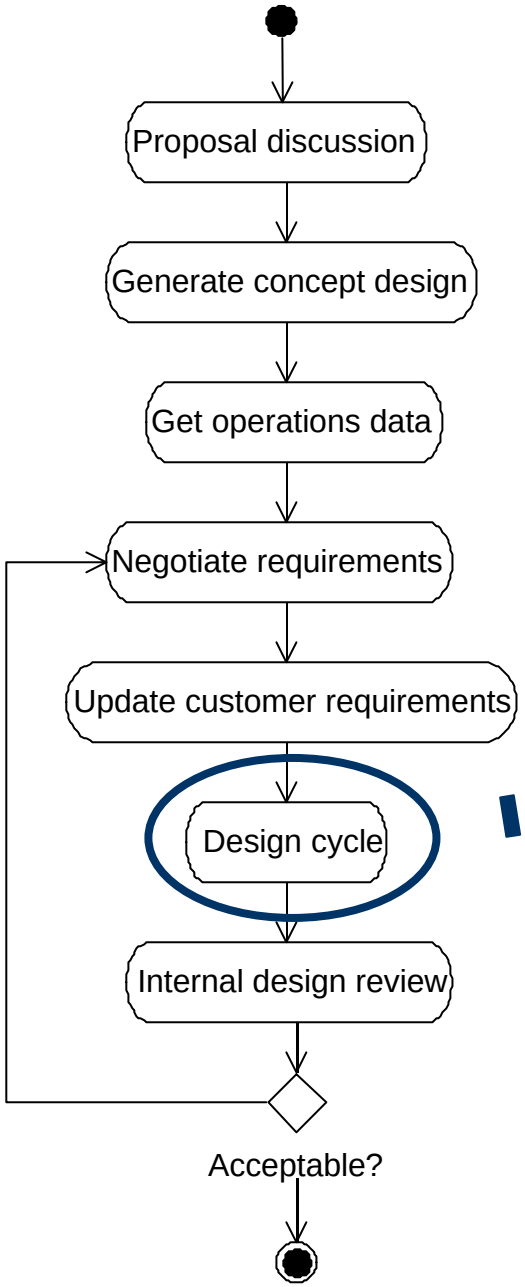
Unwanted incidents



<<ThreatScenario>>
Unfaithful SI employee discloses customer confidential information



<<Threat>>
Unfaithful SI employee



Identify Context

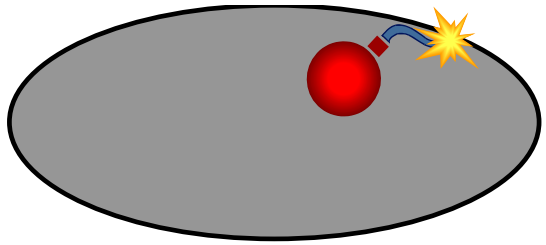
Identify Risks

Estimate risk level

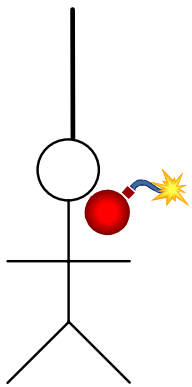
Threats

Vulnerabilities

Unwanted incidents



<<ThreatScenario>>
Information unintentionally disclosed because security policies are insufficient



<<Threat>>
Human error

Vulnerabilities

- Vulnerabilities are weaknesses in the target which may be exploited by threats
- They are associated with assets, but are not necessarily weaknesses of the assets themselves
- Vulnerabilities are identified in a similar way as threats, and with the help of questionnaires and checklists

Vulnerability	**Asset**
Security policies not sufficient	Designs
Insufficient protection of PDD	Designs
Security policies not sufficient	Requirements

Summary

- So far we have covered
  - Introduction to the Collaborative Engineering VO case
  - Context identification
  - First part of risk identification
    - Threats and threat scenarios
    - Vulnerabilities
  - Documentation of assets and threat scenarios using the CORAS language

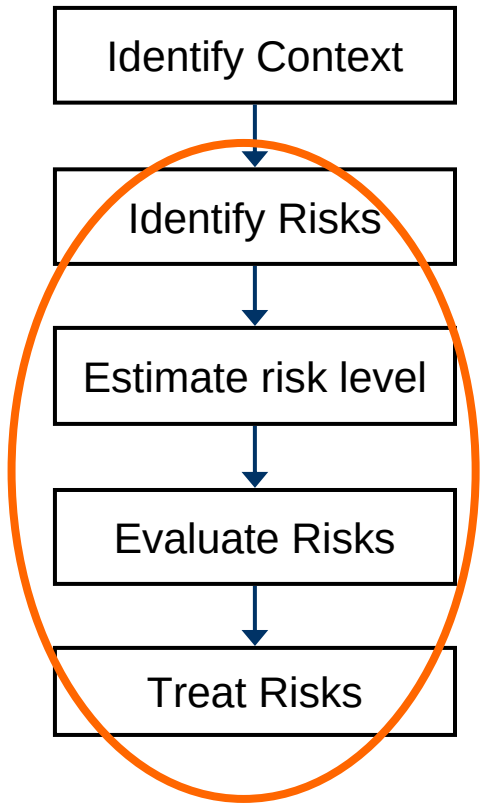
Risk Evaluation & Treatment

Model-based analysis of security and trust using CORAS

4. november 2005

Overview

- Risk identification cont.
  - Unwanted incidents
- Risk level estimation
  - Consequence
  - Frequency
  - Risk level
- Risk evaluation
  - Risk categories
  - Acceptance/need for treatment
- Treatment
  - Treatment identification
  - Treatment evaluation



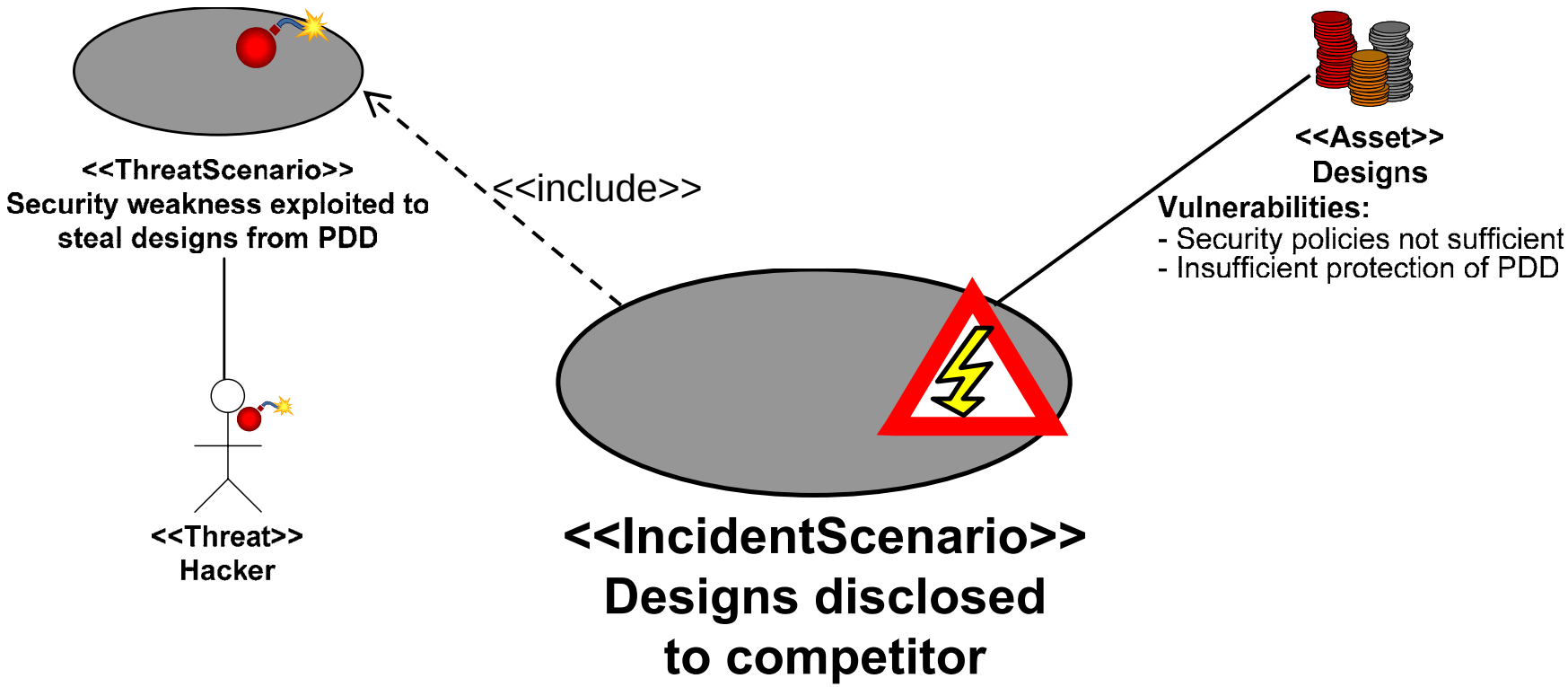
Unwanted incidents

- Unwanted incidents are the bad things happening that may reduce the value of your assets
- Bad things happen when a threat is able to exploit a weakness of the system

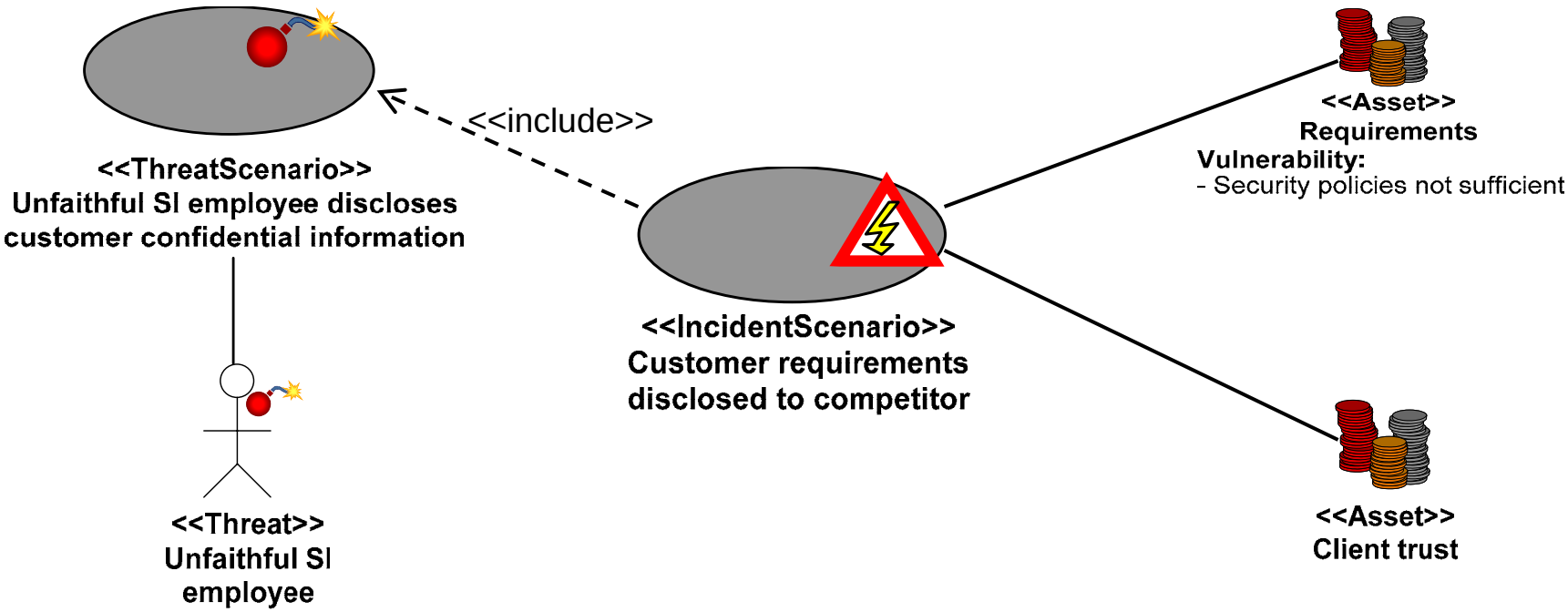
Unwanted incidents

- The brainstorming sessions of threat and vulnerability identification usually produce large amounts of data
- By modelling the scenarios we structured this information and identified matches between threats and vulnerabilities
- From this matching, unwanted incidents are identified and modelled

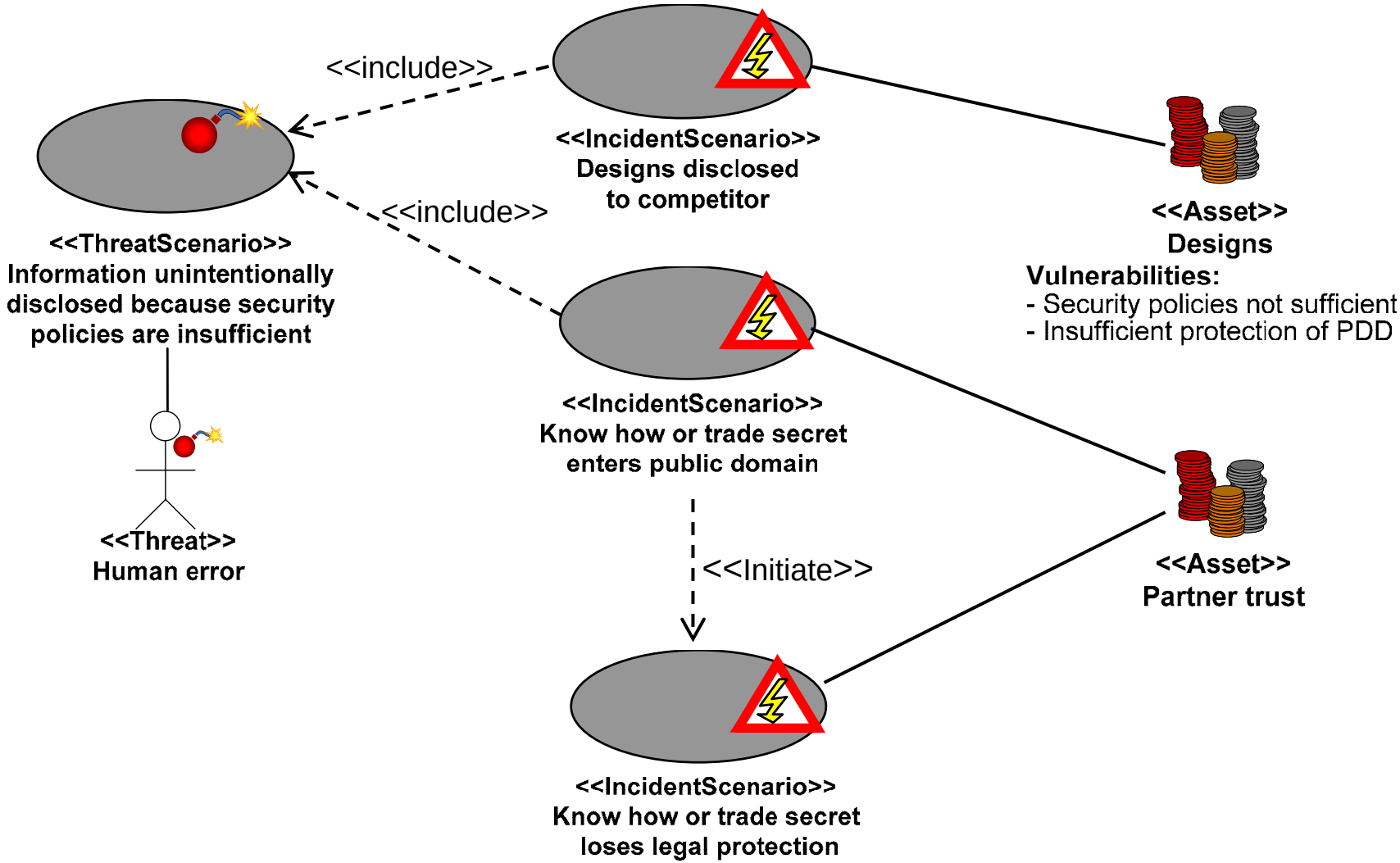
Unwanted incidents



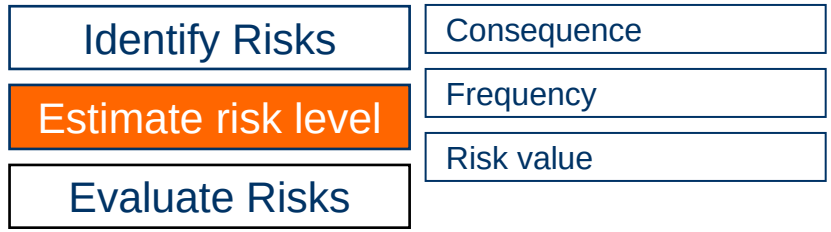
Unwanted incidents



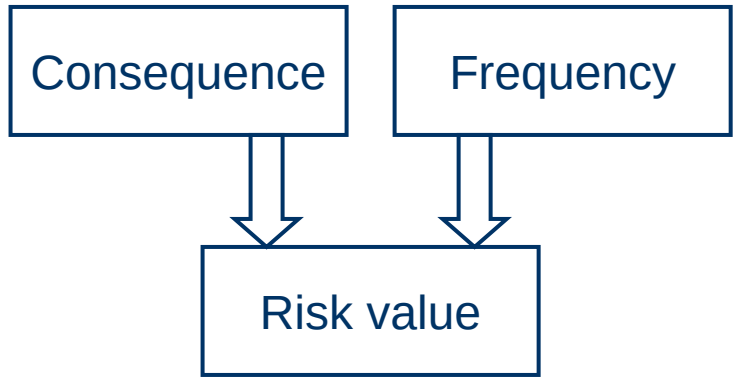
Unwanted incidents



Estimate risk level

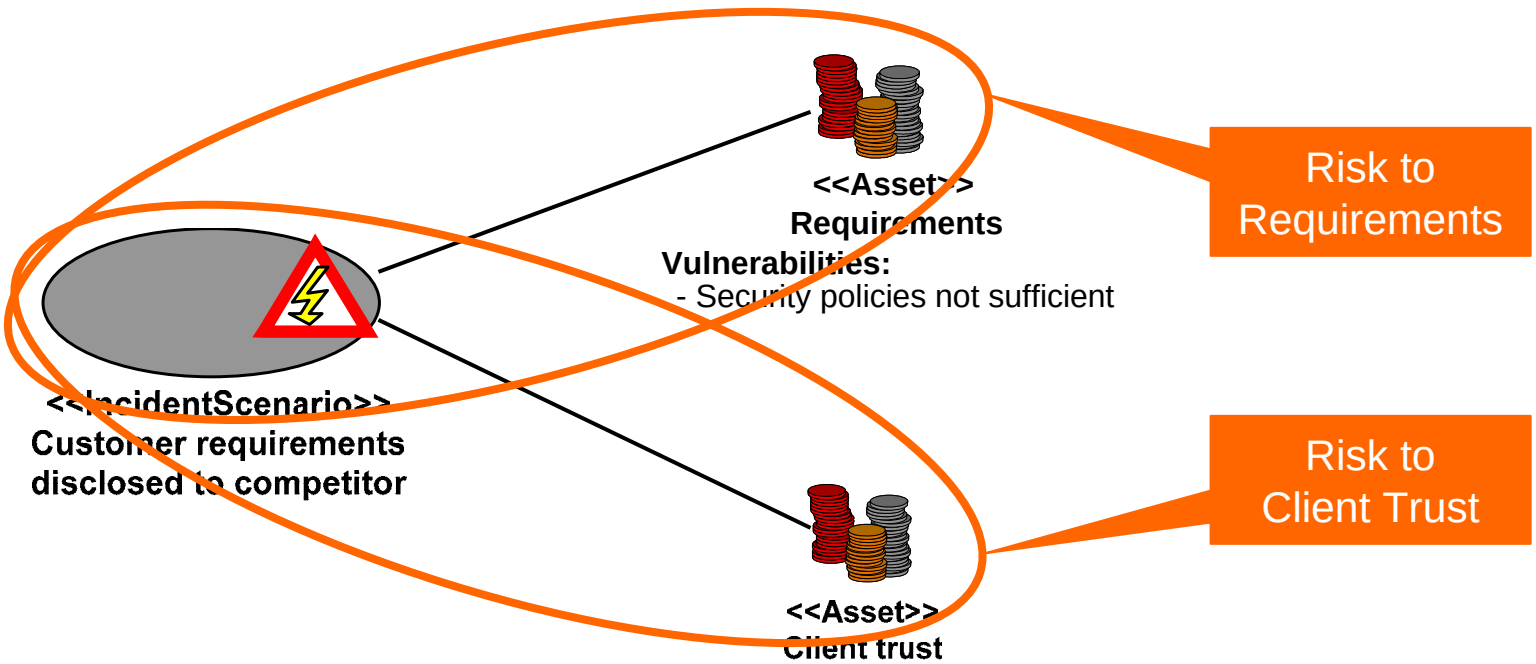


- A risk is an unwanted incident that has been assigned
  - a consequence value, and
  - a frequency value
- From these values the risk value is calculated



Estimate risk level

- An unwanted incident may harm several assets
- We always document a risk relative to one asset
  - The asset values and consequence values may differ from asset to asset
  - The treatments may vary between assets



Consequence and Frequency

Identify Risks

Estimate risk level

Evaluate Risks

Consequence

Frequency

Risk value

- Consequence is a measure of loss of asset value
  - Based on available historical and financial data and methods like FMEA/FMECA
  - Estimates from client and domain experts
- Frequency value is a measure of how often an unwanted incident occurs
  - Probability based on historical data and statistical methods like Fault Tree Analysis (FTA) and Markov analysis
  - Estimates from client, users and domain experts

Consequence and Frequency

Identify Risks

Estimate risk level

Evaluate Risks

Consequence

Frequency

Risk value

Risk ID	Asset	Unwanted incident	Consequence	Frequency
R1	Designs	Designs disclosed to competitor	Moderate	Unlikely
R2	Requirements	Customer requirements disclosed to competitor	Moderate	Unlikely
R3	Client trust	Customer requirements disclosed to competitor	Major	Unlikely
R4	Partner trust	Know how or trade secret enters public domain	Major	Possible
R5	Partner trust	Know how or trade secret loses legal protection	Moderate	Possible

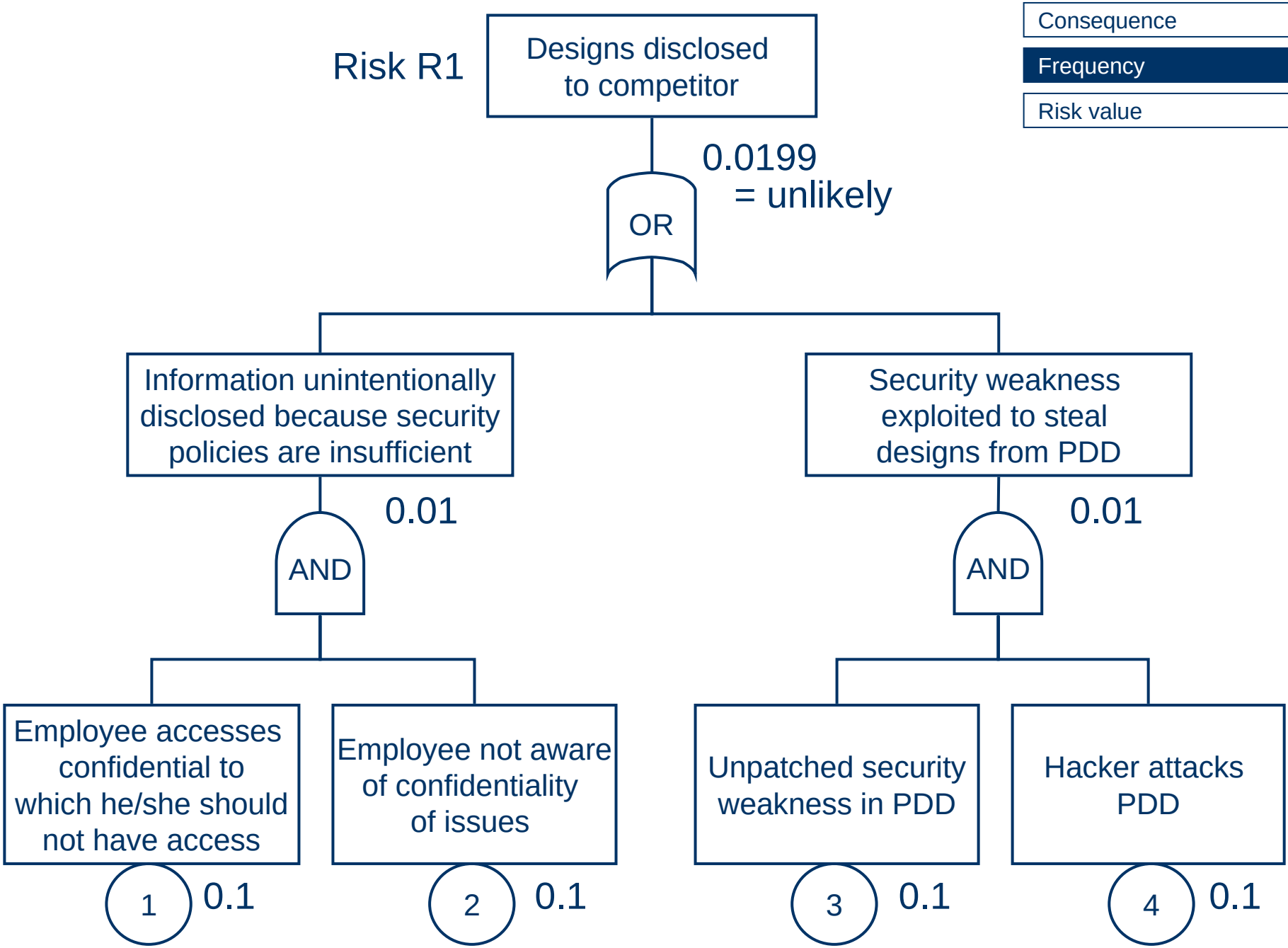
Frequency

- Fault Tree Analysis (FTA) is a useful technique for analysing frequency
- An incident is broken up in its basic events
- The frequency of the top event is aggregated from the basic events using statistical methods

Consequence

Frequency

Risk value



Risk value

- Risk value is a function of consequence and frequency
  - *e.g. Risk value = Consequence value * Frequency value*
- In case of qualitative values, the risk value is estimated by means of the risk matrix

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Low	Low	Low	Moderate	Major
	Unlikely	Low	Low	Moderate	Major	Major
	Possible	Low	Moderate	Major	Major	Extreme
	Likely	Moderate	Major	Major	Extreme	Extreme
	Certain	Moderate	Major	Extreme	Extreme	Extreme

Risk value

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Low	Low	Low	Moderate	Major
	Unlikely	Low	Low	Moderate	Major	Major
	Possible	Low	Moderate	Major	Major	Extreme
	Likely	Moderate	Major	Major	Extreme	Extreme
	Certain	Moderate	Major	Extreme	Extreme	Extreme

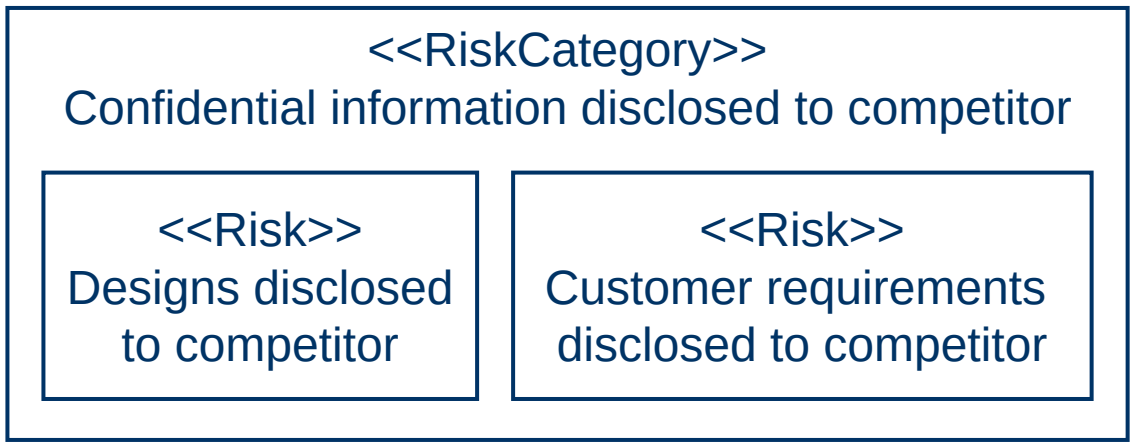
Risk ID	Consequence	Frequency	Risk value
R1	Moderate	Unlikely	Moderate
R2	Moderate	Unlikely	Moderate
R3	Major	Unlikely	Major
R4	Major	Possible	Major
R5	Moderate	Possible	Major

Risk evaluation

- Risks are prioritised (not applied in this analysis)
  - Which risks are most in need of treatment?
  - We may not be in a position to treat all of them
- Risks are grouped into risk categories
- Finally, the risks are evaluated with respect to the risk evaluation criteria

Risk categories

- Risks may be grouped or categorised according to different cross cutting concerns
- We use this as a structuring mechanism
- Similar risks often have common treatments and grouping may reduce the work on treatment identification



Risk evaluation

- To decide which risks to treat, we apply the risk evaluation criteria
- Risks R3, R4 and R5 need treatment

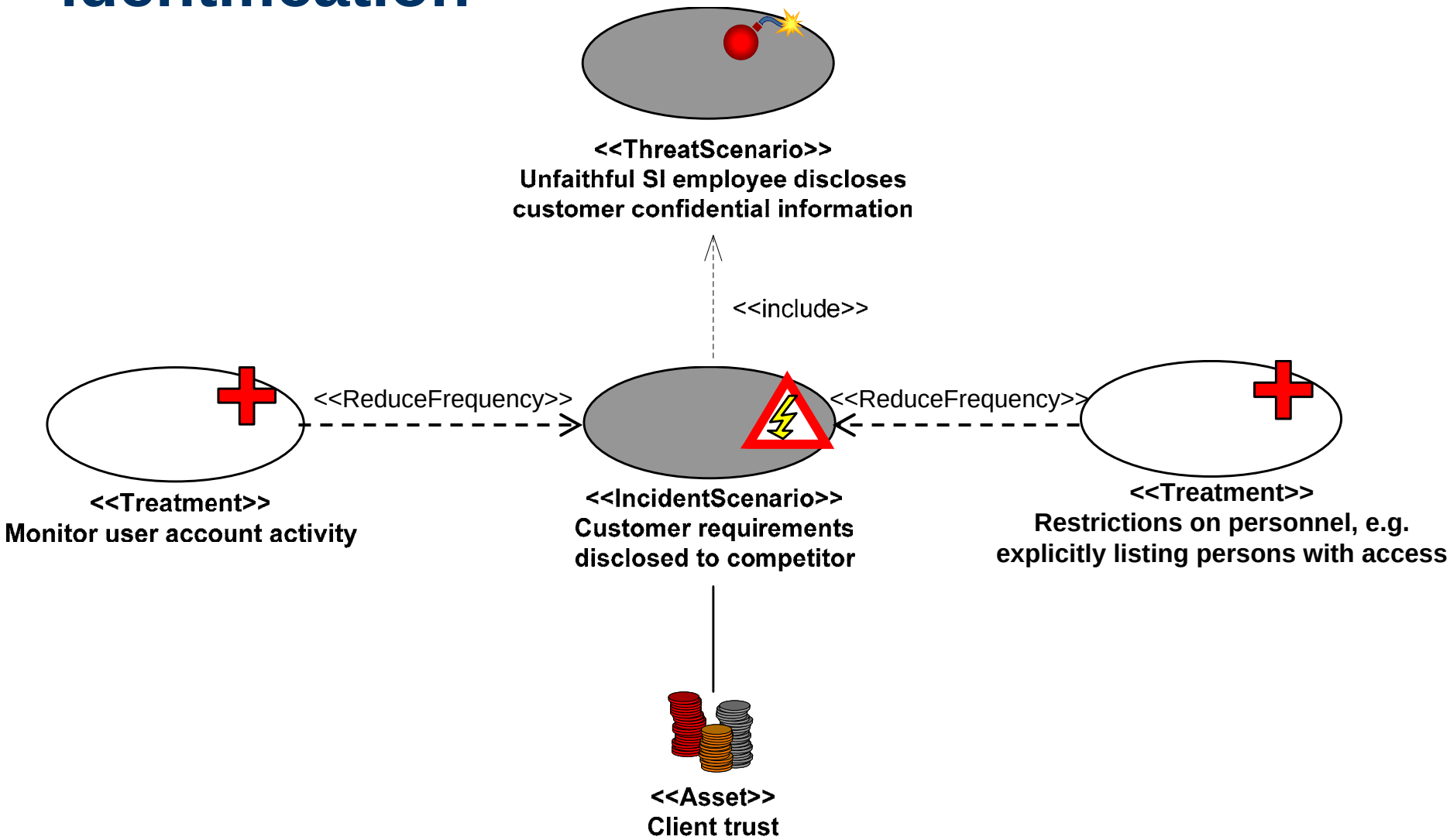
		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Low	Low	Low	Moderate	Major
	Unlikely	Low	Low	**R1, R2**	**R3**	Major
	Possible	Low	Moderate	**R5**	**R4**	Extreme
	Likely	Moderate	Major	Major	Extreme	Extreme
	Certain	Moderate	Major	Extreme	Extreme	Extreme

Accept **Monitor** **Treat**

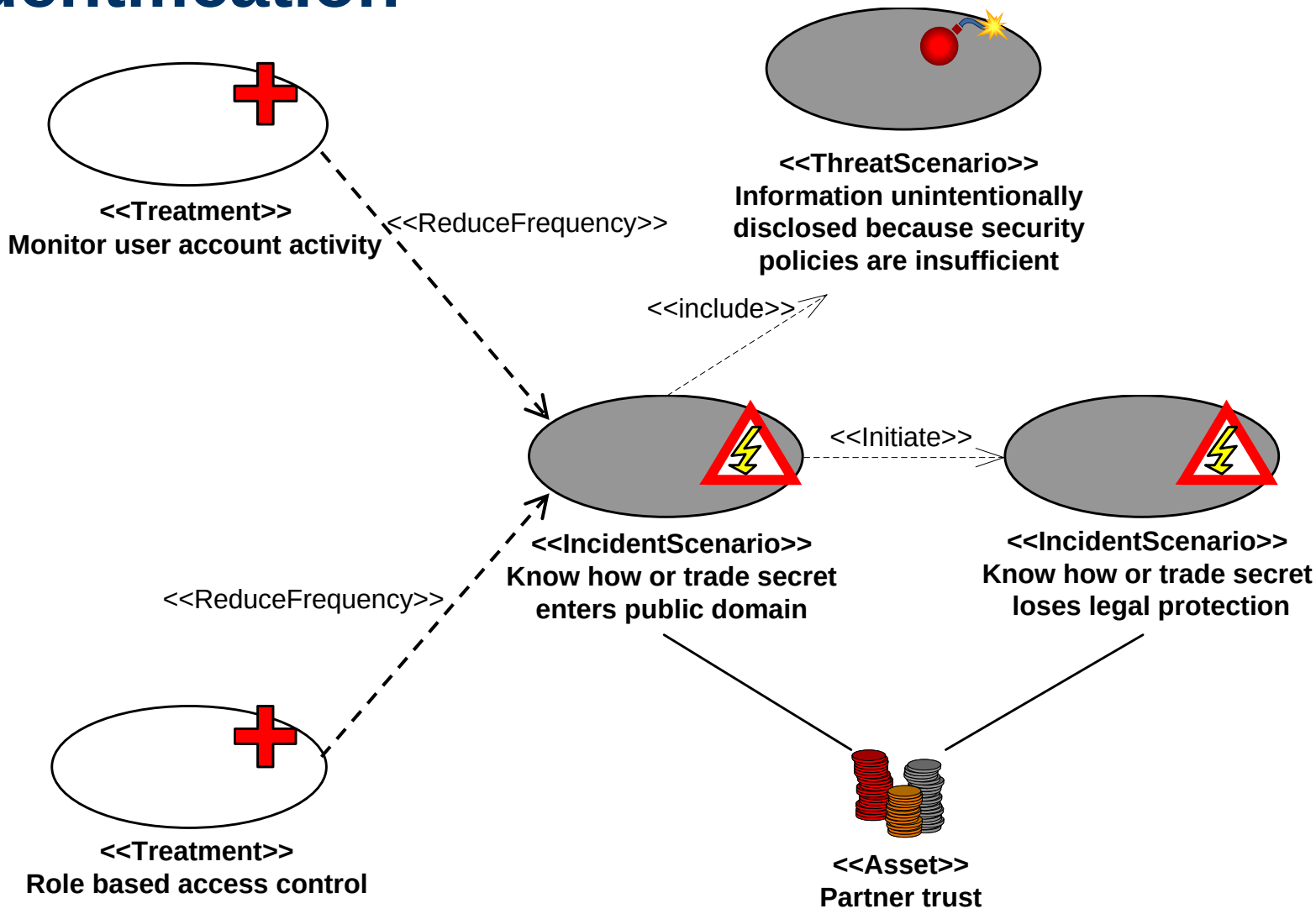
Risk treatment

- When a risk is not accepted, it needs to be treated
- There are three main approaches to treatment
  - Reduce risk level through reducing frequency or consequence
  - Transfer risk, e.g. through insurance or outsourcing
  - Avoid risk by not performing risky activity
- Treatments are identified in a similar fashion as risks, and documented in the same modelling language
- After identification, treatments must be evaluated
  - Risk reduction
  - Cost/benefit

Treatment identification



Treatment identification



Treatment evaluation

- The identified treatments are evaluated with respect to their usefulness
- The evaluation is relative to risk

Risk ID	Treatment	Risk reduction	Cost/ benefit
R3	Monitor user account activity	Major -> Moderate	Low
R3	Restrictions on personnel	Major -> Moderate	High
R4	Monitor user account activity	No	N/A
R4	Role based access control	Major -> Moderate	Medium
R5	Monitor user account activity	Major -> Moderate	Low
R5	Role based access control	Major -> Low	Medium

Summary

- We have been through the risk analysis process
  - Identified threats to and vulnerabilities of assets
  - Identified unwanted incidents from threats and vulnerabilities
  - Identified risks by assigning values to unwanted incidents
  - Evaluated risks with respect to risk evaluation criteria
  - Identified and evaluated treatments
- Made use of the CORAS modelling language
  - Modelling of threat scenarios
  - Modelling of unwanted incidents
  - Modelling of treatments

The CORAS Tool

Model-based analysis of security and trust using CORAS

4. november 2005

Overview

- Motivation
- Overview of the tool
- Tool demonstration
- Future work

Motivation

- Precise, unambiguous and efficient risk analysis
  - Documentation, maintenance and reuse
- Complex systems
- Involves people as well as computerised tools
- Large amounts of information
  - System documentation, analysis data, etc.
- Information is dynamic, changes as the system evolves
- CORAS methodology provides process and guidelines

CORAS Tool

- Fully supports the CORAS methodology
- Easy to use
- Based on open standards, e.g. XMI for UML
- Built on production level open source components
  - JBoss application server, eXist XML database, etc.

- The CORAS Tool and methodology are available under an open source license (LGPL):
  - http://coras.sourceforge.net/

CORAS Tool facilities

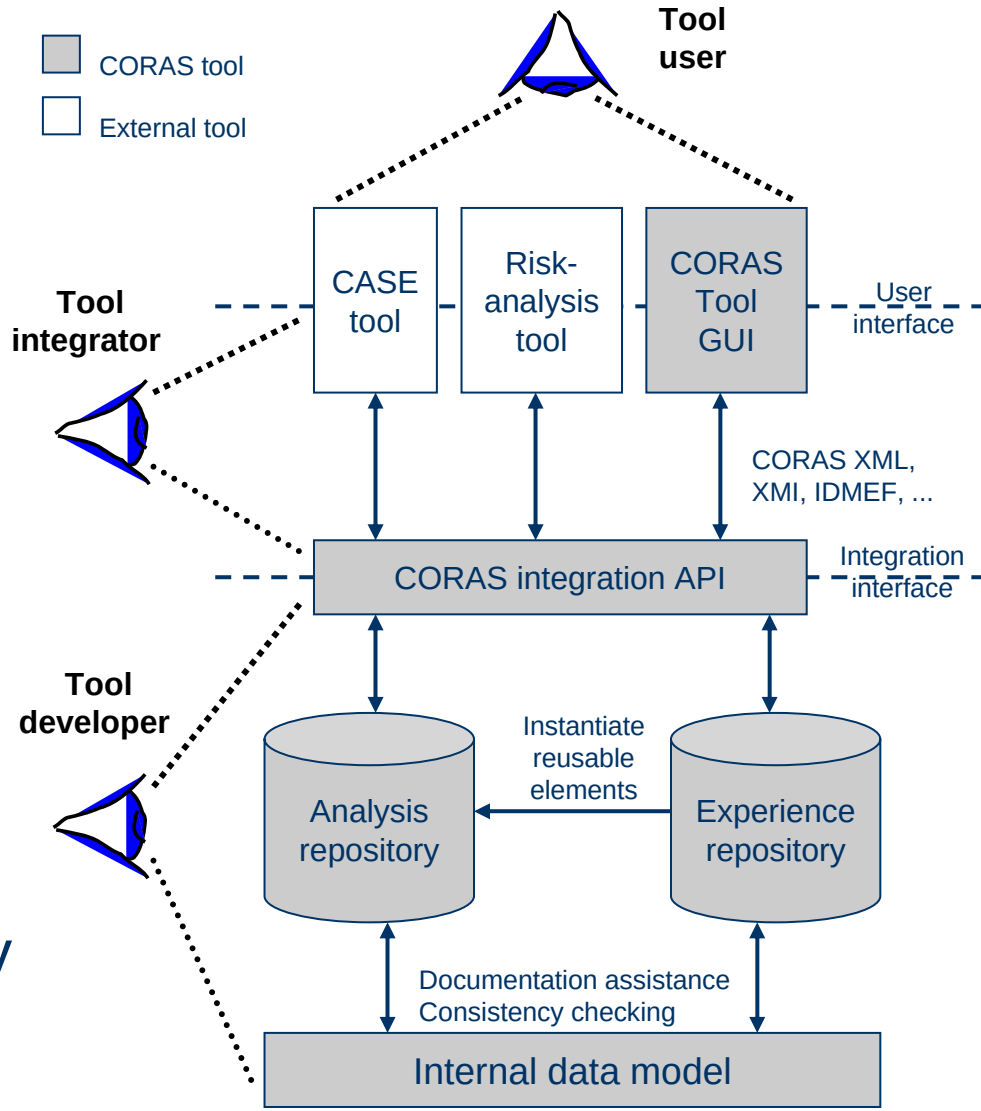
- Repositories for storage, management and reuse of risk analysis data
- Integration with existing modelling and risk analysis tools through standardised open data formats
- Integration of diverse risk analysis methods through underlying risk analysis data model
- Facilitates documentation through e.g. assisting user in filling in table data
- Facilitates maintenance through consistency mechanisms
- Generates risk analysis reports
- Integrated online methodology and user guide

Version 2.0

- Released: 26th September 2005
- Main features:
  - New and improved user interface
  - Improved usability of risk analysis methodology
    - Updated methodology based on user experiences
    - Simplified and more flexible table formats
  - Integrated modelling tool supporting the CORAS language
  - Improved integration with 3rd party applications
  - Keeps track of change history through versioning of all data
  - Generates editable risk analysis reports (RTF format)

Tool architecture

- Two repositories
  - Analysis data
  - Experiences
- Integrate tools for
  - Modelling
  - Risk analysis
- XML integration
- Risk analysis data model
  - Documentation assistance, e.g. filling in table data
  - Consistency checking
- Online help & methodology



Tool demo

Future work

- More automation
  - Documentation assistance
    - E.g. generating tables from UML models and vice versa
  - Consistency repair
- Closer integration with 3rd party tools
  - E.g. cut & paste tables to and from Word/Excel
- Workflow support
  - Tighter integration between tool and methodology

Status and future of CORAS

- Methodology and tool freely available: http://coras.sourceforge.net/
- Results are being taken further in the context of several national and EU-funded projects
  - TrustCoM – Workpackage on risk analysis of trust and legal issues
  - ENFORCE – Formalisation, analysis and enforcement of policies within trust management
  - SECURIS – Security analysis of component based systems
- Current work is focusing on revising the CORAS methodology and language and improving tool support

Further reading

- ***Model based security risk analysis for web applications.*** T. Dimitrakos, D. Raptis, B. Ritchie, K. Stølen. In Proc. Euroweb 2002, British Computer Society, 2002
- ***The CORAS tool-supported methodology for UML-based security analysis***, F. Vraalsen, F. den Braber, I. Hogganvik, K. Stølen, SINTEF Technical report STF90 A04015, SINTEF ICT, February 2004.
- ***Using risk analysis to assess user trust – a net-bank scenario.*** G. Brændeland, K. Stølen. In Proc. Second International Conference on Trust Management (iTrust'04), LNCS 2995, pages 146-160, Springer, 2004.
- ***Specifying Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experience and the Way Forward.*** F. Vraalsen, M.S. Lund, T. Mahler, X. Parent, K. Stølen. To appear in Proc. Third International Conference on Trust Management (iTrust'05), Springer, 2005.
- ***Integrating security in the development process with UML.*** F. den Braber, M. S. Lund, K. Stølen, F. Vraalsen. In Encyclopedia of Information Science and Technology. Mehdi Khosrow-Pour (ed), pages 1560-1566, Idea Group, 2005.
- ***Experiences from Using the CORAS Methodology to Analyze a Web Application.*** F. den Braber, A.-B. Mildal, J. Nes, K. Stølen, F. Vraalsen. To appear in Journal of Cases on Information Technology.
- ***Using the CORAS threat modelling language to document threat scenarios for several Microsoft relevant technologies.*** F. den Braber, M. S. Lund, K. Stølen. Technical report STF90 A04057, SINTEF, 2004.

Contact information

- Folker den Braber
  - E-mail: folker.den.braber@sintef.no
- Fredrik Vraalsen
  - E-mail: fredrik.vraalsen@sintef.no
- CORAS webpage: http://coras.sourceforge.net/