

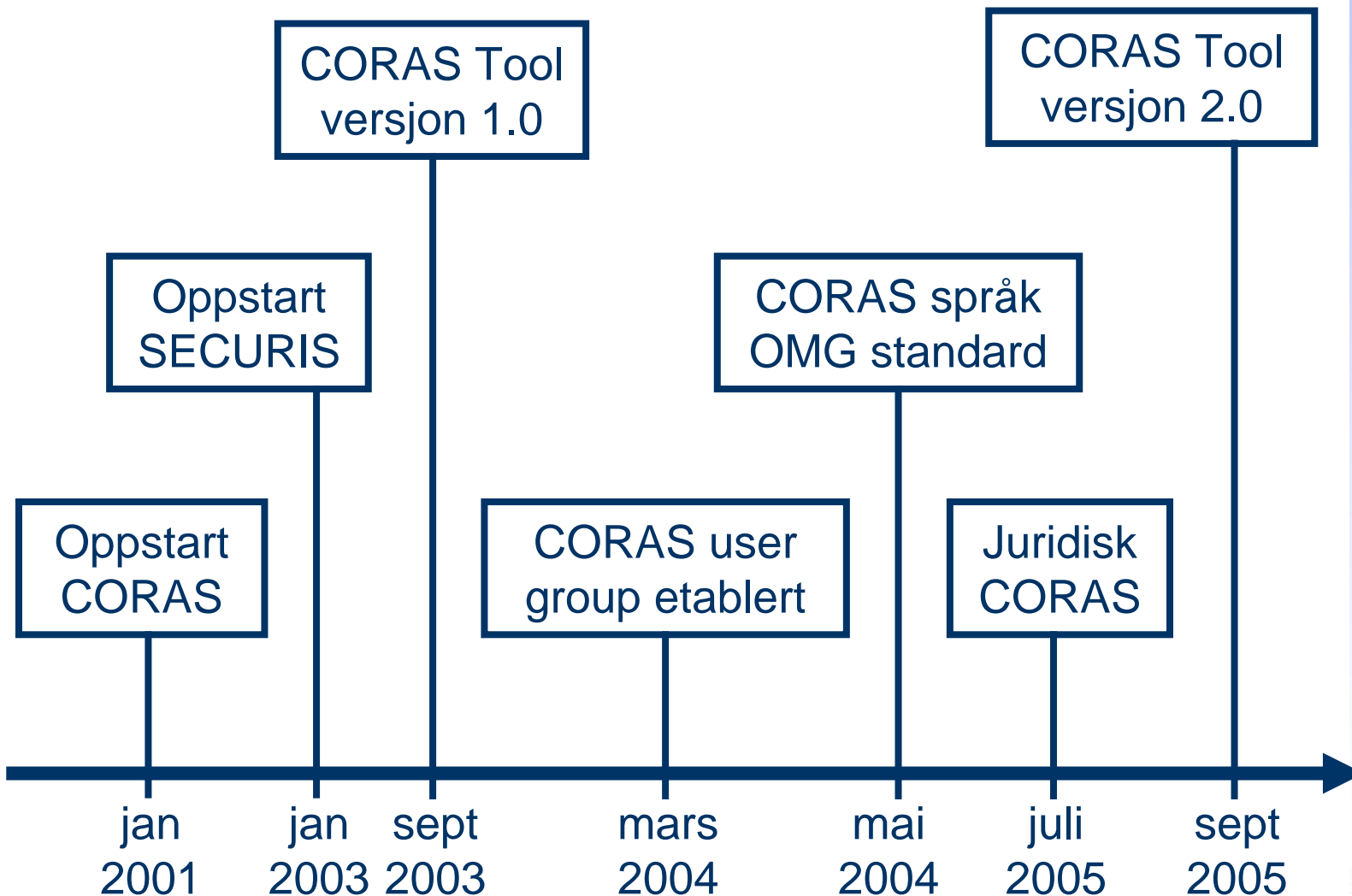
Sikkerhetsanalyse ved hjelp av CORAS 2.0

Fredrik Vraalsen
SINTEF

24/11-05



CORAS' historie



CORAS
Tool
2.0



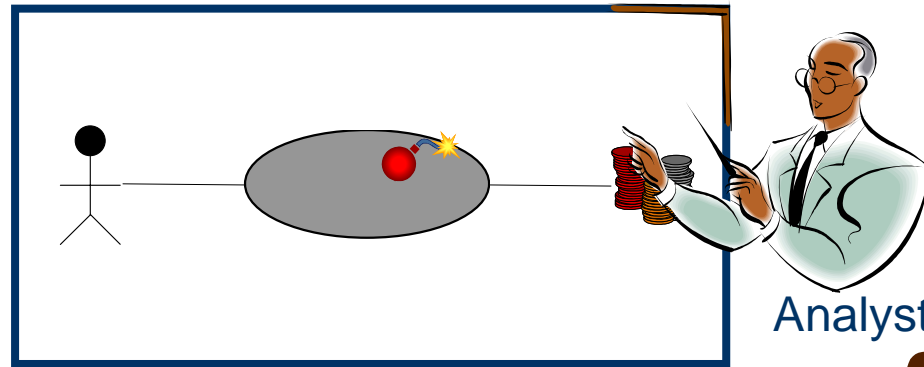
© 2003-2005 SINTEF
<http://coras.sourceforge.net>

CORAS i praksis

- 7 feltstudier i løpet av selve CORAS-prosjektet
 - E-handel og telemedisin
- Risikoanalyser i nasjonale og internasjonale prosjekter
 - Autentisering i mobile tjenester
 - Elektronisk dokumenthåndtering
 - Mobil tilgang til informasjonssystemer
 - Tillit og juridiske problemstillinger i virtuelle organisasjoner
 - Kraftforsyning
 - Prosesskontroll



Modellbasert risikoanalyse



Analyst



System manager



Security expert



System developer



System user:
medical doctor



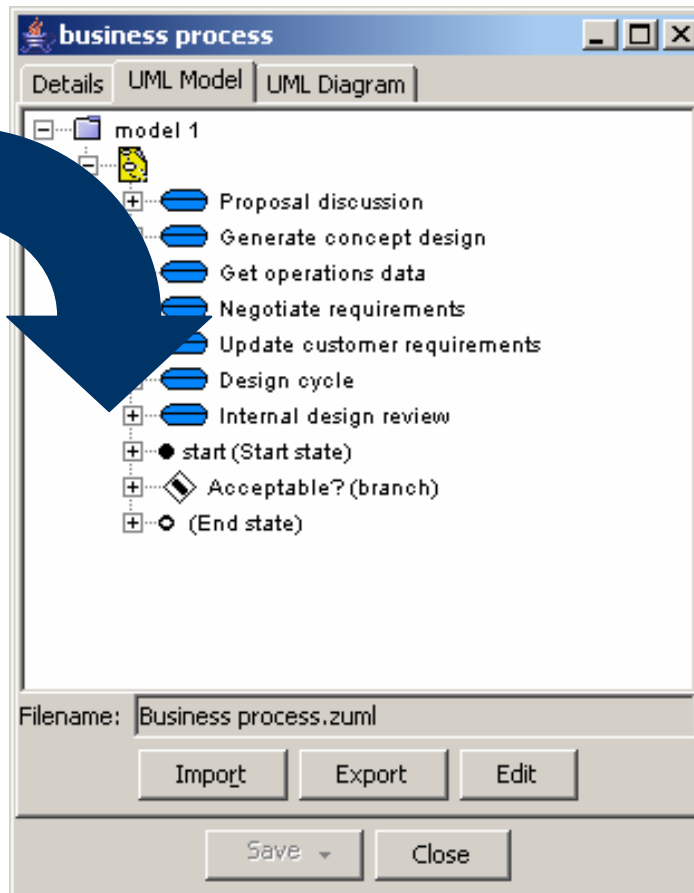
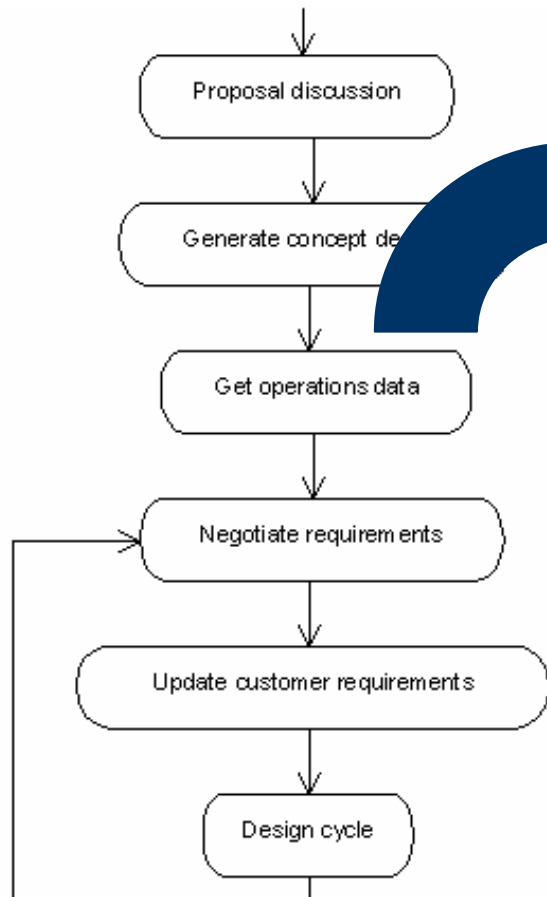
CORAS-verktøyet

- Understøtter risikoanalysemetodikken
 - Dokumentasjon, presentasjon, vedlikehold og gjenbruk av risikoanalyser og resultater
- Integrasjon med 3dje-parts verktøy
 - Systemutvikling, f.eks. UML-modellering
 - Risikoanalyse, f.eks. feiltreanalyse
 - Basert på standardiserte dataformater
 - Muliggjør samvirke med verktøy som allerede er i bruk



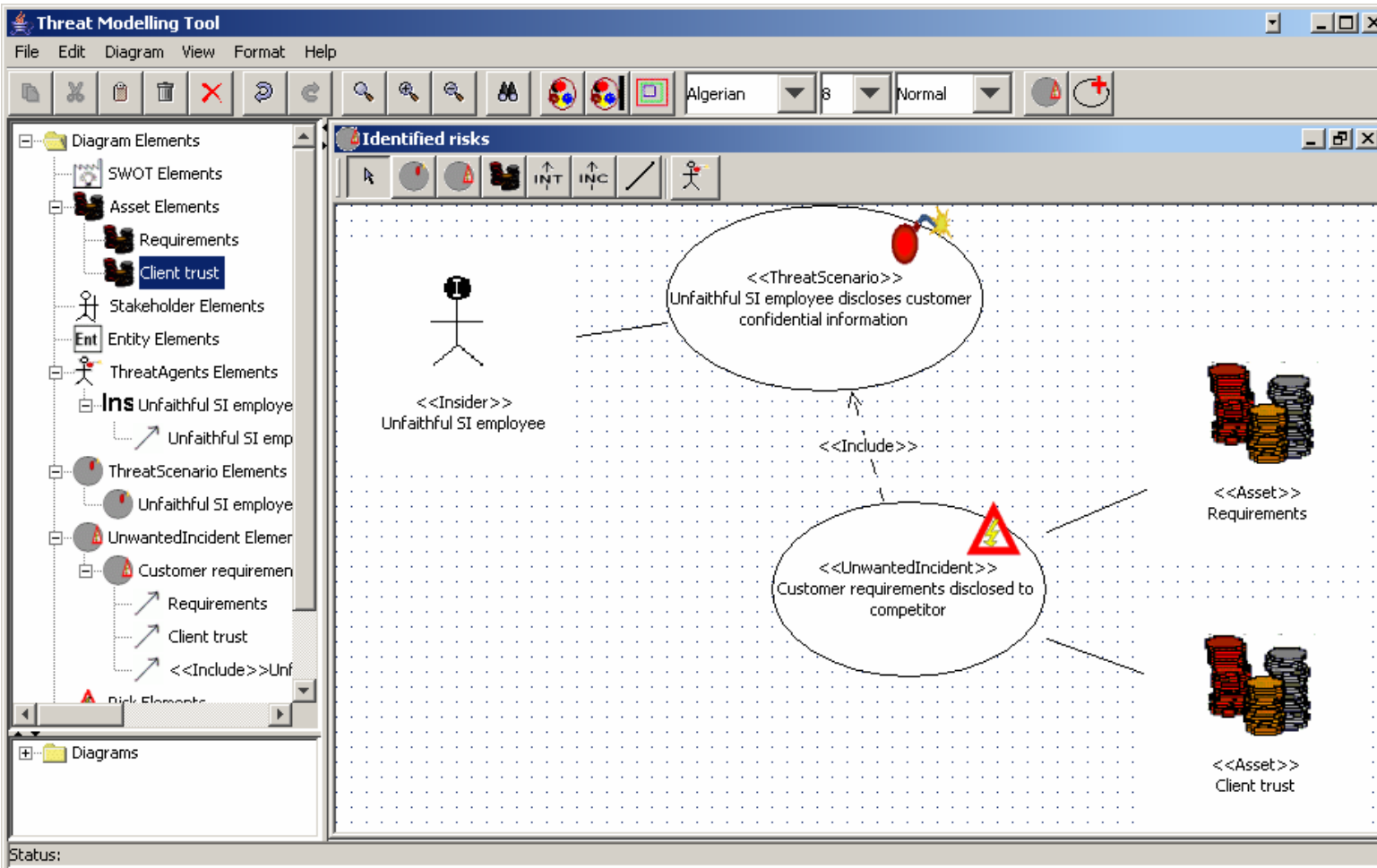
Integrasjon med UML-verktøy

Systemdokumentasjon i UML,
f.eks. aktivitetsdiagrammer



Direkte støtte for CORAS-språket

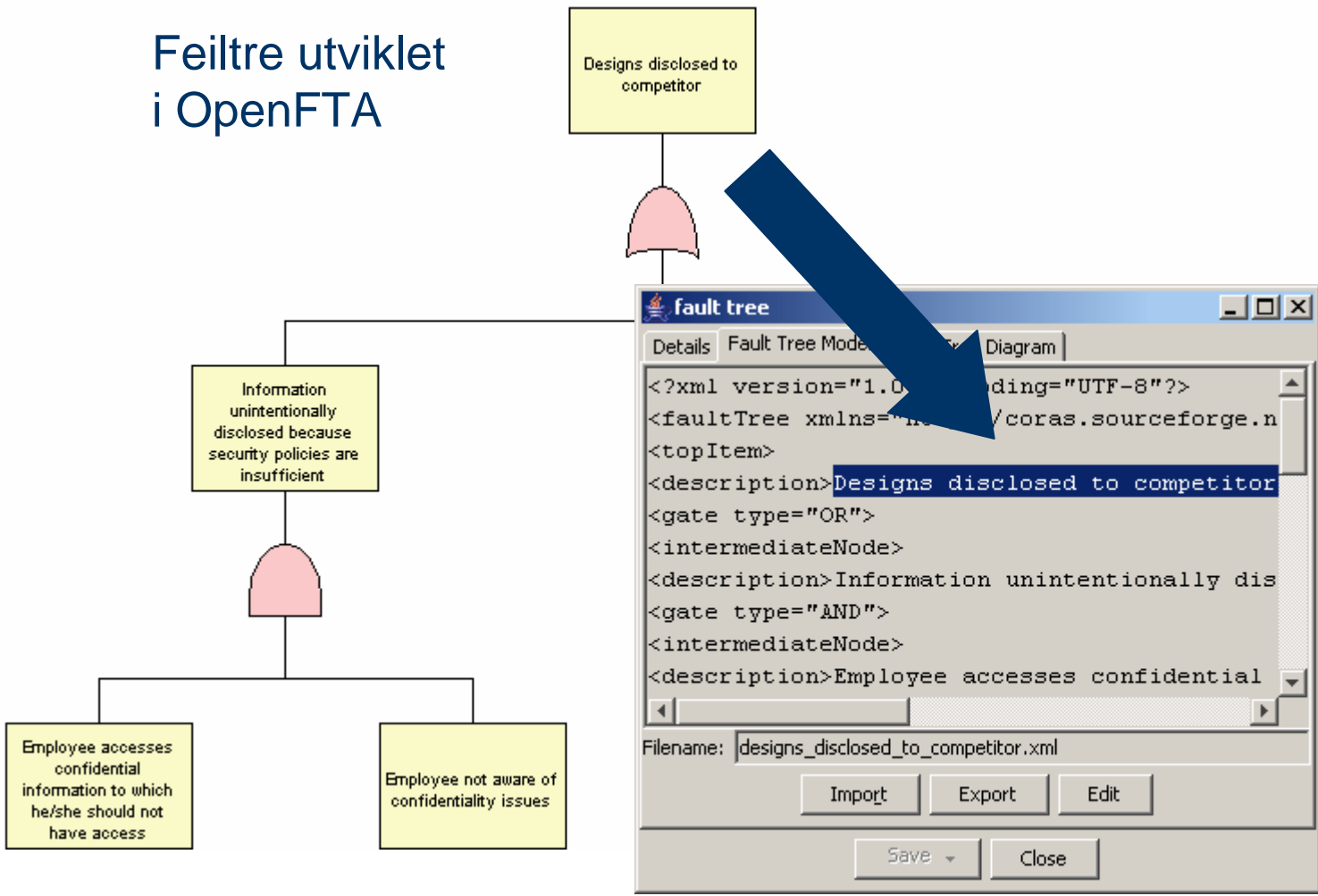
CORAS
Tool
2.0



© 2003-2005 SINTEF
<http://coras.sourceforge.net>

Import av feiltreanalyse

Feiltre utviklet i OpenFTA



Elektronisk versjon av metodikk

CORAS
Tool
2.0

The screenshot shows the CORAS Risk Analysis Tool interface. The title bar reads "CORAS Risk Analysis Tool". The menu bar includes "File" and "Help". Below the menu bar are three tabs: "Risk Analysis Project", "Experience Library", and "CORAS Methodology". A navigation bar contains "Home", "Back", and "Forward" buttons. The main content area is titled "CORAS Methodology" and features a "Welcome to the CORAS Methodology Guide!" section. A left sidebar lists sub-processes: Context Identification, Risk Identification, Risk Estimation, Risk Evaluation, and Risk Treatment. A blue box in the sidebar contains instructions: "Use the menu buttons above to navigate through the different sub-processes. This main menu is always available under the dark blue square at the top of the main content window." The main content area also includes sections for "Context Identification", "Risk Identification", "Risk Estimation", and "Risk Evaluation". The status bar at the bottom shows the file path: "file:///D:/CORAS%20Tool%202.0.2/client/help/help/navmeny.html#".

CORAS Methodology

Welcome to the CORAS Methodology Guide!

Use the menu on the left to navigate through the different sub-processes. This start page is always available under the dark blue square at the top of the main content window.

Context Identification

The context identification sub process consists of four main activities that should be carried out in a sequential order.

Risk Identification

The risk identification sub-process consists of three activities of which the first two are complementary and may be carried out in arbitrary order. The third is advised to be performed after the other two have been completed.

Risk Estimation

The chosen methods for consequence and frequency evaluation depend on the results from the risk identification sub process, the historical information available and the analysis group's ability to assign consequence values and frequency values. It is often advisable to combine complementary approaches, for example, a bottom-up and a top-down approach.

Risk Evaluation



© 2003-2005 SINTEF
<http://coras.sourceforge.net>

Understøtter dokumentasjon

The screenshot displays the CORAS Risk Analysis Tool interface. The main window is titled "CORAS Risk Analysis Tool" and has a menu bar with "File" and "Help". Below the menu bar are three tabs: "Risk Analysis Project", "Experience Library", and "CORAS Methodology".

The left sidebar shows a tree view of the project structure under "demo":

- Context identification
 - value definitions
 - business process**
 - assets
- Risk identification
 - identified risks
 - risk scenarios
- Risk analysis
 - Fault tree
- Risk evaluation
- Risk treatment

The "Element Info" panel on the left shows details for the selected "business process":

- Type: Other Diagram
- Name: business process
- Description:
- Concern: SWOT
- Viewpoint: Enterprise, Information, Computational, Engineering, Technology
- Full description:

The main workspace shows a "risk scenarios" window with a "Table Editor" tab. The table has columns: Scenario ID, Asset ID, Reference, Threat, Vulnerability, Incident, Scenario. The "Partner trust" asset is listed under "Asset ID". A context menu is open over the table, listing actions:

- Proposal discussion
- Generate concept design
- Get operations data
- Negotiate requirements
- Update customer requirements
- Design cycle
- Internal design review

A large blue arrow points from the context menu to a diagram view below it, which shows a state transition diagram with nodes and transitions. The nodes include:

- Proposal discussion
- Generate concept design
- Get operations data
- Negotiate requirements
- Update customer requirements
- Design cycle
- Internal design review
- start (Start state)
- Acceptable? (branch)
- (End state)

The diagram view also shows a "Filename: Business process.zuml" field and buttons for "Import", "Export", "Edit", "Save", and "Close".



Vedlikehold – konsistens

The screenshot displays the CORAS Risk Analysis Tool interface. The main window is titled "CORAS Risk Analysis Tool" and has a menu bar with "File" and "Help". Below the menu bar are three tabs: "Risk Analysis Project", "Experience Library", and "CORAS Methodology".

On the left side, there is a tree view under the "demo" folder containing the following sub-folders: "Context identification" (with sub-items "value definitions", "business process", and "assets"), "Risk identification" (with sub-items "identified risks" and "risk scenarios"), "Risk analysis" (with sub-item "fault tree"), "Risk evaluation", and "Risk treatment".

Below the tree view is the "Element Info" panel, which shows the following details for the selected "assets" element:

- Type: Asset Table
- Name: assets
- Description:
- Concern: Assets
- Viewpoint:
 - Enterprise
 - Information
 - Computational
 - Engineering
 - Technology
- Full description:

The main workspace contains two windows:

1. "risk scenarios" window (Table Editor):

Scenario ID	Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
	Partner trust	Proposal discussion	Unfaithful SI employee		Designs disclosed to competitor	

Buttons: Insert Row Above, Insert Row Below, Delete Row, Save, Close.

2. "assets" window (Table Editor):

Asset ID	Description	Category	Value
Designs	SI's share in the designs of the passenger aircraft	Information	Very High
Partner trust	The CO partners' trust in SI	Other	High

Buttons: Insert Row Above, Insert Row Below, Delete Row, Save, Close.



Vedlikehold – konsistens

The screenshot displays the CORAS Risk Analysis Tool interface. The main window is titled "CORAS Risk Analysis Tool" and has a menu bar with "File" and "Help". Below the menu bar are three tabs: "Risk Analysis Project", "Experience Library", and "CORAS Methodology". The "Risk Analysis Project" tab is active, showing a tree view of the project structure. The "risk scenarios" window is open, displaying a table with the following data:

Scenario ID	Asset ID	Reference	Threat	Vulnerability	Incident	Scenario
	Partner trust	Proposal discussion	Unfaithful SI employee		Designs disclosed to competitor	

A "Consistency check result for risk scenarios" dialog box is overlaid on the main window. It contains a table with the following data:

Description	
	Row 1: Asset with ID 'Partner trust' is not defined.
	Row 1: Missing scenario ID.
	Row 1: No vulnerability defined.
	Row 1: No scenario defined.

At the bottom of the dialog box, there is a checked checkbox labeled "Show warnings" and a "Close" button.



Oppsummering

- CORAS 2.0 integrerer
 - forskjellige risikoanalyseteknikker
 - metodikk for systemutvikling
- Grafisk språk for dokumentasjon av risiko
 - Understøtter kommunikasjon og forståelse
- Verktøystøtte
 - Dokumentasjon, presentasjon, vedlikehold og gjenbruk av risikoanalyser og resultater
- Verktøy og metode gratis tilgjengelig (åpen kildekode)
 - <http://coras.sourceforge.net/>



**Lyst til å prøve?
Behov for en analyse?
Ta kontakt!**

Fredrik Vraalsen

fredrik.vraalsen@sintef.no

Gratis CORAS 2.0 CD deles ut til alle som
vil ha 😊

