

# Towards a UML Profile for Model-Based Risk Assessment

Siv-Hilde Houmb<sup>1</sup>, Folker den Braber<sup>2</sup>, Mass Soldal Lund<sup>2</sup>, Ketil Stølen<sup>2</sup>

<sup>1</sup>Telenor R&D, Norway, siv-hilde.houmb@telenor.com

<sup>2</sup>Sintef Telecom & Informatics, Norway, {fbr,msl,kst}@sintef.no

## abstract

The EU-funded CORAS project (IST-2000-25031) is developing a framework for model-based risk assessment of security-critical systems. This framework is characterised by: (1) A careful integration of aspects from partly complementary risk assessment methods. (2) Guidelines and methodology for the use of UML to support and direct the risk assessment methodology. (3) A risk management process based on AS/NZS 4360 and ISO/IEC 17799. (4) A risk documentation framework based on RM-ODP. (5) An integrated risk management and system development process based on UP. (6) A platform for tool-inclusion based on XML.

This paper focuses on one specific aspect of the CORAS framework, namely the CORAS UML profile for risk assessment. In particular, it explains its role in the CORAS risk management process and demonstrates its use in the risk assessment of an e-commerce system.

## 1. Introduction

CORAS aims for improved methodology and computerised support for precise, unambiguous, and efficient risk assessment of security-critical systems. CORAS addresses security-critical systems in general, but places particular emphasis on IT security. IT security includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems [6]. An IT system for CORAS is not just technology, but also the humans interacting with the technology, and all relevant aspects of the surrounding organisation and society.

The main result of the CORAS project is the CORAS framework. This framework is characterised by: (1) A careful integration of aspects from partly complementary risk assessment methods like HazOp [10], FTA [5], FMEA [3], Markov analysis [17] and CRAMM [2]. (2) Guidelines and methodology for the use of UML [12] to support and direct the risk assessment methodology. (3) A risk management process based on AS/NZS 4360 [1] and ISO/IEC 17799 [7]. (4) A risk documentation framework based on RM-ODP [13]. (5) An integrated risk management and system development process based on UP [9]. (6) A platform for tool-inclusion based on XML [19].

An important aspect of the CORAS project is the practical use of UML to support the risk management process in general, and risk assessment in particular. Risk assessments are costly and time consuming and should not be initiated from scratch each time we assess a new or modified system. Documenting risk assessments using a modelling language like UML supports reuse of risk assessment documentation, both for systems that undergo maintenance and for new systems, if similar systems have been assessed earlier. The CORAS UML profile for risk assessment provides rules and constraints for risk

assessment relevant system documentation, and hence increases the possibility of reuse of risk assessment documentation by introducing a common use of models in risk assessment.

One major challenge when performing a risk assessment is to establish a common understanding of the target of evaluation, threats, vulnerabilities and risks among the stakeholders participating in the assessment. The CORAS UML profile has been designed to facilitate improved communication during risk assessments. The CORAS UML profile aim at making the UML diagrams easier to understand for non-experts, while at the same time preserve the well-definedness of UML.

Requirements to security documentation and the demands for documented security are increasing. This will impel standards for ensuring and documenting the security of IT systems. The CORAS UML profile for risk assessment constitutes a contribution in this direction.

The remainder of the paper is divided into five main sections and one appendix. Sections 2, 3 and 4 provide background on the CORAS risk management process, the CORAS model-based risk assessment methodology, and the CORAS risk documentation framework, respectively. Section 1 exemplifies the use of the CORAS UML profile in the risk assessment of an e-commerce system. Section 6 draws the main conclusions. The appendix provides a more formal definition of the CORAS UML profile for model-based risk assessment.

## 2. The CORAS risk management process

As indicated by Figure 1, the CORAS risk management process is sequenced into sub-processes for context identification, risk identification, risk assessment, risk evaluation, and risk treatment. In addition, there are two sub-processes, targeting communication and consultation as well as monitoring and review, running in parallel with the other five.

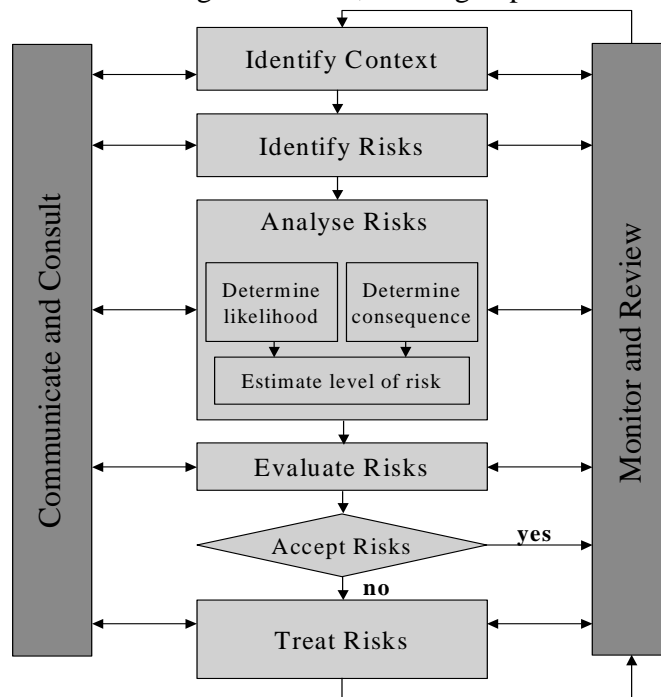


Figure 1: The CORAS risk management process

The sub-processes for context identification, risk identification, risk analysis, risk evaluation and risk treatment are decomposed into activities as specified in Figure 2.

<p><b>Sub-process 1: Identify Context:</b></p> <ul style="list-style-type: none"> <li>• Activity 1.1: Identify areas of relevance</li> <li>• Activity 1.2: Identify and value assets</li> <li>• Activity 1.3: Identify policies and evaluation criteria</li> <li>• Activity 1.4: Approval</li> </ul> <p><b>Sub-process 2: Identify Risks:</b></p> <ul style="list-style-type: none"> <li>• Activity 2.1: Identify threats to assets</li> <li>• Activity 2.2: Identify vulnerabilities of assets</li> <li>• Activity 2.3: Document unwanted incidents</li> </ul> <p><b>Sub-process 3: Analyse Risks</b></p> <ul style="list-style-type: none"> <li>• Activity 3.1: Consequence evaluation</li> <li>• Activity 3.2: Frequency evaluation</li> </ul>	<p><b>Sub-process 4: Risk Evaluation</b></p> <ul style="list-style-type: none"> <li>• Activity 4.1: Determine level of risk</li> <li>• Activity 4.2: Prioritise risks</li> <li>• Activity 4.3: Categorise risks</li> <li>• Activity 4.4: Determine interrelationships among risk themes</li> <li>• Activity 4.5: Prioritise the resulting risk themes and risks</li> </ul> <p><b>Sub-process 5: Risk Treatment</b></p> <ul style="list-style-type: none"> <li>• Activity 5.1: Identify treatment options</li> <li>• Activity 5.2: Assess alternative treatment approaches</li> </ul>
---	--

Figure 2: Activities of the CORAS risk management process

### 3. The CORAS model-based risk assessment methodology

As illustrated in Figure 3, the CORAS risk assessment methodology is model-based in the sense that it makes use of models for three different purposes: (1) Models are used to describe the target of evaluation at the right level of abstraction and to direct and guide the use of assessment methodology. (2) Models are used as medium for communication and interaction between different groups of stakeholders involved in a risk assessment. (3) Models are used to document risk assessment results and the assumptions on which these results depend.

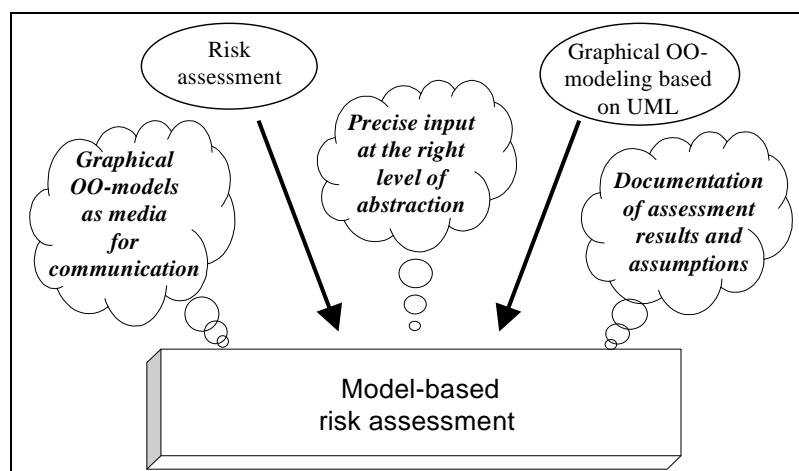


Figure 3: Model-based risk assessment

To facilitate model-based risk assessment, a CORAS specific UML profile is under development. The profile defines UML stereotypes to further communication and interaction among stakeholders involved in an assessment. It also defines more specialised kinds of UML diagrams, to further the documentation of risk assessment results. Currently, the CORAS UML profile for risk assessment consists of six packages:

- *Actors Package* (Figure 17), which defines actor stereotypes;
- *SWOT Model Package* (Figure 18), which defines SWOT diagrams;
- *Asset Model Package* (Figure 19), which defines Asset diagrams;
- *Threat Model Package* (Figure 20), which defines Threat diagrams;
- *State Analysis Model Package* (Figure 21), which defines State Analysis diagrams;
- *Treatment Model Package* (Figure 22), which defines Treatment diagrams.

Section 1 introduces and presents the concrete syntax of stereotypes and diagrams in an example-driven manner. The appendix provides a more formal definition of the profile.

#### 4. The CORAS risk documentation framework

The CORAS risk documentation framework divides the RM-ODP viewpoint structure into 22 concerns targeting security in general and model-based risk assessment in particular. As indicated by Figure 4, concerns are cross-viewpoint perspectives linking together related information within different viewpoints.

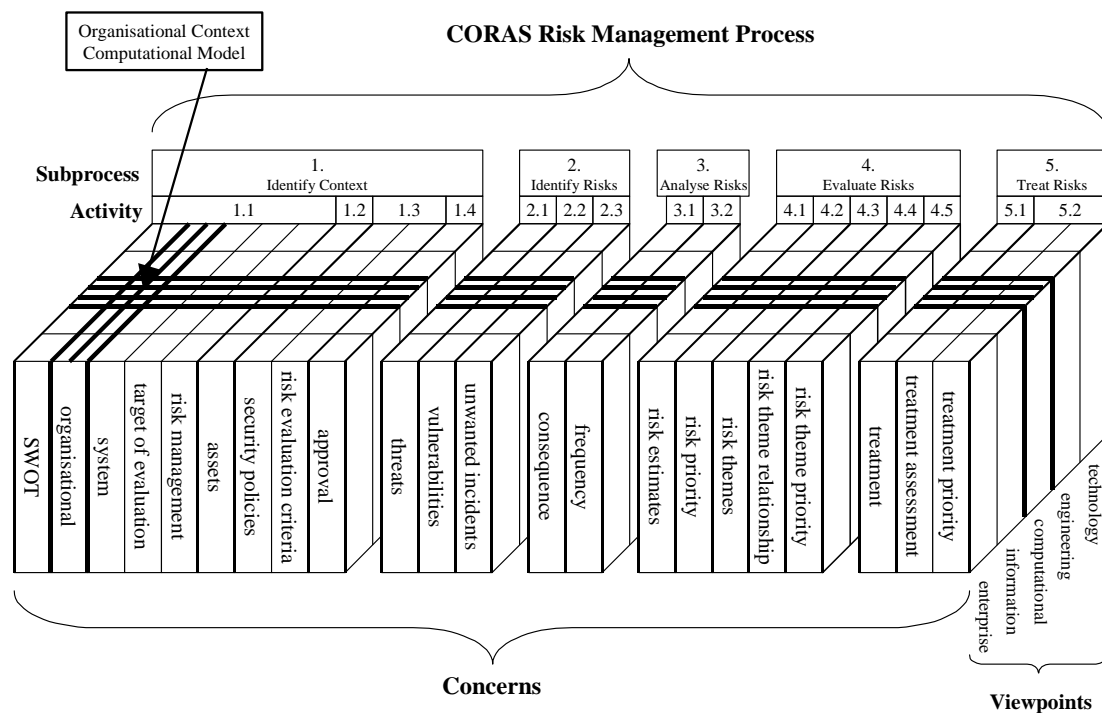


Figure 4: The CORAS risk documentation framework

Each concern is divided into the five RM-ODP viewpoints. One or several of its viewpoints may be empty depending on the concern in question as well as the target and rigour of evaluation. However if not empty, each concern-viewpoint will contain a set of element instances. An element may be a model, a risk assessment table, a tree, natural

language text, etc. Different instances of the same element may occur within different viewpoints of the same concern. Elements may be classified into:

- Elements containing non-CORAS specific documentation, which refers to elements that are not prepared as a part of the CORAS risk management process. Since CORAS should be applicable to a wide scope of systems, including already existing systems, this kind of elements is unconstrained.
- Modelling elements (constructed as part of the risk management process) expressed in UML.
- Logs from intrusion detection tools and computerised vulnerability assessment represent.
- Risk assessment tables and trees.

As indicated by Figure 4, the concerns are structured in accordance with the CORAS risk management process. Each concern is assigned a specific activity under a sub-process.

## **5. Using the CORAS UML profile to assess an e-commerce system**

In the following we demonstrate the use of the CORAS UML profile in the risk assessment of an e-commerce system. Due to space limitations we can for obvious reasons only address a few of the many steps such an assessment involves. We will focus on the following:

- SWOT analysis under Activity 1.1
- Identification and valuing of assets under Activity 1.2
- Model-based threat and vulnerability identification under Activities 2.1 and 2.2
- Model-based consequence and frequency evaluation under Activities 3.1 and 3.2
- Model-based risk treatment under Activity 5.1

Before going into details on the risk assessment process, some background on the e-commerce system, SecureBuy, to be assessed is required. The description is based on the specification provided in [4], which aims at developing a stochastic model for analyzing risk for e-Commerce systems in general.

We assume that the system owner, the company Secure e-Commerce, has developed the system themselves, has prior experience in both developing and using e-Commerce systems, and has employees with experience in working with security issues in software systems. However, the SecurePay system is new and security issues have not yet been an issue, which means that no security mechanisms are implemented at the time of the risk assessment, and that risk assessment is not a part of the company's development process. The UML use-case in Figure 5 focuses on the purchase process. It presents the main stakeholders and provides ten services: Request for service, Offer service, Push service, Order service, Control order, Cancel order, Payment, Deliver service, Cancel delivery and Return of service, which interact between three stakeholders; Consumer, Supplier and BBS (the interface between Bank/Finance network and Internet in Norway).

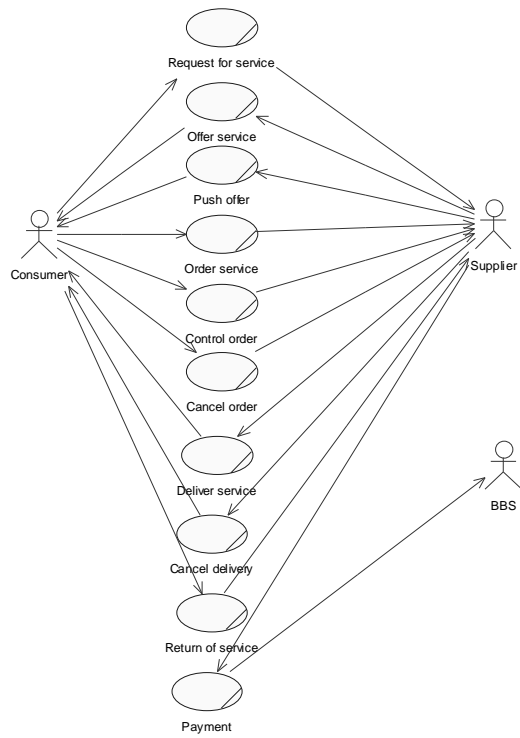


Figure 5: Use case diagram specifying main stakeholders and services

The sequence diagram in Figure 6 specifies an example-run addressing five of these use-cases.

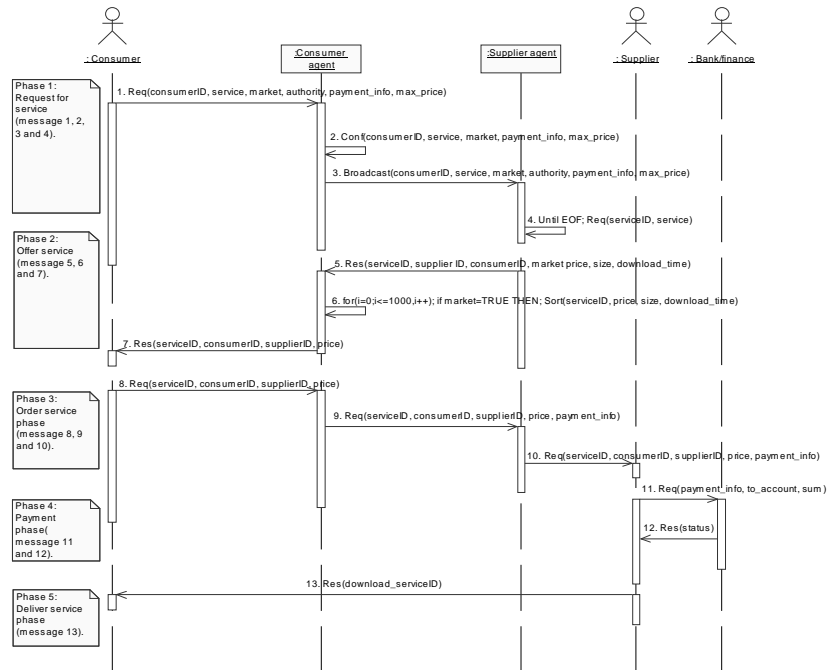


Figure 6: Specification of interaction between stakeholders

The interaction is described using four kinds of messages:

1. Req - Request message.
2. Res - Result (of a prior request) message.
3. Conf - Configuration message.
4. Broadcast - Broadcast message.

### 5.1 SWOT analysis under Activity 1.1

In the CORAS methodology a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is normally used to define the relationship between the organisation within which the target of evaluation is situated and its environment (but it may also be employed at a more technical level). The SWOT analysis is used for identifying high-level strengths, weaknesses, opportunities and enterprise threats, and will often identify the general direction of the rest of the assessment.

The results from the SWOT analysis are documented in the SWOT concern that consists of three elements: a SWOT results table, a stakeholder table and a SWOT diagram. The SWOT diagram in Figure 7 summarises results from a SWOT analysis targetting Secure e-Commerce.

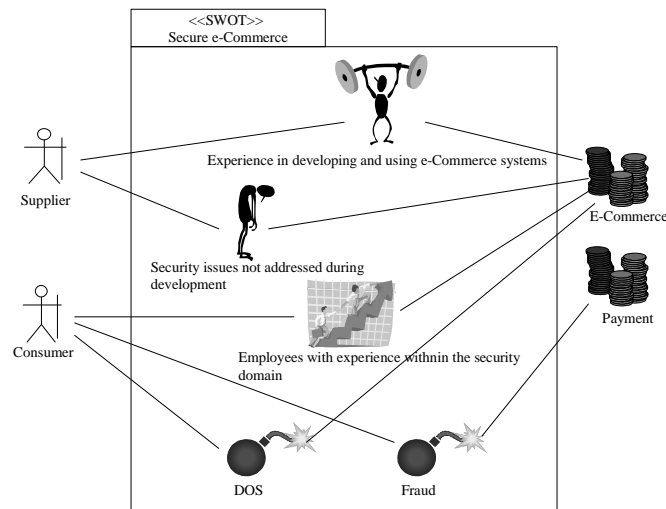


Figure 7: SWOT for the organization Secure e-Commerce

SWOT for the organization Secure e-Commerce:

Strengths

- Experience in developing e-Commerce systems
- Experience in using e-Commerce systems

Weaknesses

- Security issues not assessed during development process

Opportunities

- Employees with experience within the security domain

Threats

- Fraud against Consumers based on information an attacker has gained through the e-Commerce system
- Denial of service (DOS)

## 5.2 Identification and valuing of assets under Activity 1.2

Assets identification and valuing are a very important aspects of a security assessment. If there are no assets there is nothing to protect, and no reason to worry about security. In fact, the CORAS methodology is asset directed in the sense that the set of assets identified under Activity 1.2 strongly determine the assessment activities following thereafter. The results from the asset identification and valuing are documented in the assets concern, which contains two elements: an asset table and an asset diagram. Asset diagrams are specialised Class diagrams. Assets are grouped in themes with the Asset theme stereotype, and the relationships between assets are expressed by standard associations. The asset diagram is also used to document the valuing of the assets.

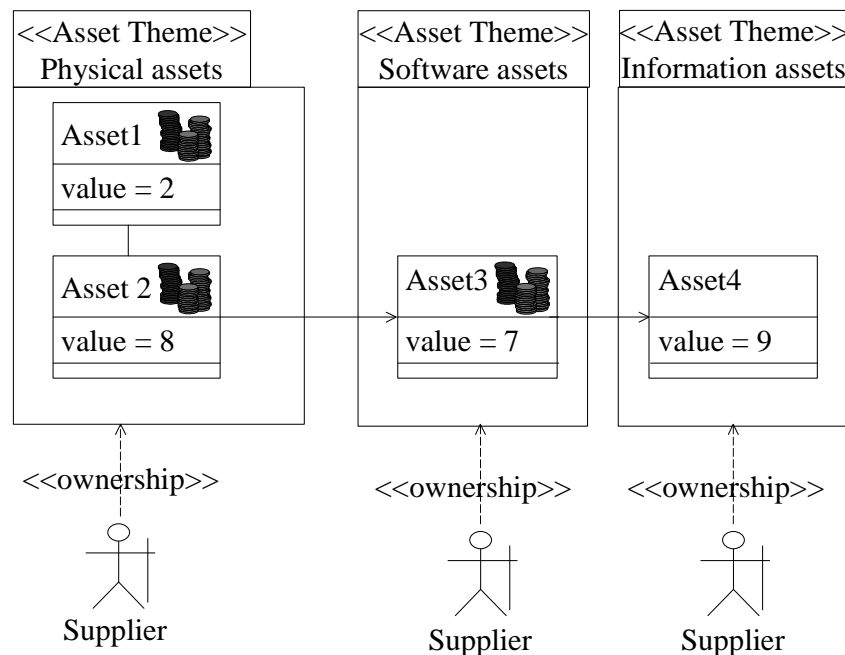


Figure 8: Asset diagram for SecurePay

Figure 8 presents an asset diagram for the company Secure e-Commerce with respect to SecurePay. The asset diagram contains all identified assets, the assets value and which asset theme it belongs to. Stakeholders are included to express which stakeholder own the Asset Themes. For the system SecurePay we use three Asset Themes and have identified 4 assets, which are Internet (Asset1), SecurePay software (Asset 2), SecurePay server (Asset3), and Payment (Asset4). The stakeholder supplier, which represent the company Secure e-Commerce owns all Asset Themes.

### 5.3 Model-based threat and vulnerability identification under Activities 2.1 and 2.2

The risk identification sub-process consists of three activities of which the first two are complementary and may be carried out in any order. The third is performed first after the two others have been completed. The Activities 2.1 and 2.2 address the identification of unwanted incidents from two different angles. Activity 2.1 focuses of identifying threat scenarios that may result in unwanted incidents causing loss in asset value. Activity 2.2 focuses on identifying the vulnerabilities of assets (or the associated system) that may be exploited by threats to cause unwanted incidents resulting in loss of asset value.

When identifying threats in activity 2.1 information from both SWOT, and asset identification and valuingas are used as input. The main purpose of the threat identification is to focus on the important assets identified and valued by the stakeholders, and try to reveal threats exploiting vulnerabilities or other threats that directly or indirectly reduces the value of an asset.

HazOp is one of the methods used for threat identification in activity 2.1. CORAS describes procedures for using models to support risk assessment. Type of models supported by CORAS is Sequence, Activity, Component and Deployment diagrams. In



Table 2: HazOp table for SecurePay

ID	Stakeholder	Asset	Item	<guideword>	<attribute>	Threat	Threat scenario	unwanted incident
1a	Supplier	Payment	to_account	other than	original content	Fraud	Attacker changes to_account and Consumer pays to attacker instead of to supplier.	Unauthorised transfer of money from Consumer`s account.

Threats and vulnerabilities may be illustrated by threat diagrams. Threat diagrams are specialised use-case diagrams for documenting the results from threat and vulnerability identification inspired by [16]. As with use cases, threats are specified by textual descriptions, sequence diagrams or activity diagrams.

In the SWOT analysis, two threats were identified at the enterprise level, fraud against consumer and denial of service. Fraud is basically a threat against consumer, but it is also expected to propagate serious effects on the supplier, the company Secure e-Commerce, such as e.g. loss of confidence relationship to customers.

Figure 10 illustrates that the vulnerability identification in activity 2.2 has identified one operation and two attributes that may be exploited by the two threats. The operation identified to be subject to exploitation is transfer\_money. The attributes identified as potential vulnerabilities in the system are no\_authentication, which means that no authentication of users is required when using the system, and no\_firewall, which means that the system is placed directly on the Internet and not protected by a Firewall.

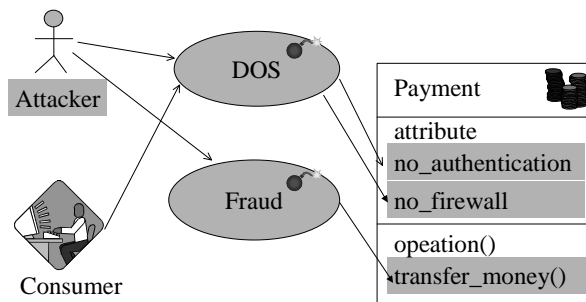


Figure 10: Threat diagram for Secure e-Commerce

Figure 10 illustrates the relationship between the identified threats, vulnerabilities and assets. Users and mis-users are included to show who are able to cause these threats and whether or not they are authorized users or potential mis-users. In Figure 10 the Attacker is modeled as a mis-user and the Consumer as an authorized user.

#### **5.4 Model-based consequence and frequency evaluation under Activities 3.1 and 3.2**

The objective of consequence and frequency evaluation is to estimate and document the consequence and frequency values of unwanted incidents. Frequencies may be qualitative or quantitative values, depending on what is known about the assessed system.

Consequences and frequencies are documented in state analysis diagrams together with the identified unwanted incidents. State analysis diagrams are extended UML state diagrams, inspired by [4]. A state analysis diagram specifies the undesired, as well as the desired, behaviour of the system. In addition to the states and transition describing the normal behaviour, a state analysis diagram consists of bad transitions and bad states that describe mis-behaviour. A bad transition is always triggered by an unwanted incident, which is modelled by a stereotype derived from Event. A bad state can only be reached by the means of a bad transition, and a bad state may not have any outbound transitions. Figure 11 provides a state analysis diagram for the assessed scenario. In the following we explain how it was constructed.

The desired behaviour of the assessed scenario is described in the sequence diagram in Figure 6 . In this sequence diagram, five phases of the behaviour are identified. In the state analysis diagram, these phases are used as the states when normal behaviour is specified, which gives us the following states:

1. Request for service state;
2. Offer service state;
3. Order service state;
4. Pay for service state; and
5. Deliver service state.

In the state analysis diagram we also specify the undesired behaviour of the system by the means of a set of bad states. The identified unwanted incidents – “Unauthorised transfer of money from Consumer’s account” (ui1), “Request for service is prevented” (ui2), “Offer of service is prevented” (ui3) and “Delivery of service is prevented” (ui4) – become the triggers of the transitions to the bad states. Consequence values are attached to the bad states and (qualitative values for) frequencies are represented as parameters to the unwanted incidents.

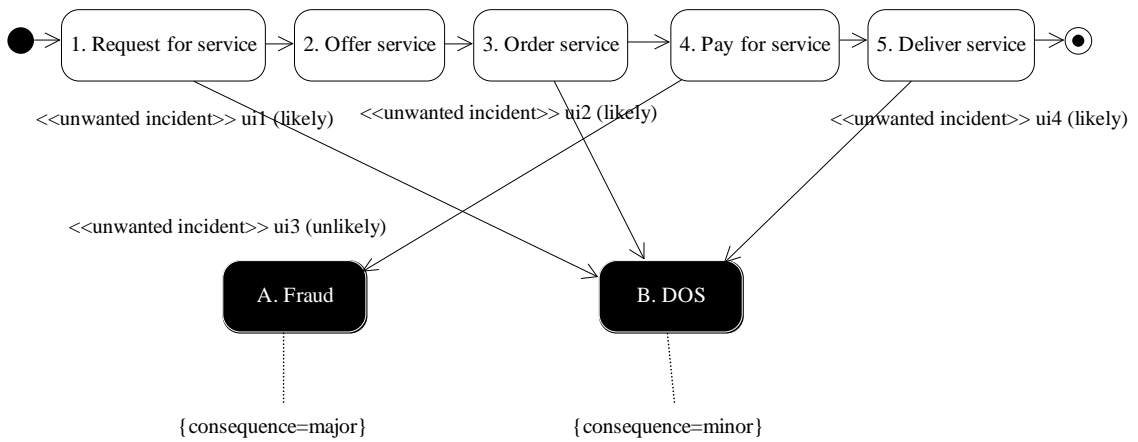


Figure 11: State analysis diagram for the system Secure e-Commerce

The state analysis diagram may be used to generate a state probability matrix for Markov-analysis or simulation. Figure 12 provides an example of a state probability matrix for the state analysis diagram for the SecurePay system, where  $P_{xy}$  is the probability (i.e., the frequency) of transition between state  $x$  and state  $y$ . Since we are using the values  $P_{xy}$  in the state probability matrix for Markov analysis or simulation the values must be given as quantitative values. However, it is not always easy or even possible to obtain quantitative values. In such cases qualitative values can be used as long as they are converted to appropriate quantitative values before inserted into the state transition matrix or if the Markov analysis or simulation are capable of handling qualitative input values.

		To State							
		0	1	2	3	4	5	A	B
From State	0	0	$P_{01}$	0	0	0	0	0	0
	1	0	0	$P_{12}$	0	0	0	0	$P_{1B}$
	2	0	0	0	$P_{23}$	0	0	0	0
	3	0	0	0	0	$P_{34}$	0	0	$P_{3B}$
	4	0	0	0	0	0	$P_{45}$	$P_{4A}$	0
	5	0	0	0	0	0	0	0	$P_{5A}$
	A	0	0	0	0	0	0	0	0
	B	0	0	0	0	0	0	0	0

Figure 12: State probability matrix

### 5.5 Model-based risk treatment under Activity 5.1

The objective of model-based risk treatment is to identify and document possible treatments of the identified risks. Identified treatments are documented in Treatment diagrams, which are Threat diagrams extended with specialised use-cases representing treatments. The prevent relationships shows which threats the different treatments is intended for. Option relationships specific which assets are protected and which kind of treatment is being used. The options are reduce likelihood, reduce consequence, transfer and avoid.

When identifying and evaluating treatment options for the two threats identified, we found one possible treatment option for the threat fraud and two possible treatment options for the threat denial of service (DOS). Figure 13 illustrates the threat-treatment pair fraud and encryption, Figure 14 illustrates the threat-treatment pair DOS and FireWall and Figure 15 illustrates the threat-treatment pair DOS and authentication with username and password.

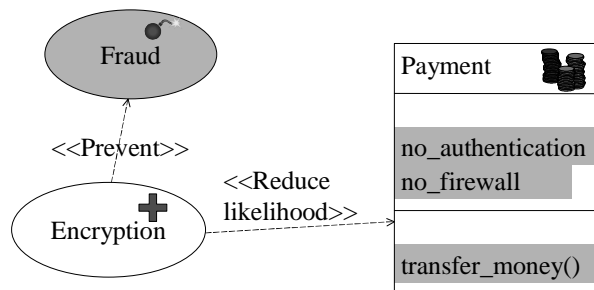


Figure 13: Treatment diagram 1 for the threat fraud

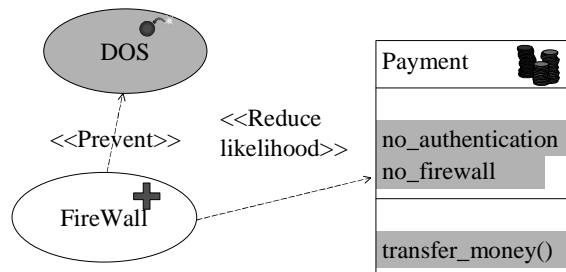


Figure 14: Treatment diagram 1 for the threat DOS

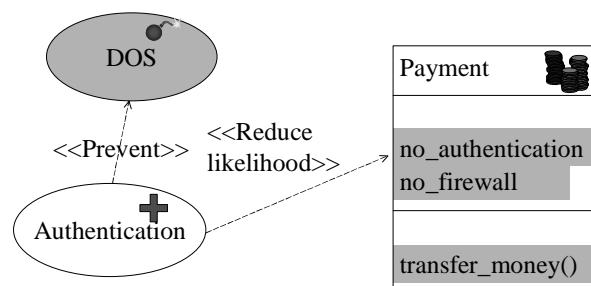


Figure 15: Treatment diagram 2 for the threat DOS

## 6. CONCLUSIONS

This paper has introduced the CORAS UML profile for model-based risk assessment and demonstrated its use in the assessment of an e-commerce system. Model-based risk assessment is motivated by several hypotheses:

- Risk assessment benefits from correct descriptions of the target of evaluation, its context and security issues. The modelling methodology furthers the precision of such descriptions, and this is likely to improve the quality of risk assessment results.
- The graphical style of UML facilitates communication and interaction between stakeholders involved in a risk assessment. This may improve the quality of risk assessment results, and reduce the danger of throwing away time and resources on misconceptions.
- The modelling methodology facilitates a more precise documentation of risk assessment results and the assumptions on which their validity depends. This is likely to reduce maintenance costs by increasing the possibilities for reusing and updating assessment results when the target of evaluation is maintained.
- The modelling methodology provides a solid basis for the integration of assessment methods. This may improve the effectiveness of the assessment process.
- The modelling methodology is supported by a rich set of tools from which the risk assessment benefits. This may improve the quality of assessment results and reduce costs. It may also improve further productivity and maintenance.
- The modelling methodology provides a basis for tighter integration of risk management in the system development process. This may considerably reduce development costs and ensure that the specified security level is achieved.

To validate these hypothesis and guide the R&D work, six trials has been planned for the CORAS project; three within e-commerce (one of which has already been completed; see [14] for preliminary results) and three within telemedicine (one of which has already been completed; see [18] for preliminary results).

## ACKNOWLEDGEMENTS

The CORAS consortium consists of eleven partners from four countries: CTI (Greece), FORTH (Greece), IFE (Norway), Intracom (Greece), NCT (Norway), NR (Norway), QMUL (UK), RAL (UK), Sintef (Norway), Solinet (Germany) and Telenor (Norway). Telenor and Sintef are responsible for the administrative and scientific coordination, respectively. The results reported in this paper have emerged through the joints efforts of the CORAS consortium.

## REFERENCES

- [1] AS/NZS 4360: 1999 Risk managment.
- [2] Barber, B., Davey, J., The Use of the CCTA Risk Analysis and Management Methodology CRAMM in Health Information Systems, in MEDINFO 92, Lun, K.C., Degoulet, P., Piemme, T.E., Rienhoff, O. (eds.), North Holland Publishing Co, Amsterdam, pp1589 –1593, 1992.

- [3] Bouti, A., Ait Kadi, D., A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety Engineering* 1:515-543, 1994.
- [4] Houmb, S. H., *Stochastic Models and Mobile E-Commerce: Are stochastic models usable in the analysis of risk in mobile c-commerce?* Master's Thesis, Østfold University College, Faculty of Computer Sciences, 2002.
- [5] IEC 1025: 1990 Fault tree analysis (FTA).
- [6] ISO/IEC TR 13335-1:2001 Information Technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.
- [7] ISO/IEC 17799: 2000 Information technology – Code of practise for information security management.
- [8] Jacobson, I., Rumbaugh, J., Booch, G. *The unfied software development process*. Addison-Wesley, 1999.
- [9] Krutchten, P., *The Rational unified process, an introduction*. Addison-Wesley, 1999.
- [10] Leveson, Nancy G., *SAFWARE, System, Safety and Computers*, Addison-Wesley, ISBN: 0-201-11972-2, 1995.
- [11] Littlewood, B., A reliability model for systems with Markov structure. *Appl. Stat.* 24:172-177, 1975.
- [12] OMG, *Unified Modeling Language Specification, version 1.4*, 2001.
- [13] Putman, J. R., *Architecting with RM-ODP*, Prentice-Hall, 2000.
- [14] Raptis, Dimitris, Dimitrakos, Theo, Gran, Bjørn Axel, and Stølen, Ketil, *The CORAS Approach for Model-based Risk Management applied to e-Commerce Domain*, CMS-2002.
- [15] Rumbaugh, J., Jacobson, I., Booch, G., *The unified modeling language reference manual*. Addison-Wesley, 1999.
- [16] Sindre, G., and Opdahl, A.L., *Eliciting Security Requirements by Misuse Cases*. In Proc. TOOLS-PACIFIC 2000. Los Alamitos, CA: IEEE Computer Society Press; pp. 120-131 Sydney, Australia, 2000.
- [17] Storey, Neil, *Safety-critical computer systems*, Addison-Wesley, ISBN: 0-201-42787-7, 1996.
- [18] Stølen, Ketil, and Mantzoranis, Eva, *Experience from using model-based risk assessment to evaluate the security of a telemedicine application*, TICD-2002.
- [19] World Wide Web Consortium, *Extensible Markup Language (XML) v1.0, W3C Recommendation, Second Edition*, 6 Oct. 2000.

## Appendix: UML Profile for risk assessment

The UML Profile for risk assessment is a refinement of the UML Profile as defined in the UML Standard, version 1.4 [12]. The profile defines UML stereotypes, as well as rules for specialised UML diagrams, for support of the model-based risk assessment process of the CORAS project.

At the moment the profile consists of six packages that extend the standard UML Profile:

- *Actors Package* (Figure 17), which defines actor stereotypes;
- *SWOT Model Package* (Figure 18), which defines SWOT diagrams;
- *Asset Model Package* (Figure 19), which defines Asset diagrams;
- *Threat Model Package* (Figure 20), which defines Threat diagrams;
- *State Analysis Model Package* (Figure 21), which defines State Analysis diagrams;
- *Treatment Model Package* (Figure 22), which defines Treatment diagrams.

Figure shows dependencies between the packages of the CORAS Profile and dependencies to packages of the UML standard. In all the below figures, meta-classes from the UML standard is coloured.

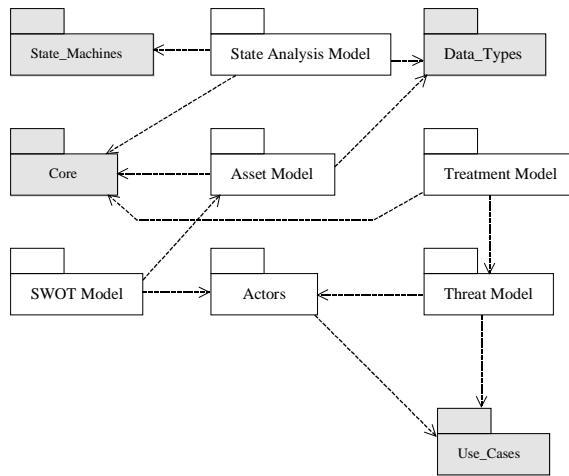


Figure 16: Packages of the CORAS Profile

Each of the packages is defined by a meta-model (Figure - Figure ). The meta-models define stereotypes and syntactic rules for the specialised diagrams. The syntactic rules are defined by the use of aggregate and composition relationships, and constraints attached to the meta-classes of the meta-models.

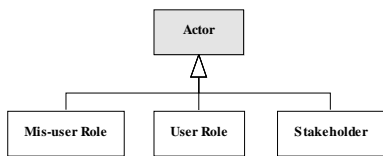


Figure 17: Actors Package

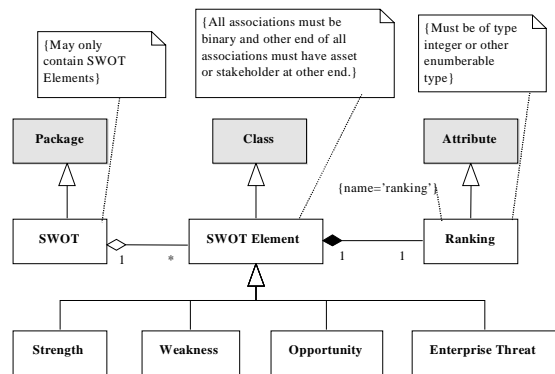


Figure 18: SWOT Model Package

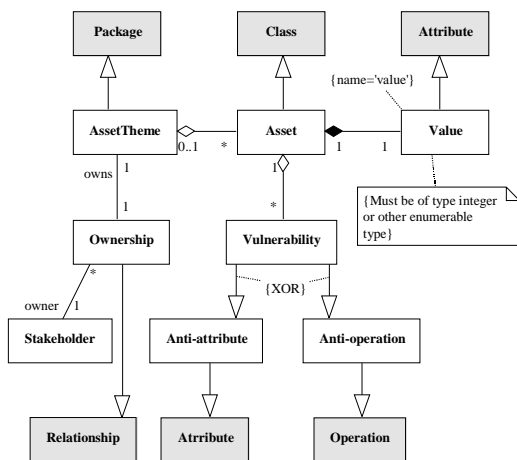


Figure 19: Asset Model Package

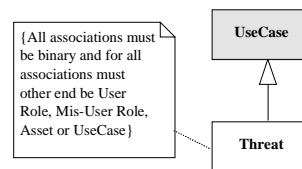


Figure 20: Threat Model Package

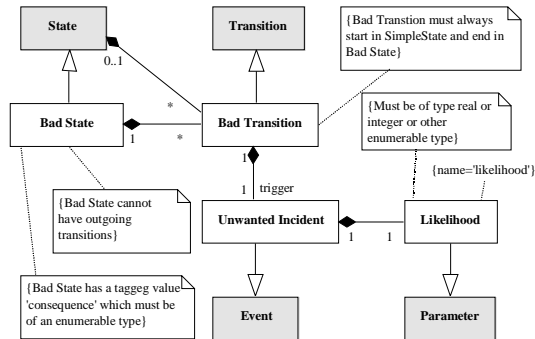


Figure 21: State Analysis Model Package

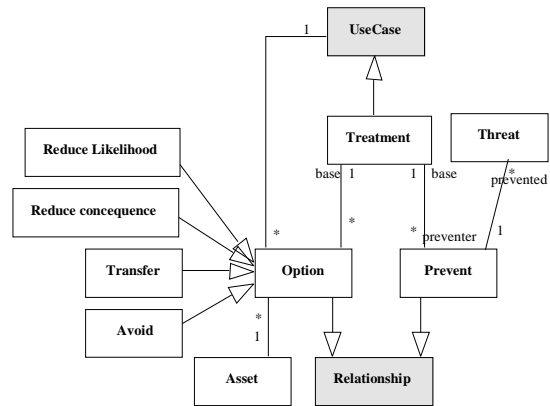
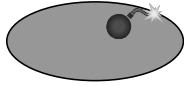

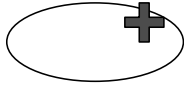


Figure 22: Treatment Model Package

In order to increase the readability of the UML diagrams, most of the defined stereotypes are represented by intuitively understandable icons. The stereotypes are described in the below table.

	Stereotype	Description	6.1 Representation
Actors	User Role	Human user roles of the system or enterprise that is being modelled.	
	Mis-User Role	User roles (of the system or enterprise that is being modelled) that are unauthorised or have malicious intentions.	
	Stakeholder	Stakeholders of the system or enterprise that is being modelled.	
SWOT	Strength	Strength at enterprise level	
	Weakness	Weakness at enterprise level	
	Opportunity	Opportunity at enterprise level	
	Enterprise Threat	Threat at enterprise level	
Asset	Asset	Asset of the system or enterprise that is being modelled.	
	Asset Theme	Categorisation/grouping of assets.	Package with label

	Vulnerability	Properties of assets that may be exploited by threats.	Attribute or operation with shaded background
	Ownership	Relation between asset theme and the stakeholder that owns it.	<<Ownership>> ----->
Threat	Threat	A potential scenario that may cause unwanted incident by exploiting the vulnerabilities of an asset.	
State Analysis	Bad State	Undesired state or fault state (of the system that is being modelled) reached by a Bad Transition.	
	Bad Transition	Transition to a Bad State, triggered by an unwanted incident.	Same as Transition
	Unwanted Incident	Undesired event that causes the system (that is being modelled) to reach a Bad State.	Event with label, and likelihood value as parameter
Treatment	Treatment	Scenario that treats a risk.	
	Prevent	Relation between a Treatment and the Threat that it prevents.	<<Prevent>> ----->
	Reduce Likelihood	Relation between Treatment and the Asset it is concerned with.	<<Reduce Likelihood>> ----->
	Reduce Consequence	Relation between Treatment and the Asset it is concerned with.	<<Reduce Consequence>> ----->
	Transfer	Relation between Treatment and the Asset it is concerned with.	<<Transfer>> ----->
	Avoid	Relation between Treatment and the Asset it is concerned with.	<<Avoid>> ----->

The six packages of the profile provide stereotypes and modelling rules that correspond to the general concepts of the CORAS risk management process and risk documentation framework. The profile may however easily be extended with, e.g., domain specific packages. In such packages could for example the Asset stereotype be further specialised to a Computer stereotype that could have a picture of a computer as icon.