STF90 A04036 – Unrestricted

REPORT

A Conceptual Specification for Architectural Descriptions in Risk Analysis with basis in IEEE Std 1471

SINTEF ICT

2004

SINTEF

SINTEF ICT

Address: NO-7465 Trondheim, NORWAY
Location: Forskningsveien 1
Telephone: +47 22 06 73 00
Fax: +47 22 06 73 50

Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

A Conceptual Specification for Architectural Descriptions in Risk Analysis with basis in IEEE Std 1471

AUTHOR(S)

Ida Hogganvik, Ketil Stølen

CLIENT(S)

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
STF90 A04036	Unrestricted		
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Unrestricted	82-14-03368-3	40332800	17/1
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
CADRArapportforside		Ketil Stølen	Jan Øyvind Aagedal
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2004-04-22	Bjørn Skjellaug, research director	

ABSTRACT

This report provides a conceptual specification for architectural descriptions in risk analysis with basis in the IEEE Recommended Practice for Architectural Description of Software-Intensive Systems (IEEE Std 1471) and CORAS. CORAS is a tool-supported methodology for UML-based security (risk) analysis developed in the EU-funded CORAS project (IST-2000-25031). CORAS builds upon the Australian standard for risk management (AS/NZS 4360). The conceptual specification, referred to as CADRA, is intended to serve as a conceptual foundation for risk analysis in the setting of software engineering. People with different background need to cooperate and understand the risk analysis documentation, without making the mistake of using too general documentation. Risk analysis is always about stakeholders and their assets in relation to unwanted incidents and how to handle them. This makes it natural to describe the stakeholders' interests regarding assets in architectural descriptions with associated risks, threats, unwanted incidents and vulnerabilities. CADRA ensures this by conforming to IEEE Std 1471 which enforces the documentation-makers to focus on the intended audience.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	ICT	IKT
GROUP 2	Information systems	Informasjonssystemer
SELECTED BY AUTHOR	Risk analysis	Risikoanalyse
	Architecture	Arkitektur
	Documentation	Dokumentasjon

A Conceptual Specification for Architectural Descriptions in Risk Analysis with basis in IEEE Std 1471

Ida Hogganvik and Ketil Stølen
SINTEF Information and Communication Technology

Contents

1 Introduction **1**

2 Background and Overall Context **3**
2.1 Architectural Description of Software-intensive Systems 3
2.2 Documentation in Analysis of Security Critical Systems 4

3 The Conceptual Specification **6**
3.1 System and Target of Evaluation 7
3.2 Stakeholder and Role 7
3.3 Concern 9
3.4 Model and Modeling Element 10
3.5 Viewpoint and View 11

4 Conclusion **11**

1 Introduction

How should architecture be described? And what concepts should an architectural description include in a risk analysis setting? How does risk analysis relate to software engineering? These are the problems we address by creating a conceptual specification for architectural descriptions in risk analysis. The conceptual specification provides the basic concepts for documentation in an integrated software engineering and risk analysis methodology.

It is possible to describe the architecture of a building, a process or a system in different manners, but the goal is always to illustrate the structure in a way that other people understand and find useful. When an architect draws a building, he or she decides where walls, doors, water pipes and electrical lines will be placed in order to function properly. The drawing will be a common point of reference for the architect, the buyer, the contractor and possible subcontractors.

IEEE Std 1471 Recommended Practice for Architectural Description of Software-intensive Systems [13] defines architecture as "the fundamental structure of an entity and the interrelationships among its parts. The architecture of an entity captures its essential features and principal properties, it also captures its main components, how they are structured, how they interact, and the principles guiding their design and evolution" [13]. In general it may be claimed that everything containing components has an architecture, i.e. a structure of how the components relate to each other.

In a risk analysis context, well written architectural descriptions are important to the participants in the challenge of understanding the target of evaluation. Risk analysis is not only used for assessing existing systems, it is also an important vehicle when designing and developing new systems. To make accurate and understandable models of the system is crucial and can be a major challenge when dealing with more abstract systems like IT-systems

It is generally accepted that risk analysis of systems during their development and operation is necessary in order to achieve security, safety, reliability and cost-effectiveness. Risk analysis methodologies are often specialized to fit particular system domains and to emphasize the different systems characteristics. There are specialized approaches for the health sector, the safety sector, the process industry and the security business. These are often further refined into even more specialized directions. However, much of the risk analysis methodology is common even if it is used in different domains. By gathering these common elements into a general specification, it can become a foundation for the development of risk analysis and software development methodologies. This will facilitate interoperability between domains since a methodology intended for one domain have the ability to utilize parts of methodologies or tools from other domains. This report takes the first steps towards characterizing such a common core with respect to documentation of target of evaluation, the system analyzed in what is known as model-based risk analysis.

Typical model-based approaches are RSDS [18], CRAMM [4], ATAM [7], OCTAVE [2] and CORAS (presented in Section 2.2). The system models used in model-based risk analysis often have basis in semi-formal system specification languages with a well defined semantics. The models are used to describe the system and the relevant part of its context. They also facilitate communication and interactions between different groups of people involved in the analysis and document the analysis results. Our objective is not so much to capture what is common for these methodologies, but rather center on how we think such a documentation core should be, based on the experiences from the CORAS project. More explicitly, we have developed a Conceptual specification for Architecture Descriptions in model-based Risk Analysis (CADRA).

CADRA should facilitate reuse of best experiences from documentation in model-based risk analysis and provide a common documentation core for risk analysis within different domains. CADRA should be a reference for standardizing documentation formats in integrated system development and risk analysis methodologies.

In order to make this a well defined reference specification we have a thorough

foundation in existing standards and accepted methods or techniques. Although the IEEE Std 1471 is meant for the software domain, its notion of system and other terminology is very general and captures a much wider area. IEEE Std 1471 serves as a basis and starting point, and our specification is IEEE Std 1471 compliant. CORAS has been selected due to its similarities in terminology with IEEE Std 1471, especially in its documentation-centric part, making a relation natural. They both characterize and structure architectural documentation according to the "audience" it is intended for, using mechanisms discussed in subsequent sections. We have chosen to specify CADRA in UML 2.0 class diagrams (Unified Modeling Language) [20]. The UML notation is well-known in the system development community and is more and more becoming the leading standard for modeling and specification. CADRA is intended for people like methodologists, process and process-improvement engineers, researchers, producers of standards, tool-builders and trainers.

In the Section 2 we give an overview of IEEE Std 1471 and CORAS. In Section 3 we discuss CADRA terminology and present the conceptual specification. Our conclusions are given in Section 4, followed by an appendix containing the CADRA glossary.

2 Background and Overall Context

In the following we first give a brief introduction to architectural descriptions according to IEEE Std 1471 and then present how CORAS handles risk analysis documentation.

2.1 Architectural Description of Software-intensive Systems

IEEE Std 1471 Recommended Practice for Architectural Description of Software-intensive Systems focuses on how to describe the architecture of software-intensive systems, providing a basic framework for the content of such a description. Software intensive systems are systems where software contributes essential to the design, construction, deployment and evolution of the system. An architecture is defined as "the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution", and an architectural description is a collection of products to document an architecture. Every system has one or more stakeholders with some concerns about the system. Figure 1 provides a summary of the key concepts in an architectural description from IEEE Std 1471 like view, viewpoint, concern, stakeholder and architectural description. In the following we explain these terms; their exact definitions are given in the appendix.

A system has a mission, a use or operation for which a system is intended by one or more stakeholders. The system is required to meet some set of objectives and the system is influenced by its environment. An architectural description

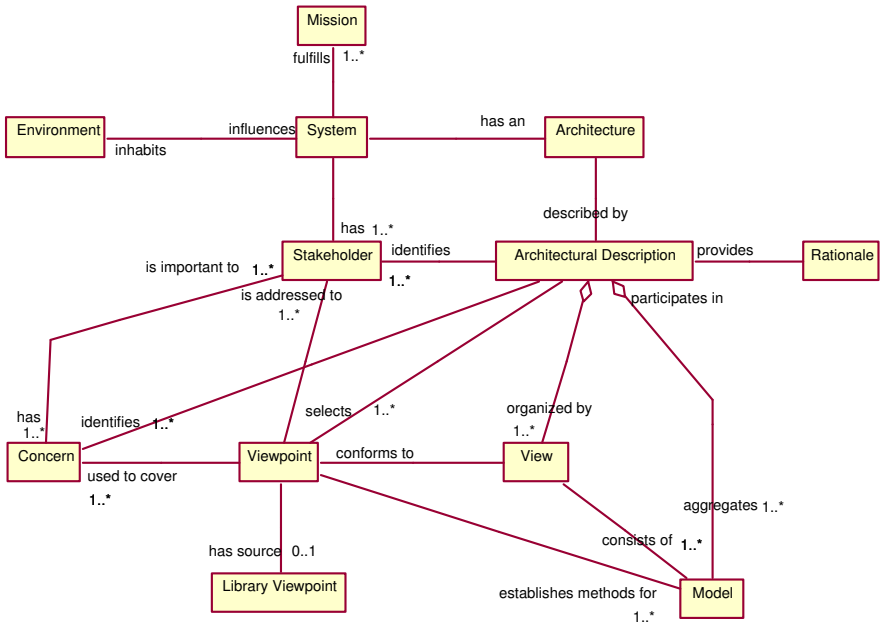

Figure 1: The conceptual specification of an architectural description from IEEE Std 1471

of a system conforming to IEEE Std 1471 is organized in views. A view is a representation of the entire system from a single perspective and consists of one or more architectural models (e.g. figures, diagrams, text or other). The view conforms to a viewpoint which defines what aspects the models in the view shall cover. These are aspects like how to construct the models, what audience they are meant for and what type information the models shall illustrate. The specification of a viewpoint is based on what the stakeholders are interested in, or concerned about. A stakeholder is someone or something with interests relative to the system. A stakeholder like "management" would probably be interested in enterprise information and therefore it should exist an enterprise viewpoint that defines how information related to this is best captured and presented.

2.2 Documentation in Analysis of Security Critical Systems

CORAS is a tool-supported methodology for UML-based security (risk) analysis developed in the EU-funded CORAS project (IST-2000-25031) (http://coras.sourceforge.net),[8],[9],[1]. CORAS integrates aspects from partly complementary risk analysis techniques like HazOp [22], FMEA [5] and FTA [11] and was refined through several field trials. CORAS builds upon the Australian

standard for risk management (AS/NZS 4360) [3].

The terminology in CORAS integrates terms from international standards for security ([16],[17],[14],[12]) and risk analysis ([3],[6],[10]) with standardized terminology for system documentation ([15]).

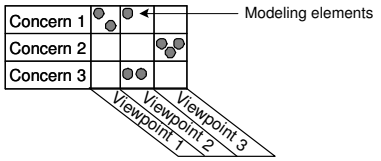

Figure 2: Cross linking documentation between concern and viewpoint

CORAS has five predefined viewpoints taken from the reference model for distributed processing (RM-ODP) [21],[15]. In addition to viewpoint the documentation is also linked to a concern. CORAS structures risk analysis documentation into a number of concerns, each instructing the user to capture information of a specific type. As illustrated by Figure 2, based on this concern-viewpoint structure one can either view all the risk analysis documentation(modeling elements) from a specific point of view (viewpoint) or one can see all documentation from one specific part (concern) of the risk analysis.

In the following we explain the basic risk analysis terms used in CORAS, illustrated in Figure 3 using a UML class diagram.

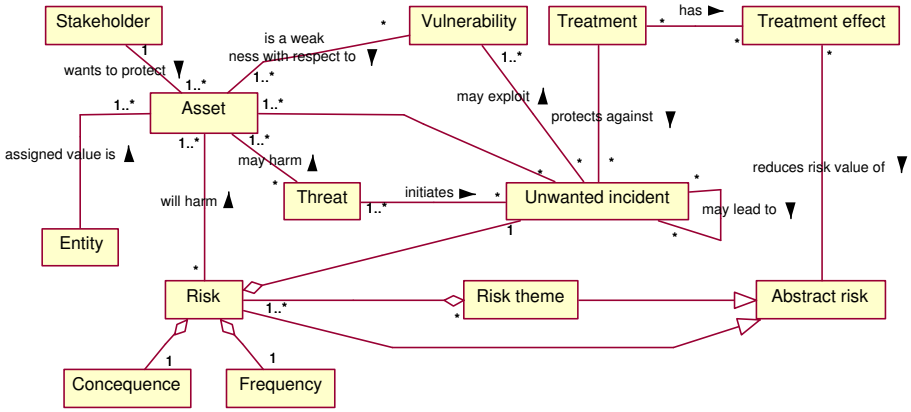

Figure 3: Concepts in risk analysis

The system or part of a system, assessed during a risk analysis is called the target of evaluation. Everyone with interests in the target is stakeholders of the system. System users, system maintainers and system developers are typical stakeholders. Different stakeholders often value the system differently; a system

user who is dependent on the system will put a high value on it, while other stakeholders might not value the system equally high. The same entity may be assigned different values by different stakeholders. We refer to these entities with their values as assets. An asset is something to which a stakeholder directly assigns value and, hence, for which the stakeholder requires protection. An asset is therefore uniquely linked to a single stakeholder.

A stakeholder wants to protect his/her assets from loosing value. Examples of assets are customer information, source code, company routines, critical system services etc. Target system stakeholders and their assets are normally identified early in the risk analysis process.

Figure 3 includes four important risk analysis concepts related to asset: vulnerability, unwanted incident, threat and risk are all linked to the notion of asset.

A vulnerability is a weakness or lack, making an asset vulnerable to harmful actions. One may understand a vulnerability as something that is missing, e.g. if a company network lacks a firewall then this may be a vulnerability with respect to some assets in the network.

An unwanted incident is an event that may harm the asset and something we want to prevent. An unwanted incident is the result of a threat exploiting a vulnerability. If the company network is an asset, then an unwanted incident is unauthorized access to the network by intruders.

A threat is someone or something that wants to destroy, remove or interfere with the asset and a risk is the chance of this happening. With respect to the already mentioned company network a threat may be a person who knows or discovers the vulnerability and want to exploit it. First the company does not recognize the situation as a potential risk because nobody outside the company is aware of the security hole, but when an employee is fired, they suddenly realize that there is a risk for unauthorized network access by people familiar with the company infrastructure. The risk is characterized by a risk value (e.g. low, medium, high or other scales) which is based upon an estimate of frequency for it to happen and its consequence in loss of asset value. If a risk is estimated to occur two times a year and the consequence is a loss of 200000 dollars each time, a risk value could be "high" which means the risk should be treated. In a risk analysis the risks will be prioritized according to risk value, and similar risks are often gathered into risk themes. By doing this one becomes aware of the relationships between the risks and may be able to treat the risks as a whole rather than one by one. This also helps avoiding that a treatment introduces new risks or in other way affects the system in a negative manner. The treatment is applied to the target's vulnerability and the desired effect is reduced frequency and/or consequence, i.e. reduced risk value.

3 The Conceptual Specification

In the following we discuss the similarities in terms and concepts between IEEE Std 1471 and CORAS. The purpose is to develop the conceptual specification

with foundation in IEEE Std 1471 (Figure 1) and extended with risk analysis documentation aspects from CORAS (Figure 3) and the standards on which CORAS builds.

The selected terms are key terms in IEEE Std 1471 with equal or similar interpretations to terms in CORAS. IEEE Std 1471 terms not used in CORAS, were adopted into CADRA with only minor adjustments in the definitions. This applies for Environment, Mission, Architecture, Architectural description, Rationale and Library viewpoint, explained in Section 2.1.

The subsequent sections discuss *system* & *target of evaluation*, *stakeholder* & *role*, *concern*, *element*, *model* & *modeling element*, *view* & *viewpoint*.

3.1 System and Target of Evaluation

Central in the IEEE Std 1471 is *system*, the "thing" with an architecture we want to describe. A system is defined "a collection of components organized to accomplish a specific function or set of functions". An architectural description describes the system's architecture using different models like graphical representations, textual representations etc. IEEE Std 1471 does not restrict a system to have only one architecture or architectural description but allows for multiple of both.

CORAS also address systems, but in a risk analysis setting where the purpose is to evaluate a system, or part of it, the system is called *target of evaluation* and defined "an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation" [6]. The IEEE Std 1471 definition covers the definition in CORAS, but the latter stresses the point that often a part of the system is assessed rather than the complete system. Therefore, target of evaluation is more suitable than the general notion of system in a risk analysis centric setting like CADRA.

3.2 Stakeholder and Role

IEEE Std 1471 defines a *system stakeholder* as "an individual, team or organization (or classes thereof) with interests in or concerns relative to, a system". A system has one or more stakeholders and a stakeholder may have different roles regarding the system; each role is treated separately as a new stakeholder in the architectural description.

CORAS' definition of a stakeholder is taken from (AS/NZS 4360) [3] where a stakeholder is defined "those people and organizations that may affect, be affected by, or perceive themselves to be affected by a decision or activity in the risk management process". The risk management process consists of several activities and in the different activities the participants may play different roles according to the purpose of the activity. If a stakeholder plays several different roles in the risk analysis process, the stakeholder is assigned a role name for each role. A risk analysis process may involve people with roles like project leader, risk analysis leader, risk analysis secretary, target owner, target developer, field expert and risk analysis expert etc.

In principle IEEE Std 1471 and CORAS have the same interpretation of stakeholder, i.e. anyone in contact with the target of evaluation, allowing multiple roles. Stakeholders in a risk analysis may be people responsible for conducting and leading the analysis, people participating, people making decisions based on the results from the analysis and people affected by these decisions. We may divide these into two types of stakeholders, the ones with concerns regarding the risk analysis results and documentation; and the ones with concerns related to the target of evaluation. The two different types of concerns and stakeholders introduce a problem in the stakeholder-concern relation in IEEE Std 1471. Stakeholders who find the risk analysis documentation highly valuable are people like decision makers and risk analysts, which we call *risk analysis stakeholders*. The risk analysis stakeholder is related to the risk analysis process itself, interested in e.g. which techniques to use, how to reuse information from previous risk analysis and how to interpret the information in order to draw risk analysis conclusions. The risk analysis stakeholder is therefore a stakeholder with interests in the risk analysis results and documentation.

Stakeholders participating mostly because they have expertise on a particular target aspect, we name *target stakeholders*. The target stakeholder provides information to the risk analysis team and knows technical aspects, routines or user behavior. He or she is often familiar with the target system; a direct or indirect user of the system. This interpretation of target stakeholder complies with both CORAS' and IEEE Std 1471's definition of stakeholder. The definition of stakeholder in IEEE Std 1471 is however more general than the one in CORAS, and due to CADRA's particular focus on risk analysis the definition from CORAS emphasizes more clearly what we mean with target stakeholder.

In order to emphasize the distinction between the types of stakeholders we specialize the term stakeholder in Figure 1 into two different types: risk analysis stakeholder and target stakeholder (Figure 4).

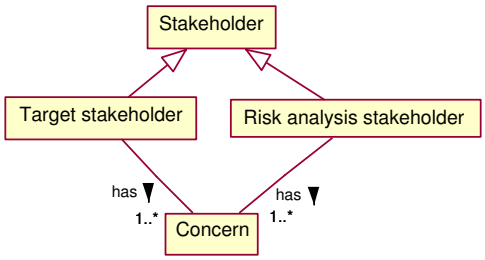

Figure 4: Specialization of stakeholder

3.3 Concern

CORAS use the same definition of *concern* as IEEE Std 1471, but the *practical use* of concern in CORAS differs from IEEE Std 1471. Concern in IEEE Std 1471 are "those interests which relates to the system's development, its operation or any other aspect that are important to one or more stakeholders". As discussed earlier, a stakeholder may have more than one role related to the target and according to which role the stakeholder plays, the same stakeholder may have multiple, and possible different, concerns related to the same object. Concerns are discovered and formulated through interaction with stakeholders. IEEE Std 1471 says nothing about which concerns to use, the user is free to define its own.

CORAS uses concerns for linking related information from a risk analysis activity to the five different viewpoints as depicted in Figure 2. The concern description says what type of information that is expected to be produced at the current stage, like risk analysis tables or trees, models, logs and other documentation [8]. The concern in CORAS is important to the risk analyst and addresses aspects on a sort of a "meta-level" of the target of evaluation. If we recognize this distinction, we need to divide concerns into concerns on system-level and concerns on meta-level. In our interpretation, CORAS-concerns are related to the "meta-level" of the system in a risk analysis context and IEEE-concerns are related to the actual "system-level". This is an extension of IEEE Std 1471 where a concern is related to the system stakeholders and address elements on system level. As formalized in Figure 4, CADRA then defines two types of concerns: *risk analysis concern* (referring to the concern as a part of the risk analysis process like in CORAS) and *target concern* (referring to concern in IEEE Std 1471), respectively. The risk analysis concerns are related to risk analysis stakeholders and target concerns to target stakeholders.

Identification of concerns in IEEE Std 1471 resembles the activity of asset identification and valuing in CORAS where stakeholders identify and assign value to the assets (Figure 5). In IEEE Std 1471 a stakeholder with concerns about a specific part of the system would probably recognize this as an asset. Based on this we assume a relationship between target concern and asset in our conceptual specification.

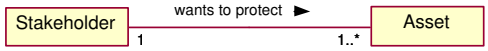

Figure 5: Relation between asset and stakeholder in CORAS

The decisions made in this and the previous section implies changes to, or more correctly extensions of the conceptual specification of IEEE Std 1471, illustrated in Figure 6.

If we then combine Figure 6, with the risk analysis elements from CORAS in Figure 3, the result is our conceptual specification for architectural descriptions in risk analysis, illustrated in Figure 7.

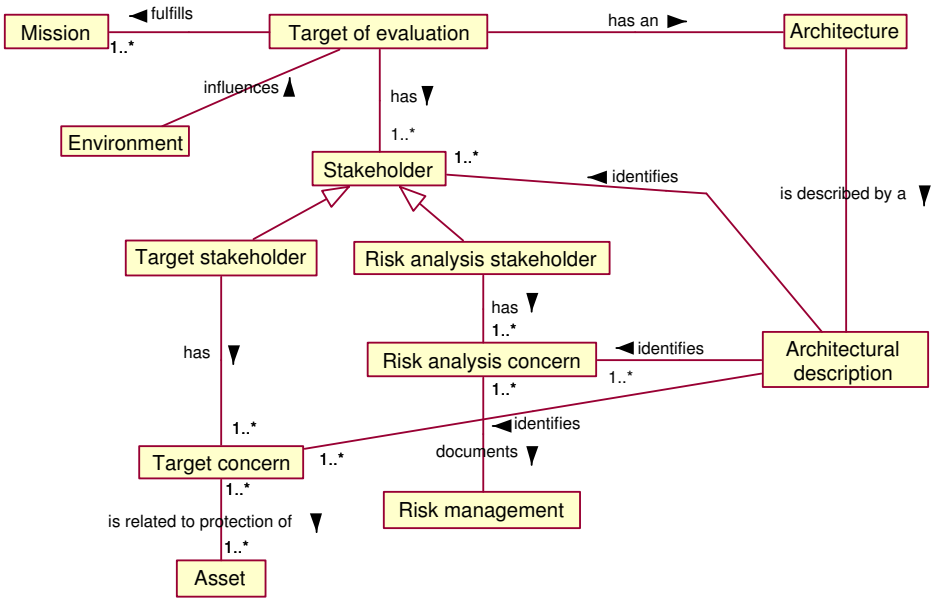

Figure 6: Specialization of stakeholder and concern

3.4 Model and Modeling Element

In IEEE Std 1471 a system, or target view, consist of architectural *models* according to rules defined by its associated architectural viewpoint. Models are all figures and diagrams comprising a view on the system, used to illustrate the system architecture.

In CORAS *modeling elements* are pieces of information related to specific stages of the risk analysis process. The elements have a commonly agreed semantics and a well-defined syntax. They have a certain format (e.g. UML) and hold the same interpretation for all readers. Elements can be everything from non-CORAS specific documentation, modeling diagrams, logs and risk analysis tables/trees [19]. They are stored with a cross-link to viewpoint and concern illustrated as black circles in Figure 2.

It is reasonable to assume that a modeling element in CORAS corresponds to a model in IEEE Std 1471. According to IEEE Std 1471, models constitute a view of the system which expresses the system's architecture in some way. The different types of elements are all models according to IEEE Std 1471's definition where an architectural model express the whole, or a part of, the system in order to address a concern. Since this definition includes CORAS' modeling element, we will use the term *model* in CADRA.

3.5 Viewpoint and View

An architectural description according to IEEE Std 1471 is organized by one or more views. A view conforms to a set of rules defined by its corresponding viewpoint. The viewpoint establishes how a view is created, depicted and analyzed. The view addresses one or more of the stakeholders concerns and consists of one or more models, which express the system architecture. When constructing an architectural description, the architect first selects a set of viewpoints to use, and thereafter constructs the corresponding views. The standard gives no guidance on which viewpoints to use.

CORAS is based on RM-ODP which categorizes documentation into five viewpoints, i.e. abstractions, which yields a specification of the whole system according to the type of viewpoint. RM-ODP defines a viewpoint: "a form of abstraction achieved using a selected set of architectural concepts and structuring rules (a viewpoint specification), in order to focus on a particular concern within the system" [8]. From a viewpoint you get a view of the system which addresses the areas of concern for a specific stakeholder type. Each cross-pair of concern/viewpoint contains information related to a viewpoint on the belonging risk analysis activity. The five different viewpoints used in CORAS focus on different aspects: *enterprise viewpoint, information viewpoint, computational viewpoint, engineering viewpoint*, and *technology viewpoint* (for more details see [21]). The viewpoint provides "the concepts and the structure for any system specification from that viewpoint. The use of that viewpoint, and refinement of the architecture concepts of that viewpoint, is considered a view" [21]. According to [21] the viewpoints of RM-ODP can be somewhat related to viewpoint templates in IEEE Std 1471, and the use of the RM-ODP viewpoints is related to a set of IEEE Std 1471 views.

While view is an important term in IEEE Std 1471, used to organize the architectural description, it is only used briefly in CORAS to explain what a viewpoint is. CORAS is based on the five viewpoints defined in RM-ODP, whereas IEEE Std 1471 does not give any restrictions on which viewpoints to use as long as they are defined in the architectural description. The reason for RM-ODP to predefine five viewpoints is based on the assumption that these viewpoints are sufficient to meet most demands, but it is possible to use additional viewpoints. We choose to use the interpretations of view and viewpoint from IEEE Std 1471 and leave it up to the user to choose appropriate viewpoints according to the risk analysis situation.

4 Conclusion

People with different background need to cooperate and understand the risk analysis documentation, without making the mistake of using too general documentation. This makes it important to describe the same aspects in several ways, targeted a specific audience by using the concept of views and viewpoints. CADRA ensures this by conforming to IEEE Std 1471 which enforces

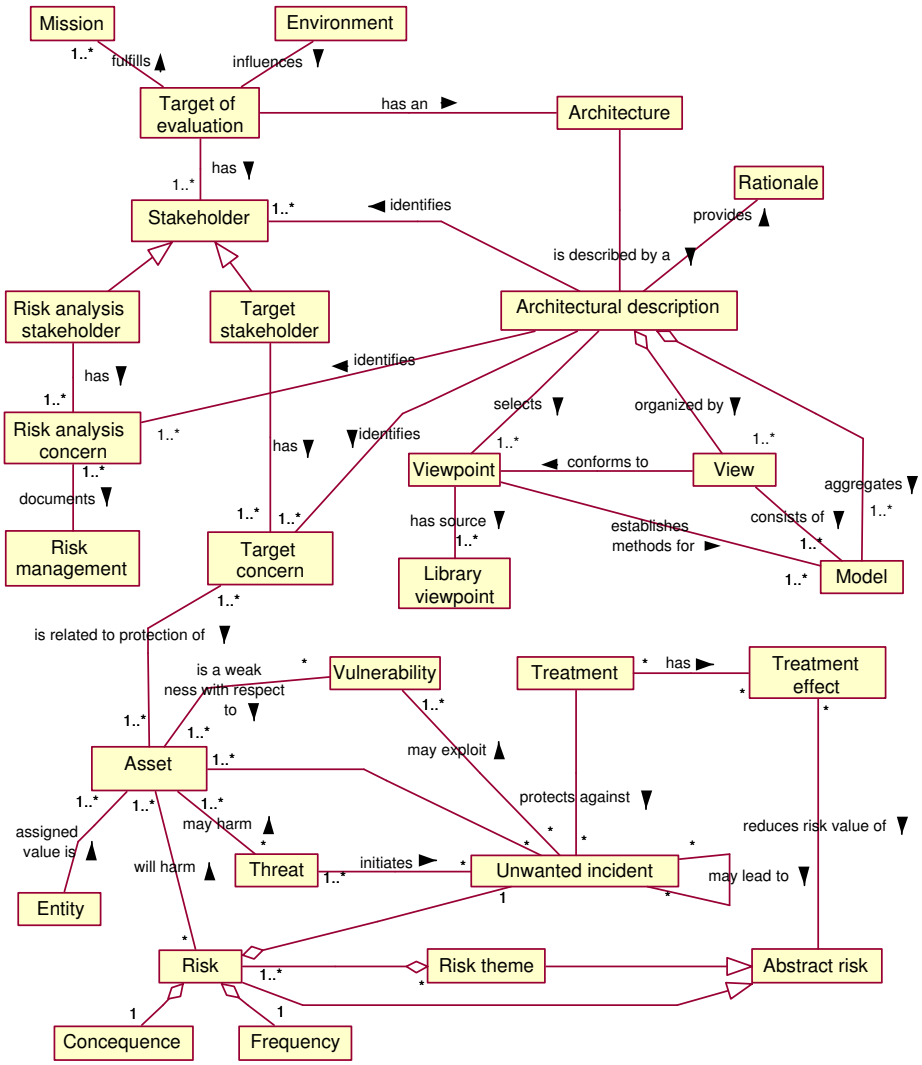

Figure 7: The conceptual specification for architectural description in risk analysis

the documentation-makers to focus on the intended audience (e.g. a viewpoint suitable for one organization might not fit a different organization).

The risk analysis documentation logically reflects the risk analysis process in that it builds on, or uses, documentation from previous stages of the process. This implies that documentation should include a reference to the risk analysis process as it does in CADRA. The separation of concerns related to what the process should produce of results during the different stages, from the concerns related to the target of evaluation, provides the foundation for understanding risk analysis in a system development setting.

The main contribution of this work is the adaptation, extension and integration of terminology from model-based risk analysis as used in CORAS with IEEE Std 1471's terminology for architectural description. CADRA builds on highly recognized international standards within software engineering and risk analysis. This provides assurance that the concepts are well founded, thoroughly evaluated and formally defined. With only a few adaptations the terminology use standardized definitions. The aspects from CORAS are all tested and evaluated through practical use in several field studies in the CORAS project. Embedding CADRA in risk analysis and system development methodologies implies that all architectural descriptions used in the methodology apply CADRA terms and their inter-relationships. This will again ensure a consistent understanding of different architectural descriptions as they follow the same standard.

Appendix - Glossary

Syntax: **Term** - *Definition* [Origin]

Abstract risk - *A generalization of a risk or a risk theme.* [CORAS]
Architecture - *The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution.*[IEEE1471]
Architectural description - *A collection of products to document an architecture.* [IEEE1471]
Asset - *Something to which a stakeholder directly assigns value and, hence, for which the stakeholder requires protection*[1]. [CADRA]
Consequence - *The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.* [AS/NZS4360]
Entity - *A physical or abstract part or feature of the system under assessment that becomes an asset when assigned value by a stakeholder, for example a service provided by the system.* [CORAS]
Environment - *A target of evaluation inhabits an environment. A target of evaluations environment can influence that target of evaluation. The environment, or context, determines the setting and circumstances of developmental, operational, political, and other influences upon that target of evaluation. The*

[1] As in HB 231 with "stakeholder" substituted for "organisation".

environment can include other systems that interact with the target of evaluation of interest, either directly via interfaces or indirectly in other ways. The environment determines the boundaries that define the scope of the target of evaluation of interest relative to other systems[2]. [CADRA]

Frequency - *A measure of the rate of occurrence of an event expressed as either*[3]*:*

A) *a quantitative description of probability or frequency.*

B) *a qualitative description of probability or frequency.*

C) *a number between 0 and 1, with 0 indicating an impossible event or outcome and 1 indicating an event or outcome is certain.*

Library Viewpoint - *A viewpoint definition may originate with an architectural description, or it may have been defined elsewhere. A viewpoint that is defined elsewhere is referred to as a library viewpoint.* [IEEE1471]

Mission - *A use or operation for which a target of evaluation is intended by one or more stakeholders to meet some set of objectives*[4]. [IEEE1471]

Model - *A view may consist of one or more architectural models. Each such architectural model is developed using the methods established by its associated architectural viewpoint. An architectural model may participate in more than one view.* [IEEE1471]

Rationale - *An architectural description (AD) shall include the rationale for the architectural concepts selected. An AD should provide evidence of the consideration of alternative architectural concepts and the rationale for the choices made. When the AD describes a system that pre-exists the development of the AD, the rationale for the legacy system architecture shall be presented, if known.* [IEEE1471]

Risk - *The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and frequency* [5]. [CADRA]

Risk analysis concern - *A concern linking related information from a stage of the risk analysis process to viewpoints.* [CADRA]

Risk analysis stakeholder -*A stakeholder whose primarily interest is the result and documentation of the risk analysis process.* [CADRA]

Risk theme - *A group of risks with similar treatment.* [CORAS]

Risk management - *The culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects.* [AS/NZS4360]

Target concern - *Those interests which pertain to the systems development, its operation or any other aspects that are critical or otherwise important to one or more stakeholders. Concerns include system considerations such as performance, reliability, security, distribution, and evolvability*[6]. [CADRA]

[2] As in IEEE Std 1471 with "target of evaluation" substituted for "system".

[3] Includes the definitions of likelihood, frequency and probability from AS/NZS 4360.

[4] As in IEEE Std 1471 with "target of evaluation" substituted for "system".

[5] As in HB 231 with "frequency" substituted for "likelihood".

[6] As the definition of concern in IEEE Std 1471.

Target of evaluation (TOE) - *An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.* [BS4778]
Target stakeholder - Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity[7]. [CADRA]
Threat - *A potential cause of an unwanted incident, which may result in harm to a system or organisation and its assets*[8]. [CADRA]
(Risk) Treatment - *Selection and implementation of appropriate options for dealing with risk.* [AS/NZS4360]
Treatment effect - *The effect of a risk treatment is either reduced frequency, reduced consequence, risk transfer (in full or in part) or risk avoidance.* [AS/-NZS4360]
Unwanted incident - *An incident such as loss of confidentiality, integrity and/or availability.* [AS/NZS4360]
View - *A representation of a whole system from the perspective of a related set of concerns.* [IEEE1471]
Viewpoint - *A specification of the conventions for constructing and using a view. A pattern or template from which to develop individual views by establishing the purposes and audience for a view and the techniques for its creation and analysis.* [IEEE1471]
Vulnerability - *Is a weakness of an asset or group of assets which can be exploited by one or more threats.* [ISO/IEC13335]

Acknowledgements

The research on which this paper reports has partly been carried out within the context of the IKT-2010 project SECURIS (152839/220) funded by the Research Council of Norway.

References

[1] J. Ø. Aagedal, F. den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stølen. Model-based risk assessment to improve enterprise security. In *Proc. EDOC2002*, pages 51–62. IEEE Computer Society, 2002.

[2] C. Alberts and A. Dorofee. *Managing Information Security Risks: The OCTAVE (SM) Approach 1/e*. Addison Wesley Professional, July 2002.

[3] *AS/NZS 4360: Risk Management*, 1999. Standards Australia, Strathfield.

[7] As the definition of stakeholder in AS/NZS 4360.
[8] As in ISO/IEC 13335 with "incident" substituted for "event".

[4] B. Barber and J. Davey. The use of the CCTA risk analysis and management methodology CRAMM. In *Proc. MEDINF. North Holland (1992)*, pages 1589–1593, 1992.

[5] A. Bouti and D. Ait Kadi. A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety Engineering*, 1:515–543, 1994.

[6] *British Standard (BS4778): Quality vocabulary: Availability, reliability and maintainability terms. Glossary of international terms.*, 1991. British Standards Institute.

[7] P. Clements, R. Kazman, and M. Klein. *Evaluating software architectures: methods and case studies*, chapter The ATAM - A Method for Architecture Evaluation. The SEI Series in Software Engineering. Addison-Wesley, 2002.

[8] F. den Braber, T. Dimitrakos, B. A. Gran, M. S. Lund, K. Stølen, and J. Ø. Aagedal. *UML and the Unified Process*, chapter The CORAS methodology: model-based risk management using UML and UP. IRM Press, 2003.

[9] T. Dimitrakos, B. Ritchie, D. Raptis, J.Ø. Aagedal, F. den Braber, K. Stølen, and S.-H. Houmb. Integrating model-based security risk management into eBusiness systems development: The CORAS approach. In *Proc. I3E2002*, pages 159–175. Kluwer, 2002.

[10] *HB 231: Information security risk management guidelines*, 2000. Standards Australia, Strathfield.

[11] *IEC 1025: Fault Tree Analysis (FTA)*, 1990.

[12] *IEC 61508: Functional safety of electrical/electronic/programmable safety related systems*, 2000.

[13] *IEEE Std 1471: Recommended Practice for Architectural Description of Software-intensive Systems*, 2000.

[14] *IEEE Std 610.12: Standard Glossary of Software Engineering Terminology*, 1990.

[15] *ISO/IEC 10746 Information technology - Basic reference model of Open Distributed Processing*, 1998.

[16] *ISO/IEC TR 13335-1: Information technology - Guidelines for the management of IT Security-Part 1: Concepts and models for IT Security*, 2001.

[17] *ITU-T X.800: Security architecture for open system interconnection for CCITT applications*, 1991. (Technically aligned with ISO 7498-2).

[18] K. Lano, K. Androutsopoulos, and D. Clark. Structuring and design of reactive systems using RSDS and B. In *Proc. FASE 2000*, LNCS 1783, pages 97–111. Springer, 2000.

[19] M. S. Lund, I. Hogganvik, F. Seehusen, and K. Stølen. UML Profile for Security Assessment. Technical Report STF40 A03066, SINTEF Telecom and Informatics, Norway, December 2003.

[20] Object Management Group (OMG). *UML Superstructure 2.0 Draft Adopted Specification (ptc/03-08-02)*, 2003.

[21] J. R. Putman. *Architecting with RM-ODP*. Prentice Hall PTR, 2001.

[22] F. Redmill, M. Chudleigh, and J. Catmur. *Hazop and software Hazop*. Wiley, 1999.