



701 E. Chocolate Avenue, Hershey PA 17033-1117, USA Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com **ITB9263**

Chapter XVII

The CORAS Methodology: Model-based Risk Assessment Using UML and UP

Folker den Braber SINTEF Telecom and Informatics, Norway

Theo Dimitrakos CLRC Rutherford Appleton Laboratory, UK

Bjørn Axel Gran Institute for Energy Technology, Norway

Mass Soldal Lund SINTEF Telecom and Informatics, Norway

Ketil Stølen SINTEF Telecom and Informatics, Norway

Jan Øyvind Aagedal SINTEF Telecom and Informatics, Norway

ABSTRACT

This chapter introduces the CORAS methodology in which Unified Modeling Language (UML) and Unified Process (UP) are combined to support a model-based risk assessment on security-critical systems. The hypothesis is that modeling techniques like UML

This chapter appears in the book, *UML and the Unified Process* by Liliana Favre. Copyright © 2003, IRM Press, an imprint of Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

contribute to increased understanding for the different stakeholders involved during a risk assessment. In the CORAS methodology, a traditional risk management process is integrated with UP, which is a well-accepted system development process. CORAS tries to show how UML can contribute to better understanding, documentation, and communicating during the different phases of the risk management process. CORAS addresses both systems under development and systems already in use.

INTRODUCTION

After the development of information technology (IT) in the last part of the previous century, it has become impossible to imagine a world without IT systems. The impact of this development has been enormous and has opened up a lot of new possibilities and challenges. One of these challenges regards risks. To make use of these new techniques in a dependable way, it is of vital importance to get an overview and understanding of the different risks connected to the use of IT systems. This chapter addresses model-based risk assessment; a methodology developed in the CORAS project. CORAS (2000) is funded by the European Union and develops a tool-supported framework for precise, unambiguous, and efficient risk assessment of security-critical systems. CORAS aims at a methodology for risk assessment that is easy to understand and that functions as a natural part of both the IT system development and the maintenance life cycle. To achieve this CORAS leans on the knowledge gained from the use of models in graphical, semiformal languages like the Unified Modeling Language (UML) (OMG, 2001b). The main focus of this chapter lies on the part of the CORAS project that addresses the integration of risk management and system development.

The remainder of this chapter is divided into five sections. First, some background is presented. The section thereafter addresses model-based risk assessment and some of the problems connected to this. The main part of the chapter is contained in the section on the risk management process and the integrated risk management and system development process. After a section on related work, a brief conclusion is given.

BACKGROUND

The CORAS approach focuses on the tight integration of viewpoint-oriented UML modeling in the risk management process. An important aspect of the CORAS project is the practical use of UML and the Unified Process (UP) (Kruchten, 1999) in the context of security and risk assessment. This chapter concentrates on the integration of UML and UP in the risk assessment process.

CORAS addresses security-critical systems in general, emphasizing 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 (ISO/IEC TR 13335:2001). An IT system, in the sense of CORAS, is not just technology. It is also the humans interacting with the technology and all relevant aspects of the surrounding enterprise context.

Copyright © 2003, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: <u>www.igi-</u> <u>global.com/chapter/coras-methodology-model-based-</u> risk/30550

Related Content

Forward Engineering and UML: From UML Static Models to Eiffel Code

Liliana Favre, Liliana Martinezand Claudia Pereira (2003). UML and the Unified Process (pp. 199-216).

www.irma-international.org/chapter/forward-engineering-uml/30542

Modeling of Web Services using Reaction Rules

Marko Ribaric, Shahin Sheidaei, Milan Milanovic, Dragan Gasevic, Adrian Giurcaand Sergey Lukichev (2009). *Handbook of Research on Emerging Rule-Based Languages and Technologies: Open Solutions and Approaches (pp. 422-446).* www.irma-international.org/chapter/modeling-web-services-using-reaction/35869

Variability Expression within the Context of UML: Issues and Comparisons

Patrick Tessier, Sébastien Gerard, François Terrierand Jean-Marc Geib (2005). Advances in UML and XML-Based Software Evolution (pp. 322-349). www.irma-international.org/chapter/variability-expression-within-context-uml/4942

XML Stream Processing: Stack-Based Algorithms

Junichi Tatemura (2010). Advanced Applications and Structures in XML Processing: Label Streams, Semantics Utilization and Data Query Technologies (pp. 184-206). www.irma-international.org/chapter/xml-stream-processing/41505

A Framework for Managing Consistency of Evolving UML Models

Tom Mens, Ragnhild Van Der Straetenand Jocelyn Simmonds (2005). *Software Evolution with UML and XML (pp. 1-30).* www.irma-international.org/chapter/framework-managing-consistency-evolving-uml/29608