# Experiences from using model-based risk assessment to evaluate the security of a telemedicine application

**Yannis C. Stamatiou[1], Eva Henriksen[2], Mass Soldal Lund[3], Eva Mantzouranis[4], Michalis Psarros[5], Eva Skipenes[2], Nikos Stathiakis[5], Ketil Stølen[3]**

[1]Computer Technology Institute (CTI), 61 Riga Ferraiou Str., P.O. Box 1122, Patras, GR-262 21, Greece. E-mail: stamatiu@cti.gr
[2]Norwegian Centre for Telemedicine, University Hospital of North Norway. E-mail: {Eva.Henriksen,Eva.Skipenes}@telemed.no
[5]SINTEF Telecom and Informatics, P.O.Box 124 Blindern, N-0314 Norway. Email: {Mass.S.Lund,Ketil.Stoelen}@sintef.no
[4]University General Hospital, University of Crete, Dept. of Paediatrics, Greece. E-mail: mantzoura@med.uoc.gr
[5]ICS-FORTH, P.O. Box 1385, GR 711 10, Heraklion, Greece. E-mail: {psarros,statiaki}@ics.forth.gr

## 1. Introduction

CORAS is a EU funded RTD project (IST-2000-25031) developing a methodology and a tool-supported framework for model-based risk assessment targeting security critical systems. CORAS addresses security critical systems in general, but puts particular emphasis on IT security, which includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems (ISO/IEC TR 13335-1:2001 – see [10]). An IT system in the sense of CORAS is not just technology, but also the humans interacting with the technology and all relevant aspects of the surrounding organisation and society. In what follows, we briefly describe the CORAS framework and summarize our experiences from applying this framework for the evaluation of the security of the IP-based videoconference service for remote follow up of asthmatic children of the ATTRACT telemedicine application. The assessment described in this paper is the first of several trials within the CORAS-project. We refer to [1] for an introduction to risk management and assessment.

## 2. A brief description of the CORAS framework

The CORAS framework has four main anchor-points, (1) a risk documentation framework based on the Reference Model for Open Distributed Processing [8][10] (RM-ODP), (2) a risk management process based on AS/NZS 4360 [2], (3) an integrated risk management and system development process based on the Unified Process [9] (UP), (4) and a platform for tool-integration based on XML [7]. The risk documentation framework is used both to document the target of assessment as well as to record risk assessment results. The risk management process provides a sequencing of the risk management process into sub-processes for context establishing, risk identification, risk assessment, risk evaluation, and risk treatment. This paper concentrates on experience from applying the risk management process.

One of the central ideas behind the CORAS methodology is the use of semi-formal graphical description techniques. The descriptions are mainly expressed in the Universal Modelling Language (UML) [11], and they are used: (1) In order to describe the relevant aspects of the target of analysis at the right level of abstraction. Semi-formal techniques improve the precision of such descriptions, which can improve understanding and, thus, the quality of risk assessment results. (2) As media for communication and interaction between different groups of stakeholders involved in a risk assessment. The use of graphical techniques is expected to speed up the assessment process since the danger of wasting time and resources on misconceptions is reduced. (3) To document risk assessment results and the assumptions on which these results depend, which can possibly reduce maintenance costs by increasing the possibilities for reuse.

The CORAS risk assessment methodology is a careful integration of techniques and templates inspired by HazOp Analysis [6], Fault Tree Analysis (FTA) [5], Failure Mode and Effect Criticality Analysis (FMECA) [4], Markov Analysis [1][12] as well as CRAMM [3].

## 3. The telemedicine application ATTRACT and experiences from its assessment

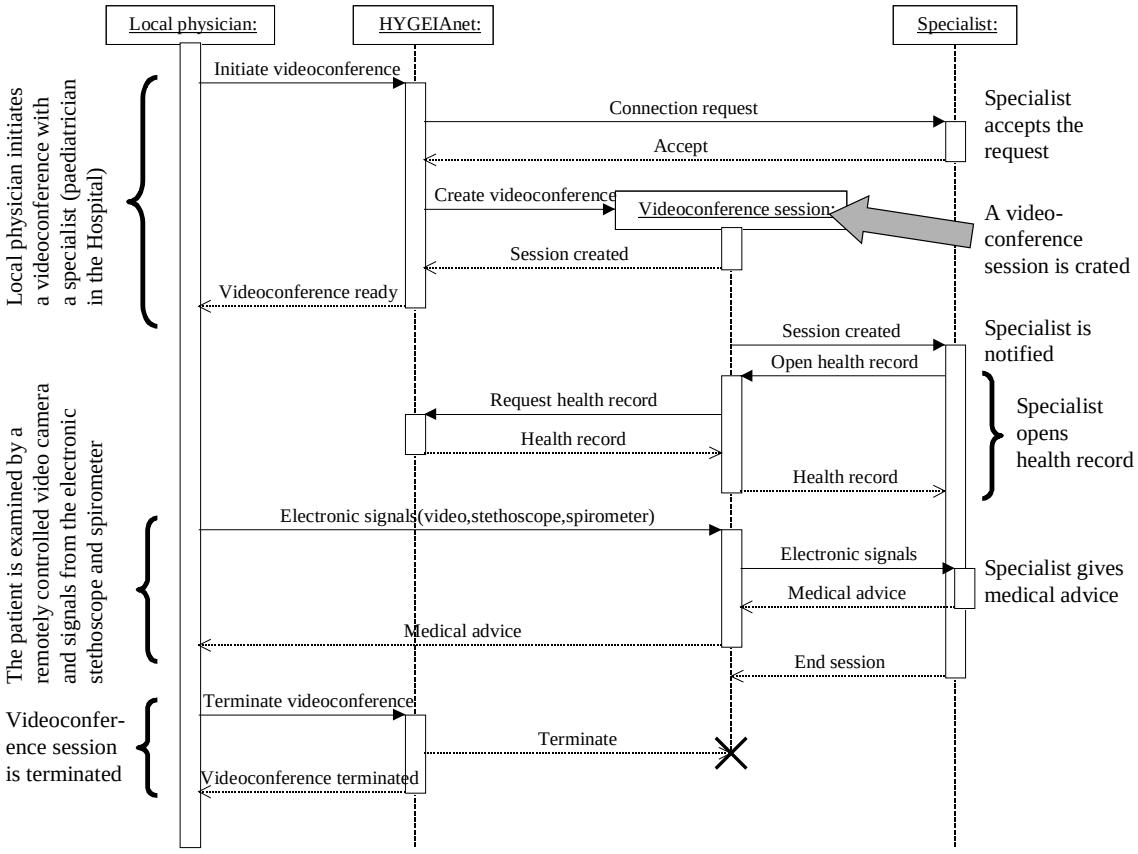
In this section, the assessment of the ATTRACT application, which is the first trial of the CORAS-project, is described. The general idea of having trials during the development phases of CORAS and

not after the framework is completed is, mainly, to offer the opportunity to the CORAS developers to reconsider and adjust progressively parts of it, taking into account the experiences of each of the trials.

The description of the assessment follows the risk management process. The process is divided into five sub-process which, again, comprise a number of activities:

**Sub-process 1: Identify Context.**

- **Activity 1.1: Identify areas of concern.** The target of the first telemedicine trial held in Crete was the tele-consultation telemedicine application ATTRACT. The ATTRACT application is used for follow-up examination of asthmatic children in Heraklion, Crete, in Greece. It involves one paediatric specialist at the hospital and doctors from other primary health care centres or district hospitals. The aims of the first risk assessment session were the following: (1) To experiment with as many aspects of the CORAS framework as time allowed providing feedback for improvements to the framework and offering an overall evaluation of the CORAS framework to partners that are involved in its development. (2) To involve the medical professionals (University of Crete) in the risk management/assessment process in order to have their views and experiences as an invaluable input to the process as well as to educate them in security related aspects of the telemedicine applications they use in their daily practice. (3) To provide to the platform developers (University of Crete and FORTH) with a risk assessment report concerning the identified threats to their systems, their causes and consequences along with an evaluation of their severity. The scenario we chose to model and assess is described in the below UML sequence diagram. In relation to the use of models, we would like to comment that during the risk analysis session, a special type of diagrams prescribed by CORAS, the *context use case diagram* helped the risk analysis team to discover and correct some misconceptions about the scenario with the help of the medical expert present at the session. We believe that the use of models constructed using a well-defined graphical language, in general may help towards this direction as it helps both the risk analysis experts and the stakeholders to see the description of only the essentials of the target scenario without any distractions stemming from different views or experiences about the system.



- **Activity 1.2: Identify and value assets**. The asset identification and evaluation was conducted by means of the CRAMM method and the construction of a variety of UML-based models of the ATTRACT application scenario. This method seemed rather difficult to apply, however, due to a large number of cases that the method requires to be examined by the analyst.
- **Activity 1.3: Identify security requirements.** The most important security requirements were identified and discussed with the doctors. Briefly, the identified requirements for the chosen scenario were *availability*, *integrity* and *confidentiality* and *non-repudiation*.

**Sub-process 2: Identify Risks.**

- **Activity 2.1: Identify hazards/threats to assets.** The HazOp method was applied in order to identify possible threats for each of the identified assets. In general, the medical professionals found HazOp easy to understand and participate in. Most of the identified threats were already known to them but some new threats were also brought to the their attention during the process. In all, HazOp was useful to carry out, at least as a means to document the threats of the target system.
- **Activity 2.2: Identify vulnerabilities of assets.** Results from identification of vulnerabilities were not obtained, as CORAS was not sufficiently developed yet to include such capability.

**Sub-process 3: Analyse Risks.**

- **Activity 3.1: Consequence/impact evaluation.** FTA was applied in order to analyze the least understandable of the threats identified by the HazOp. One of the advantages of FTA, observed and remarked by all participants in the trial, stems from the fact that the way it is structured (visually) helps the risk assessment experts to communicate and explain the threats to non-experts (like doctors) and, likewise, helps non-experts understand the causes of threats and the cause combinations that lead to the appearance of the threats. The FTA trees built during the risk analysis session also helped the network and system experts that participated to structure their view of the causes of the different threats. In order to conduct a more detailed analysis of some of the identified risks, FMEA (a variant of FMECA) was performed. FMEA was very time-consuming, but it gave the opportunity for uncovering many interesting details about the analyzed threats. For these reasons it is used only for the most security-critical parts of a system and it seems to require the participation of the experts on the specific aspect that is being analyzed.
- **Activity 3.2: Evaluate likelihood of occurrence.** An important step towards the end of the risk assessment session is the assignment of likelihoods and consequences severity to the identified threats. It should be noted that the likelihoods given to the threats were based, to some extent, on the past experience of the participating developers and users of the application.

**Sub-process 4: Risk Evaluation.**

- **Activity 4.1: Determine level of risk.** Having determined the consequences/impact and the likelihoods of the identified threats to assets, the next step is to determine how risky is the use of the target system according to the conducted risk analysis. This is accomplished by defining a matrix such as the one shown on the next page. This matrix has as rows the levels of consequence in increasing severity while as columns it has the likelihoods, ordered from left to right in increasing frequency. Each (*consequence*,*likelihood*) combination is then assigned a risk ("danger") level that is depicted using a scale of grey levels: the whiter corresponding to low risk and the darkest to extreme. It should be remarked that the opinions of the involved stakeholders may vary as to which risk level should be assigned to each (*consequence*,*likelihood*) combination due to their different interests in the system as well as their different experiences from its use.

| Consequence | Likelihood | | | | |
|---|---|---|---|---|---|
| | *Rare* | *Unlikely* | *Possible* | *Likely* | *Almost certain* |
| *Insignificant* | Low | Low | Low | Moderate | High |
| *Minor* | Low | Low | Moderate | High | High |
| *Moderate* | Moderate | Moderate | High | High | Extreme |
| *Major* | High | High | Extreme | Extreme | Extreme |
| *Catastrophic* | Extreme | Extreme | Extreme | Extreme | Extreme |

The rest of Sub-process 4, which is concerned with prioritising the risks, and the whole of Sub-process 5, which is concerned with treatment of risks, where not conducted due to time constraints. However, the activities omitted during this risk assessment will be performed in a second risk assessment round that will continue at the point that the performed risk assessment stopped.

## 4. Conclusions

The application of the CORAS framework was an interesting and educating experience for the people who took part in it and provided a useful feedback to the ongoing development of the CORAS framework. The medical experts appreciated the fact that the threats they already knew were organized and classified according to their severity. The technical people, who developed the application along with the medical experts, found the CORAS methods very useful for the detection and correction of the various problems, especially FTA for its structure and FMEA for its detail. An important characteristic of risk assessments is the involvement of stakeholders with different backgrounds and, thus, communication between the different stakeholders was always a critical issue. In particular, the trial highlighted the need for methodology and guidelines for how to reach a consensus among the involved stakeholders. Two more trials within telemedicine are planned (in addition to three e-commerce trials).

## References


[1] Andrews, J. D. and Moss, T. R., (1993): *Reliability and Risk Assessment*, 1st Ed. Longman Group UK.

[2] Australian Standard (1999): Risk Management. AS/NZS 4360:1999, Strathfield: Standards Australia.

[3] Barber, B. and Davey, J., (1992): The Use of the CCTA Risk Analysis and Management Methodology CRAMM in Health Information Systems, in *MEDINFO 92*, edited by Lun K. C., Degoulet P., Piemme T. E. and Rienhoff O., pp 1589 –1593, North Holland Publishing Co, Amsterdam.

[4] Bouti, A. and Ait Kadi, D., (1994): A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety Engineering*, **1** (4), pp 515-543.

[5] British Standard BS 5760, (1991): *Reliability of systems, equipment and components,* Part 7: "Guide to fault tree analysis".

[6] Draft Interim Defence Standard 00-58/1, (1985): *A Guide to HAZOP Studies on Systems which Incorporate a Programmable Electronic System*, Ministry of Defence, UK.

[7] Grose, T. J., Doney, G. C., Brodsky, S. A., (2002): *Mastering XMI: Java Programming with XMI, XML, and UML*, Wiley.

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

[9] Krutchten, P., (1999): *The Rational Unified Process, An Introduction*, Reading, MA: Addison-Wesley.

[10] Putman, J. R., (2000): *Architecting with RM-ODP*, Prentice-Hall.

[11] Rumbaugh, J., Jacobson, I. and Booch, G., (1999): *The Unified Modeling Language, Reference Manual*, Addison-Wesley.

[12] Siu, N., (1994): Risk Assessment for dynamic systems: An overview, *Reliability Engineering and System Safety*, Vol. 43, pp 43-73.