



**The
SARDAS
Manifesto**

Ketil Stølen

July 7, 2004

Executive summary

The SARDAS project is developing novel tool supported methodology for robust design, assessment and specification to ensure availability. SARDAS approaches availability in a model-oriented manner emphasizing modularity and is oriented towards UML 2.x. Real cases in the area of telecom and e-commerce are addressed in order to assure the practicality of the approach. The added complexity introduced by dynamics and mobility is considered important for the relevance of the results. SARDAS aims to provide:

- A tool supported UML inspired language for the specification and modelling of systems for high availability.
- A tool supported methodology for model-based assessment and testing to ensure availability.
- A tool supported methodology for modular design and implementation of systems with high availability.
- Results and experiences from using the resulting technologies in practise.

SARDAS is funded by the Research Council of Norway under the Basic ITC Research Programme and runs from January 1 2003 until December 31 2006.

SARDAS is a joint initiative between:

- Department of Informatics at the University of Oslo.
- SINTEF ICT in Oslo.
- Department of Telematics at the Norwegian University of Science and Technology in Trondheim.
- Ericsson Applied Research Center (NORARC) in Asker.



List of content

EXECUTIVE SUMMARY	2
1 THE SARDAS MANIFESTO	4
2 THE SARDAS BASICS	4
3 THE SARDAS OBJECTIVES	4
3.1 TECHNICAL OBJECTIVE.....	4
3.2 DEMONSTRATION OBJECTIVE	5
3.3 DISSEMINATION OBJECTIVE.....	5
4 THE SARDAS PRESUPPOSITIONS	5
5 THE SARDAS FRAMEWORK	6
6 THE SARDAS WAY FORWARD	7
7 THE SARDAS FIELD TRIALS	8
8 THE SARDAS TEAM	9
8.1 DOCTORAL FELLOWS	9
8.2 GUEST SCIENTISTS	9
8.3 PRINCIPAL RESEARCHERS.....	9
9 THE SARDAS ADVISORY BOARD	10
REFERENCES	10

1 The SARDAS manifesto

The main purpose of this document is to provide an overview and describe the key aspects of the SARDAS project. This includes:

- The SARDAS basics: the funding, duration and partners.
- The SARDAS objectives: the overall success-criteria of the SARDAS project.
- The SARDAS presuppositions: the context in which the research is conducted.
- The SARDAS framework: the main SARDAS deliverable.
- The SARDAS way forward: how we intend to reach our objectives.
- The SARDAS field trials: the way the SARDAS research activities is driven by real cases.
- The SARDAS team: the doctoral fellows, principal researchers and guest scientists.
- The SARDAS advisory board: the industrial and academic advisors.

2 The SARDAS basics

The SARDAS project is funded by the Research Council of Norway under the Basic ICT Research Programme.

SARDAS runs from January 1 2003 until December 31 2006 with an overall funding of eight million NOK.

The full project title is "Securing Availability by Robust Design, Assessment and Specification".

SARDAS is a joint initiative between:

- Department of Informatics at the University of Oslo.
- SINTEF ICT in Oslo.
- Department of Telematics at the Norwegian University of Science and Technology in Trondheim.
- Ericsson Applied Research Center (NORARC) in Asker.

3 The SARDAS objectives

3.1 *Technical objective*

The principal technical objective of SARDAS is to improve on state-of-the-art for the specification, design and development of systems with high availability by providing:



- Novel notations and constructs for the specification and modelling of systems for high availability.
- An integrated methodology and prototype tool for model-based assessment and model-based testing of availability.
- Methodology and tools for compositional design and implementation of systems with high availability.

3.2 Demonstration objective

Another important objective of SARDAS is to try out and evaluate the technical results; in particular:

- SARDAS aims to demonstrate the usefulness of the technical results by applying them in practical cases.

3.3 Dissemination objective

Dissemination of technical results and their evaluations in relevant international and national fora is a third SARDAS objective. We aim to disseminate SARDAS results by:

- 4 doctoral theses;
- 17 high-quality conference articles;
- 4 journal articles;
- 4 popular scientific articles;
- 1 public workshop;
- contributing towards the standardisation of novel language constructs for robustness specification in general, and the specification of availability in particular, with particular focus on the Object Management Group.

4 The SARDAS presuppositions

SARDAS understands *model-based* system development as system development where:

- Models are expressed in UML [11] like languages.
- The development is documented in terms of models at different levels of abstraction and addressing different concerns through "views".
- Models play a fundamental role, not only in the initial development phases, but also in maintenance, reuse and further development.
- Models document the relations between levels of abstraction, between views and between levels of abstraction and views.

SARDAS ignores that model-based system development, as described above, is not common practise today and assumes a model-based approach to system development. SARDAS aims

to provide specialised support for the specification and analysis of availability under this assumption.

SARDAS addresses availability within a security context. *Security* is defined as [4] the preservation of:

- *confidentiality*: ensuring that information is accessible only to those authorized to have access;
- *integrity*: safeguarding the accuracy and completeness of information and processing methods;
- *availability*: ensuring that authorized users have access to information and associated assets when required.

5 The SARDAS framework

The SARDAS framework, as illustrated in Figure 1, aims to support model-based development of available systems through novel notations, constructs, approaches and tools supporting specification, modelling and various kinds of analysis based on models. The framework will support:

- Modelling in terms of
 - sequence diagrams as for example proposed in UML2.0 [11] and MSC [10],
 - role-based description as for example proposed in [3], and
 - state machines as for example proposed in UML2.0 and SDL2000 [9].
- Analysis in terms of
 - model checking as described in [8], and
 - model testing as suggested in [7].
- Refinement in terms of narrowing, supplementing and detailing as described in STAIRS [4].

The SARDAS framework will have a uniform semantics expressed in mathematics based on formal methods like for example [2].

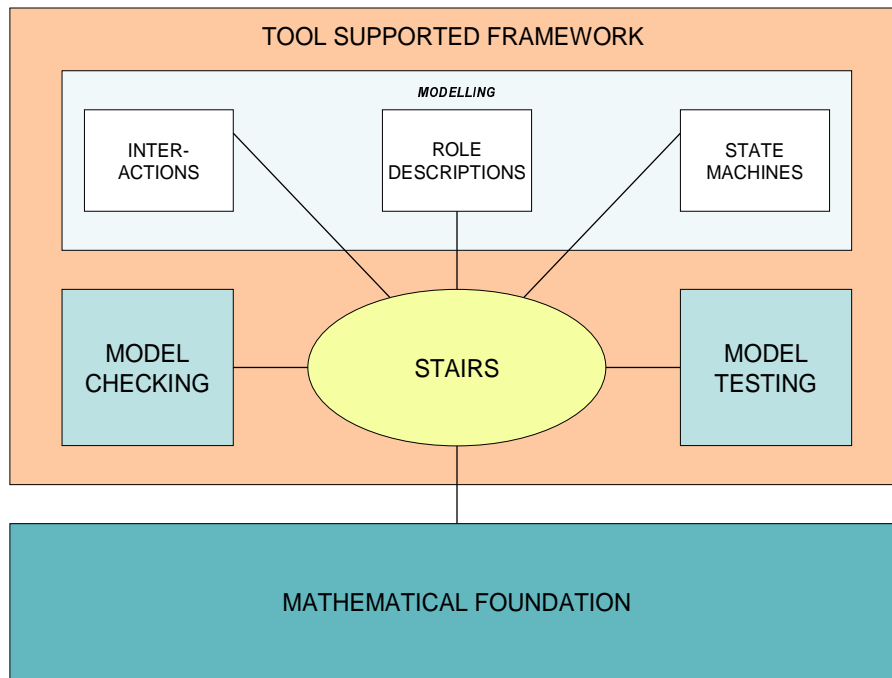


Figure 1: The SARDAS tool supported framework

6 The SARDAS way forward

SARDAS is based on an iterative research process with a uniform distribution of resources throughout the duration of the project. There are three main iterations, in the following referred to as Research Phase 1, 2 & 3, each of which is terminated by a field trial where the tools and methodology developed to that point in time are tried out and assessed. There is also an Establishment Phase before the “real” research work is initiated and a Concluding Phase after the field trials have been completed.

Month	Year	Activity	Result
Establishment phase			
3	2003	Establish an advisory board of five members with strong industrial background	Plan for the use of the advisory board
1-6	2003	Identification of current state	Report
6	2003	Advisory board meeting	Recommendations
6	2003	Planning	Refined project plan
First R&D phase			
6-15	2004	Research	Technical papers

15-18	2004	First field trial	Assessment report
18	2004	Advisory board meeting	Recommendations
18	2004	Planning	Refined project plan
Second R&D phase			
18-27	2005	Research	Technical papers
27-30	2005	Second field trial	Assessment report
30	2005	Advisory board meeting	Recommendations
30	2005	Planning	Refined project plan
Third R&D phase			
30-39	2006	Research	Technical papers
39-42	2006	Third field trial	Assessment report
42	2006	Advisory board meeting	Recommendations
42	2006	Public workshop	Proceedings
Concluding phase			
42-48	2006	Finalising research	Technical papers Submitted theses
46-48	2006	Evaluation and assessment	Report

7 The SARDAS field trials

Three major field trials are planned for the SARDAS project. The field trials have four main objectives:

- To ensure that the SARDAS framework is applicable to a wide range of availability critical systems and applications.
- To guide the development of the SARDAS framework by providing feedback to the SARDAS research activities throughout the lifetime of the SARDAS project.
- To benefit the trial sites whose systems and applications were targeted by the field trials.
- To assess and evaluate the SARDAS framework.

To this point in time, only the first of the three field trials has been defined. It addresses a service called AMIGOS (Advanced multimedia in group organized service) that was

developed in the AVANTEL project funded by the Research Council of Norway. The AMIGOS service has been specified and partly implemented. The AMIGOS service is quite comprehensive so in the SARDAS context we consider only a restricted part of it.

The main idea in AMIGOS is that persons may log into the service using various types of terminals like PDA and PC and get access to their private accounts identified by a so-called UserAgent. The UserAgent represents the user in the system and contains all relevant information that the user will need in order to interact with services. There are different types of meetingplaces available. In SARDAS we focus on the specification and analysis of a chatting service.

8 The SARDAS team

8.1 *Doctoral fellows*

The SARDAS team includes five doctoral fellows of which four are directly funded by the project:

- Knut Eilif Husa, University of Oslo / Ericsson
- Mass Soldal Lund, University of Oslo / SINTEF ICT
- Atle Refsdal, University of Oslo
- Judith Rossebø, Norwegian University of Science and Technology / Telenor
- Ragnhild Kobro Runde, University of Oslo (associated, but not funded by SARDAS)

8.2 *Guest scientists*

The project funds three guest scientists – each on a two months guest fellowship:

- Manfred Broy, Professor (Munich University of Technology)
- Ina Schieferdecker, Professor (Technical University Berlin) / Head of Competence Center for Network Interoperability and Performance (Fraunhofer FOKUS, Berlin)
- Thomas Weigert, Director of Software Technologies and Standards (Motorola Global Software Group)

8.3 *Principal researchers*

The SARDAS team has four principal researchers. They act as supervisors for the doctoral fellows.

- Rolv Bræk, Professor (Norwegian University of Science and Technology)
- Øystein Haugen, Associated Professor (University of Oslo)
- Birger Møller Pedersen, Professor (University of Oslo)



- Ketil Stølen, Professor (University of Oslo) / Chief Scientist (SINTEF ICT)

Ketil Stølen is the leader of the SARDAS project.

9 The SARDAS advisory board

The project has an advisory board of seven members including industrialists as well as academics.

- Dag Belsnes, Consultant (Pharos) / Professor (University of Oslo)
- Petter Christensen, Norwegian Defence Logistics Organisation
- Bjarne Helvik, Professor (Norwegian University of Science and Technology)
- Arne Bjørn Mildal, Development Manager IT & Internet (NetCom)
- Ove Olsen, Director (Centre for Information Security)
- Olaf Owe, Professor (University of Oslo)
- Jon Ølnes, Senior Security Consultant (IBM Norway)

The advisory board had two full day meetings with the project team in 2003.

References

- [1] Avizienis A., Laprie, J.-C., Randell, B. Fundamental Concepts of Dependability, Research Report N01145, LAAS-CNRS, April 2001.
- [2] Broy, M., Stølen, K. Specification and development of interactive systems: Focus on streams, interfaces and refinement. Springer, 2001.
- [3] Floch, J. Towards plug-and-play services: Design and validation using roles. PhD-thesis, Norwegian University of Science and Technology, 2003.
- [4] Haugen, Ø., Stølen, K. STAIRS – Steps to analyze interactions with refinement semantics. In Proc. Sixth International Conference on UML (UML'2003), LNCS 2863, pages 388-402, Springer, 2003.
- [5] Haugen, Ø., Møller-Pedersen, B., Weigert, T. Structural Modeling with UML 2.0. In UML for Real. Lavagno, L., Martin, G. and Selic, B. (eds.). Kluwer, 2003.
- [6] ISO/IEC 17799: 2000 (E) Information technology – code of practice for information security management. First edition 2000-12-01.
- [7] Lund, M.S. Testing decomposition of component specifications based on a rule for formal verification. In Proc. Third International Conference on Quality Software (QSIC'2003), pages 154-160, IEEE Computer Society, 2003.



- [8] Clarke, E.M., Grumberg, O., Peled, D.A. Model checking. MIT Press, 1999.
- [9] Specification and Description Language (SDL). ITU-T Recommendation Z.100, 1999.
- [10] Message Sequence Charts (MSC). ITU-T Recommendation Z.120, 1999.
- [11] Unified Modeling Language: Superstructure. OMG ad/03-04-01, 2003.