Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

An Extended Goal-oriented Development Methodology with Contextual Dependability Analysis

Danilo F. Mendonça

Dissertação apresentada como requisito parcial
para conclusão do Mestrado em Informática

Orientadora
Prof. Dr.ª Genaína Nunes Rodrigues

Brasília
2015

Universidade de Brasília — UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Mestrado em Informática

Coordenadora: Prof.ª Dr.ª Alba Cristina Magalhaes Alves de Melo

Banca examinadora composta por:

Prof. Dr.ª Genaína Nunes Rodrigues (Orientadora) — CIC/UnB
Prof.ª Dr.ª Vander Alves — CIC/UnB
Prof. Dr. Luciano Baresi — Politecnico di Milano

CIP — Catalogação Internacional na Publicação

Mendonça, Danilo F..

An Extended Goal-oriented Development Methodology with Contextual Dependability Analysis / Danilo F. Mendonça. Brasília : UnB, 2015.
21 p. : il. ; 29,5 cm.

Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2015.

1. LaTeX, 2. metodologia científica

CDU 004.4

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

An Extended Goal-oriented Development Methodology with Contextual Dependability Analysis

Danilo F. Mendonça

Dissertação apresentada como requisito parcial
para conclusão do Mestrado em Informática

Prof. Dr.ª Genaína Nunes Rodrigues (Orientadora)
CIC/UnB

Prof.ª Dr.ª Vander Alves	Prof. Dr. Luciano Baresi
CIC/UnB	Politecnico di Milano

Prof.ª Dr.ª Alba Cristina Magalhaes Alves de Melo
Coordenadora do Mestrado em Informática

Brasília, 30 de janeiro de 2015

Dedicatória

Agradecimentos

Resumo

A static and stable operation environment is not a reality for many systems nowadays. Context variations impose many threats to systems safety, including the activation of context specific failures. Goal-oriented software-development methodologies (SDM) adds the ‘why’ to system requirements, i.e., the intentionality behind system goals and the means to meet then. Contexts may affect what requirements are needed, which alternatives are available and the quality of these alternatives, including dependability attributes. In order to allow a formal and probabilistic analysis of systems affected by context variation and elicited with Goal-Oriented Requirements Engineering (GORE) approach, we have proposed an extension to the TROPOS goal-oriented methodology to include dependability constraints to goals and to provide a more precise and formal requirements verification by translating a contextual goal-model annotated with a behavioural regular expression into a PRISM probabilistic model to be checked against properties defined with the Probabilistic Computation Tree Logic (PCTL). We evaluated the proposal with a case study of a Mobile Personal Emergency Response System (MPERS).

Palavras-chave: LaTeX, metodologia científica

Abstract

Keywords: LaTeX, scientific method

Sumário

1 Introduction **1**

1.1 Problem definition 1

1.2 Proposed solution 2

1.3 Evaluation 3

1.4 Summary of Contributions 3

1.5 Document organization 4

2 Baseline **5**

2.1 Goal-oriented Requirements Engineering 5

2.2 Contexts 6

2.3 Dependability Analysis 7

2.4 PRISM Probabilistic Model Checker 7

3 Related Work **9**

3.1 Contextual Goal Model 9

3.2 Runtime Goal Model 10

4 Proposal **11**

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introduction

1.1 Problem definition

According to Lamsweerde, a poor requirements engineering (RE) is the major source of system failures [citation]. Goal-oriented requirements engineering (GORE) has gained the attention of both academic and industrial practitioners due to its ability to model the intentionality behind system requirements. More than just presenting the 'what' and the 'how' of a system, goal models also express the 'why' of different requirements to exist. Also, its simple graphical notation allows non-technical stakeholders to take part in the modelling and analysis process or at least to have a clear view of the proposed system-to-be and its social dependencies, both strategically through higher level goals and operationally through lower level goals and tasks.

The contextualization of an information means that its validity is not absolute in respect to the state of the world it relates to. Mobile and pervasive computing, among others, are examples of new computer paradigms for which the operation environment is not static, but dynamic. Battery, signals strength, component's availability and the quality of resources and relevant information such as the user geographic location may vary through time, posing a new sort of challenge to the development of socio-technical systems based on these paradigms. The contextualization of the informations gathered at RE phase becomes imperative once its validity may be threatened by changing environment conditions [Finkelstein, CGM].

In traditional GORE methodologies [GORE CA comparison], contribution analysis are based on domain knowledge about the positive, neutral (implicit) or negative impact of a given system alternative to one or more system soft-goals. By comparing the overall contribution of two or more alternatives, a decision is made about which one should be adopted for the system-to-be. The problem with this approach is threefold. First, it is based on domain knowledge information that may not exist or may not be precise and reliable enough. As a consequence, the decision of which alternative to use, both at design time and at runtime, may be biased and lead to unacceptable system failures. Second, it is limited to a static representation of the system goals and activities without any temporal/behaviour information that could be used to verify the bigger picture of the system behaviour for dynamic properties such as its availability, performance, reliability, power consumption, etc. Finally, contribution assertions are deterministic and do not allow a probabilistic verification, i.e., if non-determinism is present either in the model, in its technical or social components or in its environment.

1.2 Proposed solution

In order to provide a more solid and precise approach for the non-functional verification of different system alternatives and to improve the GORE contribution analysis, we propose the extension of the TROPOS goal-oriented software development methodology with a probabilistic model checking (PMC) approach that has already been explored and is supported by tools such as PRISM model checker[genaína PMC, PRISM]. The resulting verification model should represent activities of the system-to-be, including its elicited alternatives with particular metrics that, combined to the context effects and the properties defined using the Probabilistic Computation Tree Logic (PCTL), will provide estimations for the local or global value of attributes required as constraints associated to the system, e.g., its global reliability and power consumption.

The PMC technique should be performed with a probabilistic model representing system activities of the goal model enriched with a runtime specification and a contextual notation as proposed in different works by Dalpiaz et al. [CGM, RTGORE]. Context variables and adoptable alternatives should be parametrized to produce a formula that can check the system and its alternatives for different contexts of operation. This verification, performed as part of the Validation & Verification (VV) phase in RE, should anticipate any violations to the constraints required for the system. Treating a detected violation at design time may correspond to actions such as making a different choice for underlying technical components used by tasks, the optimization of these components behaviour specification or even the disposal of this alternative as a means to satisfy its goal. PMC technique also allows the identification of system parts with the most influence on each metric through sensitive analysis.

1.3 Evaluation

The proposal was evaluated with the application of the extended TROPOS methodology to the development of a Mobile Personal Emergency Response System (MPERS). This system may be seen as a body area network (BAD) with extended functionalities related to emergency response and mobile computing [BAD]. Instead of a home or hospital static environment, the MPERS is conceived to allow patients with different health risk degrees to maintain mobility while they are monitored and assisted. If a medical emergency is detected, a geolocation feature should identify where the emergency response team should be addressed to. The MPERS features were based on real emergency response systems available at the industry and also at the BAD proposed by Fernandes[Fernandes].

The evaluation process has pointed out the major benefits and limitations of the extended TROPOS proposal. Time to market is an important aspect for any software development methodology, therefore an automated generation of the PRISM probabilistic model was implemented based on an existing open source tool for TROPOS named TAOM4E[citation] in order to optimize the verification step. Also, the soundness and precision of the probabilistic verification results are crucial aspects to be evaluated as they should try to eliminate any violation that could lead to a system failure, specially failures considered severe or catastrophic.

1.4 Summary of Contributions

This section summarizes the contributions of this proposal.

1. A new contribution analysis approach for the TROPOS Goal-oriented software development methodology.

2. Conversion rules among different decomposition and runtime constraints in a runtime goal model to a PRISM probabilistic model.

3. Inclusion of context effects over goals, means and metrics in the PRISM model using appropriate constructs and parameters for each case.

4. A parser implementation for the regular expression (regex) language used in runtime goal-models to specify temporality, cardinality and goals priority.

5. An automatic generation of the PRISM model representing activities from a TROPOS goal-model annotated with the runtime regex and graphically modelled using the TAOM4E tool that supports TROPOS methodology.

1.5 Document organization

This dissertation is organized as follows. Chapter 2 presents the base concepts of this work and the most important related works. Chapter **??** details the problem tackled by this proposal. Chapter 4 presents the new extended TROPOS methodology, the rules for the translation between the contextual goal model and the probabilistic verification model, the parser for the runtime regex and finally the implementation approach for the automatic generation of the probabilistic model in PRISM language. Chapter **??** evaluates the proposal and describes its benefits and limitations. Finally, Chapter **??** concludes this work with final considerations about the current proposal, related proposals and our future work.

Capítulo 2

Baseline

2.1 Goal-oriented Requirements Engineering

Goal-oriented requirements engineering brings forward the intentionality behind system requirements. More than just presenting the *what* and the *how* of a system-to-be, it provides the justification for each requirement, that is, they also present the *why*. Through a directed graph tree that begins with a root goal, goals are connected trough decomposition links. Higher level goals are related to strategical concerns, while lower level and specially leaf-goals are related to technical and operational features of the system.

The purpose of a goal model is to structure the process of RE, including the elicitation of social needs and requirements, the actors involved in delivering functionality and resources, the decomposition of higher-level requirements into more granular and detailed requirements, the operationalization through means-end plan/task decomposition and finally the comparison between different alternatives for the system-to-be. A goal model is said to be valid and complete if it follows all its syntactic rules and if all system goals are either decomposed, delegated to other actors or fulfilled by operational system tasks.

Three frameworks/methodologies, namely KAOS, i* and TROPOS, represent the foundations for the goal model analysis used by a variety of other proposals [KAOS, i*, TROPOS]. Despite some differences among their syntax, they all share a set of core concepts:

<u>Entities</u>

- **Actor:** an entity that has goals and can decide autonomously how to achieve them. They represent a physical, social or software agent.

- **Goal:** are actors' strategic interests. A goal with a clear-cut criteria for its satisfaction is called a hard goal. In opposition, softgoals has no clear-cut criteria for deciding whether they are satisfied or not and are usually associated to non-functional requirements of an actor.

- **Task:** an operational means to satisfy actors' goals.

Relations

- **AND/OR Decomposition:** a link that decomposes a goal/task into sub-goals/sub-tasks, meaning that all (at least one) decomposed goal(s)/task(s) must be satisfied/executed in order to satisfy its parent entity.

- **Means-end:** a means to fulfil an actor's goal through the execution of an operational task by the same actor.

- **Contribution link:** a positive or negative contribution between a given goal/task to a softgoal. Contribution links are used for deciding between alternative goals/tasks at design time (contribution analysis).

2.2 Contexts

Context may be defined as the reification of the environment that surrounds the system operation [FINKElSTEIN]. Contexts, as already stated, may not be static, but dynamic. An actor, that may be a system, has no control over its context of operation. Accordingly, an actor must be able to support different contexts of operation without violating its goals. Moreover, actors should be able to monitor the state of its surrounding environment and decide which alternative means will be used to fulfil its goals, as some may only be valid or optimized in specific contexts.

In GORE, dynamic contexts may affect what goals a system have to reach, the means available to meet them and also the quality achieved by each alternative[CGM]. Root goal and higher level strategical goals are not contextualized as they represent the main purpose of a system [Finkelstein]. As these goals are decomposed in more granular sub-goals, a context condition may dictate if the goal is required for that context, limiting 'what' a system should do, or if it is adoptable, limiting the option of 'how' to fulfil a required goal. Finally, a context may also dictate the positive, neutral or negative contribution of using some goal or task to another goal, usually a qualitative softgoal. This last effect is the main focus of this work, as it is related to the GORE contribution analysis that we aim to contribute to.

2.3 Dependability Analysis

The concept of dependability is related to dependence and trust as well as the ability of a system to avoid failures that are more frequent and more severe than certain threshold. According to Avizienis et al., dependability encompasses the following attributes [AVIZIENIS]:

- Availability: readiness for correct service.
- Reliability: continuity of correct service.
- Integrity: absence of improper system alterations.
- Safety: absence of catastrophic consequences on the user(s) and the environment.
- Maintainability: ability to undergo modifications and repairs.

2.4 PRISM Probabilistic Model Checker

The state based, probabilistic model checking technique used in this approach is supported by the PRISM model checker tool [PRISM]. PRISM allows the modelling and analysis of systems which exhibit random or probabilistic behaviour. The decision of using PRISM as the probabilistic state based model checker was due to the number of successful case studies that have used this tool, indicating its maturity [PRISM CS], and also due to its rich environment that is able to represent different kinds of probabilistic models and their evaluations.

PRISM may be used for many different kinds of model evaluations depending on the abstraction level, the type of probabilistic model and the PCTL properties to be analysed. PRISM language offers a rich set of constructs that may represent system modules and components, among others architectural and design configurations.

To evaluate the current proposal with the MPERS case study, we have used the a discrete-time Markov chain (DTMC) probabilistic model and focused on the verification of properties related to dependability, i.e., the reachability of the final success state of a set of goal model activities that represents:

- if the set is composed of the minimum set of activities that satisfies the root goal: its global reliability;
- if the set is composed of the minimum set of activities that satisfies any lower-level goal: its local reliability.

It will be up to the analyst and stakeholders to define which type of probabilistic model and which PCTL properties must be analysed for each different system. Dependability attributes may be relevant for any sort of system, but are certainly important for systems with some criticality degree, i.e., for those whose failure could have severe or catastrophic consequences for users or for the environment.

Capítulo 3

Related Work

3.1 Contextual Goal Model

The Contextual Goal Model (CGM) [CGM] proposed the contextualization of required goals, adoptable means (goals/tasks) and contribution links values. The main benefit of this work is to provide proper syntax to the contextualization of goal model entities and relations affected by context variations and to provide a rationale for context analysis. The main problem tackled by the current work is the verification of system non-functional attributes that requires a more precise and formal approach instead of the existing contribution analysis that is based on analysts direct evaluation of the forward impact between goals/tasks and softgoals. In this regard, the CGM provided more realistic and precise contribution analysis contextualized by environment conditions, but did not extended the basis of the contribution analysis process. Our work also aims to provide a formal verification of non-functional attributes also in a context-dependent fashion, i.e., including the context effects in the probabilistic model used to estimate the value of a given alternative selection of the contextual goal model.

3.2 Runtime Goal Model

Despite the use of goal models to support the monitoring and adaptation functions at runtime, Dalpiaz et al. argued that these works are 'using design artefacts for purposes they are not meant to, i.e., for reasoning about runtime system behaviour'. As such, they proposed a conceptual distinction between the static goal model, named Design Goal Models (DGM), and the Runtime Goal Model (RGM) that extend DGM with 'additional state, behavioural and historical information about the fulfilment of goals'.

Capítulo 4

Proposal

In the PMC technique adopted by this proposal, a behavioural specification, usually provided by UML activity and sequence diagrams, are manually converted to a probabilistic model in PRISM language. As a goal model goes from strategical to operational leaf-goals, and each leaf-goal describes a desired state reachable by either a delegation to other actor or by a operational task, then a behaviour specification as proposed by the RGM may be seen as an activity diagram and be used to generate a probabilistic model in PRISM language. This allows the model checking of the corresponding goal model as a set of activities for which temporal and other behaviour aspects are specified by the runtime regex of the RGM.