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.
69 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
CIC/UnB

Prof. Dr. Luciano Baresi
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 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 methodology to associate dependability constraints to goals and to provide a more precise and formal non-functional requirements (NFR) verification by translating a contextual goal model (CGM) annotated with a behavioural regular expression into a probabilistic model to be checked against properties defined with the Probabilistic Computation Tree Logic (PCTL). We evaluated the proposed TROPOS extension with a case study of a Mobile Personal Emergency Response System (MPERS).

**Palavras-chave:** LaTeX, metodologia científica

# Abstract

**Keywords:** LaTeX, scientific method

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

Among the different causes that lead a system to fail, some can be tracked back to design decisions in early system development process, others are caused by variations in the context of operation. Dynamic contexts increases even further the complexity of the development activities, as different contexts may change what the system should accomplish and the available means to do it. Also, some failures are only activated in specific contexts, posing a new threat to the development of dependable systems.

According to Finkelstein et al. [2], contexts are the reification of the system environment whrereas the environment is whatever over which the system has no control and surrounds its operation - battery status, signals strength, sensors availability, infrastructure restrictions, user characteristics, physical environment conditions, etc. A self-adaptive system should be able to adapt to different context conditions to avoid deviations from its specified behaviour, i.e., to avoid failures.

Contexts might directly affect on systems requirements, particularly the non-functional ones. Dependability is a paramount requirement to be fulfilled on software systems. That property defines the system ability of delivering a service that can justifiably be trusted. Different dependability attributes are used to characterize the correct system behaviour, its ability to undergo modifications and the consequence of failures. In dependability analysis, fault forecasting should provide an evaluation of the system behaviour in respect to fault occurrence or activation, while fault removal includes the verification, diagnosis and correction of faults [3].

A systematic requirements engineering process aims to improve the quality of the delivered systems. However, not many methodologies and frameworks investigate the conformance of the system-to-be to qualitative goals and metrics related to system failures, nor provide adequate means for the monitoring and analysis of these metrics as part of a self-adaptation loop. We argue that, despite the robustness of self-adaptive architectures, a faulty or biased analysis may result in severe or catastrophic system failures.

## 1.1 Problem Definition

In recent works, goal-oriented requirements engineering (GORE) has been adopted for the development of self-adaptive systems. Among others, goal models have been used for deriving a self-adaptive architecture [23] and a high-variability design [25]. Also, goals become live requirements entities that can be self-adapted according to the context [5, 6] or are complemented with a special class of meta-requirements that refers to their success/failures and other metrics that must be satisfied through self-adaptation [22]. Finally, a contextual goal model formalizes the context influence on the autonomous decision of which alternative should be adopted at runtime in accordance to relevant information in the operational environment [1].

Goal models are not restricted to higher-level strategical goals. Through AND/OR-decomposition, goals are further detailed and means-end tasks are responsible for the operationalization of leaf-goals. Thus, tasks may be directly mapped to activities that composes the system behaviour. Dalpiaz et al. [8] proposed a paradigm shift for the goal modelling and analysis. Instead of a static model for design-time analysis, a regular expression for behaviour specification over goals and tasks composes the runtime goal model (RGM). RGM is suitable for verifying the conformance of the execution and fulfilment of monitored tasks and goals instances to their class specification.

Despite the contribution to the runtime conformance verification, detailed measurement of the success and failure rates over temporal frames are not yet supported by the RGM framework. Consequently, it does not provide the means to analyse if the system is able to fulfil the expected level of dependability. Moreover, RGM relies on measurements over the past execution like 'the percentage of success for a given goal over the past month' and 'the trend for failure of a given goal in the last week'. Due to this limitation, the original RGM approach is not appropriate for proactive self-adaptation in which systems should avoid violations by estimating the probability of failures in future executions. Given the importance of implementing dependable systems, RGM needs to be further extended so that the runtime goal satisfaction is properly analysed.

Model checking is a formal verification technique which allows for desired behavioural properties of a given system to be automatically verified on the basis of a suitable model of the system through systematic inspection of all states of the model []. The main advantage of model checking is to provide, given a system model and one or more properties, complex querying capabilities about the correctness of the system model and its conformance in fulfilling both functional and non-functional requirements.

In specific, the probabilistic model checking (PMC) has been largely explored and is supported by tools such as PRISM model checker. As long as the verification model built from a behaviour specification is precise, this method provides a trusted estimation for

metrics as those related to dependability attributes. For instance, PMC can estimate the probability of a system to reach its final success state in a DTMC model based on the reliability of the components involved in the execution, which defines the global reliability of this system or for the analysed activity [4, 20].

Assuming the benefits of a goal-oriented requirements engineering and the behaviour specification provided by a runtime goal model, this proposal investigates the feasibility of a goal-oriented PMC approach for which the leaf-tasks representing high-level system behaviour are mapped to a probabilistic verification model. Them main objective is to provide both qualitative and quantitative analysis for the runtime satisfaction of different system goals. Accordingly, our first research question emerges:

> **Research Question 1 (RQ1):** Given a correct and consistent runtime goal model for which goals are realized by a set of leaf-tasks, is it feasible to analyse the probability of achieving one or more system goals through a probabilistic model checking technique?

As described by the contextual goal model [1], the contextualization of the informations gathered at RE and at design phases becomes imperative once its validity may be threatened by changing environment conditions. Context variation may relativize the need for a goal, restrain the adoptability of alternative means and also affect the quality of available means in fulfilling their goals. Hence, it is desirable that a system verification consider such effects in the analysis results. However, given the vast number of context states that may affect the system requirements and behaviour, scalability becomes the main threat for a contextual dependability analysis. From this, our second research question arises:

> **Research Question 2 (RQ2):** Given the goal-oriented probabilistic verification in RQ1, it feasible to consider the context effects over what goals are required, what alternatives are adoptable and the quality of each alternative?

As discussed earlier, self-adaptation must rely on an adequate analysis that conforms to the complexity and criticality of the metrics being analysed. Reliability is an important dependability attribute and a first class requirement for self-adaptation, as it defines the continuity of a correct service delivery. In goal models, runtime variability solving is based on runtime inputs and non-functional criteria measured or estimated for each alternative [25]. Considering a self-adaptation analysis for solving variability, our third research question is defined as:

**Research Question 3 (RQ3):** Is it feasible and scalable to employ a goal-oriented dependability verification based on parametric PMC as part of a self-adaptation analysis for solving variability at runtime?

Finally, considering the complexity and the analysis overhead caused by the manual generation of a probabilistic verification model from a runtime/contextual goal model as required by our previous research questions, a fourth and final research question arises:

**Research Question 4 (RQ4):** Is it possible to automatically generate the probabilistic verification model for the dependability analysis defined in RQ1-2?

## 1.2 Proposed Solution

To the best of our knowledge, a goal-oriented approach for dependability analysis of system behaviour based on a formal verification method with temporal logic have not yet been proposed. In order to achieve the probability estimation of the fulfilment of different system goals, it is important to realize that the primitive goal models as proposed in [7, 9, 24] are designs artefacts and, as argued by Dalpiaz et al., not tailored for runtime analysis. Nonetheless, the RGM filled this gap by adding a behavioural specification to the static goal model [8].

In contrast to previous approaches for dependability analysis through PMC, this work proposes a verification that is directly mapped to a system runtime goal model. Instead of building the probabilistic verification model from traditional UML behaviour models, we benefit from the RGM syntax that specifies the behaviour for goals and tasks to build a high-level DTMC model for reliability verification of different system goals (RQ1). This model, comparable to a high-level UML activity diagram, should also include the context effects over goals, means and qualitative metrics as defined by the contextual goal model [1] (RQ2).

PRISM tool provides a rich analysis environment for PMC. However, a runtime self-adaptation analysis must be automatic, i.e., based on computable processes without human intervention. The parametric PMC fulfils this requirement by generating a parametric formula for a given probabilistic model and property to be analysed with parameters in the place of constant variables[PMC REF]. Thus, different runtime analysis may be performed by just initializing the parameters with values corresponding, e.g., to a specific context of operation, and evaluating the resulting formula. In our proposal, we investigate the feasibility of a parametric PMC as the formal method for the goal-oriented reliability analysis in self-adaptive systems (RQ3).

Finally, to reduce the analysis overhead and to improve the scalability and the feasibility of our goal-oriented reliability analysis, a JAVA implementation was integrated to a tool that supports TROPOS goal modelling and analysis, namely TAOM4E. This extension provides automatic generation of a DTMC model in PRISM language from a RGM with or without additional context effect notations (RQ4).

## 1.3 Evaluation

The proposal has been evaluated with the application of the goal-oriented reliability analysis for self-adaptive systems to the development of a Mobile Personal Emergency Response System (MPERS). This system fits in the context of ambient assisted living systems [18**?** ] where a ubiquitous emergency response system runs on a mobile device **??**. Instead of a static environment, the MPERS is conceived to allow patients with different health risk degrees to preserve their mobility while they are monitored and assisted. As a mobile system, MPERS is affected by context variations and self-adaptation becomes a mandatory feature to avoid failures, as safety is of paramount importance for this system.

The MPERS features were based on real emergency response systems available at the industry and also at the BAN explored in previews works [20]. In this evaluation, we focus on the development process of the MPERS and demonstrate the feasibility of the goal-oriented approach for the dependability analysis with a probabilistic model checking technique. In specific, our main goal is to provide reliability analysis capability for the MPERS system with a verification model mapped to the contextual/runtime goal model of the system-to-be, empowering the system with a precise method for reliability verification aimed for runtime self-adaptation.

## 1.4 Contributions Summary

This section summarizes the contributions of this proposal.

1. A goal-oriented approach for explicit account for contexts in dependability modeling and analysis.
    - Probabilistic model checking of runtime goal models;
    - Inclusion of the context effects over goals and tasks in the verification model as defined by the contextual notations in the runtime goal model.
    - Probabilistic and temporal querying capabilities for different metrics related to the reliability of one or more goals in the system goal model.

2. An automated generation of the DTMC model in PRISM language from a contextual/runtime goal model.

    - A parser implementation for the regular expression (regex) language used in runtime goal models with support for execution order, cardinality, alternative execution, optional execution, conditional execution and multiple parallel or sequential executions of the same task.

    - Definition of conversion rules between different decomposition types and behaviours rules in the contextual/runtime goal model to a DTMC model in PRISM language.

    - JAVA implementation of DTMC generator integrated to the TAOM4E tool that supports the TROPOS methodology using the Eclipse plugin architecture.

## 1.5 Document Organization

This dissertation is organized as follows. Chapter 2 presents the base concepts of this work. Chapter 3 describes the most important related works. Chapter 4 details the motivation for this work and the requirements for the proposed goal-oriented reliability analysis. Chapter 5 describes and evaluates the proposal with the MPERS cases study. Chapter 6 presents the rules for the automatic generation of a DTMC model in PRISM language from the runtime goal model with additional context effects notations. Chapter 7 validates the proposal with some relevant metrics. Finally, Chapter 8 concludes this work with final considerations about the current proposal and our future work.

# Chapter 2

# Background

## 2.1 Goal-oriented Requirements Engineering

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

The main purpose of a goal model is to support the early process of RE, including the elicitation of social needs and dependencies, the actors involved in delivering functionalities and resources, the decomposition of higher-level goals into more granular and detailed requirements chunks, the operationalization through means-end tasks 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.

Frameworks and methodologies like the i* [24], KAOS [9] and TROPOS [7] represent the foundations for the goal model analysis used by a variety of other proposals. Despite some syntax differences, most goal-oriented approaches share a set of common and core important concepts:

### 2.1.1 Intentional Entities

- **Actor:** an entity that has goals and can decide autonomously how to achieve them. They represent a physical, social or software agent. For example: a patient, an emergency center, a doctor and a Mobile Personal Emergency System running in patient's smartphone.

- **Goal:** actors' strategic interest. A goal with a clear-cut criteria for its satisfaction is called a hard goal. In opposition, softgoals have no clear-cut criteria for deciding whether they are satisfied or not and usually represent non-functional requirements. For example: vital signs are monitored, emergency is detected, emergency center is notified (hard goals) and emergency awareness, precise assistance, feel supported (softgoals).

- **Task:** an operational means to satisfy actors' goals. For example: monitor temperature sensor, persist vital signs data, request emergency assistance.

- **Resource:** an information data or a physical resource that is generated or required by an actor. For example: a form input from the user, an exported file, the power from the battery component, etc.

### 2.1.2 Relations

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

- **Means-end:** a relation that indicates 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).

- **Dependency link:** a delegation of a goal, task or resource (*dependum*) from an actor (depender) to another (dependee).

## 2.2 TROPOS Methodology

TROPOS is a GORE methodology based on the i* framework [7]. Its main improvement to the i* framework is the addition of new phases of requirements engineering, architecture and system design, namely:

- Late requirements engineering: Beyond the social dependency modelling with actors diagrams representing stakeholders and their needs in early requirements phase, a

late requirements phase focuses on the system actor analysis. In this phase, system goals are inherited from stakeholders needs and represent both functional and non-functional requirements. Each goal has to be further decomposed in more granular sub-goals, delegated to other actors or to be fulfilled by means-end tasks.

- Architectural design: In this phase, new actors representing sub-systems are created to fulfil different system goals. The idea is to shape the solution using a multi-agent architecture style instead of a monolithic system approach. Data and control interconnections are represented as dependencies.

- Detailed design: The last phase is characterized by the specification of agent capabilities and interactions though UML activity and sequence diagrams. Also, the implementation platform and other specific implementation details are addressed in order to directly map the design to system code.

## 2.3 Goals, Means and Contexts

Context may be defined as the reification of the environment that surrounds the system operation [2]. Contexts, as already stated, may not be static, but dynamic, and a system has no control over the context variation. Accordingly, a system must be able to support different contexts of operation without violating its functional and non-functional goals. To achieve this, systems must be able to monitor the state of their surrounding environment and take adaptive actions regarding the alternatives used for fulfilling their goals.

In a contextual goal model (CGM), 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 [1]. Root goals and higher-level strategical goals are generally not contextualized as they represent the main purpose of a system [2]. As these goals are decomposed in more granular sub-goals, a context condition may affect:

1. If one or more goals are required for that context, limiting *what* a system should do. For instance, the goal 'track person's location' is only required in the context 'patient is not at home'.

2. If a sub-goal or task is adoptable, limiting the 'means' to fulfil a required goal. For instance, 'track by GPS' may not be used in the context 'battery is low' (stakeholder preference) or 'no GPS signal' (technical impediment).

3. The positive, neutral or negative contribution of one alternative to a qualitative softgoal or to a non-functional metric. For instance, the precision of each geolocation method - voice call, mobile triangulation and GPS variate according to contexts like the health condition of the person and the strength of mobile and GPS signals.

Context effects may have different causes, among them:

- **Stakeholders preferences:** At a certain context, a stakeholder need (dependency) that justifies a system goal may cease to exist (goal restriction); or it may prefer a given alternative to another (means restriction).

- **Technical impediments:** At a certain context, a required information or physical resource may not be available, imposing a restriction on the selection of one or more alternatives (means restriction).

## 2.4 Variability in GORE

Given the possibility of an OR-decomposition in a goal model, more than one alternative can exist in terms of which subgoal should be achieved to satisfy its upper goal, which subtask should be executed to satisfy its upper task or which task should be executed to satisfy its upper goal. Accordingly, multiple paths may lead to the satisfaction of the root goal. They are called alternative behaviours, or alternatives. Solving the variability problem in goal models has different meanings according to the development phase it takes place.

### 2.4.1 Design-time analysis

At design time, multiple alternatives are elicited through goal-oriented analysis, but not all are selected to be part of the system-to-be. In traditional GORE, contribution analysis is used for the comparison of how each alternative contributes for one or more softgoals. Usually, only one alternative with the more positive contribution sum is selected for the system-to-be. Or, as in the simplistic example of Figure 2.1, the decision relies on the softgoals priorities [12].

### 2.4.2 Runtime analysis

In contrast to the design-time variability in goal models, runtime variability depends on runtime input and must be preserved at runtime, i.e., variability is inherited by the

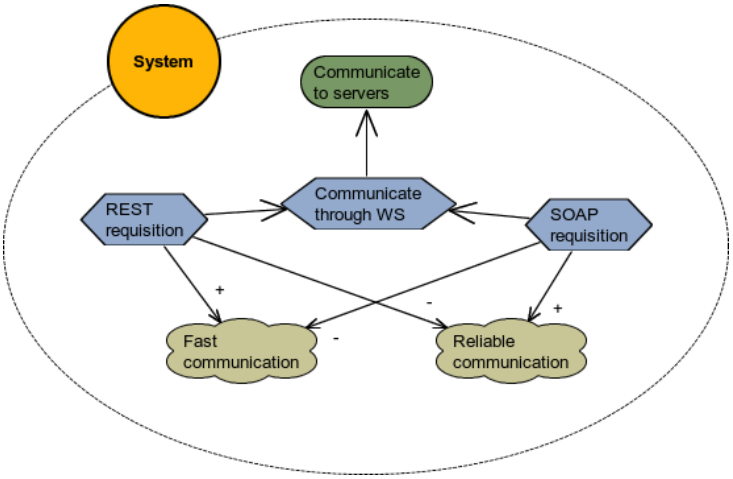



Figure 2.1: Contribution analysis in TROPOS GORE.

solution design [25]. A runtime analysis should select the valid alternative according to stakeholders preferences and the current context of operation.

The contextual goal model tackles the influence of the context on the autonomous decision of which alternative should be selected [1]. For instance, if the monitored traffic condition is 'jammed' and the patient's condition is 'critical', an emergency chopper is selected for assistance in the place of an ambulance. We call this 'direct context implication'.

In other cases, alternatives should be monitored and analysed in terms of non-functional metrics to decide which one is suitable or for selection. Here, the context of operation does not directly defines the adoptable alternative, but its effect on the quality of each alternative is considered as a decision criteria. For instance, a more complex analysis must estimate the probability of the ambulance to reach the patient in less than X time units given a traffic condition. We call this 'indirect context implication'.

In Figure 2.2, the availability of the emergency resources are contexts that directly restricts the adoption of corresponding means to reach a patient. In contrast, the traffic condition affects the time to reach the patient, i.e., this context indirectly affects the selection of an ambulance and requires further analysis to estimate the assistance time in different traffic conditions. Also, the context 'patient health' affects the time restriction in the 'fast assistance' quality goal. This scenario leads to the following question: Among the available functional alternatives, which also fulfils the quality goal in the current context?

## 2.5 Dependability

The concept of dependability is related to dependence and trust as well as to the ability of a system to avoid failures that are more frequent and more severe than certain

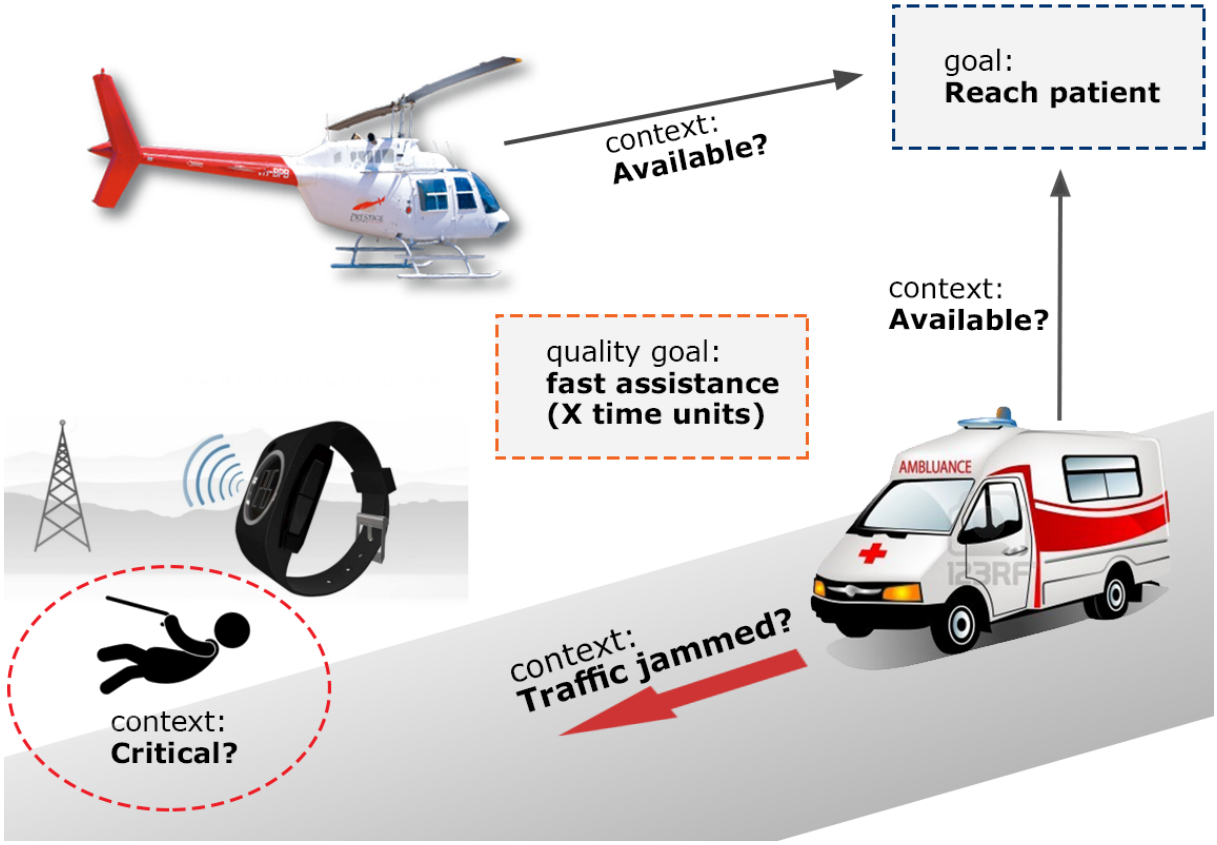



Figure 2.2: Contribution analysis in TROPOS GORE.

threshold [3]. According to Avizienis et al., dependability encompasses the following attributes:

- 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.

A failure is a perceived deviation from system expected behaviour that may have variable degrees of consequence on the user(s) and the environment. These failures are caused by specification faults or specification violations. In the first case, requirements and behaviour models fails to describe the system: either the goals or the means to fulfil then are incorrect, inappropriate or incomplete. In the second case, software or hardware

behaviour did not follow its specification due to a natural phenomena, a human-made fault, a malicious fault or an interaction fault [3].

Avezienis et al. distinguishes faults from errors and failures in a fault causality chain. In their definition, errors are part of the system's total state that may lead to failures. Failures are characterized by deviations in the external service state, i.e., by external errors. In turn, errors are caused by faults, resulting in the following chain:

$$fault \rightarrow error \rightarrow failure$$

In most cases, a fault first causes an error in an internal state of a system. Not all internal deviations results in external deviations, i.e., not all internal errors result in failures. External faults may also result in internal errors and possibly subsequent service failure(s), but only if a prior vulnerability exists, i.e., a previous internal fault enabling the external fault to harm the system.

Failures can be characterized by different viewpoints. In this work, one important aspect is the failure consequence level, as it describes the consequence of failures to user(s) and to the environment. Two limiting levels are defined by Avezienis et al.:

- **Minor consequence:** where the harm caused by a failure is not higher than the benefit of the correct system behaviour. For instance, a momentary interruption in a video streaming service.

- **Major consequence:** where the failure harm is incommensurable higher than the benefit of the correct service. For example, the death of a user.

Other intermediary levels may exist according to each case. In a goal model, the consequence level viewpoint may characterize the failure in achieving one or more system goals. For instance, a failure in fulfilling a goal with higher relevance in the goal tree of a critical system would have a catastrophic consequence. There are many means to attain systems dependability. Avezienis et al. groups them in four major categories:

- **Fault prevention:** means to prevent the occurrence or introduction of faults.

- **Fault tolerance:** means to avoid service failures as a consequence of faults.

- **Fault removal:** means to reduce the number and severity of faults.

- **Fault forecasting:** means to estimate the present number, the future incidence, and the likely consequence of faults.

The scope of this work is restricted to specification violations, i.e., we assume that a system specification is complete and consistent. Failures are caused by anomalous behaviour of the components participating in the execution of system tasks, including technical components and human actors. Regarding the different means to attain dependability, our goal-oriented dependability analysis is classified as a fault forecasting, as it aims to estimate the probability of different system goals in being fulfilled.

## 2.6 Probabilistic Model Checking

Many systems are susceptible to various phenomena of stochastic nature and to non determinism in their behaviour. For example, failures may be caused by unpredictable events and by unreliable components. In contrast to model checking techniques for which the absolute correctness of a system is verified, a probabilistic model checking aims to verify properties over transitions systems enriched with probabilities [4]. Accordingly, PMC allows quantitative statements to be made about the system's behaviour, expressed as probabilities or expectations, in addition to the qualitative statements made by conventional model checking [14].

Among the most popular types of transition systems employed in PMC are those based on Markov chains, e.g., the discrete-time Markov chain (DTMC) and the Markov decision process (MDP) [14]. Also, probabilistic operators extends the conventional time-bounded or unbounded temporal logics for property specification. Regarding dependability, the PMC technique enables the forecasting of system performance and dependability based on probabilistic events and behaviour described in probabilistic models. As a model checking technique, PMC requires:

1. a description of the system to be analysed, typically given in some high-level modelling language, e.g., in PRISM language.

2. a formal specification of quantitative properties of the system that are to be analysed, usually expressed in variants of temporal logic, e.g., in PCTL.

In PMC, the system description is converted to a probabilistic model. In addition to the quantitative information regarding the probability and/or timing of the transition's occurrence, Markov chains can also be augmented with *rewards* used to specify additional quantitative measures of interest [13]. In future works, the reward structure could be useful for extending our goal-oriented dependability analysis with the verification of restricted resources consumption like the battery energy.

### 2.6.1 PRISM tool

The PMC technique used in this approach is supported by the PRISM probabilistic model checker tool [17]. The decision of using PRISM as the probabilistic state-based model checker was due to the richness of its environment and to the number of successful case studies that have used this tool, indicating its maturity [15].

PRISM is suitable for different kinds of model evaluations depending on the abstraction level, the type of probabilistic model and the PCTL properties to be analysed. Both qualitative and quantitative analysis are available features in the simulation/verification environment. Other environments for modelling and property specification are also available in the tool.

### 2.6.2 PRISM language

PRISM language [16] offers a rich set of constructs that may represent system modules, components and others architectural and design abstractions. Modules are the main structure in a PRISM model. They are composed of variables and commands. The first describes the finite states a module can be in. The later describes the behaviour of a module, i.e., the actions that may result in state transitions and are guarded by predicates which in turn can be composed of any variable in the model. Finally, labels are used for command naming and synchronization. A DTMC command in PRISM takes the following form:

$$[action] < guard > \rightarrow < probability > : < update >;$$

### 2.6.3 Probabilistic Computation Tree Logic

PCTL is a temporal logic based on the Computation Tree Logic (CTL). Its main difference from CTL is the probabilistic operator $P_J(\varphi)$, where $\varphi$ is a path formula and $J$ an interval in [0,1] indicating a lower and/or upper bound on the probability. $P_J(\varphi)$ may be read as the probability of a set of paths satisfying $\varphi$ and starting at state $s$ to meet the bounds given by $J$ [4].

The specification of domain-specific dependability properties with PCTL has been explored in previous works [13, 14, 20]. For example, the reachability property expressed by formula $P =?\ [\ F\ (\varphi)\ ]$ computes the probability that a system will eventually reach a state that satisfies $\varphi$. Accordingly, the satisfaction of this formula guarantees that a final successful system state will be reached regardless of the time elapsed to reach it. A time-bounded variant would express a similar event in a restricted number of transitions or time units.

In our proposal, PCTL formulas may be specified to verify different properties of a runtime goal model mapped to a DTMC verification model. In specific, our goal-oriented dependability analysis focus in the time-unbounded reachability of the states representing the fulfilment of one or more system goals.

### 2.6.4 PARAM

The powerful analysis environment offered by PRISM tool is limited by the verification of a single combination of initialized variables at a time. For instance, if a variable represents the probability of a transition in the model, PRISM requires the initialization of this value to produce a fixed output for a given specified property. At most, PRISM allows the creation of experiments with undefined variables ranging from two limits at a fixed step value.

A parametric model checking provides a more flexible analysis, as constant variables in the model can be replaced by parameters [11]. Regarding the PMC, the PARAM tool extends the PRISM language with the additional reserved word *param* to be used with variables describing state transition probabilities. Given a probabilistic model with additional param variables and a PCTL property, a corresponding parametric formula is generated.

The main benefit of the parametric formula generated by PARAM is to enable the verification of multiple combinations of values for each parameter in an efficient manner, as the probabilistic model checking problem has been previously solved by the tool. Also, different sorts of postprocessing operations can be performed by computer algebra packages, e.g., to find the optimal parameter settings and to evaluate the parametric formula for a given setting [11].

In our proposal, a parametric formula generated offline could be evaluated at runtime analysis and integrate a self-adaptation loop. The formula scalability is a relevant concern, as previous works have demonstrated its exponential relation with the number of parameters in the model [**?** ]. Nonetheless, depending on the modelling approach and the scope of the verification, parametric model checking can be proven an efficient approach for dependability analysis. The scalability of our goal-oriented dependability analysis based on probabilistic PMC is addressed by our fourth research question.

More recent PRISM versions also supports a parametric model checking. Nonetheless, PARAM has been successfully evaluated in more case studies in which it has been proved a reliable and stable tool, justifying its adoption by this work in detriment of the built-in PRISM parametric analysis.

## 2.7 Antlr Language Recognition Tool

ANTLR (Another Tool for Language Recognition) is a open source parser generator for reading, processing, executing or translating structured text or binary files [21]. The main purpose is to automatically generate a parser for a custom language defined in a specific grammar supported by the tool. The parser can then be imported by any JAVA compatible project to build and walk parsed trees from an input stream.

As a result, domain-specific languages may parsed using JAVA methods that will manipulate primitive attributes and objects according to what each parser rule and lexical term means for that language. In our proposal, ANTLR was successfully used to generate the parser for the regular expression language that specifies the behaviour in a runtime goal model and for the context effect notations as proposed by the contextual goal model. Listing 2.1 presents the grammar used in the RGM parser. Further details for both parser rules and lexical terms is given in later section.

Listing 2.1: ANTLR grammar for the RGM behaviour regex

```
grammar RTRegex;
rt:     expr NEWLINE                                # printExpr
  |     NEWLINE                                     # blank
  ;

expr:   expr op='+' expr                            # gCard
    |   expr op='|' expr                            # gAlt
    |   'opt(' expr ')'                             # gOpt
    |   'try(' expr ')' '?' expr ':' expr           # gTry
    |   expr op=(';'|'#') expr                      # gTime
    |   SKIP                                        # gSkip
    |   GID                                         # gId
    |   FLOAT                                       # n
    |   '(' expr ')'                                # parens
    ;

GID             : [GT] FLOAT            ;
FLOAT           : DIGIT+'.'?DIGIT*      ;
SEQ             : ';'                   ;
PAR             : '#'                   ;
ALT             : '|'                   ;
SKIP            : 'skip'                ;
NEWLINE : [\r\n]+                       ;
```

```
24 WS                : [\t]+ -> skip          ;
25
26 fragment
27 DIGIT             : [0-9]                  ;
```

# Chapter 3

# Related Work

## 3.1 Contextual Goal Model

The Contextual Goal Model (CGM) [1] proposes the contextualization of the intentional elements and relations in a goal model. From the activation of a root goal to the adoptability of tasks, CGM define different context implication that may affect the problem tackled by a system, the validity and the quality of possible solutions. CGM uses a graphical notation to associate context to their affected elements. In specific, context can be associated to root goals (activation), OR-decompositions (adoptability), means-end (adoptability), dependencies (activation), AND-decomposition (activation), contribution to softgoals (quality).

The main benefits of the CGM are twofold. First, CGM enriches the the conventional goal model with the notation for the contextualization of intentional elements and relations. Second, it provides the modelling constructs to analyse and discover relevant information the system needs to capture in order to verify if a context applies, i.e., the rationale for context monitoring. This last contribution is useful for runtime monitoring and analysis of a self-adaptive system reflecting stakeholder's rationale and the environment in which the system operates [1].

CGM provides a more realistic and precise contribution analysis contextualized by environment conditions, but does not change the nature of the GORE contribution analysis. In contrast to CGM, our work empathizes the formal verification of non-functional requirements in place of the more subjective contribution analysis based on the direct evaluation of the forward impact between alternatives and softgoals. However, our work has benefited from the CGM conceptual model and, to answer our RQ3, we evaluate the feasibility of a goal-oriented dependability analysis that preserves the context effects from a CGM over the requirements to meet and the adoptable means in the corresponding probabilistic verification model.

## 3.2 Runtime Goal Model

Despite the use of goal models in the support of runtime monitoring and adaptation in many works, Dalpiaz et al. argued that these proposals 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' [8].

The main purpose of the RGM approach is to provide a behaviour specification for the fulfilment of goals and the execution of tasks. RGM defines a class model, while the Instance Goal Model (IGM) captures instance states of monitored goals and tasks that must conform to their class model, the RGM. If an IGM violates its RGM, then a corrective action is expected to take place.

The IGM representation is built from algorithms that parses the execution traces of the instrumented implementation of a running system. The contribution, however, is restricted to the runtime regex and to the IGM algorithms. Other research questions concerning the percentage of success/failures for a given goal with or without temporal frames is not yet addressed by the framework [8].

Our proposed goal-oriented dependability analysis has benefited from the RGM as the PMC technique requires a system behaviour specification and the RGM provides a high-level description of a system behaviour. In our work, RGM leaf-tasks are mapped to a probabilistic verification model in PRISM language preserving its behaviour semantics. Our proposal aims to answer qualitative and quantitative questions about the time-unbounded success/failure probability in fulfilling different system goals. Time-bounded verification should be explored in future works.

Table 3.1 provides a textual description of each RGM rule and the corresponding meaning in terms of what behaviour it specifies and also an example from the MPERS runtime goal model of Figure 5.3. A formal and detailed description can be found in the RGM reference publication [8].

## 3.3 Dependability Contextual Goal Model

This work has been preceded by another proposal concerning goal-oriented requirements engineering, dependability analysis and dynamic contexts, namely the Dependability Contextual Goal Model (DCGM) [19]. The contribution was focused on the context effect over both dependability requirements and dependability attributes based on declarative fuzzy logic rules.

| Expression | Meaning | Example (MPERS) |
|---|---|---|
| E1;E2 | A goal/task E1 must be fulfilled/executed before E2. | $G1$;$G2$;$G3$;$G4$ |
| E1#E2 | Interleaved fulfillment/execution of goal/task E1 and E2. | $(G1; G2; G3; G4)\#G5$ |
| E+n | Goal/task E must be fulfilled/executed $n$ times, with $n > 0$. | $G22 + 2$ |
| E#n | Interleaved fulfillment/execution of $n$ instances of E, with $n > 0$. | - |
| E1\|E2 | Fulfillment/execution of goal/task E1 is alternative with respect to E2. | $T23.0 \| T23.1$ |
| opt(E) | Fulfillment/execution of goal/task E is not mandatory. | $opt(T17.2)$ |
| try(E)?E1:E2 | If goal/task E succeeds, E1 must be fulfilled/executed; otherwise, E2. | $try(T9.0)?skip : T9.1$ |
| skip | No action. Useful for conditional ternary expressions involving two elements. | $try(T9.0)?skip : T9.1$ |

Table 3.1: Description of RGM behaviour rules used by the proposal.

In DCGM, a failure classification scheme was used to classify the consequence level and domain of failures in achieving system goals. This process lead to the definition of dependability constraints that must be achieved by the means-end tasks used to fulfil leaf-goals in specific contexts of operation, i.e., to the specification of contextual dependability requirements (CDR). These requirements inherited the same form of the AwReq [22], but instead of being static, CDRs are associated to context conditions. Another DCGM characteristic is the contextual failure implication (CFI), which consisted of a dependability domain-specific contribution analysis supported by fuzzy logic to define IF-THEN rules between context conditions and the corresponding level of a dependability attribute of a given alternative, e.g., the reliability of a task in a context condition.

The main drawback of this proposal was the lack of scalability, as declarative rules must be provided for different goals, attributes and contexts, proving to be a time-consuming manual analysis task. A second problem was the subjectivity of the rules, as they were based in domain knowledge that was also used to shape membership functions. This problem, as much as in GORE contribution analysis, lead to the idea of coupling a more precise and reliable verification approach such as the PMC technique to a runtime goal

model. Still, the idea of a failure classification and the specification of dependability requirements as non-functional constraints were kept in the current work.

## 3.4 Awareness Requirements

Souza et al. [22] proposed the Awareness Requirements (AwReq) as a meta-requirements class in a goal model, i.e., AwReqs specify, among others, the success/failure rate for other requirements in the model, including goals, tasks, domain assumptions and even other AwReqs (*-meta-requirement). The objective is to enrich the original goal model with constraints for the system performance and to provide criteria for self-adaptation, as runtime AwReq violations should be addressed by corrective actions. AwReq are formalized by a temporal logic formula, namely the Object Constraints Logic with Temporal Message (OCLtm).

Despite its contribution to the specification of meta-requirements in goal models, AwReq do not provide an approach to analyse and validate its meta-requirements before system implementation or through system monitoring. Original GORE contribution analysis could be used to define the impact of a given alternative to some attribute or value composing one or more AwReqs, similarly to the DCGM [19]. In contrast, our approach tackles the verification of domain-specific dependability meta-requirements through probabilistic model checking technique that can be performed at design-time to support alternative design decision or at runtime as part of a self-adaptation loop analysis.

## 3.5 Formal TROPOS

The idea behind the formalization of a goal model, as proposed by Formal TROPOS (FTROPOS) [10], is to provide a formal specification of sufficient and necessary conditions to create and achieve intentional elements like goals, tasks and dependencies in the a goal model and also invariants for each of these elements. In addition to this, new *prior-to* links describe the temporal order of intentional elements. Also, cardinality constraints may be added to any link in the model. Finally, FTROPOS uses a first-order linear-time temporal logic as a specification language.

The nature of the verification proposed by FTROPOS is different from the PMC used by our work. FTROPOS aims to provide the information required for a consistency verification of the goal model. The verification is performed not only on the conventional goal model syntax of intentional elements and relations, but also to domain specific information about how each element is created and fulfilled in time. Once the model starts to have more elements and relations, its consistency checking becomes non-trivial, justifying

the use of a formal specification that can be automatically verified by a model checker tool.

In contrast to FTROPOS, our proposal uses a probabilistic model checking technique for the verification of properties that depend on how activities in the model are organized in terms of time, cardinality, combination, non-determinism and the success probability of individual system tasks. While the FTROPOS maps its specification into a language treated by a symbolic model checker, our work maps a RGM specification into a probabilistic model treated by the PRISM probabilistic model checker. Despite the similarity in the behaviour specification, FTROPOS focuses on consistency verification and not on the quantitative analysis of the system performance and dependability.

## 3.6 Reliability Analysis of Software Product Lines

# Chapter 4

# Modelling the Problem

## 4.1 Motivation

Goal-oriented requirements engineering (GORE) has gained the attention of both academic and industrial practitioners due to its ability to systematically model the intentionality behind system requirements. More than just presenting the 'what' and the 'how', goal models also express the 'why' of different requirements to exist. Its simple graphical notation allows non-technical stakeholders to take part in the analysis process and have a clear view of the system-to-be. Finally, automated model verification should avoid violations of the requirements specification.

TROPOS is a GORE methodology that also includes architectural and detailed design phases for the development of socio-technical, multi-agent systems. Socio-technical systems provide and control a wide range of daily used services. Often, these systems are responsible for important and even critical requirements whose failures would cause undesirable or intolerable consequences. This requires developers to take dependability into consideration as a first class requirement.

In TROPOS, as in other GORE frameworks, there is no coupling to any specific verification approach for dependability attributes and other non-functional requirements. Contribution analysis is used for the comparison and selection of alternative design solutions based on how each alternative contribute to one or more system goals, usually qualitative softgoals. This approach, however, is not tailored for measures depending on system behaviour or more complex analysis techniques.

In a previous work and following, we have extended the contextual goal model to tackled the context variation effects on dependability attributes based on declarative fuzzy logic rules [19]. From our experience, we have considered that a more scalable and precise approach for the verification of dependability metrics in dynamic contexts

was needed. Probabilistic model checking emerged as a potential option to cope a goal-oriented methodology with a formal method for dependability analysis.

To the best of our knowledge, formal methods have not yet being used for a goal-oriented dependability analysis. As a fault forecasting approach, the purpose would be to characterize the dependability and the security of a system and to compare concurring alternative solutions - in this case, goal model alternatives - according to one or more attributes. In specific, the reliability attribute should be the focus of this proposal and the resulting verification model should estimate and verify reliability related metrics as a design-time, manual analysis and specially as part of a runtime automated analysis as part of a self-adaptation loop. Finally, the context effects over goals, means and metrics as described by the CGM should be considered in the analysis.

## 4.2 Requirements for the Goal-oriented and Contextual Dependability Analysis

Based on the identified gap of a probabilistic verification of non-functional requirements in GORE methodologies, we defined the following requirements that must be addressed by our proposal:

R.1 **Backward compatibility:** Extended TROPOS runtime regex and contextual notation added to the goal model must not conflict to the existing syntax and semantic of the original TROPOS methodology.

R.2 **Verification scope:** The verification scope may be restricted to a part of the system (local goals) or encompass the whole system (root goal), according to analysts decision.

R.3 **Model generation:** The probabilistic model representing the activities of runtime goal models should be automatically generated from a runtime goal model created in TROPOS late requirements engineering phase.

R.4 **Tool integration:** The TAOM4E tool/plugin used for TROPOS modelling and analysis activities should be extended with the runtime regex, context notations and verification model generation.

R.5 **Static syntax support:** The verification model should be coherent to the AND/OR decomposition of goals/tasks and to the goal-task means-end relation of the original/static goal model syntax.

R.6 **Dynamic syntax support:** The verification model should be coherent to the goal/-tasks achievement/execution order, to cardinality and to alternative, optional and conditional achievement/execution syntaxes in a runtime goal model.

R.7 **Contextual syntax support:** The verification model should be coherent to the context effects over the activation of goals, the adoptability of sub-goals/tasks and over the individual quality metric of leaf-tasks selected for analysis.

# Chapter 5

# Goal-oriented PMC for Reliability Analysis of Self-adaptive Systems

This chapter presents our proposal for goal-oriented dependability analysis applied to the MPERS case study. Both TROPOS early and late requirements analysis phases are presented, as well as the goal-oriented probabilistic verification that requires a goal model with additional runtime regex for behaviour specification (RGM) and the context notations specifying context effects (CGM).

Figure 5.1 illustrates the goal-oriented reliability analysis process that starts with conventional goal-oriented modelling and analysis phases of the TROPOS methodology and finishes with the generation of a high-level DTMC model used for reliability analysis.

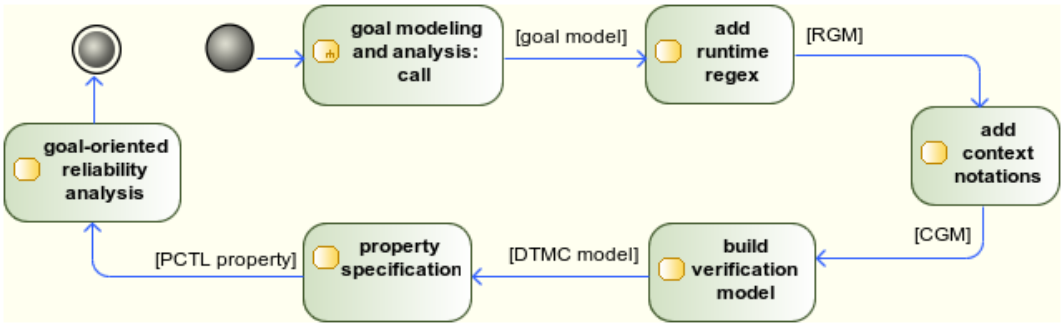



Figure 5.1: Goal-oriented dependability analysis activities.

The next sections are structured as follows. First, a goal modelling and analysis as described by TROPOS methodology is performed [7]. Next, the RGM behaviour rules are further explained and added to the MPERS goal model. Then, context notation is added to the RGM. After this, the high-level DTMC model for MPERS is built and details about the mapping of a RGM into a DTMC in PRISM language are provided, as well as the inclusion of the CGM context effects. Next, PCTL properties representing the

reliability of fulfilling different system goals are defined. Finally, we demonstrate how our verification approach may be employed in reliability analysis.

## 5.1 Mobile Personal Emergency Response System

The MPERS case study will be further detailed in later sections as the proposed goal-oriented reliability analysis based on PMC is described using the MPERS goal models created at the requirements engineering phases of TROPOS methodology. As such, this section will be limited to cover some relevant aspects of this system that justify the use of our formal verification approach to analyse its reliability.

An emergency response system is a mission-critical system for which failures in achieving its main goals by the time they are required may lead to catastrophic consequences on users, i.e., on individuals monitored by the system expecting to be promptly assisted in case of a medical emergency. Accordingly, any stakeholder that wishes to offer a service based on this system will have both ethical and contractual obligations regarding the safety of its product, that is, it must employ all means to prevent system failures and to attain dependability.

MPERS is expected to have a high availability - as it must be ready to respond to an emergency that may happen at any time - and a high reliability - as an incorrect emergency response may lead to death or to costly false-positives. Integrity is a less critical attribute in this case, but it must also be addressed as user's privacy may not be violated by disclosing his personal health or geolocation information to unauthorized persons. Maintainability is addressed, among others, by the use of a software development methodology and by the ability to update emergency rules remotely at runtime.

Environment changes is an important factor for MPERS, as the following conditions may change:

- The battery of the mobile device;
- The battery of the vital signs sensors;
- The disc memory used for storing the vital signs history;
- The mobile signal used for data communication and for geolocation triangulation;
- The GPS signal used for geolocation;
- The health risk of the patient;

## 5.2 Goal Modelling and Analysis

The goal modelling and analysis of both early and late requirements phases in TROPOS methodology are applied to our MPERS case study. Next subsections briefly describe these two phases and present the resulting models.

### 5.2.1 TROPOS Early Requirements Phase

In early requirements phase, stakeholders and their needs are modelled in a goal model diagram. Each actor may be a depender or a dependee of a goal, task or resource dependency. In this phase, only social dependencies to the system actor and between application domain stakeholders are analysed, leaving the detailed system analysis to later development phases.

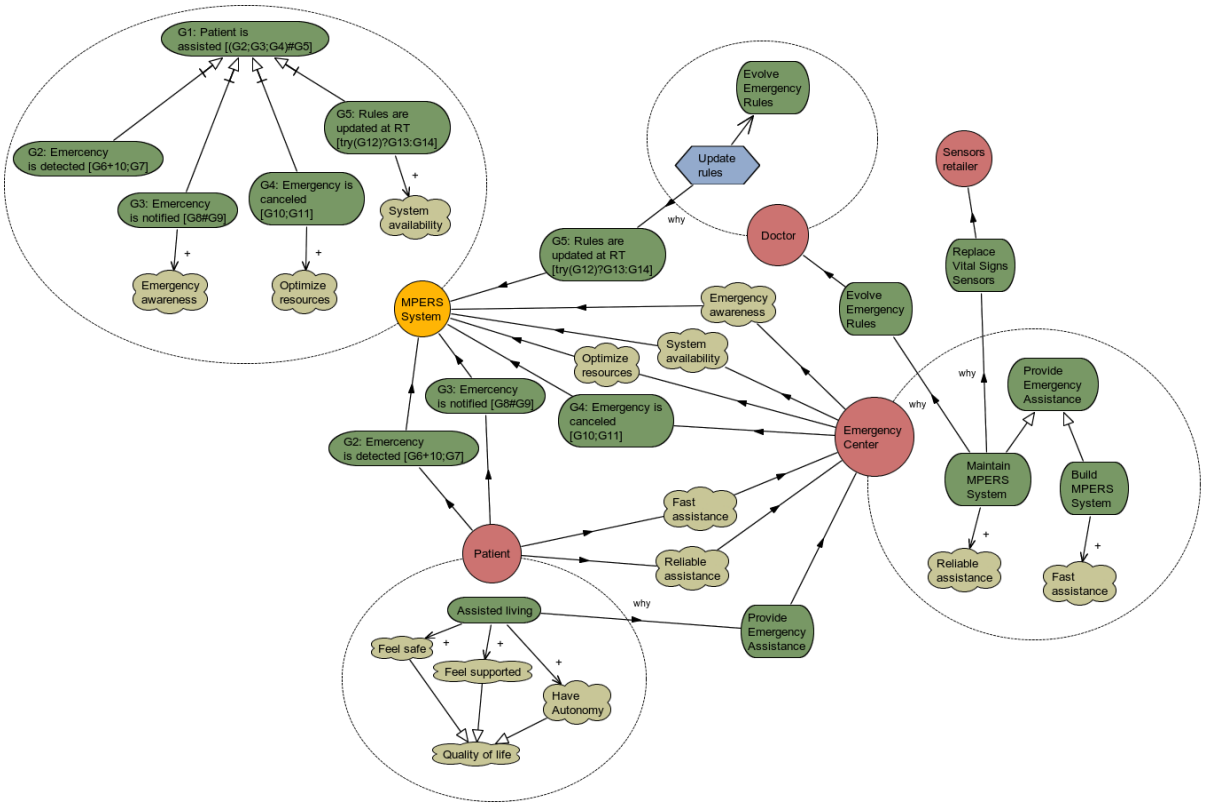



Figure 5.2: MPERS at TROPOS early requirements phase

The MPERS sytem and its social dependencies are presented by the actor model in Figure 5.2. System actors and social actors are displayed in different colors. Among the stakeholders, the emergency center represents a private or public organization interested in providing an emergency response service to patients. Patient and doctor represent, respectively, the assisted person and the medical responsible for defining and evolving the

emergency detection rules as part of an evolutionary approach for personal emergency response. Finally, sensors retailer should provide the vital signs sensors required for monitoring.

From the diagram in Figure 5.2 it is possible to have a first look of the MPERS system-to-be. Main goals are divided in detecting, notifying and checking an emergency. Also, the ability to update the emergency rules at runtime (RT) is the fourth and last mandatory goal (AND-decomposition) that fulfils the 'Patient is assisted' root goal. System goals and softgoals are directly or indirectly related to stakeholders needs.

The distinguished yellow circle indicates that MPERS is a system actor. MPERS goals can be seen with a regex indicating its dynamic behaviour as part of the runtime goal model specification required by the proposal. This notation is a reflex of the late requirements phase, as the TAOM4E tool used for goal modelling shares unique entities and relations among different development phases. The regex syntax is enclosed by brackets to differentiate then from goal name. More details on the behaviour specification can be found in later section of this chapter.

### 5.2.2 TROPOS Late Requirements Phase

Later requirements phase concentrates the analysis in the system-to-be and its operational environment. The MPERS goal model occupies the most part of the diagram and each of its main goals are further decomposed through AND/OR decomposition. Also, means-end tasks specifies how leaf-goals can/must be fulfilled and the runtime regex across goals and tasks specifies dynamic properties of the system-to-be behaviour. Figure 5.3 illustrates the late requirements diagram for the MPERS.

At this stage of the methodology, the system is represented as a monolithic actor and its goal model may be extended with the runtime specification. This extended model merges multiple views in the same diagram: goals, tasks and relations represent the requirements view for the system-to-be as well as the intentionality behind then, while the runtime specification provides the behaviour specification required for our goal-oriented dependability analysis.

To evaluate our proposal, we have explored the use of the PMC technique for the reliability verification of the system goal model resulting from the TROPOS late requirements phase. The idea is to initially evaluate the approach in a monolithic representation without the additional complexity of a multi-agent architecture. The evaluation involving later TROPOS phases should be explored in future work. The remaining of this section will focus on the proposed goal-oriented contextual dependability analysis.

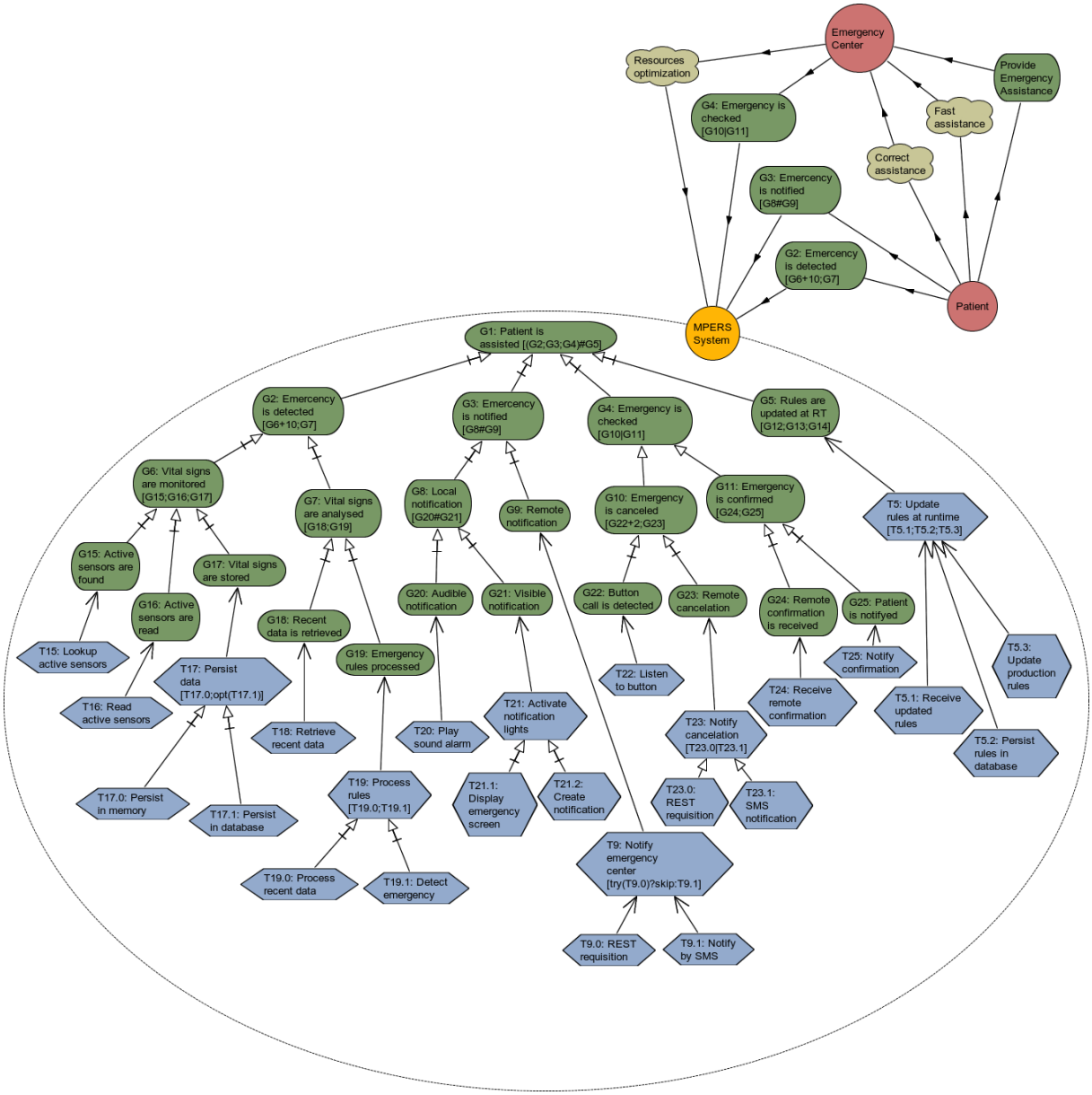



Figure 5.3: MPERS at TROPOS early requirements phase

### 5.2.3 RGM - UML activity diagram comparison

A similar behaviour specification achieved with the RGM in Figure 5.3 could be provided by an UML activity diagram with activities representing the leaf-tasks in the model. However, activity diagrams have an homogeneous abstraction level and do not clearly correlate behaviour to the requirements they are meant to satisfy. In contrast to the RGM, activity diagrams denote behaviour through graphical symbols, while the RGM mixes the original goal model notation with a runtime regex. This simple notation increases the utility of a goal model diagram. Figure 5.4 presents an activity diagram corresponding to the MPERS leaf-tasks.

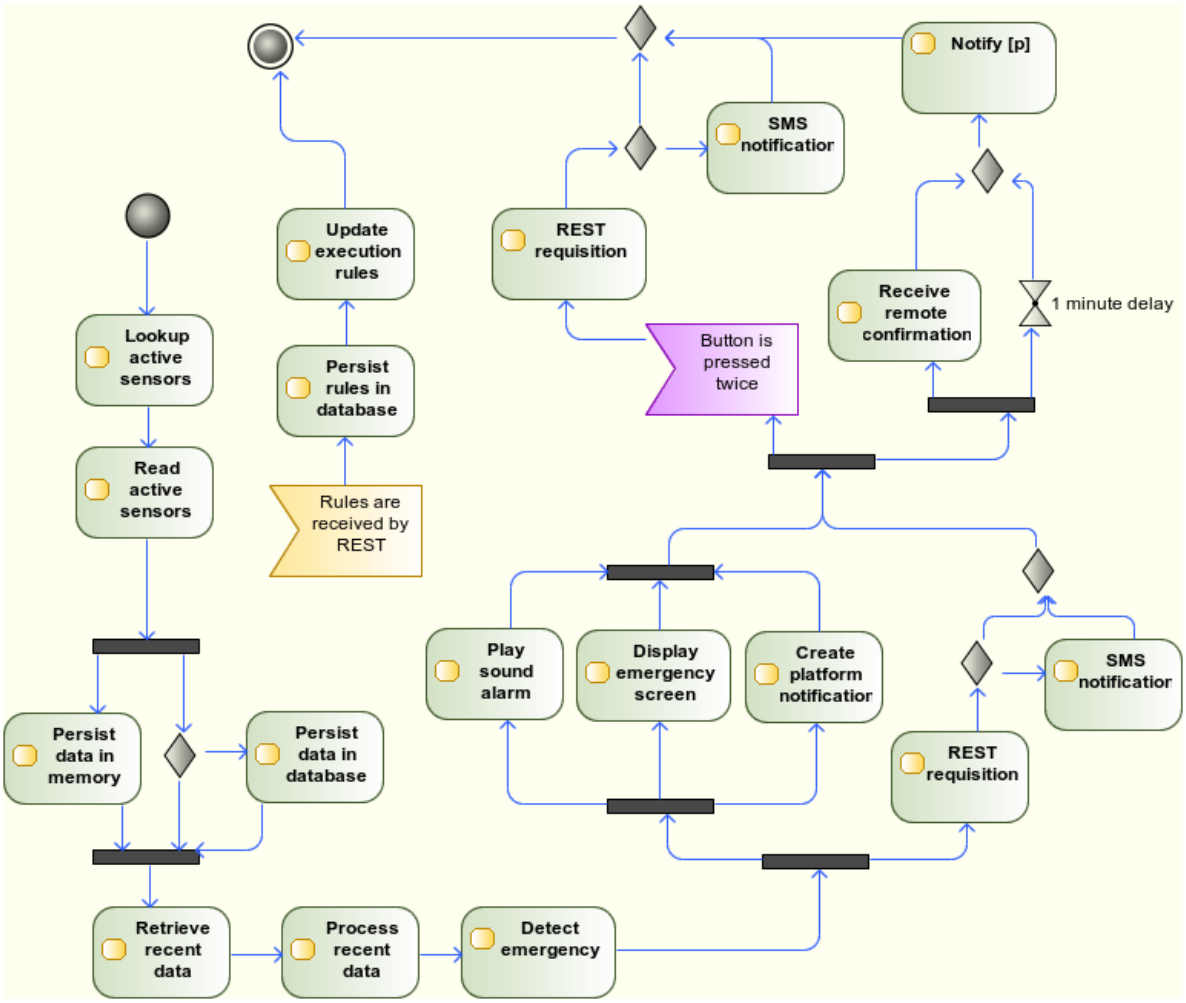



Figure 5.4: MPERS tasks represented by a UML activity diagram

Among its limitations, RGM does not express that an emergency has to be confirmed after a time (clock) or signal event as the UML activity diagram does. Both necessary and sufficient conditions for the triggering and fulfilment of goals, tasks and dependencies are provided by Formal TROPOS specification language. Still, sequential, interleaved, alternative, optional and conditional execution flows as well as multiple executions of the same task can be expressed by the RGM, providing a rich behaviour specification for the system-to-be.

The idea of a runtime goal model is not to replace UML activity diagrams, but to complement the static goal model with a clear runtime syntax that could be used for documentation, team communication and for conformance verification at both design time - e.g., through model-based verification - and during system execution - as the execution monitoring originally proposed by Dalpiaz et al [RGM]. Depending on the complexity of the behaviour specification, a more robust runtime syntax would have to be employed or

complemented by traditional UML behaviour models. In this work, RGM is used as input for our goal-oriented dependability analysis based on PMC.

### 5.2.4 Non-functional requirements analysis

TROPOS goal model also provides rationale for NFR analysis, as it originally inherited the softgoal analysis from the NFR framework [NFR]. In our approach, non-functional constraints are modelled as qualitative hard goals with a clear cut value for its satisfaction, complementing the other NFRs modelled as softgoals. As a benefit of a goal-oriented modelling for NFRs, the elicitation of a given NFR may be justified by its relation to other elements in the model. Figure 5.5 presents the NFRs for the MPERS system actor.

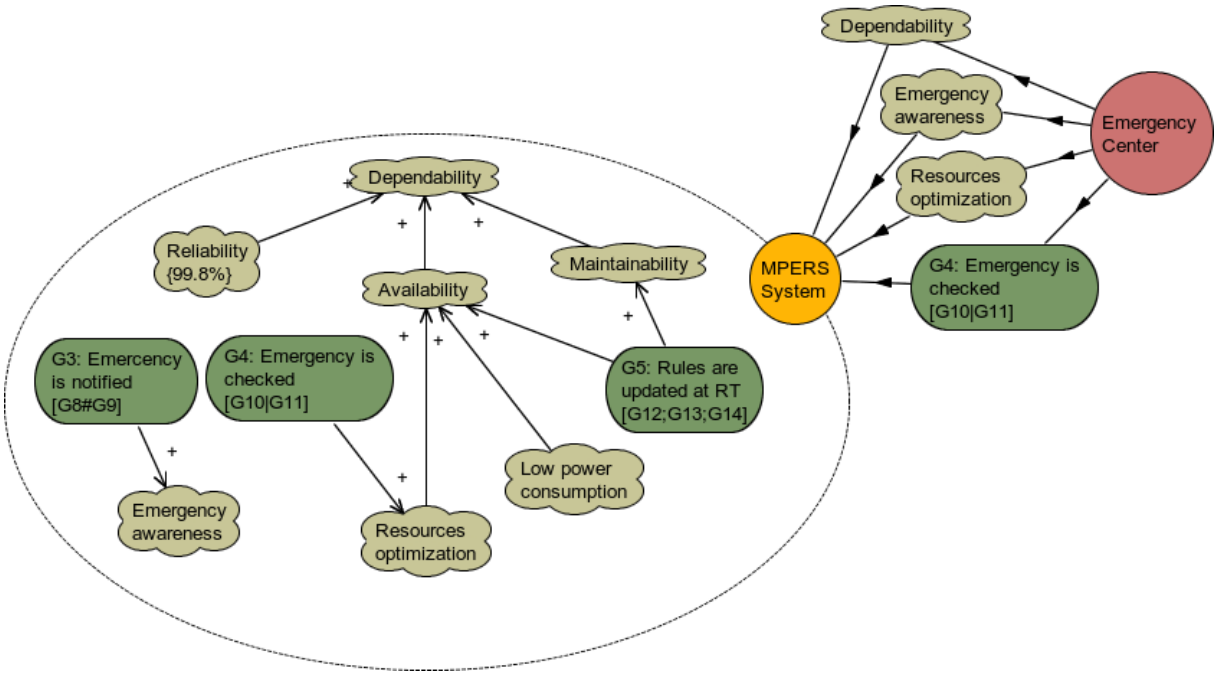



Figure 5.5: MPERS non-functional requirements.

Similarly to the Awareness Requirements by Souza et al. [22], some NFR define metrics over other requirements. These meta-requirements are not directly fulfilled by system functionalities like 'emergency awareness' is fulfilled by 'notify emergency' or 'confidentiality' could be fulfilled by 'user authentication', but by how these functionalities will perform. Reliability, for instance, is inversely proportional to the likelihood of failures. Hence, the reliability metric depends on the probability of system functionalities to successfully meeting their goals.

Other MPERS NFR are 'emergency awareness' and 'resources optimization'. These softgoals are addressed by system functionalities. The former receives a full contribution (double positive sign) from goal 'emergency is notified', meaning it is fully satisfied by

this goal. The later is just assumed to be partially satisfied by the 'emergency is checked' functional goal.

Each requirement in a goal model must come from another requirement through decomposition, means-end or contribution links, or it must be directly mapped to stakeholder needs through dependency links. Emergency center attended the patient's needs by providing and maintaining the MPERS system itself and by assuring other NFR for the system.

Reliability was selected as metric over the system execution (meta-requirement), while availability and maintainability are partially satisfied by the 'low power consumption' softgoal and MPERS ability to update emergency rules at runtime, respectively. This proposal focus on reliability analysis and will not discuss the verification of other relevant NFRs.

## 5.3 Goal-oriented Probabilistic Verification Model

This section describes the application of a goal-oriented PMC technique for the reliability verification of a runtime goal model with additional context effect notations. We call it a goal-oriented probabilistic verification or goal-oriented dependability analysis because the probabilistic model, in this case a DTMC model, is built directly from a runtime goal model with the purpose of evaluating PCTL properties related to the reliability of the system, i.e., to the success probability of different goals in being fulfilled.

### 5.3.1 Leaf-tasks as DTMC modules

The MPERS RGM in Figure 5.3 expands its main goals in further subgoals that are ultimately satisfied by operational tasks. Tasks can also be expanded in more granular subtasks. Tasks without outgoing relations are named leaf-tasks. In our proposal, leaf-tasks are mapped to modules in a DTMC model in PRISM language. In the DTMC model, leaf-tasks have their execution state mapped to a module variable (sT15 variable in Figure 5.7). From the RGM original set of goal/tasks instance states, we considered the following values:

- Init(sTask=0): corresponds to the initial/ready state of a given leaf-task. From this state, a transition may occur to the running state, if this task is part of a system alternative to be analysed, or directly to the final success state, if the opposite.

- Running(sTask=1): corresponds to the execution state of a given leaf-task. From this state, a transition to the final success or failure states may occur. A variable

ranging from 0 - 1 defines the task's reliability, i.e., the probability of a transition to the success state - and the complementary transition probability to the failure state (variable rTask15 in Figure 5.7).

- Success(sTask=2): corresponds to the absorbing and final success state of a singular task execution.
- Skipped(sTask=3): indicates that a task does not participate in the fulfilment of the analysed goal and should not impact the analysis results.
- Failure(sTask=4): the opposite from the final success state, meaning that a singular task execution has failed.

Figure 5.6 illustrate leaf-tasks' states in a UML state diagram, while Figure 5.7 presents a system task as a PRISM module.

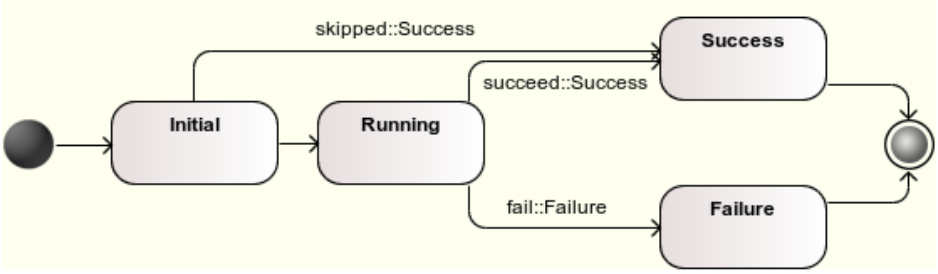



Figure 5.6: State diagram for leaf-tasks in the DTMC module.

```
const double rTaskT15;

module T15_FindActiveSensors
        sT15 :[0..3] init 0;

        [success0_0] noError & sT15 = 0 -> (sT15'=1);//init to running


        [] sT15 = 1 -> rTaskT15 : (sT15'=2) + (1 - rTaskT15) : (sT15'=3);//running to final state
        [success0_1] sT15 = 2 -> (sT15'=2);//final state success
        [failT15] sERROR = 0 & sT15 = 3 -> (sT15'=3);//final state fail
endmodule
```

Figure 5.7: A PRISM DTMC module representing T15 (mandatory) task.

### 5.3.2 Building the high-level DTMC model from a RGM

The first step in building a DTMC from a RGM is parsing the behaviour rules. All goals and tasks elements in the model receive an unique identification (ID). Numeric

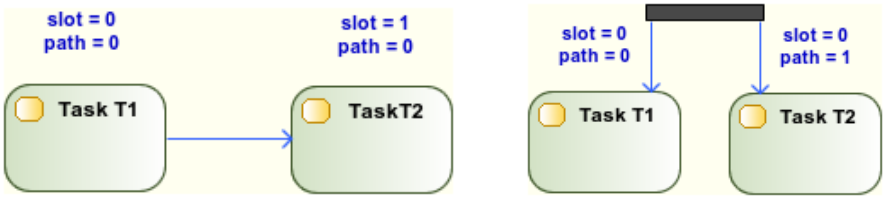
IDs are prefixed with an 'G', in the case of goals, and 'T', in the case of tasks. For each decomposed element, a corresponding runtime regex consisting of IDs and rules specifying the behaviour of all immediately underlying goals and tasks. Parenthesis are used for grouping related goals/tasks and for clarification purpose only, as temporal order is parsed from the type of the rule and its position in the regex.

Given a set of leaf-tasks that fulfils a chain of subgoals until a certain goal G, a high-level DTMC model composed of modules for each leaf-task states and transitions is build. This model must abstract the same behavioural of the corresponding RGM, i.e., it must preserve activities temporal order and other semantics specified by the runtime regex. We call the resulting verification model of a high-level DTMC because leaf-tasks are similar to activities in a UML diagram whose behaviours could be further detailed, e.g., by sequence diagrams.

Each leaf-task in the DTMC model starts at a discrete time slot. Time slots maps the sequence order of tasks executions. To differentiate the time of parallel tasks, time path is incremented by interleaved task executions, while time slot is incremented by sequential executions. Next, the representation of RGM rules in DTMC modules are presented, as well as the increment in the time slot and time path caused by each rule as illustrated by corresponding UML activity diagrams.

### Sequential order

The most trivial behaviour rule consist of the temporal fulfilment and execution order of goals and tasks. In a RGM, the ';' and '#' symbols represent sequential and parallel temporal orders, respectively. Figures 5.8a and 5.8b illustrate this behaviours in UML activity diagrams.




(a) Sequential tasks T1;T2. (b) Interleaved tasks T1#T2.

Sequential tasks ($T1;T2$) have subsequent time slots, meaning that T2's initial transition is synchronized to T1's final transition through PRISM labels. In contrast, interleaved tasks ($T1\#T2$) have their initial state transition synchronized at the same time slot through labels, but occupy different time paths, i.e., following state transitions of these tasks are interleaved. Listings 5.1 and 5.2 present the DTMC modules for each case.

```
const double rTaskT15=0.999;
module T15_LookupActiveSensors
  sT15 :[0..4] init 0;

  [success0_0]  sT15 = 0 -> (sT15'=1);//init to running
  [] sT15 =  1 -> rTaskT15 : (sT15'=2) + (1 - rTaskT15) : (sT15'=4);//running to final
      state
  [success1_1] sT15 = 2 -> (sT15'=2);//final state success
  [success1_1] sT15 = 3 -> (sT15'=3);//final state skipped
  [failT15] sT15 = 4 -> (sT15'=4);//final state failure
endmodule

const double rTaskT16=0.999;

module T16_ReadActiveSensors
  sT16 :[0..4] init 0;

  [success1_1]  sT16 = 0 -> (sT16'=1);//init to running
  [] sT16 =  1 -> rTaskT16 : (sT16'=2) + (1 - rTaskT16) : (sT16'=4);//running to final
      state
  [success1_2] sT16 = 2 -> (sT16'=2);//final state success
  [success1_2] sT16 = 3 -> (sT16'=3);//final state skipped
  [failT16] sT16 = 4 -> (sT16'=4);//final state failure
endmodule
```

Listing 5.1: Sequential tasks T15 and T16 as DTMC modules with final transitions of the first module synchronized to the initial transition of the former.

```
const double rTaskT21_0=0.999;
module T21_0_DisplayEmergencyScreen
  sT21_0 :[0..4] init 0;

  [success0_2]  sT21_0 = 0 -> (sT21_0'=1);//init to running
  [] sT21_0 =  1 -> rTaskT21_0 : (sT21_0'=2) + (1 - rTaskT21_0) : (sT21_0'=4);//running
      to final state
  [success1_3] sT21_0 = 2 -> (sT21_0'=2);//final state success
  [success1_3] sT21_0 = 3 -> (sT21_0'=3);//final state skipped
  [failT21_0] sT21_0 = 4 -> (sT21_0'=4);//final state failure
endmodule

const double rTaskT21_1=0.999;

module T21_1_CreatePlatformNotification
  sT21_1 :[0..4] init 0;

  [success0_2]  sT21_1 = 0 -> (sT21_1'=1);//init to running
  [] sT21_1 =  1 -> rTaskT21_1 : (sT21_1'=2) + (1 - rTaskT21_1) : (sT21_1'=4);//running
      to final state
  [success2_3] sT21_1 = 2 -> (sT21_1'=2);//final state success
  [success2_3] sT21_1 = 3 -> (sT21_1'=3);//final state skipped
  [failT21_1] sT21_1 = 4 -> (sT21_1'=4);//final state failure
endmodule
```

Listing 5.2: Interleaved tasks T21.0 and T21.1 as DTMC modules with initial transition synchronized.

### XOR-decomposition

In the case of OR-decomposition with additional '|' behaviour rule, a resulting XOR-decomposition specifies that only one goal/task among two or more may be selected, i.e., they are mutually exclusive. Figures 5.9 illustrate the alternative OR-decomposition in an UML activity diagram.

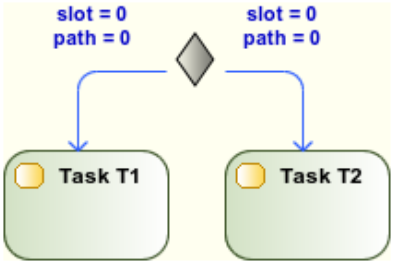



Figure 5.9: Alternative tasks T1|T2.

To represent this rule in a DTMC model, an additional parameter defines which alternative from a set of two or more is selected for analysis. Listing 5.3 presents the DTMC modules for alternative tasks T9.00 and T9.01. For this behaviour rule, both time slot and time path are equal for the alternatives, as only one task may be selected. The increment is defined by surrounding ';' or '#' rule.

```
1  const double rTaskT9_0=0.999;
2  module T9_0_RESTRequisition
3    sT9_0 :[0..4] init 0;
4
5    [success0_2] (CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=1);//init to running
6    [success0_2] !(CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=4);//init to failure
7    [] sT9_0 =  1 -> rTaskT9_0 : (sT9_0'=2) + (1 - rTaskT9_0) : (sT9_0'=4);//running to
         final state
8    [success2_3] sT9_0 = 2 -> (sT9_0'=2);//final state success
9    [success2_3] sT9_0 = 3 -> (sT9_0'=3);//final state skipped
10   [failT9_0] sT9_0 = 4 -> (sT9_0'=4);//final state failure
11 endmodule
12
13 const double rTaskT9_1=0.999;
14
15 module T9_1_SMSNotification
16   sT9_1 :[0..4] init 0;
17
18   [failT9_0]  sT9_1 = 0 -> (sT9_1'=1);//init to running
19   [success2_3] sT9_1 = 0 -> (sT9_1'=3);//not used, skip running
20   [] sT9_1 =  1 -> rTaskT9_1 : (sT9_1'=2) + (1 - rTaskT9_1) : (sT9_1'=4);//running to
         final state
21   [success2_4] sT9_1 = 2 -> (sT9_1'=2);//final state success
22   [success2_4] sT9_1 = 3 -> (sT9_1'=3);//final state skipped
23   [failT9_1] sT9_1 = 4 -> (sT9_1'=4);//final state failure
```

```
endmodule
```

Listing 5.3: Alternative tasks T9.00 and T9.01 as DTMC modules with additional integer parameter used for selection.

### Optional execution

Given a decomposed goal or task, its fulfilment or execution may be optional, meaning that at least one other goal/task must necessarily be fulfilled/executed. It is trivial to realize that optional behaviour rules $opt(E)$ are only possible in OR-decompositions. Figure 5.10 illustrate an optional decomposition.

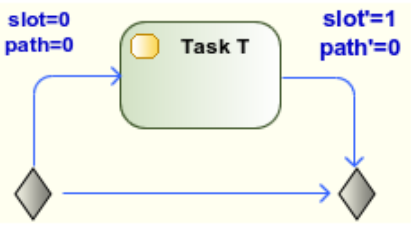



Figure 5.10: Optional task T.

Similarly to alternative execution, optional tasks are enabled for analysis by an additional parameter in the model. Listing 5.4 illustrates the DTMC module for optional task T17.2. Time slot or path increment is also defined by surrounding ';' or '#' rule.

```
const double rTaskT17_1=0.999;
const int OPT_T17_1;

module T17_1_PersistInDatabase
  sT17_1 :[0..4] init 0;

  [success1_3] (DISK <= 90) & sT17_1 = 0 -> (OPT_T17_1) : (sT17_1'=1) + (1 - OPT_T17_1) :
       (sT17_1'=3);//init to running or skip to final success
  [success1_3] !(DISK <= 90) & sT17_1 = 0 -> (sT17_1'=4);//init to fail
  [] sT17_1 =  1 -> rTaskT17_1 : (sT17_1'=2) + (1 - rTaskT17_1) : (sT17_1'=4);//running
      to final state
  [success1_4] sT17_1 = 2 -> (sT17_1'=2);//final state success
  [success1_4] sT17_1 = 3 -> (sT17_1'=3);//final state skipped
  [failT17_1] sT17_1 = 4 -> (sT17_1'=4);//final state failure
endmodule
```

Listing 5.4: An optional task T17.1 as a DTMC module with additional boolean parameter.

### Conditional execution

Some goals/tasks are conditioned to the fulfilment/execution of another goal/task. In such cases, a AND/OR-decomposition have an additional ternary rule $try(E1)?E2 : E3$

where E2 is conditioned to the success of E1, while E3 is conditioned to its failure. The skip term is used if no further behaviour is conditioned to either the success or the failure of E1, for instance, in $try(T1)?skip : T2$ where task T2 is only required for execution if T1 fails and no further behaviour is expected if T1 succeeds. Figure 5.11 illustrate a conditional decomposition.

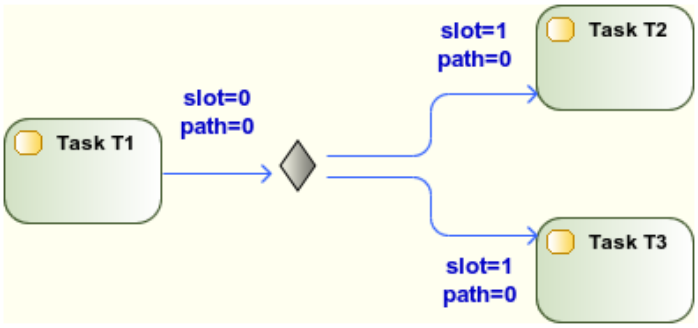



Figure 5.11: Optional task T.

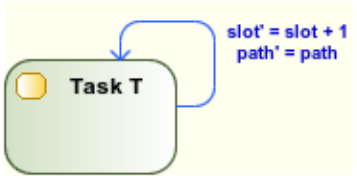
In conditional execution, labels are used to condition the execution of tasks to the success and failure of a third task. Figure 5.5 present the DTMC module for conditional tasks T9.0 and T9.1.

```
const double rTaskT9_0=0.999;

module T9_0_RESTRequisition
  sT9_0 :[0..4] init 0;

  [success0_2] (CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=1);//init to running
  [success0_2] !(CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=4);//init to failure
  [] sT9_0 =  1 -> rTaskT9_0 : (sT9_0'=2) + (1 - rTaskT9_0) : (sT9_0'=4);//running to
      final state
  [success2_3] sT9_0 = 2 -> (sT9_0'=2);//final state success
  [success2_3] sT9_0 = 3 -> (sT9_0'=3);//final state skipped
  [failT9_0] sT9_0 = 4 -> (sT9_0'=4);//final state failure
endmodule

const double rTaskT9_1=0.999;

module T9_1_SMSNotification
  sT9_1 :[0..4] init 0;

  [failT9_0]  sT9_1 = 0 -> (sT9_1'=1);//init to running
  [success2_3] sT9_1 = 0 -> (sT9_1'=3);//not used, skip running
  [] sT9_1 =  1 -> rTaskT9_1 : (sT9_1'=2) + (1 - rTaskT9_1) : (sT9_1'=4);//running to
      final state
  [success2_4] sT9_1 = 2 -> (sT9_1'=2);//final state success
  [success2_4] sT9_1 = 3 -> (sT9_1'=3);//final state skipped
  [failT9_1] sT9_1 = 4 -> (sT9_1'=4);//final state failure
endmodule
```

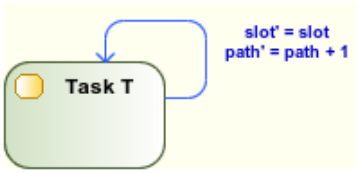
Listing 5.5: Conditional tasks T9.00 and T9.1 as DTMC modules.

### Cardinality

A small variation of the original RGM syntax was employed for the E+ and E# rules. Instead of an undetermined number of goal/task instances, analyst should provide the exact number of instances for goals achievement and tasks execution. This information is required for the generation of the DTMC verification model from a runtime goal model. Figures 5.12a and 5.12b respectively illustrate sequential and interleaved task behaviours.




(a) Sequential executions of task T.




(b) Interleaved executions of task T.

In our proposal, execution cardinality is represented by the number of retries of a given task transition from the initial state to the success state, in the case of a sequential execution ($E{+}n$), or by interleaved transitions with PRISM language module renaming, in the case of interleaved execution ($E\#n$). In the first case, only after $n$ unsuccessful retries, a transition to the failure state occurs. In the second case, $n$ simultaneous transitions from the initial state to the running state occurs before interleaved transitions from the running state to the final success/failure state may happen. The failure label is also renamed to avoid deadlocks if one or more of the interleaved tasks fails.

Despite the multiplicity of tasks instances, cardinality is seen as an execution block, i.e, the discrete time slot is only incremented once, while the time path is not incremented. Listings 5.6 and 5.7 present the DTMC modules for both cases. The former example does not come from the MPERS RGM and illustrate the module renaming.

```
1  const double rTaskT22;
2  const double maxRetriesT22=2;
3  module T22_ListenToButton
4    sT22 :[0..4] init 0;
5    triesT22 : [0..2] init 0;
6
7    [success0_3]  sT22 = 0 -> (sT22'=1);//init to running
8    [] sT22 = 1 & triesT22 < maxRetriesT22 -> rTaskT22 : (sT22'=2) + (1 - rTaskT22) : (
         triesT22'=triesT22+1);//try
9    [] sT22 = 1 & triesT22 = maxRetriesT22 -> (sT22'=4);//no more retries
10   [success0_4] sT22 = 2 -> (sT22'=2);//final state success
11   [success0_4] sT22 = 3 -> (sT22'=3);//final state skipped
12   [failT22] sT22 = 4 -> (sT22'=4);//final state failure
13 endmodule
```

Listing 5.6: Sequential cardinality with n=2 for task T22.

```
const double rTaskT22;
const double maxRetriesT22=2;
module T22_ListenToButton
  sT22 :[0..4] init 0;

  [success0_3]  sT22 = 0 -> (sT22'=1);//init to running
  [] sT22 = 1 -> rTaskT22 : (sT22'=2) + (1 - rTaskT22) : (sT22'=4);//running to final
      state
  [success0_4] sT22 = 2 -> (sT22'=2);//final state success
  [success0_4] sT22 = 3 -> (sT22'=3);//final state skipped
  [failT22] sT22 = 4 -> (sT22'=4);//final state failure
endmodule
module T22_N2 = T22_ListenToButton [ sT22_N2=sT22, rTaskT22_N2=rTaskT22 ] endmodule
module T22_N3 = T22_ListenToButton [ sT22_N3=sT22, rTaskT22_N3=rTaskT22, failT22_N2=
    failT22] endmodule
```

Listing 5.7: Interleaved cardinality with n=3 for task T22.

In Table 5.1, the final settings for the time slot, path and other dynamic aspects of leaf-tasks parsed from the RGM and used for the generation of a DTMC model are presented.

### 5.3.3 Context effects in the DTMC model

In a CGM, the analysis of the environment in which the system will operate is performed. A careful investigation of what is static and what may change during operation should list the contexts facts and variables that may potentially affect goals, operational means (tasks) and the quality of alternatives. In contrast to the world predicates in the primitive CGM, in our proposal contexts are specified as boolean formulas composed of context variables and operators. Variables can hold boolean or real numbers values. The following operators can be used in the modelling environment:

- $<$, $<=$, $>=$, $>$ (relational operators)
- $=$, $!=$ (equality operators)
- ! (negation)
- & (conjunction)
- | (disjunction)

Regarding a goal-oriented dependability analysis based on PMC, context variation may change the scope of the verification and consequently limiting the operational leaf-tasks that must be part of the analysis - either because they do not have a goal to satisfy in that context or because they are restricted by that context and cannot be selected for execution. Besides the effects over goals and tasks, we have not considered the direct

| Task | Time path | Time slot | Optional | Conditional | Alternative | Cardinality |
|---|---|---|---|---|---|---|
| **T15** | 0 | 0 | false | false | false | 1 |
| **T16** | 0 | 1 | false | false | false | 1 |
| **T17.0** | 0 | 2 | false | false | false | 1 |
| **T17.1** | 0 | 3 | **true** | false | false | 1 |
| **T18** | 0 | 4 | false | false | false | 1 |
| **T19.0** | 0 | 5 | false | false | false | 1 |
| **T19.1** | 0 | 6 | false | false | false | 1 |
| **T20** | 0 | 7 | false | false | false | 1 |
| **T21.0** | 1 | 7 | false | false | false | 1 |
| **T21.1** | 2 | 7 | false | false | false | 1 |
| **T9.0** | 3 | 7 | false | false | false | 1 |
| **T9.1** | 3 | 7 | false | **S. T9.0** | false | 1 |
| **T22** | 0 | 8 | false | false | **T24** | **2** |
| **T23.0** | 0 | 9 | false | false | false | 1 |
| **T23.1** | 0 | 9 | false | **S. T23.0** | false | 1 |
| **T24** | 0 | 8 | false | false | **T22** | 1 |
| **T25.0** | 0 | 9 | false | false | **T25.1** | 1 |
| **T25.1** | 0 | 9 | false | false | **T25.0** | 1 |
| **T5.0** | 4 | 0 | false | false | false | 1 |
| **T5.1** | 4 | 0 | false | false | false | 1 |
| **T5.2** | 4 | 0 | false | false | false | 1 |

Table 5.1: Dynamic aspects of the MPERS leaf-tasks in the DTMC model.

context effect over qualitative softgoals, but only the indirect effect over the probability of fulfilling different system tasks, as softgoals are not part of the formal analysis.

All context effects formulas specified in the goal model are then parsed. Even if a context variable occurs multiple times in the same context formula or across other contexts in the model, only one variable is declared in the DTMC model (variable declaration). A reference to this variable is then used to compose identical context formulas as guard conditions in the modules corresponding to the affected leaf-tasks, according to the type of effect it imposes.

### Goals activation/restriction

If a goal is activated/restricted by a given context selected for analysis, the corresponding verification scope must be adjusted. The MPERS RGM in Figure 5.3 has a few goals whose activation depends on a specific context condition. Consequently, they must not affect the analysis results in other contexts.

For instance, the goals 'stationary geolocation is checked' and 'moving geolocation is tracked' are mandatory subgoals for the 'patient location is monitored' goal. The first is activated by the context 'user is at home' and the later by the negation of this same context. Analysts have put this restriction to avoid an aggressive geolocation tracking that consumes too much battery when the user is known to be at home. The following formulas specify this restricting context and its negation:

$$\textbf{C1:} \quad HOME\_WIFI \,!= \, 0 \quad \& \quad LOCATION\_AGE \, < \, 10 \tag{5.1}$$

$$\textbf{!C1:} \quad HOME\_WIFI \, = \, 0 \quad | \quad LOCATION\_AGE \, >= \, 10 \tag{5.2}$$

Home WI-FI BSSID is configured once and stored by the application. If its signal is not in reach for the last 10 minutes, patient is considered to be out. To map these restrictions into the DTMC model, only one PRISM formula were declared and all leaf-tasks related to the affected goals must include C1 (or its negation) as a condition to the inclusion of these tasks in the analysis. A false evaluation of the context formula (or its negation) automatically excludes these leaf-tasks from the analysis results by forcing a deterministic transition to the skipped final state (sTask=3). Listing 5.8 presents the DTMC module of a MPERS leaf-task whose goal is restricted by a context formula.

```
1 const double HOME_WIFI;
2 const double LOCATION_AGE;
3 const double rTaskT6_0=0.999;
4
5 module T6_0_CheckHomeWI_FIRange
6   sT6_0 :[0..4] init 0;
```

```
7
8   [success0_0] (HOME_WIFI != 0 & LOCATION_AGE < 10) & sT6_0 = 0 -> (sT6_0'=1);//init to
        running
9   [success0_0] !(HOME_WIFI != 0 & LOCATION_AGE < 10) & sT6_0 = 0 -> (sT6_0'=3);//init to
        skipped
10
11
12  [] sT6_0 =  1 -> rTaskT6_0 : (sT6_0'=2) + (1 - rTaskT6_0) : (sT6_0'=4);//running to
        final state
13  [success0_1] sT6_0 = 2 -> (sT6_0'=2);//final state success
14  [success0_1] sT6_0 = 3 -> (sT6_0'=3);//final state skipped
15  [failT6_0] sT6_0 = 4 -> (sT6_0'=4);//final state failure
16 endmodule
```

Listing 5.8: Variable declaration and corresponding module with a context activation formula.

### Tasks restriction

Regarding the restriction on system tasks (means), all operations depending on a specific system resource considered to be dynamic could be notated with a context restriction. In our evaluation, we considered the restriction over the communication tasks 'REST requisition' and 'REST service' (context 'internet is available'), over the geolocation tracking tasks 'track public WI-FI' and 'track GPS' (contexts 'WI-FI is available' and 'GPS signal is available') and over the storage task 'persist in database' (context 'disk memory available') . The following boolean formulas represent these contexts:

$$\textbf{C2:} \quad CONNECTION\ != \ 0 \tag{5.3}$$

$$\textbf{C3:} \quad WI\_FI\ != \ 0 \tag{5.4}$$

$$\textbf{C4:} \quad GPS\_SIGNAL\ > \ 0 \tag{5.5}$$

$$\textbf{C5:} \quad USED\_DISK <= 95 \tag{5.6}$$

These formulas follow the same principle from the previous goal restriction formulas. For C5, we considered less than 95% of the used disk space and not 100% to avoid instabilities in the operational system. We have not considered variations in the mobile signal as a restriction to the communication tasks of 'SMS notification' and 'voice call' or any other technical impediment at this moment.

In the DTMC model, restricted leaf-tasks have an additional deterministic transition to the failure state guarded by the negation of the corresponding context formula. Con-

sequently, if the formula is evaluated as false, the leaf-task will certainly fail (sTask=4). Listing 5.9 presents a DTMC model with one restricted MPERS leaf-task.

```
const double CONNECTION;//context variable declaration
const double rTaskT9_0=0.999;

module T9_0_RESTRequisition
  sT9_0 :[0..4] init 0;

  [success0_2] (CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=1);//init to running
  [success0_2] !(CONNECTION != 0) & sT9_0 = 0 -> (sT9_0'=4);//init to failure


  [] sT9_0 =  1 -> rTaskT9_0 : (sT9_0'=2) + (1 - rTaskT9_0) : (sT9_0'=4);//running to
      final state
  [success2_3] sT9_0 = 2 -> (sT9_0'=2);//final state success
  [success2_3] sT9_0 = 3 -> (sT9_0'=3);//final state skipped
  [failT9_0] sT9_0 = 4 -> (sT9_0'=4);//final state failure
endmodule
```

Listing 5.9: Variable declaration and corresponding module with a context restriction formula.

## 5.4 Goal-oriented Reliability Analysis

Once a probabilistic verification model is built from a system RGM with additional context effects, both qualitative and quantitative analysis may be performed.

### 5.4.1 Offline analysis

At design-time, analysts may benefit from the rich graphical environment provided by PRISM probabilistic model checker tool. Given a boolean formula specifying the success in fulfilling a specific system goal $G$ whose leaf-tasks have been mapped into the DTMC model:

$$G_{success} \;=\; (sT15 = 2)\ \&\ (sT16 = 2)\ \&\ (sT17\_0 = 2\ \&\ sT17\_1 = 2) \tag{5.7}$$

And a PCTL property defining the probabilistic existence of a system behaviour that eventually leads the leaf-tasks T16, T17 and T17_1 to reach their final success state, i.e., specifying the reachability of the success system state in which G is satisfied:

$$P > 0.99[F(G_{success})] \tag{5.8}$$

Once the reliabilities of the involved leaf-tasks have been collected, the verification of this PCTL property through PRISM verification feature reveals the probability in eventually fulfilling the analysed goal. To illustrate this, for a fixed reliability of 0.98 for rT15-17_1, the reliability of $G$ is evaluated as 0.929199.

### 5.4.2 Gathering leaf-tasks reliabilities

Leaf-tasks are not necessarily atomic system operations and are generally described with a high abstraction level. For instance, the MPERS task 'Find active sensors' could be further decomposed in more granular and concrete tasks according to the platform, architecture and language used for implementation.

The more abstract a task is, the more difficult is to obtain their individual metrics - like their reliability, as the trace between an higher-level, abstract activity and the corresponding system operation(s) becomes less evident. For a global evaluation of a given metric, PCM technique requires the individual value for parts involved in the analysed system behaviour, e.g., activities, subactivities or components, depending on what the verification model represents.

In our goal-oriented approach, leaf-tasks are the parts composing a high-level system behaviour representation. Reliability variables define the probability of a successful execution of whatever the leaf-task should perform. To collect this information, analysts may follow two different approaches, as described in the next subsections.

#### Pure model-based verification

A pure model-based verification

. If internal behavioural specification like a sequence diagram is available for leaf-tasks, and if the reliabilities of the involved components are know, then a PMC approach can estimate the individual reliability of leaf-tasks. This value would then be used in the higher-level DTMC model.

The original RGM proposal relies on a strong assumption that goals and tasks instance states can be monitored through some code instrumentation. Accordingly, the success rate of tasks execution, i.e., their reliability, can be extracted by monitoring the system execution trace in controlled executions or in real production environment. Figures 5.13 and 5.14 illustrate both approaches.

#### Mean-time to failure verification

and an hybrid approach based on the analysis of the monitored execution trace of system leaf-tasks.

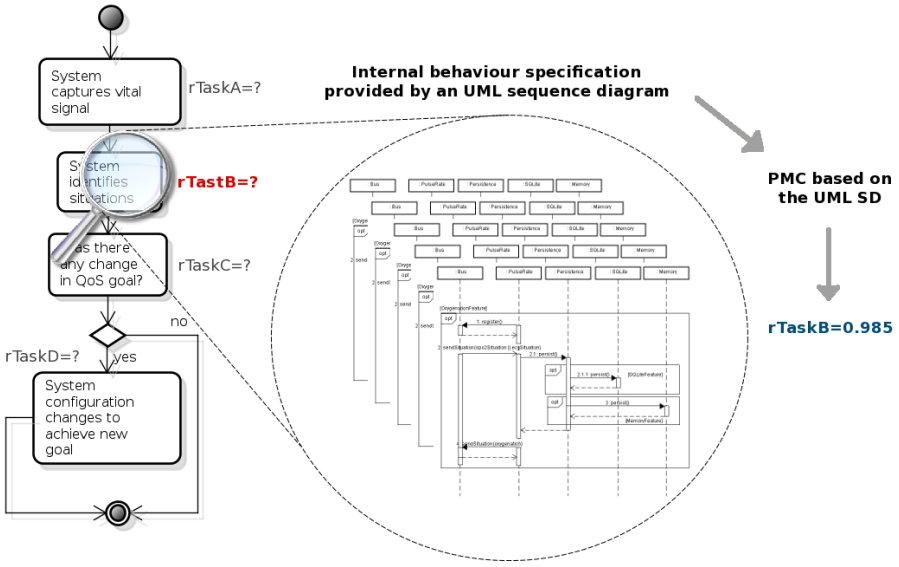



Figure 5.13: Individual reliabilities of leaf-tasks are estimated through PMC of internal behaviour specification.

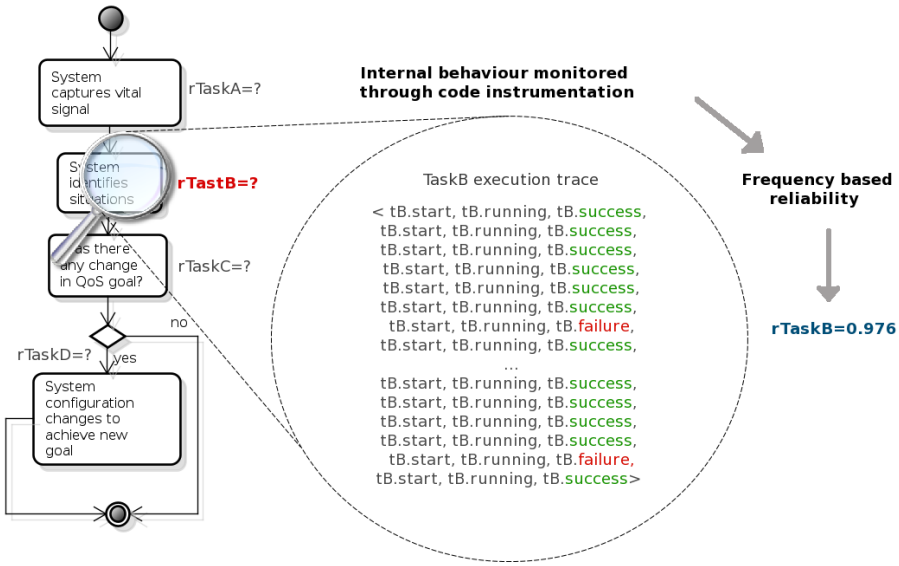



Figure 5.14: Individual reliabilities of leaf-tasks are estimated by monitoring their execution.

As our proposal focus on the runtime reliability analysis for self-adaptive systems and monitoring is already part of a self-adaptation feedback loop, our evaluation with the MPERS case study is based on individual leaf-tasks reliabilities measured through instrumented code execution.

### 5.4.3 Specifying non-functional constraints

The specification of non-functional constraints is a sensible task that depends on both expertise and domain knowledge. For instance, an analyst or a reliability engineer should be aware of what does it mean for a system to be 99.99% reliable, as this level may not be achieved by any alternative solution and must be coherent to the system criticality - a minor failure consequence could be tolerable, but a catastrophic failure should be avoided by all means. In some cases, the system will have to comply to some industry standards or contract based constraints like in service-oriented computing. Table 5.2 summarizes two possible non-functional constraints for the MPERS.

| **NFR** | **Constraint** | **Target** |
|---|---|---|
| **Reliability** | 99.8% | **G1** |
| **Power consumption** | 100 p.u. | **G2** |

Table 5.2: Non-functional metrics for the MPERS system.

As indicated by the *Target* column, each NFR constraint may be associated to a root level goal or to any of its subgoals. The corresponding probabilistic verification based on the execution of a set of leaf-tasks in the RGM is defined as:

- *Global*, if the activities set is a minimum set composed of the tasks that satisfies the chain of subgoals up to the root goal $Groot$. For instance, in Table 5.2 reliability is associated to root goal G1.

- *Local*, if the activities set is a minimum set composed of tasks that satisfies the chain of subgoals up to a goal $Gx$, where $Gx! = Groot$. For instance, in Table 5.2, power consumption is (locally) associated to goal G2.

### 5.4.4 From NFR to PCTL properties

The estimation of attributes through PMC technique is limited to those that a probabilistic model may evaluate. Dependability attributes have an abstract definition that must be associated to a concrete and verifiable PCTL property. In this evaluation, we focus on the dependability attribute of reliability.

Given a DTMC model representing system activities, global reliability may be defined as the probability of reaching a final state where all system goals are achieved. This property is called reachability and can be specified using the PCTL language. For the

MPERS root goal G1, reliability can be defined by: $P =?[G(noError)]$, with noError a boolean formula indicating that no task has transitioned to the failure state and P the steady-state probability of a true value for noError formula.

### 5.4.5 Reasoning with Ex-Tropos

The probabilistic verification of NFRs, performed as part of the Validation & Verification (VV) phase in RE, should anticipate violations of non-functional constraints. Treating a detected violation at design time may correspond to actions such as making a different choice for underlying technical components or social actors involved in the execution of tasks, optimizing the behaviour specification or even disposing a violating alternative as a means to satisfy its goal if there is at least one other valid alternative.

#### Solving variability

The variability in goal models leads to more than one minimum set of tasks capable of fulfilling local or root goals. In OR-decompositions, at least one alternative is required and the maximum number of combinations is defined by $1 + 2^{(n-1)}$, with n the number of OR-decomposed goals/tasks. Therefore, the verification of all alternatives in a goal model with individual models may prove to be inefficient or infeasible if too many variation points exist in the model.

The PMC approach has already been explored for the verification of other models that supports variability. Rodrigues et al. proposed a family-based verification of software product lines (SPL) [RODRIGUES]. The main idea is to reduce the analysis effort and boost the feasibility of the SPL verification as parameters in a PRISM probabilistic model generates a single parametric formula for all products in the SPL for a given PCTL property. Individual product evaluation is achieved by the initialization of corresponding parameters in the formula.

In our proposal, PCM verification follows the same principle of the SPL family-based verification. A parametric DTMC model should be generated from the runtime goal model. Alternatives are selected by passing values to parameters. For instance, if both GPS and triangulation are available means for identifying the patient location, a parameter with values 0 or 1 will indicate which alternative is enabled for verification, as described in Section 5.3.

#### Context selection

In a contextual goal model, or CGM, contexts may restrict which goals must be achieved, limit the adoptable alternatives (means) and also affect the non-functional met-

rics of individual tasks. These effects must be considered in a realistic verification. As a novelty, our approach for the verification of non-functional metrics through PMC will also include variable contexts of operation and their effects in the verification model.

We considered two different approaches for the NFR verification of system with dynamic contexts of operation:

- *Deterministic context activation, or DCA*: a single context is activated by parameters in the model. In this approach, a parametric formula evaluates a given alternative for a specific context of operation. It is useful for the individual verification of context-alternative pairs, e.g., a context where battery is fully charged and all vital signs sensors are activated.

- *Probabilistic context selection, or PCA*: a probability distribution will define the likelihood of a context to be activated and the corresponding context implications in the verification model to be enabled. It is useful for the emulation of an approximate scenario in which the context of operation varies following some probabilist distribution. The resulting model evaluates an activated alternative for multiple contexts.

Both approaches are complementary as the first verifies the selected alternative for one context at a time and the former verifies a realistic scenario with multiple possible contexts. Table 5.3 summarizes each verification approach.

| | **Context selection** | **Alternative selection** |
|---|---|---|
| **DCS** | Contexts are individually activated by parameters. | Alternative selection by the analyst is limited by the activated context. |
| **PCS** | Context selection follows a probabilistic distribution. | Verification model should select adoptable alternatives according to the activated context. |

Table 5.3: Description of the different approaches for verifying a system with variable alternatives and variable contexts.

The idea behind a probabilistic context selection is to emulate a realistic scenario in which the context of operation varies and the system must avoid requirements violations by having an adoptable alternative for each context. This holistic evaluation approach

provides measures for the validation of self-adaptive systems against non-functional constraints like reliability.

weighted by the probabilistic context distribution. For instance, if GPS signal is available 70% of the time and triangulation is available 90% of the time and if each method has its own reliability, namely rGPS and rTRI, the reliability of high-level task 'identify patient location' is defined by the expression 0.9*rGPS + 0.1*0.7*rTRI, considering that GPS has priority over triangulation.

## 5.5 Treating NFR Violations

- Making a different choice for underlying components: In some cases the replacement of a technical component for another of the same class can improve the quality of how they achieve their goal. For instance,

- Behaviour optimization: The quality may also depend on the pattern used for the activities execution. The specification of a different pattern may eliminate the non-functional violation.

- Contextualizing the alternative: An alternative may only violate a NFR in specific contexts. In this case, different valid alternatives may be used according to the context of operation.

- Alternative disposal: If the alternative is in absolute violation or if its validity is restricted to contexts that have at least one other valid alternative, this branch can be eliminated from the model.

# Chapter 6

# Automatic PRISM generation

As we wanted to automate the code generating process for the verification model, the graphical modelling environment that supports TROPOS methodology and the code generation for multi-agents was extended to also generate probabilistic models for the PMC technique.

To reduce the effort of codifying the verification model, an automated generation of the PRISM probabilistic model was implemented based on an existing open source tool for TROPOS development support named TAOM4E[citation]. TAOM4E provides a graphical environment for goal modelling with TROPOS methodology based on the well known Eclipse Modelling Framework (EMF) and Graphical Editing Framework (GEF). The GORE to PRISM generator was implemented as a Eclipse plugin and integrated to the TAOM4E environment.

The purpose of the automated code generation for the probabilistic PRISM model is to optimize the formal verification step by abstracting the PRISM language from the analysts and reduce the overhead and time of the model verification. This should increase the feasibility of adopting the extended TROPOS methodology by keeping analysts with their original responsibility of modelling and analysing the system, its social environment and its different contexts of operation.

In terms of a high level system behaviour, each activity has its own states space including success and failure. Our probabilistic verification approach requires not only a formal specification of the system behaviour, but also metrics related to how individual components involved in system activities will perform in respect to the analysed metric. In reliability verification, each component has an individual probability of successfully performing its functional task. Analysts must obtain these values by consulting their manufacturer, by individually analysing each component reliability based on their behaviour specification until the atomic level or by monitoring these components in a testing or production environment. Further details of how individual metrics may be obtained for

the PCM may be found at the literature and are out of the scope of this work.

In the PMC technique that has been adapted by this proposal, a behavioural specification, usually provided by UML activity and sequence diagrams, are manually converted to a probabilistic model in PRISM language. This tends to be a costly and error-prone process with a complexity proportional to the number of components, actions and interactions causing state transitions.

As a goal model is traversed from strategical root goal to operational leaf-goals, and each leaf-goal is reachable by a delegation to other actor or by a operational task, then a behaviour specification as proposed by the RGM may have enough information to be consumed as input for the generation of probabilistic models in PRISM language and for the verification of some important NFRs. However, the manual generation from RGM is still a costly task.

Depending on the abstraction level and the nature of the verification, PRISM models may either very complex or may follow a clear pattern. For instance, PRISM modules can be used to represent leaf-tasks of a runtime goal model. Considering a DTMC model, a task workflow can be modelled as a sequence of probabilistic state transitions according to the behavioural specification parsed from the RGM.

This probabilistic model follows a pattern that motivated the implementation of an automatic generation of DTMC models representing leaf-tasks execution directly from a runtime goal model.

# Chapter 7

# Validation

# Chapter 8

# Conclusion

# Referências


[1] Raian Ali, Fabiano Dalpiaz, and Paolo Giorgini. A goal-based framework for contextual requirements modeling and analysis. *Requirements Engineering*, 15(4):439–458, July 2010. 2, 3, 4, 9, 11, 19

[2] Anthony Finkelstein Andrea and Andrea Savigni. A framework for requirements engineering for context-aware services. In *In Proc. of 1 st International Workshop From Software Requirements to Architectures (STRAW 01*, pages 200–1, 2001. 1, 9

[3] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):11–33, 2004. 1, 12, 13

[4] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008. 3, 14, 15

[5] Luciano Baresi and Liliana Pasquale. Adaptive Goals for Self-Adaptive Service Compositions. In *2010 IEEE International Conference on Web Services*, pages 353–360. IEEE, July 2010. 2

[6] Luciano Baresi, Liliana Pasquale, and Paola Spoletini. Fuzzy Goals for Requirements-Driven Adaptation. In *2010 18th IEEE International Requirements Engineering Conference*, pages 125–134. IEEE, September 2010. 2

[7] Paolo Bresciani, Anna Perini, Paolo Giorgini, Fausto Giunchiglia, and John Mylopoulos. Tropos: An agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3):203–236, 2004. 4, 7, 8, 27

[8] F. Dalpiaz, A. Borgida, J. Horkoff, and J. Mylopoulos. Runtime goal models: Keynote. In *Research Challenges in Information Science (RCIS), 2013 IEEE Seventh International Conference on*, pages 1–11, May 2013. 2, 4, 20

[9] Anne Dardenne, Axel van Lamsweerde, and Stephen Fickas. Goal-directed requirements acquisition. *Science of Computer Programming*, 20(1):3–50, 1993. 4, 7

[10] Ariel Fuxman, Lin Liu, John Mylopoulos, Marco Pistore, Marco Roveri, and Paolo Traverso. Specifying and analyzing early requirements in tropos. *Requir. Eng.*, 9(2):132–150, May 2004. 22

[11] Ernst Moritz Hahn, Holger Hermanns, Björn Wachter, and Lijun Zhang. Param: A model checker for parametric markov models. In *CAV*, pages 660–664, 2010. 16

[12] Jennifer Horkoff and Eric Yu. Comparison and evaluation of goal-oriented satisfaction analysis techniques. *Requirements Engineering*, 18(3):199–222, 2013. 10

[13] M. Kwiatkowska, G. Norman, and D. Parker. Prism: Probabilistic model checking for performance and reliability analysis. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009. 14, 15

[14] M. Kwiatkowska and D. Parker. Advances in probabilistic model checking. In T. Nipkow, O. Grumberg, and B. Hauptmann, editors, *Software Safety and Security - Tools for Analysis and Verification*, volume 33 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 126–151. IOS Press, 2012. 14, 15

[15] Oxford University Computing Laboratory. PRISM case studies. http://www.prismmodelchecker.org/casestudies/, 2015. [Online; accessed 25-january-2015]. 15

[16] Oxford University Computing Laboratory. PRISM language manual. http://www.prismmodelchecker.org/manual/ThePRISMLanguage/Introduction, 2015. [Online; accessed 25-january-2015]. 15

[17] Oxford University Computing Laboratory. PRISM web site. http://www.prismmodelchecker.org/, 2015. [Online; accessed 25-january-2015]. 15

[18] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor Networks for Emergency Response: Challenges and Opportunities. *IEEE Pervasive Computing*, 3(4):16–23, October 2004. 5

[19] Danilo F. Mendonça, Raian Ali, and Genaína N. Rodrigues. Modelling and analysing contextual failures for dependability requirements. In *Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, SEAMS 2014, pages 55–64, New York, NY, USA, 2014. ACM. 20, 22, 24

[20] V. Nunes, P. Fernandes, V. Alves, and G. Rodrigues. Variability management of reliability models in software product lines: An expressiveness and scalability analysis. In *Software Components Architectures and Reuse (SBCARS), 2012 Sixth Brazilian Symposium on*, pages 51–60, Sept 2012. 3, 5, 15

[21] Terence Parr. *The Definitive ANTLR Reference: Building Domain-Specific Languages*. Pragmatic Bookshelf, 2007. 17

[22] Vítor E. Silva Souza, Alexei Lapouchnian, William N. Robinson, and John Mylopoulos. Awareness requirements for adaptive systems. In *Proceeding of the 6th international symposium on Software engineering for adaptive and self-managing systems - SEAMS '11*, page 60, 2011. 2, 21, 22, 33

[23] Shan Tang, Xin Peng, Yijun Yu, and Wenyun Zhao. Goal-directed modeling of self-adaptive software architecture. In Terry Halpin, John Krogstie, Selmin Nurcan, Erik Proper, Rainer Schmidt, Pnina Soffer, and Roland Ukor, editors, *Enterprise,*

*Business-Process and Information Systems Modeling*, volume 29 of *Lecture Notes in Business Information Processing*, pages 313–325. Springer Berlin Heidelberg, 2009. 2

[24] Eric Siu-Kwong Yu. Modelling strategic relationships for process reengineering. January 1996. 4, 7

[25] Yijun Yu, Alexei Lapouchnian, Sotirios Liaskos, John Mylopoulos, and JulioC.S.P. Leite. From goals to high-variability software design. In Aijun An, Stan Matwin, ZbigniewW. Raś, and Dominik Ślęzak, editors, *Foundations of Intelligent Systems*, volume 4994 of *Lecture Notes in Computer Science*, pages 1–16. Springer Berlin Heidelberg, 2008. 2, 3, 11