Modelling Risk and Identifying Countermeasure in Organizations

Yudistira Asnar and Paolo Giorgini

Department of Information and Communication Technology
University of Trento, Italy
{yudis.asnar,paolo.giorgini}@dit.unitn.it

Abstract. Modelling and analysing risk is one of the most critical activity in system engineering. However, in literature approaches like Fault Tree Analysis, Event Tree Analysis, Failure Modes and Criticality Analysis focus on the system-to-be without considering the impact of the associated risks to the organization where the system will operate. The Tropos framework has been proved effective in modelling strategic interests of the stakeholders at organizational level. In this paper, we introduce the extended Tropos goal model to analyse risk at organization level and we illustrate a number of different techniques to help the analyst in identifying and enumerating relevant countermeasures for risk mitigation.

Keywords: risk analysis, countermeasure identification, goal modelling.

1 Introduction

Software systems are more and more part of our life (look how many computers and electronic gadgets are around us), and very often they have a strong influence in our daily life decisions. Considering software systems as integral and active part of the organization introduces the needs of including the software development as part of the organizational development. In this direction, some software engineering methodologies have been proposed (e.g., Tropos [1] and KAOS [2]) to capture relationships between system-to-be and the organizational setting since the early phases of software development. Traditional techniques for modelling and analysing risk, such as Fault Tree Analysis (FTA) [3], Event Tree Analysis (ETA) [3], Failure Mode Effect and Criticality Analysis (FMECA) [4], are commonly used in Reliability and Safety community. Unfortunately, these techniques are not conceived to model risks at organizational level and they focus mainly on risks at the system level.

In this paper we present a modelling and reasoning framework that considers risk (in more general *uncertain event*) at organizational level. Several models have been proposed in literature to represent the intentions of the stakeholders in an organization, such as Tropos/i^* [1,5], KAOS [6], GBRM [7], and ERM-COSO [8]. We propose a framework, called Goal-Risk Model, that extends the

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 55–66, 2006.

Tropos methodology [9,10] with three basic layers (i.e., goal, event, and treatment). The framework introduces also number of techniques to analyse risk and identify countermeasures. The rest of the paper is organised as follows. Section 2 overviews briefly about Goal-Risk framework introducing the London Ambulance Service (LAS) [11,12] case study, then using this framework we define several categories of countermeasures that can be applied as a part of the solution to protect an organization from its risks. We define the guidelines to choose and model them in Section 3 and draw an example in LAS and Vehicle company case study. Finally, we conclude the paper and outline the future work in Section 4.

2 Tropos Goal-Risk Framework

Tropos goal model [9,10] proposes a formal framework to do requirement analysis by refining stakeholders' goals and ending up with the elicitation of the requirements. The framework results in a number of goal models represented as graphs $\langle \mathcal{G}, \mathcal{R} \rangle$, where $\mathcal{G}$ are goals and $\mathcal{R}$ are relations (decomposition or contribution relations). In Tropos, a goal is defined as a strategic interest of a stakeholder that intended to be achieved [1].

Each goal has two attributes SAT- $Sat(G)$ and DEN- $Den(G)$, which quantify the value of evidence for the goal being satisfied and denied, respectively[1]. The values of the attributes are qualitatively divided in the range of *(F)ull*, *(P)artial*, *(N)one*. These attributes can infer the probability of the goal to be satisfied and denied.

Goal analysis in Tropos starts with a number of top goals (i.e., ellipse in Fig. 1) of stakeholders and each of them is refined by decomposition (AND or OR) into subgoals. For example, consider in modelling the strategic objectives of London Ambulance Service (LAS) where an ambulance needs to reach the location of Accident and Emergency (A&E) in time (Fig. 1). The goal reach the location A&E in time can be achieved by distributing ambulance over the area or dispatching the closest ambulance from the A&E location to handle the accident. Moreover, distributing ambulance over area can be achieved either by organizing the movement of ambulance s.t. cover all the area or by building many ambulance pools all over the area. This decomposition and refinements will continue until the goals are considered tangible goals, i.e., when there is an actor that can fulfil the goal.

Moreover, Tropos goal analysis allows the analyst to model the influence of the satisfaction (denial) of a goal to the satisfaction (denial) of other goals. This influence can be positive or negative and is graphically indicated by "+/−" contribution relations. Tropos also has "++" and "−−" to express *strong positive contribution* and *strong negative contribution*, respectively. For example, the goal, applying dispatch to the closest ambulance from the A&E location to reach

[1] There is no relation between SAT and DEN, unlike Probability Theory P'(x) = 1 - P(x).