Chapter 15

A Formalised Approach to the Management of Risk: Process Formalisation

Mike Brownsword
Atego, UK

Rossi Setchi
Cardiff University, UK

ABSTRACT

Observations made while working with industry and government organisations have shown a number of issues with the implementation of current risk management best practice. A major issue in many cases is the lack of pragmatism associated with the risk management process and the need for a more formalised approach to risk management. In this paper, the authors propose and validate a multi-view approach to defining the processes required to carry out risk management. The formalised approach proposed includes a definition of risk, an ontology, a set of processes, and a pragmatic methodology, which shows an application of these processes enabling pro-active management of change. The ability of the processes to be applied to different types of risk has been demonstrated through a case study highlighting health and safety issues. Within the current engineering and economic climate this logical approach provides a visualisation which is consistent, repeatable, view based, and pragmatic.

1. INTRODUCTION

Observations made whilst working with aerospace, rail, defence and government organisations have shown a number of issues with the implementation of current risk management best practice. In some cases these issues arise due to a lack of willingness to carry out thorough risk management or to react when risks are revealed. However in many cases these managerial issues are compounded by fundamental issues of duplication of information, complexity of process, incoherence of terminology, and lack of pragmatism associated with the risk management process. All these issues drive the need for a more formalised approach to risk management. To ensure that complexity is reduced...
rather than increased a tried and tested method of understanding complex, diverse and multifaceted systems must be applied. Having a consistent, formalised approach supports repeatability by focusing on modularisation and re-use without forgetting the overall needs of the whole. Pragmatic application is achieved through the timely execution of relevant processes. It has the added advantage of improving the accuracy of project plans and records as each process provides a concise set of activities to be carried out showing which artefacts, documents or information, are consumed and produced by each activity. Relationships between artefacts are also defined.

The aim of this paper is to propose and validate a multi-view approach to defining the processes required to carry out risk management. Within the current engineering and economic climate this logical approach must provide a visualisation which is consistent, repeatable, view based and pragmatic.

The paper is organised as follows. Section 2 provides the background understanding of risk and reviews the relevant literature. Section 3 focuses on defining a set of processes which can be used to carry out risk management. Within this logical approach must provide a visualisation which is consistent, repeatable, view based and pragmatic.

2. RELATED WORK

There are many understandings of the term ‘process’. This section focuses on understanding what risk experts and standards mean when they discuss the ‘risk management process’. The focus will be on contributions which have defined a process and standards presenting a baseline approach to risk management.

In his tutorial on software risk management Boehm (1989) defines a number of steps aimed at identifying, addressing and eliminating software risks before they cause re-work or failure, and a life cycle model, called ‘Boehm’s spiral model’, in which these steps can be applied. This work was carried out when software risk management was considered to be an emerging discipline, however many of the concepts are still applied. The spiral model provides an incremental approach to defining requirements, architecture and design through the re-use of the four main elements: ‘determine objectives, alternatives, constraints’, ‘evaluate alternatives; identify, resolve risks’, ‘develop, verify next level product’ and ‘plan next phases’.

Boehm (1989) states that the objectives of software risk management are to identify, address, and eliminate software risk items before they become either threats to successful software operation or major sources of software rework. He defines two primary steps within risk management: risk control and risk assessment. Three sub-steps exist within each; risk control covering management, monitoring and resolution, and risk assessment involving identification, analysis and prioritisation. The disadvantage of the spiral model is that it specifies the work to be completed in each step: this constrains the flexibility of the model and therefore its application to other areas. Boehm’s contribution is the differentiation between risk assessment, which he called ‘control’, and risk management, which provides in many cases a useful delineation between the work of identifying and fully defining risks, and the plans and controls which need to be in place to ensure that risks are dealt with effectively.

Hughes and Cotterell (1999) have extended Boehm’s model of risk management by re-partitioning of the risk management steps into planning, staffing, directing, monitoring and control activities, and the risk analysis area focused on the identification, estimation and evaluation of risk. It is believed that many of the differences between the two models are in the meaning of the word ‘management’. In Boehm’s work the use of ‘risk management’ was used to signify the whole area