A Formalised Approach to the Management of Risk: A Conceptual Framework and Ontology

Mike Brownsword, Atego, UK
Rossitza Setchi, Cardiff University, UK

ABSTRACT

Taking pragmatic, systems engineering approach, this paper identifies a number of fundamental issues that presently arise in risk management, primarily as a result of the overly complex approach conventionally taken in process definition and a lack of coherence within the current risk management vocabulary. The aim of the paper is to enable a fundamental simplification of the risk management process and an improved understanding of the associated terminology. The outcome of this work is a formalised but pragmatic approach to risk management resulting in the development of a conceptual framework and an associated ontology, which emphasises the understanding of people and their environment as part of risk management. The approach has been validated in a number of case studies of varying depth and breadth from the IT domain, defence, rail industry, and education, covering health and safety, business, project and individual needs.

Keywords: Framework, Ontology, Risk, Risk Management, Standards, Systems Approach, Terminology

INTRODUCTION

Background

The consideration of risk is a day-to-day phenomenon used by individuals and Small to Medium Enterprises (SMEs) as well as large national, multinational and global organisations. Although in many instances risks may be ‘mitigated’ this does not mean that all complex issues have been well understood.

Risk management proposes to be a solution to understanding and removing the worry associated with issues which may arise in the future. As a discipline it has existed since the 1960s, emerging from an historic need and desire to insure. From the 1980s clear reference can be made to a process for risk management which has remained relatively unchanged.

There are many tools available to assist in the modelling of complex systems. Modelling allows simplification of the system to allow the complexity to be understood or at least to aid the recognition that there is a complex issue. These tools vary from high level business strategy identification to Failure Modes and Effects Analysis (FMEA) examining the detail associated with failures of components in a system.
Many industries recognise the need for risk management. The UK railway industry for example has a defined and documented regime for addressing risk. This regime is documented and controlled through the use of standards such as EN 50126 (1999). It introduces risk as a safety concept which can be seen to run throughout a project lifecycle. However many industries have not recognised either the importance of formalising risk management and the surrounding issues or that the technology they are working with has associated risk. This lack of recognition may have legal, personal and technological impact.

**Context and Scope**

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 complexity and lack of pragmatism associated with the risk management process. Inhibiting the resolutions of many of these issues is the lack of understanding and agreement on terminology used to describe and discuss risk. As a result, the word ‘risk’ means something different almost every time it is used.

The aim of the paper is to propose a conceptual framework and an ontology enabling a fundamental simplification of the risk management and an improved understanding of the associated terminology. The outcome of this work is a formalised but pragmatic approach to risk management, which emphasises the understanding of people and their environment as part of risk management.

The paper introduces generic risk management frameworks, standards and terminology, providing a critical analysis of the risk terminology and definitions. Next, a conceptual framework and an associated ontology is proposed, followed by a conclusion.

**LITERATURE REVIEW**

Much of the literature relating to risk management is specific to industry, applications and tools. Instead, this literature review is focused on generic risk management frameworks, standards and associated terminology.

**Frameworks**

One of the first frameworks for risk management is Boehm’s spiral model (1986) which is risk driven and reflects the incremental nature of most software development projects. Boehm (1989) defines software risk management as a discipline whose objectives are to “identify, address, and eliminate software risk items before they become either threats to successful software operation or major sources of software rework” (p. 1). 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. Boehm’s approach provides a differentiation between risk assessment and risk control, and a useful delineation between 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 by defining risk engineering as involving risk analysis and risk management. The management area groups all planning, staffing, directing, monitoring and control activities whilst the analysis area focuses on the identification, estimation and evaluation of risk. It is believed that many of the changes are in the meaning of the word ‘management’. In Boehm’s work, the term ‘risk management’ is used to signify the whole area of risk assessment, analysis and control Whereas Hughes and Cotterell are using management to specify only the control, planning and resource issues leaving identification, estimation and evaluation to risk analysis. Kirchsteiger (2008) takes a similar view when he explains risk assessment as the
Iterative Fault Tolerant Control for General Discrete-Time Stochastic Systems Using Output Probability Density Estimation
www.igi-global.com/chapter/iterative-fault-tolerant-control-general/69670?camid=4v1a

The Role of Coordinators in Software Off-Shoring: A Knowledge Management Perspective
Nguyen Thu Huong, Umemo Katsuhiro, Dam Hieu Chi and Dang Thi Viet Duc (2014). International Journal of Knowledge and Systems Science (pp. 1-18).
www.igi-global.com/article/the-role-of-coordinators-in-software-off-shoring/114945?camid=4v1a

Towards Adaptive and Scalable Context Aware Middleware
www.igi-global.com/chapter/towards-adaptive-scalable-context-aware/63572?camid=4v1a