Norman Fenton[1] and Martin Neil[2]

Visualising your Risks

Making sense of risks by letting them tell a story

Have you ever had to do a project risk assessment and not known where to start? Have you ever looked at a long list of risks and wondered how you could make more sense of it? You probably won't have been helped by the literature on risk assessment. In the first of a series of articles we show you how to visualise your risks by turning them into what is technically known as a causal model, Bayesian net or 'risk map'. It's best to think of risk assessment as telling a story. And it's a story that will help you understand what your risks really are.

1. Typical risks

The following are examples of potential 'risks' that we have seen listed for major IT projects:

- "There are tight budget constraints"
- "The project overruns its schedule"
- "The company's reputation is damaged externally by publicity about poor final system"
- "The customer refuses to pay"
- "The delivered system has many faults"
- "The requirements are especially complex"
- "The development staff are incompetent"
- "Key staff leave the project"
- "Joe Bloggs leaves the project"
- "Joe Bloggs leaves the project causing the customer to cancel the contract because he is the only person they really trust".
- "The staff are poorly motivated"
- "Generally cannot recruit good staff because of location"
- "There is a major terrorist attack"
- "A major terrorist attack wipes out all systems"
- "All backup systems are lost"
- "There is no interaction with customer"
- "Many defects are found during testing"
- "Testing takes longer than expected"
- "Not enough time is spent on requirements capture"
- "Additional time is spent on requirements capture"

From this list it is clear that different experts have different definitions of risk and that risks can be considered at very different levels of granularity and perspective. What some people regard as a risk, others might regard as a *cause*, a *consequence*, a *control* or a *mitigant*. Others still might even regard

[1] (Agena CEO and Professor of Computer Science at Queen Mary, University of London)
[2] (Agena CTO and Reader in Computer Science at Queen Mary, University of London)

it as an *opportunity*. Also, it is clear that some of the above 'risks' are controllable (or can be mitigated against) while others are not.

It is unlikely that anybody will ever produce a definition of risk that is universally accepted, even in a narrowly defined application domain like that of IT projects. What we ***can*** do is produce a set of terms and a simple framework that is both unambiguous in a given context and genuinely useful for decision-makers involved in risk modelling and assessment. We have yet to encounter a risk scenario for which this framework is not applicable.

2. Causal framework for risk

COSO [4] defines a risk as an ***event*** that can have negative impact (and conversely an event that can have a positive impact is an ***opportunity***). The RiskIT definition [6] is much more general, defining risk as:

> *"a possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility".*

We will use the COSO definition because it is clear and simple. But it turns out that the RiskIT definition can be regarded as equivalent using our approach. This will become clear in the accompanying white paper [5] where we look explicitly at how you measure risk.

Since a risk is an event that can have negative impact it follows that such events may be characterised by a causal chain involving (at least) the risk event itself and at least one consequence event (which characterises the impact). Additionally there may be one or more *trigger* events, one or more *control* events, and one or more *mitigating* or inhibiting events. This is shown in the example of Figure 1 (diagrams like this are called *causal models*, *Bayesian nets*, or *risk maps;* we will use the latter term).

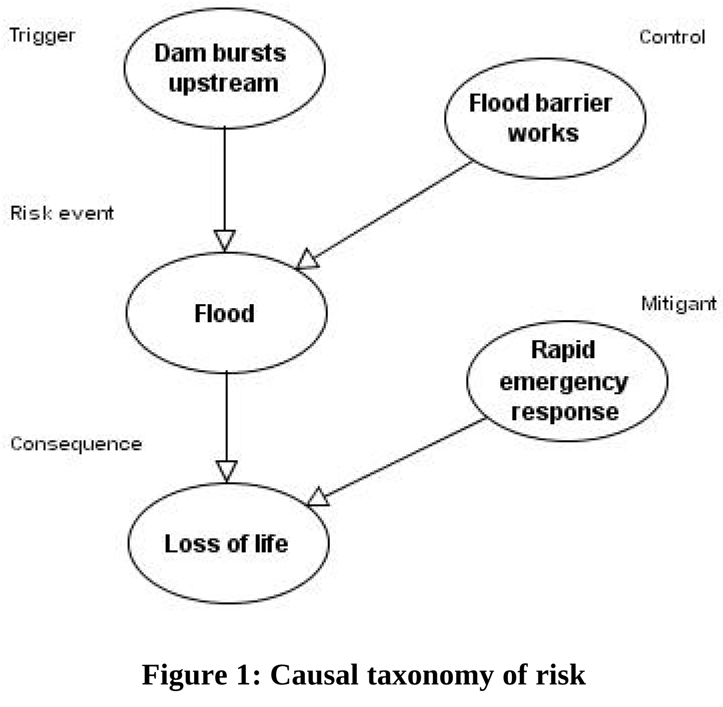

Figure 1: Causal taxonomy of risk

A risk is therefore characterised by a *set of events* as shown. These events each have a number of possible outcomes (in the simplest case you can assume each has just two outcomes *true* and *false*). Of course the 'uncertainty' associated with a risk is not a separate notion (as assumed in some approaches). Every event (and hence every object associated with risk) has uncertainty that is characterised by the probabilities of the event's outcomes. But this is something we cover separately in [5]

Clearly risks in this sense depend on stakeholders and perspectives, but the benefit of this approach is that, once a risk event is identified from a particular perspective, there will be little ambiguity about the concept and a clear causal structure that 'tells the full story". For example, since "Flood" is the risk event (taking the central role in the diagram) the perspective must be of somebody who has responsibility for both the associated control and mitigant. Hence, in Figure 1 the perspective is definitely not that of, for example, a householder in the village, but rather something like the local authority responsible for amenities in the village. A householder's perspective of risk would be more like that shown in Figure 2.

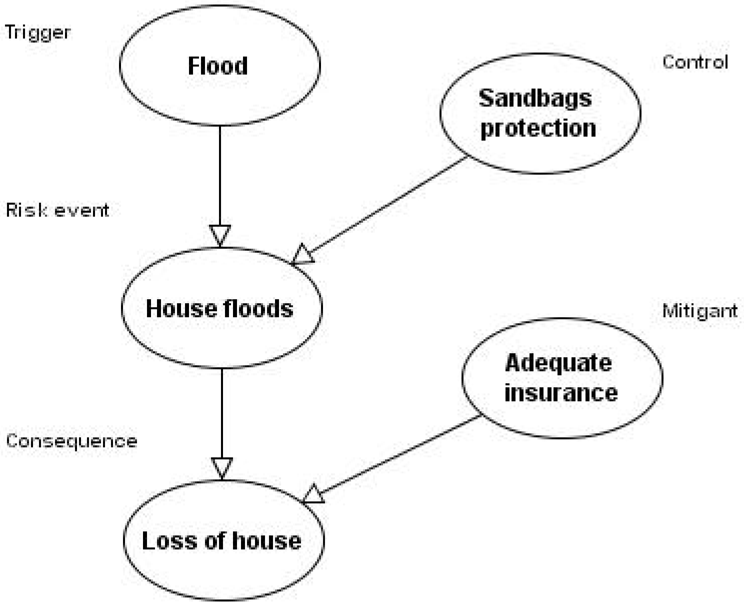

Figure 2: Flood risk from the householder perspective

What is intriguing is that the types of events are all completely interchangeable depending on the perspective. Consider the example shown in Figure 3.

The perspective here might be the Local Authority Solicitor. Note that:

- The risk event now is "Loss of life". This was previously the consequence;
- "Flood" is no longer the risk event, but the trigger.
- "Rapid emergency response" becomes a control rather than a mitigant.

It is not difficult to think of examples where controls and mitigants become risk events and triggers. This interchangeability should be considered a benefit rather than a restriction since it stresses the symmetry and simplicity of the approach.

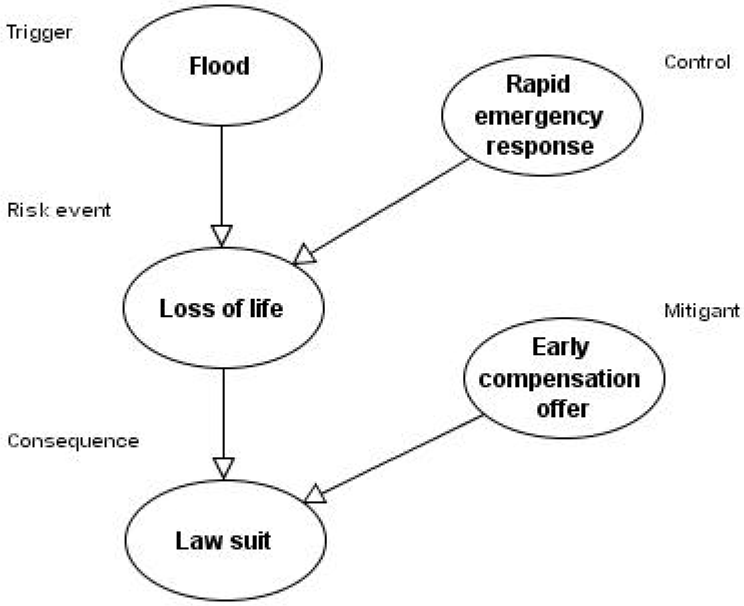

Figure 3: Interchangeability of concepts depending on perspective

3. Building risk maps

Using risk modelling software like AgenaRisk [2] it is possible to build arbitrarily large risk maps based on the above approach. This involves the following steps:

1. Consider the set of risk events from a given perspective
2. For each risk event identify any triggers and/or controls
3. For each risk event identify any consequences and mitigants

To get the risk map to generate quantified risk predictions and other great stuff like *simulation*, *backward reasoning* and *what-if-analysis* you also need to define some probabilities (we look at that in [5] and you will see there that it not only avoids the irrationality that characterises traditional approaches to risk quantification, but it actually makes the whole thing much simpler).

By 'chaining' together different risks we can model multiple risks, risks from different perspectives, and common causes, consequences and mitigants, all within the same model. So you really can turn your risk list into a meaningful story.

4. References and Further Reading

[1] Adams J, 'Risk', Routledge, 11 New Fetter Lane, London EC4P 4EE, ISBN 1-85728-068-7, 1995

[2] AgenaRisk, www.agenarisk.com, 2006

[3] Chapman C and Ward S, 'Estimation and evaluation of uncertainty: a minimalist first pass approach', International Journal of Project Management, 18, 369-383, 2000

[4] COSO (Committee of Sponsoring Organisations of the Treadway Commission), 'Enterprise Risk Management: Integrated Framework', www.coso.org/publications.htm, 2004

[5] Fenton NE and Neil M, 'Measuring Risk', White paper, www.agenarisk.com, 2006

[6] Kontio J, 'The Riskit Method for Software Risk Management', version 1.00, CS-TR-3782, 1997. Computer Science Technical Reports. University of Maryland. College Park, MD, 1997