2B – BACKGROUND INFORMATION

1 REVIEW OF THE ITS AMERICA APPROACH

This chapter provides a brief review of the Risk Analysis methodology used in the US ITS National Architecture programme by its development team. This is probably the only other comparable work that has been carried out recently on Risk Analysis within the area of Transport Telematics.

The US team used an approach consisting of the following three steps: Identify the Risks, Assess the Risks, and Produce Risk Mitigation strategies. Risks were identified by a structured search for a response to the question “What events may reasonably occur that will impede the achievement of key elements of the ITS architecture ?” For each Risk a word description was provided, plus allocation into one of eight categories, definition of the stage in the product life cycle that would be affected, the major sub-systems and architecture components that would be affected, and identification of the stakeholders most likely to bear the Risk.

The next step involved assessing the Risks to assign them a rating. The rating was based on the likelihood of the Risk occurring and the impact if no preventative action was taken. In each case three levels were used comprising High, Moderate and Low. They were then combined and a summary Risk rating determined. The summary rating used a colour coding such that RED was used for the most severe Risk, YELLOW was used for the moderate Risks, and BLUE for those Risks with negligible impact

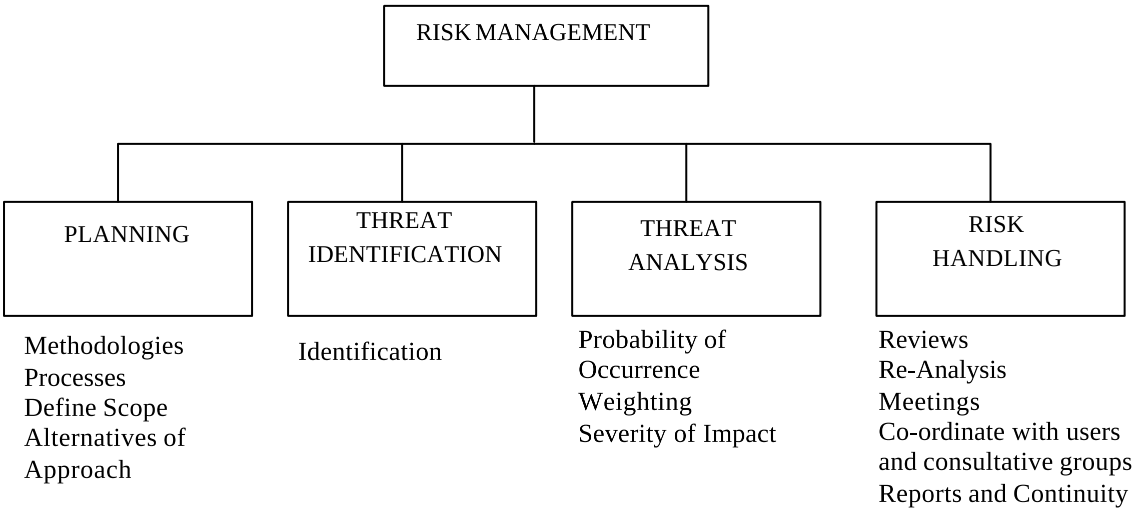
The final step identified the mitigation strategies for each Risk that was rated as RED. The strategies each defined the actions that can be taken to mitigate the Risk, and the organisation that should take responsibility for carrying out the action. The mitigation actions were designed to enable the Risk bearer to reduce or eliminate the Risks.

The process was conducted across the three time frames and three scenarios that the US Architecture was designed to address. It involved an individual definition of Risks and assignment of ratings followed by interactive group review for completion. The same method was employed in the creation of the Risk mitigation strategies.

It is worth noting that at the end of the US ITS Architecture programme a total of 61 Risks were analysed. Of these, ten were classified as RED, thirty six as YELLOW and 3 as BLUE. The only category not represented in the ten RED Risks was Operating Costs & Maintenance. These RISKS were evenly spread across the architectural components, scenarios and time frames. Of the four life cycle stages defined, only Production was not represented and half the ten RED Risks were assigned to the Deployment & Sales stage. Consumers were the largest stakeholder to bear these Risks.

2 THEORY OF RISK

This chapter wants to clarify and define the terms threat assessment, threat analysis and risk management so that communications regarding ″threat″ can be more effective. Risk management consist of four separate but related activities as depicted in the picture below. Risk management is the umbrella title for the processes used to manage threats.



Picture A: Risk management Structure and Activity

1st Step: Planning. The purpose of risk management planning is simply to force organised purposeful thought to the subject of eliminating, minimising, or containing the effects of undesirable occurrences. The Risk Management Approach should describe (declare) the intended approach (specific to the program) for executing the processes of: (1) Threat Assessment; (2) Risk Analysis and (3) On-Going Risk Handling.
2nd Step: Threat Identification. This is the first step in the Risk assessment process. Threats cannot be assessed or managed until they are identified and described in an understandable way. Threat identification is an organised thorough approach to seek out the real threats associated with the program. It is not a process of trying to invent highly improbable scenarios of unlikely events in an effort to cover every conceivable possibility of outrageous fortune.
3rd Step: Threat Analysis. Some organisation and stratification of the identified threats are beneficial. Preliminary quantification is intended to provide some prioritisation of the threats for further evaluation. The process generally becomes more of a top level analysis with the impacts being evaluated against total project/program completion of subsystem changes in the threat input variables.
4th Step: Risk Handling. This is the last critical element in the risk management process. It is the action taken to address the threat issues identified and evaluated in the Risk assessment and threat analysis efforts.