Factors in Technical Risk Assessment

Robbert J. Hamann; Barry T.C. Zandbergen
Delft University of Technology
Aerospace Engineering
The Netherlands
R.J.Hamann@lr.tudelft.nl

3rd European Systems Engineering Conference
Systems Engineering: a focus of European expertise
Pierre Baudis Congress Centre, TOULOUSE, May 21st - 24th, 2002

Abstract. It is a common opinion, that technical risk assessment is an important activity in small and large design and development projects in the space industry. Not only managers profess that belief, but also the engineers within a project agree with that view. It is, however, astonishing to see how rarely a thorough and continuous effort in this field is undertaken in day-to-day project life, especially in small to medium size companies and in small projects.

The paper attempts to identify possible reasons for this phenomenon, based on methods and tools used for technical risk assessment in a medium sized company and on the practice of applying these on a range of projects.

Basic requirements for any method or tool used were that it did not require specialist knowledge, was directly related to the technical content of the work (and hence made sense to the people performing that work) and that it would not become a significant effort to use method or tool within the project. In addition, a necessary condition for acceptance of method or tool was a good introduction into the organization and sufficient support for the users. In addition, it should be possible that method and tool are used directly by the full team. Also company processes have to take the risk assessment into account.

The technical risk assessment methods used are discussed and their main characteristics summarized. The introduction of the methods and tools, and the adaptations initiated on request of the users are described. The results of an evaluation of actual use of the methods and tools within the company are given, as well as the results of a limited check on the positive and negative aspects of method and tool by an out-of-company "control group". Conclusions are drawn relative to possible barriers to the routine application of technical risk assessment in the design and development process.

Based on these findings an tentative approach is defined to arrive at a better acceptance and use of the method and tool by the target group: the engineers performing the design and development work on a small to medium sized project.

INTRODUCTION

Technical risk assessment is considered to be an important activity in design and development projects in space industry, as they are generally dealing with (at least partially) new developments in technology, in application as well as in the design and development process. If risk assessment is properly applied throughout the project life, it enables a proactive attitude and makes it possible to prevent the related problems. Although this is recognized both by managers and engineers, and usually the company rules require such an assessment to be done, it can often be observed that risk assessment is not done explicitly or even not done at all, even if methods and tools to do so are at hand. The paper investigates this phenomenon, based on the practice of technical risk assessment in a medium-sized space company.

First the methods and tools available in the company and the way they have been introduced in the company are described.

The results of a questionnaire on the actual application of technical risk assessment are summarized and the results of an evaluation of the methods and tools by an out-of-company control group are presented.

Possible barriers to the routine application of the assessment are identified and a tentative approach is defined to arrive at a better acceptance and use of the method and tool by the engineers.

TECHNICAL RISK ASSESSMENT METHODS AND TOOLS

History. The company initiated structured technical risk assessment in the early 90's. Before this time risk assessment was mainly linked to the cost and schedule control process, monitoring actual project progress against the planned progress, and translating differences into their probable impact on the project's result. As such there was little, if not any coupling with the technical content of the work. If any technical risk assessment was done, it was done in an implicit and ad-hoc manner.

When the company became an important candidate to become a prime contractor for a large and complex contract, it was decided to initiate a major overhaul of engineering practices and technical risk assessment was one of these. Over the years three different, but related methods were offered:

- A risk assessment method based on the estimate of risk related to individual work packages,
- A simple risk map technique,
- An extension of the risk map technique with more detailed evaluation questions and tool providing quantitative support.

Supporting tools were offered and the term "technical risk assessment" appeared in checklists for proposals and reviews. The methods were included in course material for engineers and finally a specific workshop has been developed to initiate engineers in their application.

Risk assessment related to work packages. The technique [Innovation] was introduced in the early 90's and originated from the cost and schedule control side of the project. It was partly based on the work break down structure of the project and the estimated cost of the related activities. The responsible work package managers were asked to provide a nominal, maximum and minimum estimate of the effort required for each work package. The range minimum-maximum effort was assumed to cover a 99% probability. Statistical processing of these data yielded the total financial risk related to the project and the relative risk related to each work package. These results were used to specify risk mitigation measures and to determine the management reserve required (or the part of the management reserve, which could be shifted to project profit).

A second element in this technique was the characterization of the project in terms of a matrix as shown in figure 1.

	Technical	Social	Economic
External	Many interfaces which can not be influenced		
Project		No "flight" hardware (risk of underestim-ation)	
Internal		Good team spirit	

Figure 1: Project characteristics

The influence of these characteristics on the project hours and cost was also assessed in terms of nominal, minimum and maximum impact and given the same statistical treatment as the work package hours. From it resulted a ranking of the characteristics in terms of risk, which were the basis of risk mitigating actions.

The risk assessment was performed by the controller function of the project, based on inputs from the project team. The assessment process was performed for proposals and sometimes repeated as part of the estimate-to-completion process during the project. It was almost exclusively done for projects of intermediate to large size in the full-scale development phase. The practice was discontinued in the mid 90s, formally because the function of (financial) risk analyst was abandoned.

A clear disadvantage of the technique is the weak relation to the mission and the design of the system under development. This led to weak acceptance of its results within the engineering team. Another disadvantage was the decision to use it only in the later phases of the project, when it is already rather difficult to introduce important design changes.

Simple Risk Map technique. The Risk Map technique is used to identify risks and to rank them in importance [Yates]. To this purpose the system to be developed is split into risk elements (hardware, software, and even programmatics) and to each of these elements a probability of occurrence factor and a severity of impact factor (if the risk actually becomes true) is attached.

Probability of occurrence is defined in terms of Technology Maturity or State of Technology (SOT), ranging from "feasible in theory" to "proven flight design". Severity of impact is set equal to Mission Criticality (i.e. what happens to the mission, if the risk becomes true) and ranges from "low" to "high". Judgments are based on experience of the engineers involved. Figure 2 shows a typical Risk Map.

risk element		RISK MAP			
1	Subsystem A	State of Technology / Technology Maturity	*Feasible in Theory*		**2**	**4, 7**
2	Unit a					
3	Function 1		*Working Laboratory Model*		**3**	
4	Subsystem B					
5	Unit b		*Based on Existing Design*	**8, 9**	**13, 14, 15**	**5**
6	Unit c					
7	Test X		*Extrapolated from Existing Design*	**1**	**10**	**11**
8	Simulation S/W Z					
9	.....		*Proven (Flight) Design*	**6**	**12**	
10						
11						
12						
13						
14				*low*		*high*
15				**Mission Criticality**		

Figure 2: Risk Map

The Risk Map was generally generated by inputs from the full technical team. Risk mitigation concentrates on the risks in the top right corner. Measures are taken to move them down (accelerating -partial- development) or to the left (design change);

the technique offers in this way a clear indication, which actions are required to mitigate a risk.

The technique was introduced in 1991 [Fokker Space]. Practical experience showed that the technique works easily and is a good tool to disseminate the knowledge of priorities. Engineers appreciate its use, because they handle the risk assessment themselves. However, it appeared mandatory to redefine the Mission Criticality in terms meaningful to the particular project, and it was preferred to link it at least to the results of a preliminary FMECA in terms of failure consequences. In addition there was generally a strong desire to reword or amplify the State of Technology factor also to a more meaningful sense or to introduce other than technical aspects (e.g. the aspects as addressed in figure 1). This was one of the reasons to refine the technique.

Quantitatively supported risk assessment. In 1998 the company was evaluating a set of Systems Engineering techniques and tools (CASETS, Computer Aided Systems Engineering Tool Set, developed and marketed by Rockwell International, later Boeing) on applicability in its engineering processes [Rockwell, 1996; Elseth, 1998]. Contained in this package was a technical risk assessment technique and supporting tool in MS Excel®, which resembled very much the simple risk map tool, that had been used up to that moment. Additional features, making the risk assessment more explicit, were:

- The risk category State of Technology or Technology Maturity (SOT) factor had been amplified by a Design Engineering Difficulty (DED) factor, related to the complexity of the risk element. SOT and DED are combined into a Technical Risk Index TRI.
- Five factors in risk categories related to production and test had been added:
  - Manufacturing Process Difficulty (MPD),
  - Production Equipment Status (EQI),
  - Personnel Resource Status (PER),
  - Material Resource Status (MAT),
  - Test Resource Status (TST).

  MPD, EQI, PER, MAT and TST are combined into a Manufacturing Risk Index MRI.
- A specific set of risk categories for software items (separate spreadsheet) was provided,
- For each of the risk categories a checklist relating the status of the risk element within the category to a rating was provided,
- The relation between these new risk categories, resulting in an overall probability of the risk related to a risk element, was quantitatively given, based on practical experience.

Severity of impact of development failure was expressed, as in the simple risk map, as Mission Criticality, but supported by a more extensive checklist (figure 3).

The full algorithm for the probability of failure (Development Difficulty Risk Index, DDI) is:

$$TRI = \frac{SOT \cdot DED}{risk\ categories\ included}$$

$$MRI = \frac{MPD \cdot (EQI + PER + MAT + TST)}{risk\ categories\ included}$$

$$DDI = TRI + MRI - TRI \cdot MRI$$

Total risk is expressed as:

$$Risk\ index = DDI \cdot severity\ of\ impact$$

An example of a checklist behind one of the risk categories (State of Technology) and the Mission Criticality (severity of impact) is shown in figure 3.

Rating	State of Technology (SOT). Actual application in your project may be different from ref. application => adjust your rating. If applied in different mission context: increase rating by +1.
0	Currently operational and deployed
1	Manufacturing process defined
2	Prototype hardware passed qualification tests
3	Prototype hardware in test, passed performance requirements
4	Brass board fabricated and tested for performance and qualification
5	Critical function/characteristics demonstrated at breadboard
6	Concept design tested for performance and qualification concerns
7	Concept design formulated for performance and qualification
8	Scientific research on-going

Rating	Performance Consequences (Mission Criticality)
0.1	Negligible: Failure to meet the requirement would create inconvenience or non-operational impact. Reduction in technical performance
0.5	Marginal: Failure to meet the requirement would result in degradation of the secondary mission. Minimal to small reduction in technical performance.
0.7	Critical: Failure to meet the requirement would degrade system performance to a point where mission success is questionable. Some reduction in technical performance
0.9	Catastrophic: Failure to meet the requirements would result in mission failure. Significant degradation/non-achievement of technical performance

Figure 3: Ratings for risk category State of Technology and severity of impact Mission Criticality

The tool has been evaluated on its applicability by a graduate student [Elseth, 1999] and by a number of experienced systems engineers of the company. Conclusions of the evaluation were:

- The risk categories defined in the tool were also representative for the company, but checklists had to be adapted to European references,
- The quantitative factors (ratings) related to the checklists were representative,
- It should be possible to make the checklist for State of Technology project specific (e.g. equate "Brass board fabricated and tested for performance and qualification" to "Validated by detail test; experience from other non-space programs"),
- It should be possible to exclude each of the risk categories, without losing the normalization function in the algorithm[1],
- Outputs should be possible in the same form as the risk map.

These modifications were introduced in the tool and it was made available to the engineering community at the company [Hamann, 1999]. In a later phase an option was build in to offer the choice between severity of impact in terms of Mission Criticality, Schedule or Cost, their average or their worse case impact. Figure 4 shows typical results of a risk assessment with this technique.

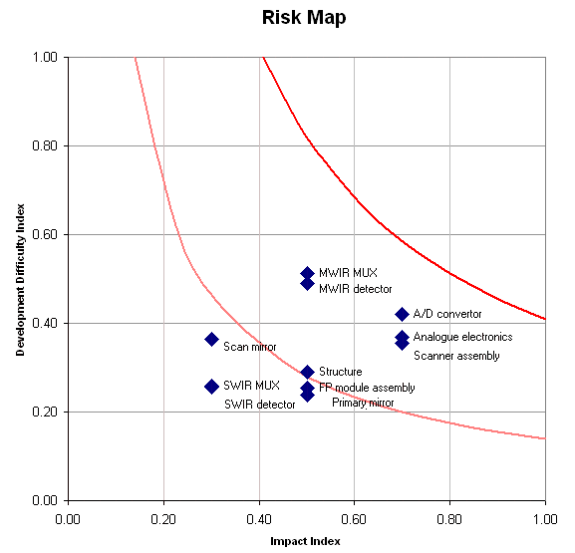

Figure 4: Risk Map with quantitatively supported technique

To familiarize the engineering community with the technique and the tool specific workshop were organized. In its final form the tool was appreciated for its completeness -the checklists addressed all aspects of importance- and the easy means it provided to do sensitivity studies. Outputs of the tool generally gave very direct indications whether a design change or a specific change in development approach were most effective. The Risk Map was generally generated by inputs from the full technical team.

RISK ASSESSMENT QUESTIONNAIRE

In 1999 the application of technical risk assessment within projects has been evaluated in the company as part of a general evaluation of Systems Engineering practices. This has been done by means of a questionnaire. The questions asked in relation with risk assessment were:

- *Has been explicitly documented, that a technical risk assessment will be done?*
- *Has that technical risk assessment been performed and when has it been performed?*
- *Can you indicate, whether the deletion or poor execution of technical risk assessment has had negative consequences for the project?*

The risk assessment techniques available to the projects at the time of the questionnaire were the simple risk map and the quantitatively supported risk assessment, the risk assessment related to work packages having been abandoned by then.

Fourteen projects responded, ranging in average size from 1 to 70 full-time equivalent staff and ranging in project duration from 2 to 47 months since kick-off. An overview of the response by these projects is shown in figure 5.

	Number of projects	14	100%
	Project size (full-time equivalents)	1 to 70	
	Projects in phase A/B[1]	10	
	Projects in phase C/D[1]	9	
	risk assessment planned	5	**36%**
risk assessment performed[1]	**never**	5	**36%**
	in proposal phase	4	**29%**
	in Project Planning Phase (after contract award)	5	**36%**
	for Project reviews	1	**7%**
	each 6 months[2]	5	**36%**
	each 3 months	1	**7%**
	poor risk assessment had negative consequences	2	**14%**
	normative number of risk assessments, assuming once per 6 months	49	100%
	number of risk assessments actually performed	23	**47%**

[1] Overlap possible

[2] After processing

Figure 5: Questionnaire response

No significant distinction between large and small projects or projects in early or late phases of the

[1] The original tool did not adapt the normalization, when a risk category was excluded; as a consequence the total risk decreased when that was done.

project life cycle was found. Remarkable is, that only five projects explicitly planned the performance of a technical risk assessment, although company procedures and proposal and review checklists prescribed, that such an assessment must be done. The other nine projects did not plan to do a risk assessment, but five of these projects still decided to perform a risk assessment. Two projects reported, that not performing the activity (to a sufficient extent) had had negative consequences for the project. One of these projects stated that a risk assessment certainly would have identified and appreciated this risk.

The remaining projects planned risk assessments and actually did execute them. One project planned risk assessment, but did not perform it in the 17 months the project had been running.

Compared to a tentative norm, that a risk assessment has to be done at least once per 6 months to be effective, only four projects managed to do so, while averaged over all projects only 47% of the total number of risk assessments was done. This figure rises to 68%, when the projects that had not planned risk assessments *and* did not do them are eliminated.

This unsatisfactory performance may partially be explained by the fact, that the company organization has been transformed in the 90s into a more and more strongly profit-oriented business unit organization, where engineering processes were reduced to the bare minimum.

The questionnaire did not explicitly ask for the reasons why risk assessment was not or less extensively done. Still a number of projects volunteered a rationale, mostly in the sense that risk was implicitly taken into account in the design process.

Personal interviews in another context revealed that the reason for doing or not doing a risk assessment were a strong function of the personal interest of the (systems) engineer. Also, sometimes bad news in the future was appreciated less than bad news now. It also appeared, that execution of a risk assessment was often prompted by request from reviewers external to the project. And, as always, today's pressures have more priority than seemingly less urgent, structured activities.

EVALUATION OF POSITIVE AND NEGATIVE ASPECTS

To investigate, whether the risk assessment technique and related tool possibly plays a role in the bad "discipline" in performing risk assessment an out-of-company experiment was set up in the spring of 2001. As part of the assignment for a graduate course in Space Systems Engineering at the Delft University of Technology the students were asked to do a risk assessment for their project, and to report explicitly inconveniences of the technique and to recommend potential improvements. Time available for the risk assessment was 16 hours, including the generation of a project description. The quantitatively supported risk assessment technique was made available to them to this purpose.

The group of students was composed of regular graduate students and of professionals from space and civil engineering industries. The group of graduate students could be considered as a group well qualified to observe undesired characteristics of the tool due to their limited burden of "usual project practices". The professionals are considered to be good evaluators of the match between technique and tool and the technical content of their work. Figure 6 summarizes the answers of both groups to the questions.

professionals	no. of professionals	8	100%
	no. of responses	*4*	*50%*
	tool/technique is easy to use	2	
	results answer common sense	2	
	interfaces with/interference from other projects not covered	1	
	firmer relation of Mission Criticality with consequences of FMECA required	1	
	tool should explicitly assess the level of expertise of the user	1	
	tool allows a probability of occurrence and impact of 0%, which is not possible	1	
	domain/application knowledge is needed to perform correct rating	1	
	new category interconnectivity required	1	
	project specific ratings decrease objectivity of the tool	1	
	better User Instructions to be build in the tool	1	
	ratings to be made project specific	1	
students	no. of students	15	100%
	no. of responses	*10*	*67%*
	tool/technique is easy to use	5	
	results answer common sense	1	
	SOT rating easiest to apply	3	
	domain/application knowledge is needed to perform correct rating	4	
	new category interconnectivity required	1	
	allow any combination of cost, schedule and mission criticality impact	1	
	tool shows some hick-ups	3	
	better User Instructions to be build in the tool	2	
	stand-alone program prefered	2	

Figure 6: Out-of-company evaluation

The results may be summarized as follows:

- Using technique and tool requires sufficient domain and application knowledge of the assessor. Even if a professional uses the tool, an assessment of his expertise in all aspects of relevance is recommended. Generally, it is recommended to involve all technical disciplines within the team in the risk assessment.
- Improve flexibility of the tool.
- Consider the inclusion of effects related to interference from other projects and interconnectivity.
- Consider an implementation as a stand-alone program.

Hardly any indication has been found that the

technique or tool could be the exclusive cause of the unsatisfactory performance of technical risk assessment observed in actual project practice.

CONCLUSIONS

Risk assessment questionnaire. Although the company rules prescribed, that regular technical risk assessments had to be done for each project, only 36% of the projects evaluated did plan a risk assessment and 64% did actually perform it. One project planned a risk assessment, but still had to perform its first one 7 months after kick-off. Risk assessments were performed with about each nine to twelve month average, while 6 months intervals are considered to be an acceptable time span.

Reasons for not performing the risk assessment were mainly related to the culture within the company and the projects; in a number of cases projects considered it sufficient to perform the activity implicitly during the design. None of the projects reported defaults or inconveniences related to assessment techniques or tools.

Only 14% or two projects reported negative effects due to the lack of risk assessment in the questionnaire, although more projects experienced unforeseen problems.

Out-of-company evaluation. The technical risk assessment technique and supporting tool was judged to be easy to use. The professional evaluators suggested a number of improvements, which did not always go in the same sense. The student evaluators were considerably more critical towards the technique and tool. A number of times the need for sufficient domain and application knowledge was stated to be very essential (which is not surprising). No indications were found, that the method or tool might be a cause for not regularly performing a technical risk assessment.

Suggested improvements. In summary the following improvements to technique and tool are suggested:

- Improve the relation of Mission Criticality with (preliminary) FMECA results (failure consequences).
- Add a method to assess explicitly the expertise of the user of the technique and tool.
- Consider the inclusion of a factor reflecting the interference from other projects.
- Improve the way a probability of 0% is handled by the tool.
- Allow project specific rating definitions, if desired.
- Include the explicit effect of interconnectivity in the method.
- Allow any combination of mission, cost and schedule impact categories.
- Consider a stand-alone program instead of a MS Excel implementation.

Although there is no firm indication, that it is essential to improve the method and tool, it seems recommended to include a number of the suggested improvements, as they certainly will increase the flexibility of application.

NEXT STEPS

The proposed research project will include the following steps:

1. Perform a literature review of risk assessment methods and techniques, which:
   - Do not require specialist knowledge,
   - Are directly related to the technical content of the work,
   - Will not become a significant effort to use within the project,
   - Can be used directly by the engineers performing the work.

   Investigate also which management and educational support was judged to be needed.
2. Generate a description of a method, which includes:
   - The improvements listed in the section conclusions of this paper,
   - Any useful outcome of the literature review.
3. Submit this description to two or three small to medium aerospace companies for evaluation.
4. Agree a basic form of the method for implementation within those companies, including supporting tool(s) required. Agree also the management measures and educational support needed for the introduction.
5. Introduce the method on a limited number of projects of different size and at a different time in the project life cycle within these companies.
6. Evaluate the results and fine-tune the method and supporting tool.

The results of the implementation of method and tool in the companies should provide

- A substantiated judgment about the applicability of method and tool,
- A substantiated judgment about an acceptable frequency of risk assessment,
- Conclusive evidence as to the real reason for performing or not performing a structured and regular application of technical risk assessment.

ACRONYMS AND ABBREVIATIONS

DDI	Design Development Index
DED	Design Engineering Difficulty
EQI	Production Equipment Status
FMECA	Failure Mode Effect and Criticality Analysis
MAT	Material Resource Status

MPD	Manufacturing Process Difficulty
MRI	Manufacturing Risk Index
PER	Personnel Resource Status
SOT	State of Technology
TRI	Technical Risk Index
TST	Test Resource Status

REFERENCES

Elseth, B.O., "An Evaluation of an Integrated Systems Engineering Tool". MSc Thesis, Delft University of Technology, Faculty of Aerospace Engineering, January 1998.

Elseth, B.O. and Hamann, R.J., "An Evaluation of Risk Management Tools". *The Cost Engineer, Journal of the Association of Cost Engineers*, April 1999.

Fokker Space, Systems Engineering Course Lecture Notes. Fokker Space, Leiden, the Netherlands, 1999.

Hamann, R.J., "RISK$, Risk Assessment Tool for Hardware and Software". User Manual, Fokker Space, Leiden, the Netherlands, 1999.

Innovation-Strategi-Management, Decision System with Future Evaluation. Innovation-Strategi-Management, Copenhagen, Denmark, 1989.

Rockwell International, CASETS User Manual. Rockwell International Corporation, USA, 1996.

Yates, D., "Introduction to Systems Engineering at BASG". Lecture notes, Ball Aerospace, Boulder, USA, 1990.

Robbert Hamann received an Aerospace Engineering education at Delft University of Technology in the Netherlands and Princeton University Graduate School, USA. From 1974 to 2000 he worked at Fokker Space, Leiden, the Netherlands as an Engineer and Systems Engineer for many space projects. From 1990 he has been in charge of introducing, developing and maintaining the Systems Engineering methodology at Fokker Space. Since that time he has been a visiting lecturer on the subject at the Delft University of Technology, the University Twente in the Netherlands, and the Ecole des Mines de Nantes in France. Since February 2000 he is employed at the Delft University of Technology as Coordinator Space Systems Engineering and Senior Lecturer.

Barry Zandbergen received an Aerospace Engineering (1986) and a Space Systems Engineering (1998) education at Delft University of Technology. From 1986 to 1987 he worked at the Ministry of Defense, The Hague, the Netherlands. Since September 1987 he is employed at the Delft University of Technology as assistant professor in the field of rocket propulsion 1987-1992, advanced launchers 1992-1996, and since 1996 in the field of space systems engineering and, again, rocket propulsion.