M-RAT: Using Rapid Risk Assessment Techniques to Combat Degraded Modes of Operation

Chris W. Johnson

School of Computing Science, University of Glasgow, Glasgow, UK, G12 8RZ.

Abstract

Risk assessment techniques have supported the development of many complex, safety-critical systems. Unfortunately, many existing tools are costly and time consuming. In consequence, they are typically only applied during development projects or during major system upgrades. They cannot easily identify the hazards that undermine everyday operations. This is a significant concern because engineers and management must continue to find work-arounds for degraded modes of operation when safety-related applications fail to meet their intended requirements. In contrast, this paper presents a range of low cost techniques that can be used to support 'rapid risk assessment'. The intention is to provide front line staff with the tools that are necessary to anticipate the everyday hazards that often combine to undermine safe and successful operation. It is argued that these concerns are particularly important in military applications where manufacturers often make inappropriate assumptions about the operational environments for the systems that they deliver.

Introduction

Risk assessments have guided decision making across a wide range of industries. For example, IEC 61508 supports the development of programmable systems in safety-critical process applications. DO-178B advocates the use of risk management during the development of avionics. ISO 27001 introduces risk assessment as a key component of security systems. ISO 14971 describes the application of these techniques to support the design and acquisition of clinical devices. Common to all of these standards is the assumption that we can increase safety by mitigating the consequences or reducing the likelihood of hazards.

This paper focuses on the application of rapid risk assessment techniques within military organisations. Hazard analysis has gradually been extended across strategic, tactical and operational planning in many armed forces (Johnson, 2011). For instance, the Chairman of the Joint Chiefs of Staff provides Congress with an assessment of the risks facing US military interests each year. The Secretary of Defense may then be asked to identify the mitigation measures that the Pentagon will use to address potential hazards. Similarly, risk assessment techniques have been used to guide a range of tactical decisions, including procurement initiatives under the Enterprise Risk Assessment Methodology (ERAM). This approach is intended to reduce systemic risk and support informed decision making by identifying program vulnerabilities in military information management. At an operational level, the development of Composite Risk Management processes has had a profound impact on decision making (Johnson, 2007). This is intended to ensure that all Army personnel have an introduction to hazard identification and mitigation as ways of avoiding mishaps both on-duty and off-duty.

Strengths and Weaknesses of Military Risk Assessment

A number of techniques have been developed to support strategic, tactical and operational decision making. For instance, US Military Standard (MIL-STD) 882D presents an eight stage process for risk management. Firstly, it is necessary to document the application of this technique, for instance using hazard tracking software. Without appropriate documentation, it can be difficult to determine whether hazards have been adequately addressed. The second stage identifies potential hazards. This process must extend across the system lifecycle to consider installation and decommissioning. Analysts must also account for interactions between a military system, its users and their environment. The third stage within MIL-STD 882D assesses the risks associated with each hazard in terms of severity and probability, using a risk matrix. The fourth stage of MIL-STD 882D's systems approach to risk management identifies mitigation measures; "Risk mitigation is an iterative process for eliminating or reducing risk to the lowest acceptable level within the constraints of operational effectiveness and suitability, time, and cost". Risk reduction techniques include hazard elimination through the development of appropriate designs. For example, the use of non-flammable materials can potentially eliminate the risk of fire. The standard also described how procedures and training can be used to mitigate risks by preparing staff for adverse events. The fifth stage involves the selection and implementation of appropriate mitigation techniques. This must also consider the costs associated with different interventions. The sixth stage verifies that the

intended risk reduction has been achieved. This raises a host of problems. For hazards with a relatively low likelihood it may not be possible to observe direct evidence that mitigation measures will continue to provide the anticipated level of protection. In such cases, monitoring and inspection must be supported by analysis and testing techniques. The penultimate stage ensures that all stakeholders in a project understand and accept the residual risks after any mitigation has been implemented. In particular, the certifying or approving authority must recognise any remaining hazards. The eighth and final stage of the MIL-STD 882D system safety process focuses on the management of risk after deployment; "the life-cycle effort shall consider any changes to the interfaces, users, hardware and software, mishap data, mission(s) or profile, system health data, and similar concerns".

MIL-STD 882D provides a framework for safety within military systems. The scope of the standard is deliberately broad. It applies to all DoD systems and to all facilities. As mentioned above, it is intended to address all phases of the systems life cycle; from design through implementation to validation and verification operation, maintenance, modification and disposal. However, the broad scope of 882D creates numerous problems. It can be difficult to apply to particular projects, especially those involving software. Human factors issues are not easily captured by standard risk assessment techniques. A further issue is that 882D only provides a framework for systems safety. Development teams must then select the more detailed techniques that are to be used within each of the eight processes identified in the previous paragraphs. Most of these techniques were not intended for military systems. Brevity prevents an exhaustive analysis of more detailed risk assessment tools, for more information see Johnson (2011). In contract, the following sections summarise experience from the application of HAZOPS and FMECA to military systems.

Hazard and Operability Studies (HAZOPs) help analysts to identify potential hazards and then assess their potential impact. Although it was initially developed in the process industries it has subsequently been used by a number of armed forces. For example, the former UK Ministry of Defense (MoD) Defence Standard 00-58 supported the application of HAZOPS in software control systems. The US Army has used HAZOPS to manage the risk associated with commissioning, operating and decommissioning a wide range of systems including nanotechnologies (Woodward-Clyde, 1992, US Army 2009). The approach starts by identifying the major functions in a potential system. Each function is associated with a set of requirements or intentions. For instance, a personal radio system should provide point to point communications over 500 square meters for 256 channels with up to 20 hours continual use. The HAZOPS team then goes on to consider what would happen if the component deviated from its intended operating parameters. They must also identify the causes for each possible deviation. The HAZOPS team must determine whether the consequences of any failure threaten safety. If this is the case then additional mitigations must be introduced. The success of the approach is built around a series of guidewords that helps analysts identify potential deviations. For instance, 'Before' prompts the analyst to consider what would happen if a function occurred before the intended point in a sequence. 'After' focuses on what would happen if a function occurred after the intended point in a sequence. Other guidewords include Early, Late, No or Not, More, Less, As Well As, Part Of, Reverse and Other Than. Guidewords can be combined during a HAZOPS analysis. For instance, 'No or Not' can be combined with 'Early' to consider failure scenarios in which the battery supply of a personal radio system failed to meet the intended endurance. The key point is that the guidewords help to direct hazard analysis within the wider risk management processes.

The next phase of the HAZOPS approach identifies the causes that could result in a particular failure. This is important because there may be additional constraints, for example from the underlying physics, which prevent a problem from arising. HAZOPS teams must then identify potential consequences. This creates considerable problems for military applications. The impact of a potential hazard often depends upon the context of use. For example, the consequences of losing a personal radio system will depend upon a host of mission-specific factors. These problems can be addressed by ensuring that HAZOPS teams draw upon a range of stakeholders with operational experience. It is also important to study any existing mishap information to determine the consequences of previous failures. After the causes and consequences of a hazard have been determined, teams must identify potential mitigations. Any potential changes must be subjected to a further round of HAZOPS analysis before they are implemented. The guidewords must be applied to the revised functional design to ensure that the mitigating actions have not introduced any new hazards. Further problems arise because this approach provides relatively limited support for the analysis of knock-on failures. A particular hazard might, in turn, trigger a more serious failure in another area of a complex system. It is for these reasons that a number of military organizations have used variants of FMECA.

Failure Modes, Effects and Criticality Analysis (FMECA) has been embedded within military standards, handbooks and technical manuals (US Army, 2006). The approach begins by developing functional block

diagrams to provide a high level overview of system processes, similar to the opening stages of HAZOPS. It is important to identify a range of mission profiles that could impose additional requirements on subsequent implementations. The next stage considers different failure modes for each function or component. For example, 'untimely operation' considers what would happen if a function occurred either earlier or later than the intended time or point in a sequence. A 'failure to operate when required' considers what would happen if a function did not occur at all and so on. The results of this analysis are, typically, recorded in a matrix where each row is used to denote a function or component. Each column represents a particular failure mode. This ensures that the same set of failure modes are considered for each part of an application.

The analysis proceeds by examining each row in the matrix. The cells are annotated to indicate the consequences of each failure mode on the component referred to in the corresponding row. These are the 'effects' mentioned within the name of the approach. They include the total failure of a system as well as degraded modes of operation. Cells in the matrix may also be annotated to show that there is no effect. These annotations are then used to prioritize design changes. This is done by calculating the risk associated with the failure mode for each cell in the matrix. The level of risk is derived from the product of severity and likelihood. This helps to distinguish low severity, improbable failures from higher consequence, more probable hazards. Any failure modes that continue to pose an unacceptable risk should become the target for mitigation. Variants of the initial FMECA process have proposed Risk Priorty Numbers (RPN) as a more elaborate means of calculating risk. These RPNs are derived from the product of detectability, likelihood and severity; where each is measured by a scale from 1 to 10. From this it follows that the highest RPN is 10x10x10 = 1000; the failure is impossible to detect, very severe and the occurrence is almost sure. However, the ranking process is the same irrespective of whether RPNs are used or risk is calculated using the product of consequence and likelihood. The final stages of FMECA identify recommendations for the high-priority failure modes derived from the previous risk computations. For example, design changes can be introduced to help end users identify a potential failure. Alternatively, analysts may recommend the redesign of critical functions or the introduction of components with higher known levels of reliability. It is important to document the output from each stage to support external, independent audit.

As with HAZOPS, there are a number of limitations with FMECA. The scope of the associated documentation can rapidly become overwhelming as analysts are forced to consider a large number of trivial or irrelevant failure modes. It is also hard to represent combined failure modes that simultaneously affect several different components/functions. FMECA can be resource intensive, requiring considerable training. Both HAZOPS and FMECA support large-scale military procurements. However, they provide little help for the tactical and operational risk assessments that are increasingly needed to inform counter insurgency and peacekeeping operations. There is no time to complete an FMECA matrix when you are under fire.

An Overview of Military - Rapid Risk Assessment Techniques (M-RAT)

Rapid risk assessment techniques have been developed to address many of the caveats and criticisms of conventional approaches such as HAZOPS and FMECA. They are not intended to entirely replace these approaches that are still appropriate for strategic procurement processes where time and resources are not significant barriers to their application. In contrast, rapid approaches are intended to provide low cost support for decision making in tactical and operational contexts where the focus is on finding a satisfactory solution without necessarily exhaustively searching for an optimal solution. This might seem like a surprising objective. However, even with additional resources the application of conventional risk assessment techniques cannot guarantee the absolute safety of any complex system.

A second motivation for the development of rapid risk assessment techniques is to address many of the criticisms that were raised in the Haddon-Cave (2009) report on the factors that contributed to the loss of a UK Nimrod aircraft in Afghanistan. This report identifies a number of short comings in the risk management processes that were intended to protect military personnel. The accident occurred when a leak developed during midair refuelling; fuel accumulated in the bomb bay where it was ignited by either an electrical fault or hot air leaking from a heating pipe. Arguments were made that these hazards might have been identified by more sustained risk assessments; "If the Nimrod Safety Case had been prepared with proper skill, care and attention, the catastrophic fire risk to the Nimrod MR2 fleet represented by the Cross-Feed/Supplementary Conditioning Packduct and Air-to-Air refuelling would have been spotted and XV230 would not have been lost". Previous guidance had advocated a systematic approach to the quantification of probability and consequence to support but not replace 'sounds judgement'. However, the subsequent review argued that the accident stemmed from "incompetence, complacency and cynicism" at various stages in the life of the aircraft. Haddon Cave went on to

argue that "there is no evidence that the MOD takes, or is able to take, a measured, broad, pan-MOD view on risk across all platforms, operations and lines of development to ensures that limited resources are used to best effect to reduce the net Risk to Life. Instead, the MOD tends to focus and spend its money in making individual pieces of equipment (*e.g.* aero-engines) extremely safe, which means that it does not have the resources to spend on other measures which might significantly reduce the overall net Risk to Life (*e.g.* collision avoidance systems such as TCAS or additional spares). This imbalance is caused by myopia and a poor appreciation of the total risk picture. The result is that resources are not targeted as effectively as they might be". He went on to advocate the development of consistent risk matrices to be used across all UK military operations. He also recommended the development of consistent practices that might support comparisons across a range of different operations.

Rapid risk assessment techniques build on may of the observations within the Haddon Cave (2009) report. They are intended to extend the scope of risk assessments from major procurement decisions and equipment updates to cover all aspects of military operations. This is particularly important given that for many armed forces the highest risks come from privately operated vehicles. This extension of risk assessment techniques builds on exisiting initiatives across the US Army, such as the development of Composite Risk Management (2007). By focussing on low cost techniques, it is hoped to support assessments in situations where it is not possible to ensure the dedicated support of personnel with training and experience in the application of more exhaustive risk assessment techniques. Above all, the provision of lightweight techniques that can be applied at all levels of a military organisation will support a bottom-up approach to risk assessment that will provide the 'total risk picture' that would be prohibitively expensive using FMECA or HAZOPS. The flexibility of rapid risk assessment tools should also enable rapid updates as the operational environment creates new hazards over time; an aspect that was arguably under-represented in the Haddon Cave report.

There are further differences between the approaches advocated in this paper and those proposed within the UK report. Haddon Cave (2009) cited studies following the Columbia accident that were intended to demonstrate the problems that can arise from abbreviated risk assessments; "When engineering analysis and risk assessments are condensed to fit on a standard form or overhead slide, information is inevitably lost". In contrast, we would argue that more information can be obscured in risk assessments that run to several hundreds of pages of analysis. The development of rapid risk assessment techniques is intended to provide an initial overview of them potential hazards from military operations. These initial overviews can then trigger more detailed studies of the sort envisaged by Haddon Cave and by existing standards such as MIL STD 882D.

Case Study One: Risk Directed Decision Forms (RD-FORMS)

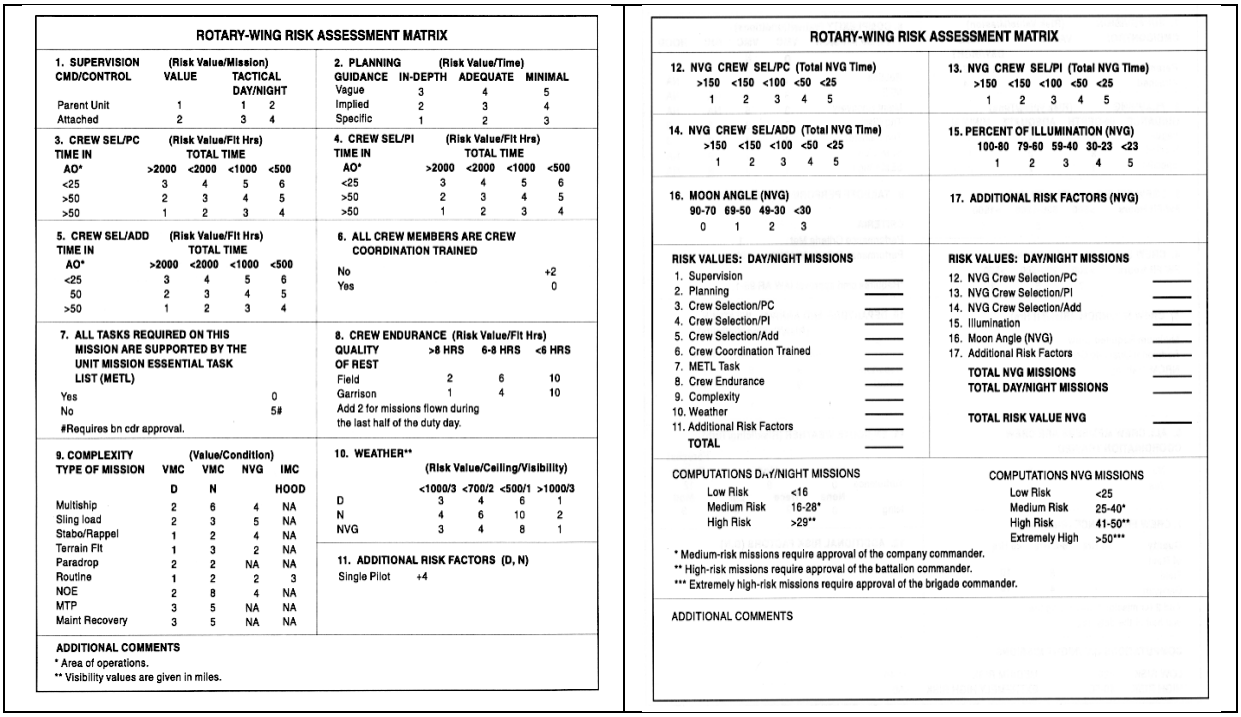
It is important to state that the approaches advocated in this paper have been gathered from a number of existing initiatives. The key point is to gather together 'leading practices' that embody a number of common principles or objectives. The principles of rapid risk assessment can be summarised by the following list. It is regrettable that these attributes are seldom demonstrated in nmore complex approaches to risk assessment:

1. *Consistency;* Rapid risk assessment techniques should encourage consistency between different 'analysts' looking at similar incidents;
2. *Repeatability;* Rapid risk assessment techniques should encourage repeatability where the same 'analyst' identified similar findings for similar incidents looked at over a period of time;
3. *Economy;* Rapid risk assessment should not require more than one day's training in safety management or hazard analysis.
4. *Validity;* Rapid risk assessment techniques should be confirmed and refined using all available information about previous accidents and incidents;
5. *Applicability;* Rapid risk assessment techniques should be applicable to operational tasks and must support everyday decision making.

As mentioned, there are several existing examples of rapid risk assessment techniques that have already been used across a range of military organisations. Figure 1 provides an example from US Army doctrine. In this case, personnel must complete the form to identify some of the hazards that can complicate the retrieval of a rotary winged aircraft from the battlefield. Before performing such an operation, teams must look at the various fields in the form to identify a scoring for the potential risks that might be involved. For instance, the first question asks whether or not the operation is being conducted by a single 'home unit'. If it is not and other groups are involved then this is associated with a higher risk score. Similarly, if the operation is conducted at night rather than during the day then the overall cumulative risk score will be increased. The individual scores

are approximations derived from expert judgement but informed by an analysis of mishap reporting systems. However, the key issue is that the values are indicative and simple rather than precise measures of probability or consequence.

This approach has numerous benefits. In particular, by listing the range of risk factors the developers of the form can encourage consistency in the decision making process; the first principle of rapid risk assessment. A further benefit is the construction and maintenance of the form is itself a useful discipline. Clearly one cannot develop forms for every possible military operation. More flexible alternatives are considered in the next section. However, by identifying a small number of high-risk operations as a focus for form development it is possible to alert personnel to the potential hazards for these particular actions. It should also be apparent that the simplicity of this approach will support the third principle of economy.



ROTARY-WING RISK ASSESSMENT MATRIX

1. SUPERVISION CMD/CONTROL (Risk Value/Mission)

	VALUE	TACTICAL DAY/NIGHT
Parent Unit	1	1 2
Attached	2	3 4

2. PLANNING GUIDANCE (Risk Value/Time)

	IN-DEPTH	ADEQUATE	MINIMAL
Vague	3	4	5
Implied	2	3	4
Specific	1	2	3

3. CREW SEL/PC TIME IN AO* (Risk Value/Flt Hrs) TOTAL TIME

	>2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

4. CREW SEL/PI TIME IN AO* (Risk Value/Flt Hrs) TOTAL TIME

	>2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

5. CREW SEL/ADD TIME IN AO* (Risk Value/Flt Hrs) TOTAL TIME

	>2000	<2000	<1000	<500
<25	3	4	5	6
50	2	3	4	5
>50	1	2	3	4

6. ALL CREW MEMBERS ARE CREW COORDINATION TRAINED

No	+2
Yes	0

7. ALL TASKS REQUIRED ON THIS MISSION ARE SUPPORTED BY THE UNIT MISSION ESSENTIAL TASK LIST (METL)

Yes	0
No	5#

#Requires bn cdr approval.

8. CREW ENDURANCE (Risk Value/Flt Hrs)

QUALITY OF REST	>8 HRS	6-8 HRS	<6 HRS
Field	2	6	10
Garrison	1	4	10

Add 2 for missions flown during the last half of the duty day.

9. COMPLEXITY TYPE OF MISSION (Value/Condition)

	VMC D	VMC N	NVG	IMC HOOD
Multiship	2	6	4	NA
Sling load	2	3	5	NA
Stabo/Rappel	1	2	4	NA
Terrain Flt	1	3	2	NA
Paradrop	2	2	NA	NA
Routine	1	2	2	3
NOE	2	8	4	NA
MTP	3	5	NA	NA
Maint Recovery	3	5	NA	NA

10. WEATHER** (Risk Value/Ceiling/Visibility)

	<1000/3	<700/2	<500/1	>1000/3
D	3	4	6	1
N	4	6	10	2
NVG	3	4	8	1

11. ADDITIONAL RISK FACTORS (D, N)

Single Pilot	+4

ADDITIONAL COMMENTS

* Area of operations.
** Visibility values are given in miles.

ROTARY-WING RISK ASSESSMENT MATRIX

12. NVG CREW SEL/PC (Total NVG Time)
>150 <150 <100 <50 <25
1 2 3 4 5

13. NVG CREW SEL/PI (Total NVG Time)
>150 <150 <100 <50 <25
1 2 3 4 5

14. NVG CREW SEL/ADD (Total NVG Time)
>150 <150 <100 <50 <25
1 2 3 4 5

15. PERCENT OF ILLUMINATION (NVG)
100-80 79-60 59-40 30-23 <23
1 2 3 4 5

16. MOON ANGLE (NVG)
90-70 69-50 49-30 <30
0 1 2 3

17. ADDITIONAL RISK FACTORS (NVG)

RISK VALUES: DAY/NIGHT MISSIONS

1. Supervision ____
2. Planning ____
3. Crew Selection/PC ____
4. Crew Selection/PI ____
5. Crew Selection/Add ____
6. Crew Coordination Trained ____
7. METL Task ____
8. Crew Endurance ____
9. Complexity ____
10. Weather ____
11. Additional Risk Factors ____

TOTAL ____

RISK VALUES: DAY/NIGHT MISSIONS

12. NVG Crew Selection/PC ____
13. NVG Crew Selection/PI ____
14. NVG Crew Selection/Add ____
15. Illumination ____
16. Moon Angle (NVG) ____
17. Additional Risk Factors ____

TOTAL NVG MISSIONS ____
TOTAL DAY/NIGHT MISSIONS ____

TOTAL RISK VALUE NVG ____

COMPUTATIONS DAY/NIGHT MISSIONS

Low Risk	<16
Medium Risk	16-28*
High Risk	>29**

COMPUTATIONS NVG MISSIONS

Low Risk	<25
Medium Risk	25-40*
High Risk	41-50**
Extremely High	>50***

* Medium-risk missions require approval of the company commander.
** High-risk missions require approval of the battalion commander.
*** Extremely high-risk missions require approval of the brigade commander.

ADDITIONAL COMMENTS

Figure 1: Suggested Format for a Rotary-Wing Risk Assessment (US Army TC 1-210)

The scoring system in Figure 1 supports the 5th principle of rapid risk assessment in that the derived values are directly used to inform decision making. This is illustrated by the closing sections of the form. The total risk scores are calculated. These can then be used to identify the level of the Chain of Command that is competent to approve any decision. If the assessment is 'low risk then the operation can be performed without further consultation about the risks involved. If the result indicates a medium level of risk, in this case scored between 25 and 40, then the decision must be referred to a company commander. High risk operations require approval from the Battalion Commander while extreme risks must be referred to Brigade level.

The form from US Army TC1-210 is deceptively simple. At first glance, it seems to associate a risk score with different hazards. This observation is reinforced when the author asked military personnel to create their own versions. Most attempts to recreate this approach associate different scores with a range of potential hazards. However, this is not what is advocated within the Army training circular. The form does not focus on potential hazards but instead associates scores with what accident investigators would term to be 'contributory factors'. These include the quality of rest that the crew has received, their experience in an area of operations and the availability of supporting documentation, including mission essential task lists. This approach is appropriate because the form does not then need to list all of the potential hazards that might arise duri9ng complex operations that may be exacerbated by enemy action, system failures etc. This focus on contributory factors also reinforces the links between risk assessments and mishap investigation, identified in the 4th principle of rapid risk assessment. The contextual factors associated with any subsequent mishaps can trigger modifications to the content of the form – introducing new questions or revising the scores associated with particular responses.

Techniques similar to those illustrated in Figure 1 have simultaneously been applied in other industries (Johnson and Kilner, 2010). In particular, the limitations of conventional risk assessment techniques have motivated a number of Air Navigation Service Providers (ANSPs) to seek lower cost alternatives. The European Common Requirements (SES CR 2096/2005) use risk assessment as the primary means of ensuring safety in Air Traffic Management. This has reinforced the need to conduct hazard analysis embedded within European regulatory requirements. However, the costs associated with risk assessments for major complex systems has ensured that these techniques are typically only applied to guide systems acquisition and 'major changes'; a phrase that is often interpreted in very different ways by different member states. Further problems arise when smaller states try to meet these requirements. It is impossible for ANSPs to conduct major hazard analyses across all of their systems when there may only be funds to support one or two safety professionals within those organisations.

In consequence, ANSPs across Europe have begun to develop a range of forms that are intended to reduce the costs associated with conventional risk assessment techniques. One example is provided by a member state in which the systems engineering teams are required to describe any system modification in three sentences. They are then asked to identify the potential adverse consequences of those modifications within a single paragraph. If the modifications involve greater complexity then a more formal risk assessment may be attached to the summary form. This is then passed to regulators who can use the same form to state whether or not they require to be informed at all stages of the development of the changes or whether they only require notification before the changes take effect or whether the modifications can go ahead without further consultation. The aim behind this relatively simply form is to ensure that regulators do not suddenly want to become closely involved in a project during the final stages of implementation when there will be less scope to make any subsequent modifications. This approach builds upon the third and fifth principles from the previous enumeration – economy and applicability in decision making. Like the approach in Figure 1, this application of rapid risk assessment is also intended to ensure adequate consultation, in this case with regulators, before a risk is accepted. The organisations involved in the development of this technique have subsequently extended it to provide notifications of potential hazards within their company and not just with regulators. Operational staff and management are asked to sign the form to show that they have read the notification prior to any updates.

The same concerns that arise within Air Traffic Management also affect many military organisations, not simply those of smaller states. There are situations in which risk assessments conducted in one team are not adequately communicated to others within the same force (Johnson, 2011). Similarly, there are significant and deep routed barriers to communication between military personnel and many of the commercial organisations that develop their equipment or support underlying infrastructures. A frequent observation of the US Government Accountability Office is that operational demands have been neglected during the procurement of systems ranging from Abrams tank engines through to a range of communications technologies. It is essential that better information is provided to manufacturers about the operational hazards that are faced by the men and women in military organisations. Conversely, the rising numbers of mishaps in many armed forces demonstrates the need for suppliers and procurement agencies to provide operational personnel with better information about the risks that arise from using the equipment that they provide. In both cases, conventional risk assessment techniques, including HAZOPS and FMECA, provide very limited means of communication.

Case Study Two: Risk Informed Fragmentary Orders (R-FRAGS)

The previous section showed how forms could be developed to support rapid risk-based decision making in a number of pre-defined operational scenarios. It also described how similar techniques have been developed to improve communication between different stakeholders during the procurement, development and modification of complex systems. Although these approaches provide examples of rapid risk assessment techniques, they cannot address the full range of dynamic and unpredictable situations facing many military personnel. In consequence, there is a need to support decision making processes in contexts where there are no applicable forms that might guide subsequent intervention.

Many military organisations use the concept of fragmentary orders (FRAGOs) to "send timely changes of existing orders to subordinate and supporting commanders while providing notification to higher and adjacent commands" (US Army Field Manual 101-5). These notes are intended to provide the flexibility that is required in military operations in situations where the weather, enemy action, system failures etc can all combine to undermine an initial plan. FRAGOs typically provide information about the date and time of the change as well as the identity of the unit issuing the update. A brief description of the update is provided together with information about the units affected by the FRAGO and about other stakeholders that must be notified. In common with the regulatory and communications forms mentioned in the previous sections, these revisions

must also, typically, be signed off to acknowledge that they have been received and understood. Each fragmentary order will also record information about the mission that is affected and the situation that led to the change. An important aspect of most orders is information about the 'intent' of any revisions. This provides the recipients of the order with important contextual information that can be used to make further revisions in response to any further changes in the tasks that they must perform.

Variations on the FRAGO approach exist across most military organisations. These abbreviated orders meet many of the objectives identified for rapid risk assessment. They fulfil principle 3 which is intended to ensure the 'economy' of any approach; they do not require significant training to issue or understand. They also embody the 'applicability' principle by directly supporting operational decision making in a flexible manner. They enable orders to be revised in response to the changing high-risk environments in which most military missions are conducted. However, fragmentary orders do not typically enumerate the hazards that might arise during particular operations.

There have been recent attempts to extend FRAGOs to support composite risk assessment (Johnson, 2011). Personnel can annotate revised orders with a subjective summary of the potential hazards that may affect a revised mission. The intention is to provide a more flexible alternative to the forms that enumerate risks associated with common operations, following the template provided by TC-1-210 shown in Figure 1. These variations on conventional fragmentary orders can be used in a number of ways. Before a decision is made, personnel can use potential hazards to identify the ways in which a mission might be revised in order to mitigate future risks. In other words, the intentions behind FRAGOs can be shaped to address the threats to military operations.

Unfortunately, it is not always possible to draft a conventional fragmentary order in situations where immediate verbal commands must be issued. This creates potential concerns for the most immediate decisions that shape military operations in the field. In many cases, it can be difficult to identify those factors that contributed to the success or failure of a mission. It is for this reason that risk-based fragmentary orders have been extended to document previous decisions during complex, high-stress operations. This is important because military personnel can document the hazards that undermined a mission and which had not been anticipated in the original orders. Conversely, the proponents of 'resilience engineering' have argued that important safety-related information is often overlooked when safety professionals focus on what went wrong rather than considered what went right. Risk-based FRAGOs can also, therefore, be extended to describe hazards that were mitigated during successful operations.

Although we have described the use of post hoc fragmentary orders as a means of documenting operational decisions, it is important not to focus on combat missions. Arguably the greatest benefits are to be derived from the application of the approach in complex engineering tasks (Johnson and Kilner, 2010). In particular, technicians are often called upon to complete maintenance tasks with partial supply lists, incomplete documentation, with time pressure and under a range of stressors including fatigue, noise and heat. In such circumstances, there are few opportunities to conduct conventional risk assessments and still meet operational requirements. Post hoc, risk based adaptations to FRAGOs provide a partial means of ensuring that such situations do not recur in the future. At their best, they can alert higher levels of command to the hazards that concern the many different teams of men and women who support complex military operations.

Pre hoc rapid risk assessments directly help to mitigate hazards by informing subsequent decision making. The role of post hoc assessments is more controversial. This approach will only work if the lessons contained in these reports helps guide future operations. There also has to be some incentive for personnel to report their concerns even when a mission has been successful. Previous attempts to promote confidential mishap reporting systems within many armed forces have not been entirely successful. However, unless we find ways of addressing these issues then there is a danger that safety initiatives will continue to focus on learning the lessons of previous accidents rather than preventing future mishaps.

A number of techniques have been developed to support the integration of risk assessments into fragmentary orders. One of the most successful has been to further abbreviate the standard approach, summarised in the previous paragraphs. Personnel have been provided with pads in their work places; potential hazards can be noted down in a few sentences either before or after an operation. These are then collected at the end of the duty period and are reviewed as part of the hand-over process, for instance by maintenance personnel. Some units have created more elaborate schemes where each team is required to provide one safety improvement each month. Unit safety officers then action those changes that are easy to implement and feedback is provided on the reasons why other concerns cannot be immediately addressed. Any outstanding requests are then carried

forward to the end of the year and published in a list of the 'top ten safety concerns' following an approach pioneered by the US National Transportation Safety Board (NTSB).

Conclusions

Risk assessment techniques, such as HAZOPS and FMECA, are intended to support the development of safety-critical systems. They help to identify and mitigate the hazards that undermine many complex applications. Unfortunately, most existing risk assessment tools are costly and time consuming. In consequence, they are typically only applied during development projects or during major system upgrades. They cannot easily be applied to identify the hazards that undermine everyday operations. This is a significant concern because engineers and management must continue to find work-arounds for the degraded modes of operation that arise when safety-related applications do not always meet their intended requirements. This paper has presented a range of low cost techniques that can be used to support 'rapid risk assessment' during everyday operations. The intention is to provide front line staff with tools to anticipate potential hazards that are not typically considered during the development of complex safety-related systems. These concerns are particularly important in military applications where manufacturers often make inappropriate assumptions about the eventual environment in which their systems are deployed.

In particular, we have presented a number of case studies of techniques that have been used by military organisations to develop low-cost, flexible alternatives to conventional risk assessment techniques. TC 1-210 provides a template for risk assessment forms that associate a simple scoring system with the contributory factors that can lead to adverse events. These scores can then be used to associate risk-based decisions with different levels in the chain of command. Unfortunately, it is impossible to develop forms that might support the diverse range of military operations. In consequence, subsequent sections have described how Fragmentary Orders (FRAGOs) can be extended to consider potential hazards. This provides a high degree of flexibility and can be coupled to existing review processes so that commanders can identify the risks that must be faced by future operations.

There are clear limits to rapid risk assessment techniques and these need to be better understood. Placing an undue focus on potential hazards can undermine military effectiveness by sustaining a culture of risk aversion. In particular, it can lead to a degree of conservatism in which scarce resources are continually deployed to minimise hazards that are seldom realised. We also recognise that existing techniques do not provide a panacea for the relatively high numbers of military mishaps. The use of FRAGOs and the introduction of risk-based assessment forms to aid decision making represent first steps in a process that is intended to extend the benefits of hazard analysis without suffering the drawbacks that affect conventional approaches. Much of the work reported in this paper stems from attempts to build on the US Army's Composite Risk Management program. However, a range of alternate techniques can be applied (Johnson, 2011). It is for this reason that we have introduced a number of generic principles that help to define the objectives of 'rapid risk' assessment rather than focussing exclusively on particular techniques. It is our intention that future work will focus on the objectives of *Consistency; Repeatability; Economy; Validity;* and *Applicability* even if the proposed approaches differ significantly from those that have been described in previous sections.

References

C. Haddon Cave, An Independent Review Into the Broader Issues Surrounding the Loss Of The RAF Nimrod MR2 Aircraft XV230 In Afghanistan IN 2006, Report HC 1025, Her Majesty's Stationery Office, London, 2009.

C.W. Johnson, The Paradoxes of Military Risk Assessment. In A.G. Boyer and N.J. Gauthier (eds.) Proceedings of the 25th International Systems Safety Conference, Baltimore, USA, International Systems Safety Society, Unionville, VA, USA, 859-869, ISBN 0-9721385-7-9, 2007.

C.W. Johnson, A Handbook of Military Risk Management, University of Glasgow, 2011 (in press).

C.W. Johnson and A. Kilner, Scaring Engineers with Degraded Modes: The Strengths and Weakness of Action Research in Air Traffic Management. In B. Kirwan (ed.), Proceedings of the 7th EUROCONTROL Experimental Centre Safety Research and Development Workshop, Bretigny, France, 2010.

UK Ministry of Defence, HAZOPS in Software Control Systems, UK Def STAN 00-58, 2000 (now superceded).

US Department of Defence, Standard Practice For System Safety: Environment, Safety, and Occupational Health, Risk Management Methodology for Systems Engineering, MIL-STD-882D w/CHANGE 1, Washington, USA, 29th March 2010.

US Department of the Army, TC 1-210: Aircrew Training Program Commander's Guide to Individual And Crew Standardization, Headquarters, Department Of The Army, Washington, DC, 3 October 1995.

US Army, Failure Modes, Effects and Criticality Analysis (FMECA) For Command, Control, Communications, Computer, Intelligence, Surveillance, And Reconnaissance (C4ISR), Facilities, Technical Manual 5-698-4, September 2006.

US Army Environmental Policy Institute, Managing the Life Cycle Risks of Nanomaterials, Arlington, Virginia, July 2009.

Woodward-Clyde Consultants, Hazard and Operability Study (HAZOP) Rocky Mountain Arsenal, Basin F Liquid Incineration, Available via US Defence Technical Information Centre, July 1992.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP,
School of Computing Science, Univ. of Glasgow, Glasgow, G12 8RZ, Scotland, UK.
Tel +44(141)3306053, Fax +44(141)3304913, Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.