Hayward, B.J., Lowe, A.R., & Branford, K. (2008). *Creating safer systems: Proactive integrated risk assessment technique.* Paper presented at the 28th Conference of the European Association for Aviation Psychology, Valencia, Spain, 27-31 October 2008.

Creating Safer Systems:
Proactive Integrated Risk Assessment Technique

Brenton Hayward; Andrew Lowe; Kate Branford
Dédale Asia Pacific, Melbourne, Australia
bhayward@dedale.net

Introduction

Major aircraft accidents are typically followed by intensive investigations to identify and address the range of factors that contributed to the event. Contemporary examples of this are the 2001 Milan Linate runway collision, the 2002 Überlingen mid-air collision, the 2006 mid-air collision over the rainforests of Brazil, the 2007 Yogyakarta and Congonhas-São Paulo runway overrun accidents, and this year's terrible crash at Madrid Barajas. Such events are tragic for those directly affected and provoke strong emotional reactions within the aviation community and broader society.

Safety investigation methods for learning from and preventing recurrence of these accidents have evolved considerably over the past 20 years. One key improvement has been the transition to systemic safety occurrence analysis methods. Examples of these include Tripod (Doran & van der Graaf, 1996; Hudson et al, 1994), the Incident Cause Analysis Method (ICAM; BHP Corporate Safety, 2000), AcciMap (Rasmussen, 1997; Hopkins, 2000), the Human Factors Analysis and Classification System (HFACS; Wiegmann & Shappell, 2003) and the Systemic Occurrence Analysis Methodology (SOAM; EUROCONTROL, 2005). Although these techniques have their differences, they share a number of common attributes:

- They are evolutions of, or at least consistent with, the work of Reason (1990, 1997) in that they focus on the systemic factors that contributed to an accident or incident, rather than just the behaviour of operators. They begin by identifying the immediate precursors to the accident and extend to consider the contextual, environmental and organisational factors that promoted, allowed, or failed to prevent the negative outcome. In considering these 'latent conditions' (Reason, 1991), the activities of frontline operators are linked with the context in which they took place, to enable a full understanding of how and why the event occurred.

- By moving beyond specific, low-level details of accidents and incidents to consider broader organisational and system factors, these techniques enable commonalities between different accidents to be identified and problem areas to be prioritised and addressed.

- The corrective actions that emerge from such techniques focus on the 'system', rather than the 'person'. Recommendations are designed to address the barriers or controls that failed as well as the areas of organisational vulnerability that contributed to the unsafe situation, rather than the behaviour of the particular personnel involved in the event. Systemic improvements have the capacity to generate significant reduction in risk throughout the system, by addressing hazards and error-producing conditions at their source.

- These systemic methods have facilitated the positive shift from a "blame culture" through "no blame" and towards a "just culture" approach to safety investigation, and to the reporting of 'normal errors'.

The investigation process concludes with the release of a report that identifies a set of contributing factors and recommends corrective actions to address each of these. The recommendations made are seldom new or unexpected, and may even evoke a sense of *déjà vu* amongst those who take an interest in accident investigation and prevention. The reason for this is that the *contributing factors* in many accidents are already known and understood. People working within the industry are seldom surprised at the findings of investigation, because the same factors have contributed to similar scenarios in the past, either as accidents or as ‘near misses’. What is surprising and frequently disappointing is the fact that the industry has not learnt from the prior events and acted effectively to mitigate the risk and prevent them from happening again.

This situation is not unique to the aviation industry. Operational personnel in most industries possess a wealth of knowledge about the latent conditions that contribute to such tragedies. This paper discusses a technique that aims to harvest this knowledge and use it to identify and address these conditions *before* their potential for harm and damage is realised.

Safety Occurrence Investigation

Regrettably, the investigation of safety occurrences will remain an inescapable activity in managing risk, in aviation and other hazardous industries. Diligent systemic occurrence investigation is essential, as most accidents and incidents provide the opportunity to understand the complete set of conditions that contributed to the outcome and to identify appropriate corrective actions. As a tool for organisational learning and safety risk management, however, investigation processes have obvious shortcomings:

- By definition, investigations are reactive, only being undertaken *after* a safety occurrence or near miss. The more serious of these events often entail terrible costs, in human and other terms, as well as secondary losses such as the damage to an organisation’s reputation and potentially a threat to its very existence. There is inevitably a high price to pay for the organisational learning derived.

- Accidents and serious incidents typically contain a random element – the confluence of a highly unusual combination of actions, events and conditions – that contribute to the fact that they were not predicted, and therefore not prevented. Investigations can tend therefore to focus in minute detail on those rare and unique conditions that contributed to the particular occurrence. This can lead to undue focus on peripheral issues and may divert attention and resources from other areas of risk within the system.

- The cost of some investigations into high profile accidents can be disproportionate to the benefits obtained. Commissions of Inquiry and other high profile investigations deliver authoritative and exhaustive findings borne of epic legal scrutiny, but at a cost much greater than a competent systemic safety investigation would incur. The inquiry itself and the implementation of its recommendations consume substantial resources that could be applied to more appropriate proactive safety management practices and other important aspects of risk reduction within the industry under investigation.

- Lastly, reactive investigations can only make a limited contribution in ultra safe industries, where accidents and serious incidents – and thus the opportunity to learn from them – are thankfully rare.

In light of these limitations, it is useful to consider whether alternative approaches exist that can produce the benefits of occurrence investigations, but without some of the associated costs. Current proactive risk management techniques include safety audits, peer reviews (eg., International Atomic Energy Agency, 2006; World Association of Nuclear Operators, 2005), inspections and LOSA-style operational assessments (Line Operations Safety Audit; Helmreich, Klinect & Wilhelm, 2001; 2003). These techniques tend to focus on deviations or gaps at the level of the operational interface, that is, *local* conditions (hazards, etc.), violations or errors that need to be eradicated, corrected or in some way managed. This is based on the reasonable assumption that addressing these deficiencies will be beneficial in reducing the likelihood of an accident. Even those safety assessment techniques that do extend to consider higher level systemic factors, such as safety culture or risk management processes, tend not to illuminate the full range of organisational elements that may contribute to accidents.

The essence of the Reason Model is that local factors combine with higher-level latent conditions to produce an ‘organisational accident’. It would be logical then to audit all of these elements in a holistic way, rather than in isolation. The following section describes an approach designed to do just that.

Proactive Integrated Risk Assessment Technique

The Proactive Integrated Risk Assessment Technique (PIRATe) is based on a contemporary adaptation of the principles of Reason's "Swiss Cheese" model to safety occurrence analysis, specifically the Systemic Occurrence Analysis Methodology (SOAM) developed for EUROCONTROL (see Hayward & Lowe, 2004; EUROCONTROL, 2005; Licu, Cioran, Hayward & Lowe, 2007). SOAM includes specific taxonomies and terminology to describe the various factors that contribute to a safety occurrence. It also prescribes standardised processes for gathering evidence, analysing contributing factors and ensuring that findings are clearly linked to recommendations, providing guidance to safety investigators and analysts in key aspects of an investigation.

PIRATe is a systemic but *proactive* approach for identifying operational risk. It enables *potential* or hypothetical safety occurrences to be analysed, drawing on the collective experience and knowledge of operational personnel about unsafe conditions and behaviours in their workplace. These risk factors are understood implicitly by frontline operators in safety-critical roles, but seldom made explicit. The aim of PIRATe is to elicit this understanding – people's insights into the hazards that confront them each day in their operational environment – and to trace these hazards back to their underlying systemic origins. To this extent, every experienced airline pilot, Air Traffic Controller and maintenance worker is a local operational safety subject matter expert (SME), who possesses valuable, first-hand knowledge about current, everyday hazards and risks and the potential for an accident.

As a derivative of the Reason Model, PIRATe integrates the contributing factors to a hypothetical event into a unique and holistic analysis. Corrective actions flow from the analysis in the same way they do following a competent systemic occurrence investigation.

PIRATe involves the following steps:

1. Assemble an appropriate group of SMEs. In the authors' experience, it is productive to use this process as a component of other safety-related training, for example, Crew Resource Management (CRM) courses, where safety issues will be top of mind for participants and they will be primed to transfer ideas into a holistic accident scenario. This can also be done via stand-alone workshops, if preferred.

2. Explain the systemic occurrence analysis approach. Participants need to have a good working understanding of the principles of the Reason Model or other systemic occurrence analysis method, to be used as a framework for developing, analysing and reporting their own scenario.

3. Ask the SMEs to work in small groups to 'design their next accident' – to identify the conditions within their system that could contribute to a realistic safety occurrence, using their implicit understanding of local operational hazards, error-producing conditions and absent or imperfect barriers. Groups are encouraged to spend some time in discussion to agree the broad nature of the accident scenario, which is itself enlightening. For aviation, the scenario might involve aircraft operations, maintenance, or perhaps a production mishap, depending on the organisation/s involved. After agreeing on a scenario, they are asked to specify the ingredients (conditions) that are likely to contribute to the occurrence.

4. Provide empirical data, where available, to guide both the selection of accident scenarios and the determination of contributing factors. For example, an airline's Flight Operations Quality Assurance (FOQA) data may suggest that an accident associated with an unstabilised approach is worth analysing. Incident database readouts might suggest particular workplace conditions (fatigue, circadian disruption, crew communication deficiencies, etc.) are common contributing factors that might be incorporated into a hypothetical scenario.

5. Ask the SMEs to analyse this hypothetical event, including the organisational factors that are responsible for each hazardous condition or inadequate barrier. They then produce recommended actions to correct each organisational factor and to strengthen safety controls. Custom-designed worksheets can be supplied to facilitate the analysis process and to provide a record of findings and recommendations. It is recommended

that facilitators experienced in accident investigation and the use of systemic investigation techniques oversee the process.

PIRATe Application ~ Examples

PIRATe has been employed successfully to identify operational risk scenarios with groups in the aviation, nuclear power, shipping and rail industries. Some of these applications and their outcomes are described in further detail below. An example of the output generated from such an analysis is provided.

1. The process was used by groups of four to six pilots in some 160 Crew Resource Management courses conducted by a major international airline. The pattern of organisational factors appearing across a large number of accident scenarios was analysed (in an internal study) to identify highest priority areas for potential action. The fact that one high-likelihood, high-consequence and realistic accident was a recurring scenario identified by independent groups of pilots reportedly influenced the airline's decision to cease operating into the location involved.

2. Groups of senior managers at a number of nuclear power facilities in Sweden identified potential safety occurrences in their 'ultra-safe' industry, drawing on local and relevant international incidents. Some groups chose to apply the process to a potential security event, identifying contributing factors, organisational deficiencies and inadequate barriers that could be addressed.

3. The technique has been used with an aircraft manufacturer to predict aircraft design and manufacturing problems, and to identify latent conditions with the potential to provoke aircraft maintenance-related occurrences and operator accidents.

4. Ships' crews from a maritime company operating a global fleet of Very Large Crude Carriers (oil tankers) employed the technique within Maritime Resource Management (MRM) training courses to identify potential accident scenarios within their sphere of operations, including ship losses and environmental disasters.

5. Mixed groups of rail safety workers (including train drivers, signallers / controllers, track maintenance workers and safety specialists) analysed five high-risk accident scenarios involving harm to track workers. These events had been previously identified through a qualitative Risk Assessment. The corrective actions from all five scenarios were collated into a set of recommendations to improve worker safety across the entire track maintenance system for a major suburban rail operator. An example of one analysis from this project is provided in Figure 1.

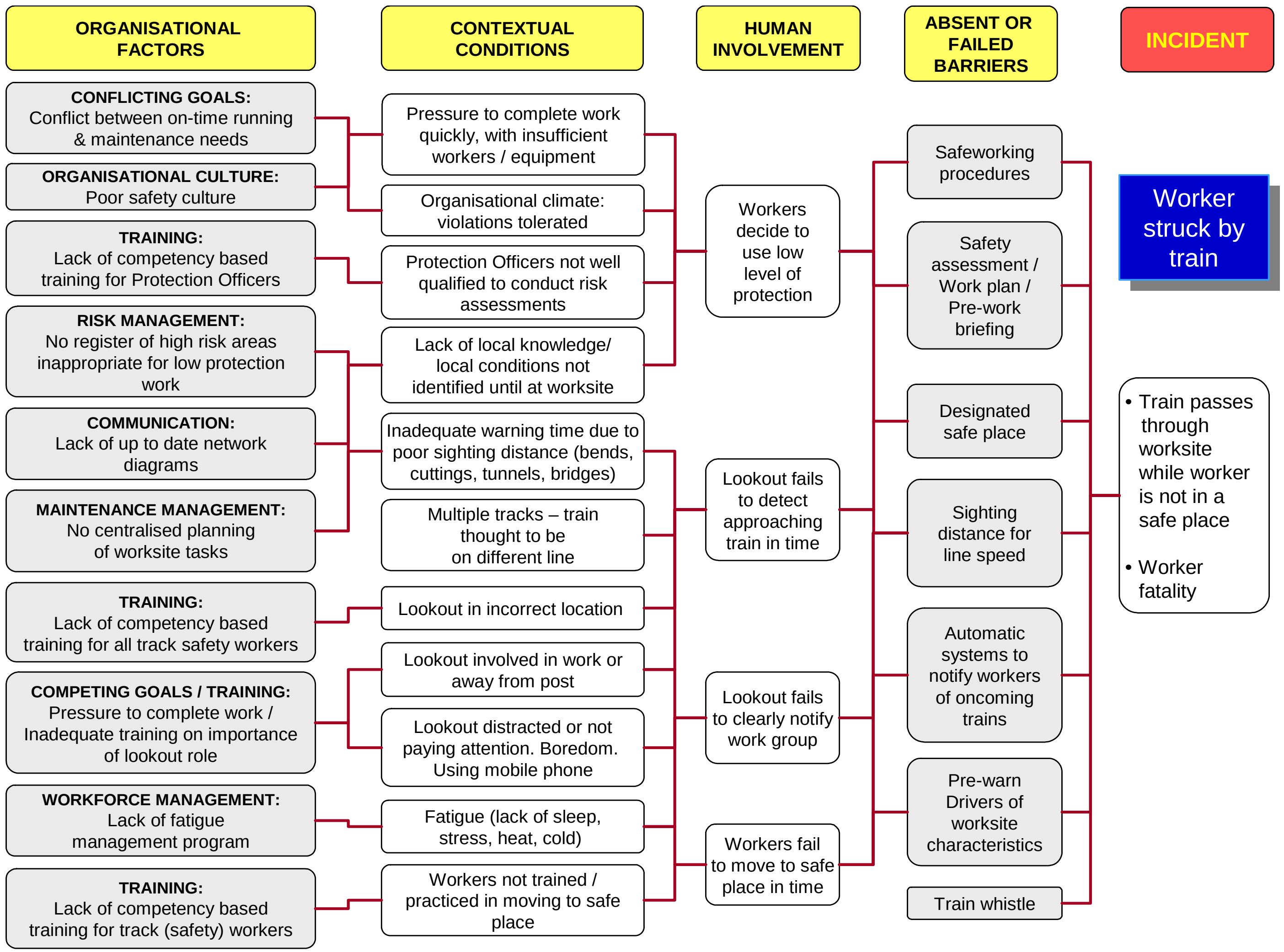

Figure 1
Example PIRATe Analysis Outcome ~ Rail Industry

Benefits

There are a number of benefits associated with PIRATe as a safety enhancement tool.

1. It is a proactive methodology that provides valuable 'free lessons' for the organisations and industries concerned. An organisation need not experience an accident to benefit from the approach – the outcomes are based on experiences of near misses from operators or from their implicit understanding of areas of the system where the potential for hazardous outcomes exists.

2. It has a sound theoretical basis, being derived from a proven accident analysis tool. Reason's "Swiss Cheese" Model is now a familiar concept in numerous industries, which enables this derivative process to be readily explained to users.

3. It is an integrated technique, combining information from many sources and the ideas from a group of experts into a holistic, systemic analysis. Most importantly, the technique enables operators to draw on their current experience of, and concern about, actual operational hazards, in a way that other risk reduction techniques do not.

4. Risk Assessment is inherent in the process. As in the examples cited within this paper, highest risk events can be identified, eg., from FOQA or other objective data, and combined with the insights of operational personnel with local knowledge and experience. Risk is directly addressed through recommendations made as part of the technique.

5. In addition to the output from PIRATe, there are important secondary benefits from taking part in the process. Participation can be expected to heighten awareness amongst those involved about the nature of industrial accidents – the human involvement (errors and / or violations), contextual conditions and latent organisational contributions, and the barriers that can fail or may be missing – and how people at all levels of an organisation can contribute to reducing risk. Like specialised safety training, it promotes wariness about the vulnerabilities of the system and the potential for accidents and incidents, countering the sense of complacency that can arise in industries with good safety records.

6. The approach can facilitate communication about safety issues between those operational personnel with a good understanding of the safety risks in their organisations, and management, who may previously have gained this understanding only after a safety occurrence. The hypothetical and systems-based nature of the approach promotes confidential, open disclosure among participants regarding the potential for hazardous outcomes, and managers can access these data to reap the benefits of this local knowledge and expertise.

7. There is potential to aggregate the findings from a number of separate PIRATe sessions. For example, the frequency with which similar accident scenarios are appearing can be determined, providing a ballpark measure of 'likelihood', and thus risk. A second option is to use a standard framework of Organisational Factors, and to ascertain how often factors such as 'Procedures', 'Training', 'Accountability', or 'Safety Culture' arise, and to look at generic remedial action in the highest priority areas. Similarly, each hypothetical accident will identify a number of barriers (defences, controls) that can be compared and strengthened where necessary.

Conclusion

Safety occurrence investigation is essential, and it is important that it is done well, using structured and standardised methods to identify the full range of conditions that contribute to an accident or incident. Investigation can, however, be complemented by proactive techniques that provide equal if not greater benefit, without significant cost. PIRATe is a proven proactive approach for identifying and reducing operational risk across several industries. It is considered a useful tool for enhancing organisational learning and helping to ensure that the commercial transport aviation industry remains one of the safest in the world.

References

BHP Corporate Safety. (2000). *Incident Cause Analysis Method investigation guide, Issue 1, March 2000*. Melbourne: Author.

Doran, J.A., & van der Graaf, G.C. (1996). Tripod-Beta: Incident investigation and analysis. In *Proceedings of the Third International Conference on Health, Safety and Environment*, New Orleans, LA: Society of Petroleum Engineers.

EUROCONTROL. (2005). *EAM2/GUI8: Systemic Occurrence Analysis Methodology (SOAM), Edition 1.0*. Brussels: Author.

Hayward, B., & Lowe, A. (2004). Safety investigation: Systemic occurrence analysis methods. In K-M. Goeters (Ed.), *Aviation psychology: Practice and research* (pp. 363-380). Aldershot, UK: Ashgate.

Helmreich, R.L., Klinect, J.R., & Wilhelm, J.A. (2001). System safety and threat and error management: The line operations safety audit (LOSA). In *Proceedings of the Eleventh International Symposium on Aviation Psychology*. Columbus, OH: The Ohio State University.

Helmreich, R.L., Klinect, J.R., & Wilhelm, J.A. (2003). Managing threat and error: Data from line operations. In G. Edkins & P. Pfister (Eds.), *Innovation and consolidation in aviation: Selected contributions to the Australian Aviation Psychology Symposium 2000*. Aldershot, UK: Ashgate.

Hopkins, A. (2000). *Lessons from Longford: The Esso gas plant explosion*. Crows Nest, NSW: Allen & Unwin.

Hudson, P.T.W., Reason, J.T., Wagenaar, W.A., Bentley, P.D., Primrose, M., & Vissler, J.P. (1994). Tripod Delta: Proactive approach to enhanced safety, *Journal of Petroleum Technology, 46* (1), 58-62.

International Atomic Energy Agency. (2006). *Report: Integrated Regulatory Review Service (IRRS), Full Scope, Report to the Government of France*. Paris: Author.

Licu, T., Cioran, F., Hayward, B., & Lowe, A. (2007). EUROCONTROL – Systemic Occurrence Analysis Methodology (SOAM) – A “Reason”-based organisational methodology for analysing incidents and accidents. *Reliability Engineering & System Safety, 92*(9), 1162-1169.

Moshansky, V.P. (1992). *Commission of inquiry into the Air Ontario crash at Dryden, Ontario: Final Report.* Ottawa: Canadian Ministry of Supply and Services.

Rasmussen, J. (1997). Risk management in a dynamic society: A modeling problem. *Safety Science, 27*(2-3), 183-213.

Reason, J. (1990). *Human error*. New York: Cambridge University Press.

Reason, J. (1991). Identifying the latent causes of aircraft accidents before and after the event. In *Proceedings of the 22nd ISASI Annual Air Safety Seminar,* Canberra, Australia. Sterling, VA: ISASI.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot, UK: Ashgate.

Wiegmann, D. A. & Shappell, S. A. (2003). *A human error approach to aviation accident analysis: The Human Factors Analysis and Classification System*. Burlington, VT: Ashgate.

World Association of Nuclear Operators. (2005). *WANO review: Safety first.* London: Author.