A Human Error-Based Risk Assessment Model

Wayne Rhodes
Rhodes & Associates Inc., Human Factors Consultants, Toronto, Canada

Abstract

A major component of risk assessment is that of human error. Identifying and calculating overall risk requires that the analyst consider how operators, maintainers, and support staff contribute to the causes of hazardous conditions that may lead to serious, disastrous, or catastrophic consequences. A computerized model has been developed by Rhodes & Associates Inc. to be run for marine, aviation, and rail operational scenarios. The model automatically calculates predicted risk values. The author will present the model's components and describe how the model may be applied to nuclear operations.

1. Introduction

Risk and error management strategies have been shown to improve safety in high-risk process industries [1]. These strategies can expose those areas where improvement should be made, and can also be used to uncover underlying causes of unsafe conditions that were present during incidents. The former is proactive, while the latter is responsive. Many techniques exist that can be used to apply both proactive and responsive approaches to risk and error management. The main thread that ties all of the approaches is the focus on human error causation. That is, getting to the root of what in a system leads people to err. The most comprehensive and practical of all of the methods is referred to as the system approach to error reduction [1]. This approach is based on Reason's model of error causation and accounts for all internal and external influences (see Figure 1).

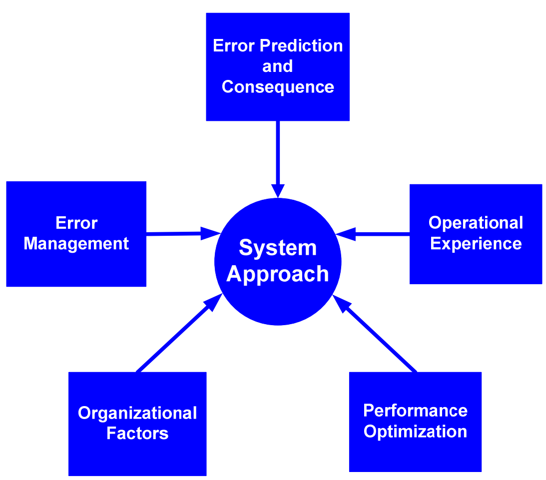

Figure 1 System Approach to Error Reduction

The system approach involves the collection and analysis of data from several sources:

- Organizational information on company safety culture, policies, the views of upper management, and mission statements
- Data from error reporting systems, error management experience, and audit reports
- Operating Experience (OPEX) and formal incident reports
- Interviews with operational staff and observations of day-to-day practices
- Design improvement and upgrade documentation (including recommended changes to equipment and procedures design)

The human error risk model proposed here is but one tool to be used to understand the impact of errors on system safety. The model can be used to obtain data on human error modes and types, and their associated risk to the operation, staff, and the public. Hence, it can fill the role of the upper most box in Figure 1, Error Prediction and Consequence.

2. Background

The model presented here was developed initially to examine the risk posed by fatigue on aircraft maintenance tasks. It was immediately realized that the mix of the tasks included both physical and cognitive tasks that were highly coupled. This required an examination of the impact of fatigue on these tasks, and a thorough analysis of the potential errors that could occur, as well as the impact of these errors on safety. An initial model was built and over the years during application to other modes of transportation (rail and marine), was refined. The model shows promise as a tool to quantify the human error contribution to the safety risk of systems, and can be used to measure the impact of error reduction and management systems.

Several approaches exist that provide practical methodologies for error reduction and management [1], [2], [3] [4]. These approaches are comprehensive and incorporate all of the elements described above for the system approach. They also handle cognitive as well as behavioural task data. This is important given that most of the activities in modern automated process systems are cognitive in nature. Some highly theoretical approaches also exist that are much more detailed and elegant, but these tend to be more difficult to apply in the field (see Hollnagel's book for one of the most comprehensive, theoretical treatments [5]). Hollnagel's description of the Cognitive Reliability and Error Analysis Method (CREAM) provides a very good understanding of the cognitive bases underlying the nature of human errors [5].

The methodology followed by the Center for the Chemical Process Safety (CCPS) entitled *Guidelines for Preventing Human Error in Process Safety* [1] appears to be the most practical to apply to nuclear power operations. In fact much of the methodology presented is based on earlier techniques used in the nuclear power industry, with considerable updating and additions to ensure adequate coverage (i.e. computer-based user interfaces and increased automation).

3. Methodology

The current work presented in this paper draws upon the methodologies mentioned above and combines the fundamental elements with an error analysis and reduction technique developed by Williams [6] referred to as the Human Error Analysis and Reduction Technique (HEART). The HEART technique is a simple approach to assign quantitative reliability information to specific tasks, modified to account for the effects of the prevailing error producing conditions for specific scenarios. HEART is used to quantify the error data in terms of frequency and to incorporate the effects of error producing conditions (called performance shaping factors [PFCs] in CCPS's approach). The error data is then incorporated into a risk table that allows calculations of risk values for each scenario. This approach has been used to integrate human error effects into the basic risk model described in CSA/CAN Q850-97 [7]. The approach consists of the following steps:

1. Collection of task, human error, EPC, hazard, consequence, and mitigation data
2. Compilation of data into a task database
3. HEART analysis
4. Event tree analysis for specified scenarios
5. Creation of scenario-based risk tables
6. Identification of associated mitigation strategies
7. Analysis of costs and benefits of mitigation strategies

Figure 2 illustrates the relationship between these steps.

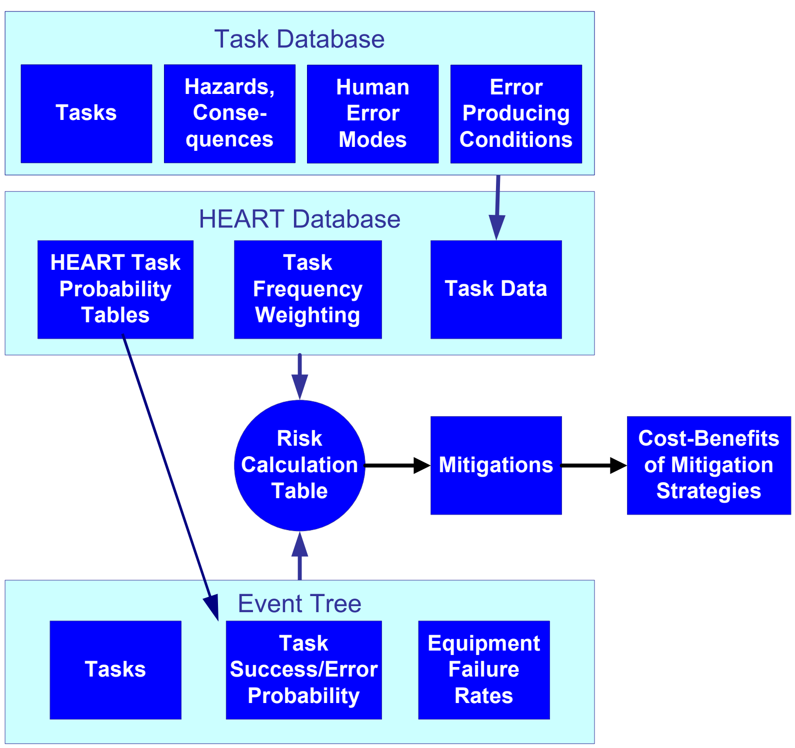

Figure 2 Steps Involved in Development of Human Error Risk Model

3.1 Collection of Task-Related Data

The data collection involves interviews with each individual of a group that is representative of the employees affected. These interviews will examine the existing and potential hazards, the tasks involved, errors that may occur, estimates of their frequency, consequences that may occur, and mitigations that may be potentially useful. Focus groups involving a representative sample of the workers also can provide such information but may be biased by the influence of certain vocal individuals. However, focus groups involving representatives from the stakeholder groups can provide general information on hazards, consequences, and mitigations. Employees should be observed during typical work scenarios while they perform their duties. During these observations important task information, potential error modes, safe practices, and risky practices may become more apparent.

3.2 Compilation of Task Database

The database contains the following data components:

- Representative scenarios that include each task
- Task and critical-subtask descriptions
- Potential critical human error modes associated with each task
- Identified hazards associated with each task performed during the selected scenarios
- Potential consequence of the error modes for each task
- Nominal error frequency for each task
- Error producing conditions (EPCs) affecting each task and their weighting according to representative scenarios

3.3 Human Error (HEART) Analysis

The task data is used to populate the HEART analysis table including the HEART calculations (application of EPC multipliers and EPC probability sums) and specific comparative calculations (e.g. fatigued condition versus rested condition; single operator operation versus two operator operation; present system versus improved system). Figure 3 illustrates the mechanics of the table.

Task	Nominal Task Error Frequency	Error Modes	EPCs Involved	EPC Multiplier	Weighting for EPC Multiplier	EPC Products Cond. A	EPC Products Cond. B
Brief Descrip tion	Derived from experience and tables	Description of all relevant error modes	List of all relevant EPCs	Multiplier for each relevant EPC	Weighting applied to each EPC multiplier	Task prob. X each weighted EPC less 1, multiplied together for first condition	Task prob. X each weighted EPC less 1, multiplied together for second condition

Figure 3 HEART Table Structure

The following equations describe the calculations necessary to arrive at the adjusted probability of unreliability for each task.

$$(EPC_i) = (EPCM - 1) \times (EPCP) + 1 \quad (1)$$

Where:

EPC_i is the contribution of a specific EPC to the overall level of unreliability
EPCM is the EPC impact multiplier
EPCP is the proportion of estimated effect of the EPC on error occurrence

The EPC multipliers are taken from Williams [6].

The proportion of estimated effect is determined by the expert judgement of the analyst using criteria that includes:

1. The proportion of time that the EPC would apply to a particular situation (scenario); and
2. The strength in which the EPC would influence the erroneous action.

The result in Equation 1 is an estimate for the contribution of particular EPC to the overall unreliability of a specific error mode.

The contributions of each EPC are multiplied together to arrive at the overall estimate of unreliability posed by a particular error mode, as shown by Equation 2:

Total EPC Effect = (Contribution of EPC_1) x (Contribution of EPC_2) x …(Contribution of EPC_n) (2)

The result in equation 2 gives the combined effect posed by the EPCs.

3.4 Event Tree Analysis

The risk table is based on the output from the event tree analysis which is done on a scenario by scenario basis. The event tree analysis uses the data produced by the task and HEART analyses, including tasks, error modes (initiating and enabling error events), calculated error and success frequencies, and final calculated frequencies of outcomes. Figure 4 shows an example from the aircraft maintenance task risk assessment.

3.5 Scenario-Based Risk Tables

The data resulting from the above analyses is placed in an Excel table that is structured to calculate the overall risk levels expected for each scenario, combined with consequence levels, resulting in overall risk outcomes for each scenario. The table automatically calculates these overall risk levels once it is populated by the data produced by the initial analyses.

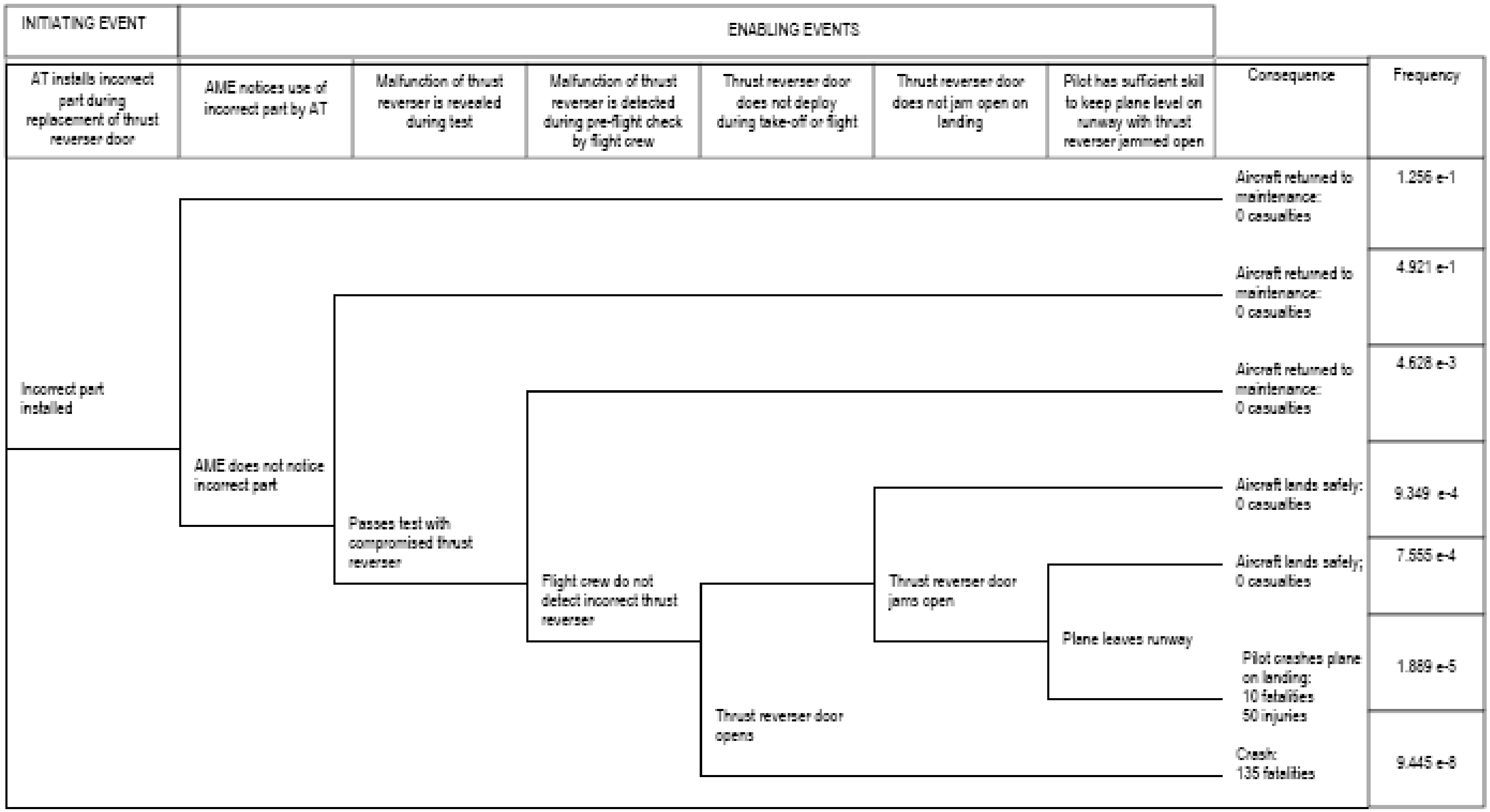

Figure 4 Example of an Event Tree

3.6 Identification of Mitigation Strategies

Some mitigation strategies are identified during the earlier data collection phase (during interviews, focus groups) and according to the types of potential errors that may occur (skill-based, rule-based, and knowledge-based). For skill-based errors, training may be required. Rule-based errors may be better resolved through improved procedures and practices. Other strategies are determined from the risk analysis and risk assessment research literature, and past risk assessments of similar problems. This multi-pronged analysis allows for optimum coverage and practicality. Each scenario containing specific mitigation strategies is compared for overall risk levels.

3.7 Costs and Benefits of Mitigations

The mitigation strategies are analysed for their costs and potential for lowering risk. Analysis of the scenarios that include each mitigation strategy are compared for:

- Results of risk comparisons for each scenario before and after introduction of each mitigation – (overall risk level = outcome consequence level X outcome frequency)
- Whether training, redesign of equipment, staffing, or policy changes are required
- Associated costs for each mitigation
- Risk reduction potential (risk before mitigation – risk after mitigation)

4. Risk Assessment

The information produced by the risk tables can be converted to standard risk terms (see Figure 5). Each scenario can be assigned an overall risk level and compared with those in the table to determine what scenarios need immediate mitigation regardless of costs, and what scenarios require a cost benefit analysis. For example those scenarios that may occur often (according to the frequency of relevant potential error modes or experience), or result in catastrophic outcomes, mitigations should be applied immediately. Of course, this also includes those that may occur often and result in catastrophic outcomes. For scenarios that are rare events and do not result in serious or catastrophic outcomes a cost-benefit analysis should be used to determine those mitigations to be applied.

6. Application to the Nuclear Power Industry

The approach described above can be effectively applied to the nuclear power industry and shows promise as a means to make risk-based decisions regarding staffing, processes and procedures, equipment and systems design, and company policies. Decisions based on these analyses will result in an optimum lower risk to personnel, the system, and the public. The method, combined with scenario-based error analysis and hardware/software reliability analysis, can be used to determine risk levels inherent in the existing systems (proactive approach). The method provides a means to integrate human actions and their associated error modes (and rates) into the probabilistic risk assessment.

	Severity of Consequence					
Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	High Risk	High Risk	Extreme Risk	Extreme Risk	Extreme Risk
	Likely	Moderate Risk	High Risk	High Risk	Extreme Risk	Extreme Risk
	Moderate	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
	Unlikely	Low Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
	Rare	Low Risk	Low Risk	Moderate Risk	High Risk	High Risk

Figure 5 Risk Table

Once the existing risk levels have been established, mitigations can be considered to improve the level of risk. A new risk level can be calculated for each mitigation under specific scenario conditions. This approach allows the analyst to run the model for all scenarios including selected mitigations as part of that scenario (e.g. new equipment design, improved training, or revised procedure etc.). All risk data for each scenario is combined to arrive at the overall system risk level. The new system risk levels for all scenarios combined can be compared to baseline levels established by the nuclear industry. Those mitigations that reduce the risk to just below accepted standard, and that are the lowest cost, would be considered to be the optimum approaches.

Also, a calculation can be made to determine the risk associated with various mitigation strategies considered as solutions to improve safety after the occurrence of a disastrous or catastrophic incident (reactive). Again the model allows the analyst to calculate the risk values for several mitigation strategies. The resulting risk levels can be compared to the baseline standard. Those strategies that are less costly can be considered to be the optimum choice.

7. References

[1] Centre for Chemical Process Safety, Guidelines for Preventing Human Error in Process Safety, New York; American Institute of Chemical Engineers. 1994.

[2] Reason, J., *Managing the Risk of Organizational Accidents*, Aldershot; Ashgate. 1997.

[3] Petersen, D., Human Error Reduction and Safety Management, New York; Van Nostrand Reinhold. 1996.

[4] Patankar, M.S. and Taylor, J.C., Risk Management and Error Reduction in Aviation Maintenance, Aldershot; Ashgate. 2004.

[5] Hollnagel, E., Cognitive Reliability and Error Analysis Method, New York; Elsevier. 1998.

[6] Williams, J. (1988) A data-based method for assessing and reducing human error to improve operational performance. *Proceedings of the IEEE Conference on Human Factors and Power Plants*, Monterey, California.

[7] Canadian Standards Association, Risk Management - Guideline for Decision-makers: A Canadian Standard, CSA/CAN Q850-97, Toronto, Canadian Standards Association. 1997.