A PREDICTIVE SAFETY MODEL

MICHAEL J. CAMET

Department of Mechanical and Industrial Engineering

APPROVED:

Dr. Rolando Quintana

Dr. Carroll Johnson

Dr. Carlos Ferregut

Associate Vice President
for Graduate Studies

To my parents Edmund and Barbara Camet,

who together serve as the standard by which I continuously measure myself.

A PREDICTIVE SAFETY MODEL

by

MICHAEL J. CAMET, B.S.M.E.

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mechanical and Industrial Engineering

THE UNIVERISTY OF TEXAS AT EL PASO

May 1999

Acknowledgment

I wish to express my sincere gratitude to Dr. Rolando Quintana, Thesis Committee Chair, for his valuable technical assistance, support and for providing the opportunity to endeavor the Master's Program at The University of Texas at El Paso. I wish to thank Dr. Carroll Johnson and Dr. Carlos Feregut, members of my thesis committee, for providing me with valuable input for the progress of the thesis research.

I would like to thank Bob Deliwala at Kennedy Space Center and Eddie Davis at Marshall Space Flight Center for their insightful comments and suggestions. I would also like to thank Dean Byess, of NAS, Incorporated, whose extensive knowledge and technical assistance was instrumental in this thesis research.

Finally, I wish to acknowledge my wife, Jennifer, whose understanding and support made the long hours involved in this thesis research possible. She took care of every detail on the home front, including our two sons, so that I could devote most of my time to this thesis.

Date of submission of thesis to committee: April 5, 1999

Abstract

This thesis introduces a predictive safety model for accident prevention and system failure, called Continuous Hazard Tracking and Failure Prediction Methodology. It combines the underlying principles of work sampling, control charts, and multivariate analysis.

The sampling is performed to observe the occurrence of conditions which may be becoming hazardous in a given system. These conditions, known as dendritics, may become hazards and could result in an accident, system malfunction, or unacceptable risk conditions.

The Continuous Hazard Tracking and Failure Prediction Methodology comprises of performing a random sampling for the occurrence of the dendritics. The data collected is plotted to generate the appropriate control chart, which depends on the characteristics of the given system and the protection desired. Based on the pattern of the control chart, a system 'under control' is not disturbed whereas a system 'out of control' is investigated for potential conditions becoming hazardous. Then appropriate steps are taken to eliminate or control these conditions in order to maintain a desired safety status of the system. The continuously running characteristic of this model allows for the verification that the corrective measures taken to ameliorate the 'out of control' conditions were satisfactory or whether more proactive action is required. Multivariate analysis can be applied to the data to determine how much each dendritic contributes to 'out of control' situations and as an additional tool for checking the safety status of the system.

Table of Contents

List of Tables

List of Figures

Chapter 1

1. INTRODUCTION

Predictive risk analyses have come into an increasing role in providing the most meaningful and useful information regarding system assessment and system safety (Cooper, 1998). Risk analysis can be used for a systematic, quantitative, and defensible way to evaluate the safety status of a system, identify and prioritize the factors that contribute to the given system's risks, and target them for improvement. The goal is to provide this information in as clear and unambiguous a way as possible.

This Chapter emphasizes the need to look at the concept of system safety with a proactive rather than a reactive view. The successful application of predictive risk assessment methods to determine, monitor and correct the status of a given system's safety status can lead to the prevention of unacceptable risks or hazards.

In Section 1.1, the problem is identified concerning the limitations of the current system safety programs in use today. It is followed with a brief description of the problem in Section 1.2 and the classification of the problem in Section 1.3. Further, Section 1.4 states the rationale for solving the problem and Section 1.5 gives a brief overview of the system that will be analyzed in order to test the methodology. In Section 1.6, the purpose and scope of the research are described, followed by Section 1.7, which gives the details of the thesis organization.

1.1 Problem Statement

Industry has been placing more and more emphasis on safety in design and operations. One way to control system safety is through the analysis of risk. There has been a great amount of interest in recent years on the subject of risk. The increasing sophistication of modern systems, coupled with a higher capability to analyze the given functions of complex systems, has encouraged efforts to predict and mitigate risk (Roland and Moriarity, 1983).

There is still much room for improvement in the present system safety programs being used in industry today. The tracking of safety hazards is essential to predictive safety, and present system safety methods typically do not do this (Firenze, 1978). These safety programs are usually established piecemeal, based on an after-the-fact philosophy of accident prevention (Roland and Moriarity, 1983). When an accident or system malfunction occurs, an investigation is conducted to determine the causes. The relevant causes are then reviewed and discussed to determine what must be done to prevent similar accidents or malfunctions. The resulting system modifications, retrofits, or correction of design safeguards or procedures are made to existing systems.

The concepts underlying the proactive approach to system safety are derived from work sampling and control chart theories, the keys to tracking hazards. These theories emphasize a cost-effective way of keeping a continuous check on the safety status of the system under observation. This new concept, entitled Continuous Hazard Tracking and Failure Prediction Methodology, involves a planned, systematically organized, and

before-the-fact process characterized as the identify-analyze-control method of safety. The emphasis is placed upon an acceptable safety level designed into the system prior to actual production or operation of the system. The continuous hazard tracking and failure prediction methodology requires timely identification and evaluation of the conditions becoming hazardous – before losses occur. A policing and inspection approach aimed at enforcement of safety and health standards cannot generate effective preventative measures because it is episodic, external and coercive. What is needed is a sustained, internal and self-governed program that is relevant and motivated.

1.2 Problem Description

In the context of system safety, safety is achieved by designing and maintaining reliable systems that function in an expected, predictable, and thus safe, manner (Cox and Tait, 1991). When a system (*i.e.*, man + machine + environment) is unable to cope with an unexpected situation, it may lead to an accident or malfunction. However, accidents or malfunctions do not happen unless a hazard exists (Marshall, 1982). Moreover, by definition, a hazard is a condition or changing set of conditions that presents a potential for mishap or malfunction. This definition carries with it two significant points. First, a condition does not have to exist at the moment to be classified as a hazard. When the total hazard is being evaluated, potentially hazardous condition must be considered. Second, hazards may result not only from independent failure or workplace components but also from one workplace component acting upon or influencing another. Thus the

existence of a hazard can be seen as a series of stochastic, dependent, and random events (Firenze, 1978).

The present safety methodologies typically provide feedback on hazards after accidents or malfunctions have happened (Firenze, 1978). What is required is a concept that indicates the system under consideration is becoming hazardous. This information would help to check and eliminate the hazard before accidents can happen.

The Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM) is a concept of providing this information in a statistically verified and economically viable manner by using the principles of work sampling and control charts. The basic hypothesis of CHTFPM is that a random sample of a sufficiently large size reflects the state of the system being observed. Further, plotting of the attribute, namely the existence or potential for a hazard, could indicate whether the system is safe or not.

The fundamental issue in the implementation of the methodology is the identification of the core conditions leading to hazards in any given system. These core conditions can be termed as the dendritics, i.e., building blocks of a particular class of hazards. If these dendritics are present, they may lead to a hazardous condition, which ultimately can result in an accident or system malfunction. An example of dendritics in the case of a fire hazard would be the presence of substances helping combustion, which may lead to a fire hazard and can finally result in a fire.

A preliminary hazard analysis (PHA) can provide an initial risk assessment of a system (Juran and Gryna, 1988). Other established safety tools that can aid in the risk

assessment of a system are fault tree analysis (FTA), safety analysis (SA), system hazard analysis (SHA), and failure mode and effects analysis/critical items list (FMEA/CIL). Pareto analysis can then be performed to get a list of dendritics based on hazard severity, hazard probability, risks, and operational constraints. Pareto analysis is used when there is a need to know the relative importance of data or variables (problems, causes, or conditions). This analysis helps to highlight the few data or variables that may be vital. It also helps to identify which problems, causes, or conditions are the most important or most frequent so they can be addressed first (Dean and Evans, 1994).

Thus, the dendritics form the basis for performing continuous safety sampling to evaluate whether the system is becoming hazardous, so that preemptive actions can be taken to avoid accidents or malfunctions. The characteristics of the continuous hazard tracking and prediction methodology make it a generic tool that can be applied to control any kind of safety hazard.

1.3 Problem Classification

The problem described in Section 1.2 can be classified as a risk analysis problem in safety engineering. An objective of safety engineering is to keep the system reasonably free of operational hazards, but the stochastic nature of hazards and the cost of eliminating them makes a 100% safe environment impractical. Although theoretically possible since most hazards can be identified and removed, incidences are repeated despite knowledge of their causes or the availability of recommended controls (Orn,

1980). In addition, as long as the human element is present in a system, it is unlikely (Brown, 1976).

Safety engineering, as a concept and practice, has been in transition since its beginning. Within the boundaries of safety engineering's emerging abilities exists a capacity for more than simply the detection of causative relationships and the design of practical controls. The implication is clear that knowledge exists which, if used, would stem the vast majority of system malfunctions. The most effective methods for accident prevention are analogous with the methods for the control of quality, cost and quantity of production (Heinrich *et al.*, 1979). This thesis espouses one such concept, namely CHTFPM, which studies the system for the occurrence of conditions becoming hazardous. Steps are then taken to eliminate these conditions when their occurrence crosses certain preset limits or when they show an unnatural pattern in their occurrence.

In essence, the CHTFPM is concerned with ascertaining and maintaining a preset degree of safety, without having adverse effects on operations, time management, cost, and other applicable interfaces to safety that can be achieved throughout the lifecycle of the system. The premise here is that continuous improvement is very much valid for the discipline of safety engineering, as has been shown in the field of quality.

1.4 Rationale for Solving Problem

The formal methods of hazard analysis, categorized as inductive and deductive (National Safety Council, 1992), are limited in their effectiveness as they only come into the picture once a system failure has taken place. They are similar to a post-mortem

report that identifies what happened and how it happened. They do not provide real-time information on whether the conditions in a system are becoming hazardous, which may finally lead to a system malfunction. Present safety methodologies provide comments on hazards before or after accidents have happened. What is required is a concept that indicates that the system under consideration is becoming hazardous. This information would facilitate in checking and eliminating the hazard before accidents or system malfunctions can happen.

Despite the advances made in safety engineering, room for improvement exists. Reports by the Air Force indicate human error was responsible for a large proportion of aircraft accidents (234 out of 313) during 1961 (Willis, 1962). Empirical and analytical studies have shown that human error contributes significantly to the accident risk in nuclear power plant operation (INPO, 1985). The Health and Safety Executive (HSE) claim that human error contributes to 90% of workplace accidents in the United Kingdom (HSE, 1989). They also indicate that as many as 70% of such accidents may be preventable. This attribution of accident causation to errors and unsafe behaviors rather than unsafe conditions tends to oversimplify the situation. It also underestimates the importance of task and environmental variables in creating error-provoking situations.

Probabilistic risk analysis has attempted to incorporate the human factor into a framework for the analysis of systems behavior. The primary focus has been on the quantification of human error into management decision, design and maintenance, and most particularly, operators (Watson and Oakes, 1988). Major accidents such as Three

Mile Island, Bhopal, and Chernobyl have emphasized not only the importance of each of these types of errors but also their interaction in the accident process (Cox and Tait, 1991).

Two points result from the acceptance of the arguments listed above. First, the accident process can be described, in the terms of general systems theory, as an interaction between factors at several different levels of analysis: individual, organizational and technical. This interaction can result in latent accidents waiting to happen, which in turn are triggered by a range of circumstances including operator error. Second, systems analysts should consider the interplay between these different factors and their context, as well as the triggering events.

Arguments can be made to move towards more fully automated systems with no potential for operator error. It can be detrimental to provide so much automation that the operator loses valuable insight into the process being executed (Knoll, 1993). Automation can turn into a double-edged sword in that it can allow a relatively untrained person to execute a process under normal conditions while requiring twice as much knowledge and analysis in case of a problem (Rodgers, 1971). The limited amount of knowledge gained in the execution of an automated process under normal circumstances often does not support the development of an understanding of the system that will be required for identifying and dealing with any problems that may arise. These systems have not always been successful in safety terms or acceptable to the public or client groups, for example in transportation systems (Marshall, 1982). Passengers in an

airplane would not feel safe with a totally automated flight control system along with an absence of pilots onboard. Furthermore, even automated systems need constant monitoring and maintenance and have their own safety problems. There has also been a disproportionate increase in incidents leading to injury during maintenance tasks (HSE, 1985).

US employers incurred more than $60 billion in direct workers' compensation costs in 1992, triple the amount spent ten years earlier. In addition, counting costs such as production delays, damage to equipment, and recruitment and training of replacement workers, brought the total cost for the year to approximately $350 billion (Olsen, 1993). And in addition, disasters such as the Challenger accident in 1986 and Three Mile Island in 1977 can be devastating in terms of public relations and the public's perception of safety inadequacies at the given company. Thus, there is a strong rationale and motivation for solving this risk analysis problem using the proactive approach espoused by CHTFPM.

1.5 Industrial Scenario Analyzed

The Continuous Hazard Tracking and Failure Prediction Methodology can be used in any industrial scenario in general, once the particular safety dendritics have been developed. To demonstrate the potential use of CHTFPM at NASA (NASA Far Grant NAG 10225), a system was chosen at Marshall Space Flight Center (MSFC) for implementation and validation purposes. While NASA has always emphasized safety in design and operations, especially for crewed spacecraft, the Challenger accident brought

home the need for a systematic and quantitative way to evaluate risk and to identify the factors that contribute to them so they can be targeted for improvement (Maggio, 1996). In the late 1980's, the successful application of probabilistic risk analysis methods to nuclear power generation, chemical processing, and other facilities and systems where technological accident risks are of concern led NASA to consider and eventually adopt probabilistic risk analysis as an answer to meet this goal (Frank, 1995).

The Upward Flammability of Materials in Gaseous Oxygen Test, located in the Materials Combustion Research Facility at MSFC, is used to determine the certain characteristics of metals in a high-pressure, 100% gaseous oxygen atmosphere. Metals, which notably defy common ignition regardless of surrounding atmosphere (even 100% oxygen), may burn uncontrollably once ignited. Thus, it is imperative that testing determine which metals are more suitable for use in conditions where ignition is a possibility.

Ordinarily, the test samples are 1/8-inch diameter, 12-inch rods of metal or alloy, although the testing chamber allows up to 18-inch rods, as shown in Figure 1. After initial placement of the test sample into the promoted combustion chamber, an aluminum igniter is attached to the sample. The chamber is then filled with 100% gaseous oxygen (GOX) bringing the chamber up to the desired test pressure, a maximum of 10,000 pounds per square inch is allowed. The sample is ignited and allowed to burn. A carbon dioxide laser provides an alternate ignition method if so desired.. Ten samples are ignited, with the burn length of each sample recorded. A burn length of more than 6

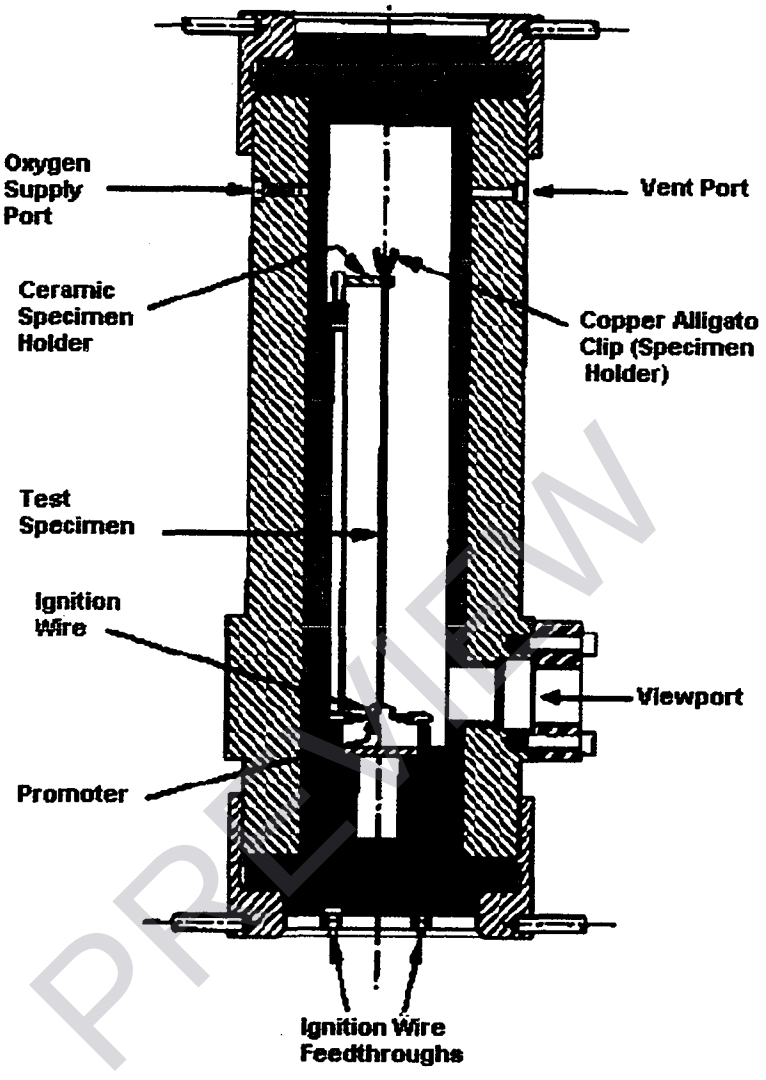

Figure 1: Cross Section of Promoted Combustion Testing Chamber

inches on any one sample constitute failure of the material. Other specific burn characteristics can be ascertained during testing, such as burn time and propagation. Additional information can be gained for variable-pressure GOX conditions through