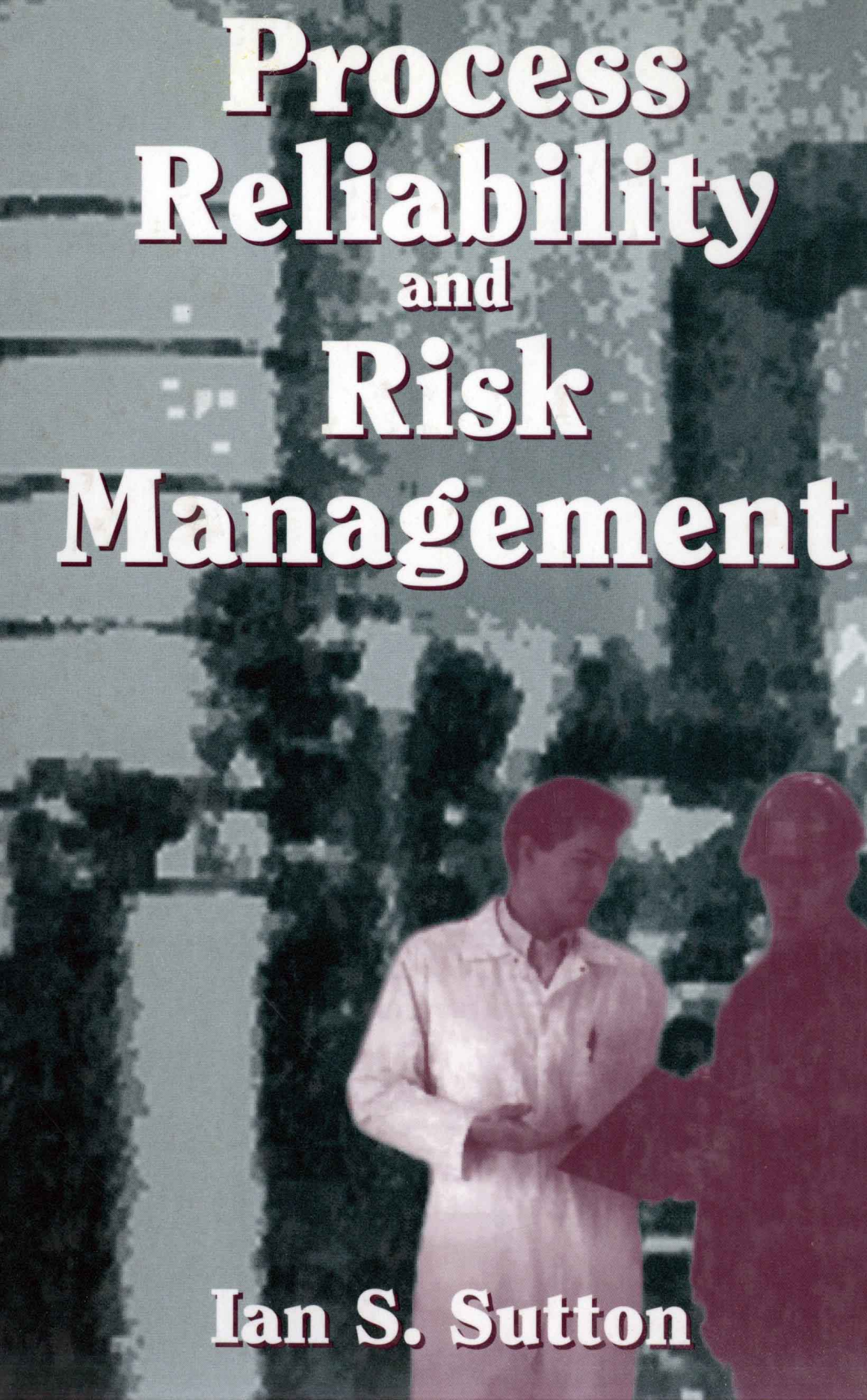
Process Reliability and Risk Management



Ian S. Sutton

Process Reliability and Risk Management

Ian S. Sutton

VNR VAN NOSTRAND REINHOLD
New York

Library of Congress Catalog Card Number 91-20726
ISBN 0-442-00174-6

Manufactured in the United States of America

Published by Van Nostrand Reinhold
115 Fifth Avenue
New York, New York 10003

Chapman and Hall
2-6 Boundary Row
London, SE1 8HN, England

Thomas Nelson Australia
102 Dodds Street
South Melbourne 3205
Victoria, Australia

Nelson Canada
1120 Birchmount Road
Scarborough, Ontario M1K 5G4, Canada

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data
Sutton, Ian S.
Process reliability and risk management / Ian S. Sutton.
p. cm.
Includes bibliographical references and index.
ISBN 0-442-00174-6
1. Risk management. I. Title.
HD61.S88 1991
658.15'5—dc20 91-20726
CIP

Process Reliability and Risk Management

Preface

My interest in reliability in the process industries developed after working at a number of large process facilities where unreliability was a chronic problem that led to large production losses and extensive equipment damage. Unreliability was also a frequent cause of environmental and safety mishaps. What particularly caught my attention was the fact that most reliability problems were completely unanticipated, and that there seemed to be no effective way of predicting what the next unpleasant surprise was going to be or how to prevent it from happening. Therefore, I decided to try to determine how process reliability could be understood in a systematic way, and what analytical tools are available for improving reliability.

Although I was unable to find much information that was directly applicable to process plant reliability, I did find that many of the well-known, safety-oriented risk management techniques can be used in a modified form to improve reliability. Therefore this book, in addition to describing process reliability, provides a description of many of the techniques for process risk management.

Two other specialties contribute to an understanding of process reliability. The first of these is reliability engineering as used in the aerospace and nuclear industries. The second is the increasingly topical subject of quality improvement—in particular statistical process control. Both of these specialties are referred to in this book and appropriate lessons are drawn from them.

I have written this book primarily for engineers and managers who are actually working in process plants. This means that the application of risk management and reliability techniques is emphasized, with theory being introduced only when necessary to provide a basic understanding of what is being discussed. Many process-oriented worked examples are provided. In particular, a very simple worked example is introduced in Chapter 1. It is then used throughout the book to explain new concepts as they are introduced. Because the focus of the book is in practical applications, I have pointed out limitations in all the techniques that are described.

The book contains many references to human performance and human error. This meant that I was faced with the problem of using inclusive language when talking about people. Because phrases such as "he/she"

are rather awkward, I decided to use the masculine pronoun only. No judgment should be inferred from this decision—other than the inadequacy of the English language.

The biggest single problem I faced in writing this book was in deciding when to stop. For example, after every HAZOP that I lead, my ideas and thoughts on the method change, as I see how it can be applied or modified in yet another way. However, as I was taught when I first moved to New York from England, "Enough is enough already!"—so here we are.

The contributions of my many colleagues, both inside Science Applications International Corporation (SAIC) and in other companies, has been absolutely invaluable. Without their knowledge, advice, criticism, and support I could never have finished this project. And, to Val, Ann, and Peter—thank you for your patience. I could never have made it without you.

Contents

1

Reliability in the Process Industries

INTRODUCTION

One of the most effective ways of increasing a process plant's profitability is to improve its reliability, either by reducing the number of unplanned shutdowns, or by minimizing the length of scheduled turnarounds. The purpose of this book, which is written primarily for engineers and managers in the process industries, is to provide an introductory explanation of reliability engineering and risk management techniques and to show how these techniques can be applied in practical situations. In particular, the well-established risk management methods for improving safety are used, in a modified form, to show how reliability can be improved. Therefore, the book also serves as an introduction to the basic concepts of risk management.

The benefits of improved reliability will generally fall into one or more of the following categories.

- **Increased Production.** A reliable plant will make more product because there will be fewer breakdowns. The extra production will not only increase revenues (assuming that the additional product can be sold), but it will also generate high incremental profits because all of the plant's fixed costs will have already been covered by the base-line production.
- **Increased Productivity.** An unreliable plant suffers from an excessive number of shutdowns. During a shutdown, particularly one that is unplanned, material and energy yields will deteriorate for reasons such as increased flaring, the need to recycle off-spec products, poor reactor selectivities, and increased maintenance costs. Increased reliability reduces these productivity losses.

- **Safety.** An unreliable plant is usually unsafe. Shutdowns (particularly when they occur unexpectedly) can lead to unanticipated and dangerous operating conditions. Also, the opening and repairing of equipment once the plant is shut down will usually be hazardous.
- **Environmental Impact.** A plant shutdown (and the subsequent restart) often leads to a release of process materials to the environment. Therefore, increasing reliability should result in reduced emissions and fewer complaints from the public.
- **Customer Satisfaction.** Increased reliability should increase customer satisfaction because there will be fewer missed delivery dates and off-spec products.

Reliability Improvement

There are two types of reliability improvement project. The first type consists simply of fixing an easily identified problem, such as the repeated breakdown of a critical piece of equipment. In this type of situation, what needs to be done to bring the situation back to normal is usually clear. The only action required is that the unreliable item be fixed—a formal analysis is not required.

The second type of reliability project is one in which there is no obvious problem that needs to be remedied; instead there is simply a desire to improve a plant's normal, base-line reliability. In situations such as these, reliability improvement is seen as a long-term, ongoing process. In this type of project, the ways in which reliability can be improved will often not be intuitively obvious, particularly for highly integrated, complex processes. Generally, a wide range of options for improving reliability is available, ranging from improving the quality of equipment already in place, to installation of backup or redundant equipment, to increasing operator training. The implementation of any of these options should lead to improved reliability, but it is important to know how to choose the most cost-effective options.

This book concentrates on the second type of reliability improvement project, i.e., improvement in long-term base-line reliability.

Quantification

A project to improve base-line reliability will often require system quantification because the differences between the various proposals for improving reliability are likely to be sufficiently small that the best choice will not be intuitively clear. Unfortunately, the quantification of reliability is

fraught with controversy. In particular, the accuracy of the basic failure rate data (for both equipment and human beings) and the infrequency with which major failure events occur are often cited as reasons for challenging the validity of quantified analyses.

The problem of data accuracy can be addressed, at least partially, by the development of plant-specific failure rate data (or, if the plant is not yet built, failure rate data from similar plants). The collection of this type of data will become increasingly practicable as more and more computer control and preventive maintenance systems are put into place. They will facilitate the recording of failure and repair data.

Reliability and Safety

Some of the reliability improvement methods described in the following chapters will be familiar to engineers who are responsible for safety improvement. The reason for this is that both safety and reliability are concerned with "things that go wrong"; it is only their goals that are different. A typical safety program focuses on injuries and fatalities, whereas reliability is concerned more with economic issues such as production, productivity, and customer satisfaction. The different objectives of safety and reliability projects mean that well-established safety techniques, such as the hazard and operability (HAZOP) methods and fault tree analysis, require some modification and adaptation in reliability projects.

REASONS FOR IMPROVING RELIABILITY

The justification for a reliability improvement program usually falls into one or more of the following five categories:

1. increased production
2. increased productivity
3. reduced maintenance expense
4. improved safety
5. reduced environmental problems.

Increased Production

The need to increase production is usually the primary motive for improving reliability. If a plant can sell all of the product that it makes, then every extra day of operation leads to increased revenues. Such incremental

revenues are often very profitable because all the fixed costs (such as depreciation) and the semi-fixed costs (such as nonhourly labor) have already been covered.

Occasionally, a long-term reliability improvement program may conflict with short-term production goals. This will occur, for example, if equipment has to be shut down for routine service and preventive maintenance.

Productivity

During a plant shutdown (and the subsequent restart), a plant's yields and efficiencies are often very poor. Typical problems that occur during these transient conditions are as follows.

- Raw materials are wasted. For example, valuable feedstocks are flared off or dumped to the fuel gas system.
- Additional energy is needed to recycle materials, to heat up equipment for restart, and to reprocess off-spec product.
- Overtime will be needed for operating and maintenance crews.
- Every time a plant shuts down and then restarts, transient shocks can build up a cumulative effect, leading to additional long-term reliability problems. A common example of this occurs with reactor catalysts, which frequently suffer from an irreversible aging effect whenever the process is shut down and then restarted.

Any increase in reliability should help reduce these problems. It should also increase productivity because the plant staff has more time to work on money-making projects instead of coping with crises.

Maintenance

A more reliable plant should save money as a result of needing less repair work. However, this may have to be balanced against the fact that a reliability program will often require that more time be spent on preventive maintenance.

Safety

Improvements in reliability usually lead to improvements in safety for the following four reasons.

1. During a shutdown (and subsequent restart), the plant is in an unusual and dynamic mode, in which both staff and equipment are operating

under unfamiliar, and sometimes high-stress conditions; thus the probability of an accident taking place is increased.
2. A shutdown is often a time during which the operations staff is permitted to ignore alarm signals and override plant interlocks.
3. Once the plant is down, equipment usually has to be opened for maintenance and repair, thus exposing operators and maintenance crews to flammable and/or toxic process materials. Maintenance activities such as moving equipment, welding, and pulling exchanger bundles are themselves often hazardous.
4. Shutting a plant down and then restarting it often leads to the accumulation of transient effects that can induce early equipment failure.

Although improvements in reliability generally lead to concomitant improvements in safety, the two do not always go together; there is sometimes a conflict, as shown by the following illustrations.

- Adding safety equipment may reduce reliability. A common example is the use of fire eyes to shut down a fired heater on loss of flame. If the fire eyes give a spurious signal, reliability will be reduced as a result of a safety improvement. (In extreme cases, additional safety equipment might reduce reliability to a point where safety is jeopardized.[1])
- A reliable plant does not undergo many shutdowns. Therefore, the operators are less familiar with shutdown and startup procedures than they would be if the plant were unreliable. This makes them less practiced at handling emergencies and major upsets.
- Unsafe engineering practices will sometimes increase reliability. For example, temporary bypasses and jumper lines are sometimes installed to keep the unit running during an operational upset. Such temporary lines can be extremely hazardous because they may be inadequately engineered and because they permit what is often a highly abnormal operation. Furthermore, although these lines were supposed to be temporary at the time of installation, they often remain in place for many years, thus becoming a permanent part of the system. "Temporary" lines of this type are often a particular problem in tank farms.
- Safety precautions (such as protective clothing) may make the plant more difficult to operate and, therefore, less reliable.

Although the goals of reliability and safety are not necessarily identical, many reliability improvement projects are partially justified by anticipated improvements in safety. With this in mind, it is useful to try to provide an estimate, no matter how rough, of the economic value of safety. This will then allow the benefits and costs of safety improvement projects to be

TABLE 1-1. Economic Benefit and Safety

Years Between Incidents	1	100	1,000	10,000
Plant damage, $	1,000	10,000	100,000	1,000,000
Public property damage, $	None	1,000	10,000	100,000
Injury at plant	None	Probable	Yes	Yes
Public injury	None	Marginal	Yes	Yes
Death at plant	None	None	Slight	≦1
Public death	None	None	Slight	≦1

evaluated on the same basis as other projects. Of course, it is not possible to place a definitive value on human life, nor is it possible to calculate the cost of pain and suffering; nevertheless some value judgment is made (however implicitly) whenever investments are made in safety improvement projects.

Some companies use a matrix such as that shown in Table 1-1 to assign some numerical value to *acceptable risk.** This matrix shows one company's judgment as to the acceptable frequency with which various types of accident and loss can occur. So, for example, column 4 of the table indicates that a death rate of 1 in 10,000 years and a plant loss of $1 million per 10,000 years are both "acceptable." Note that some risks are shown as having a value of "None," i.e., they are deemed to be totally unacceptable. Although risk must always have a value that is greater than zero, the use of this word simply implies that the probability of such an incident should be very low indeed.

It can be seen that a matrix such as this puts safety and economics on the same footing. Referring once more to Table 1-1, it can be inferred that an investment that reduces the fatality rate from 1 in 100 years to 1 in 10,000 years is "worth" about $1 million.

Since death is inevitable, some companies try to determine the cost effectiveness of safety measures in terms of life *extension* per dollar spent,[2] rather than simply estimating an accident rate. This provides more rational basis for risk analysis, particularly when the objective is reducing long-term risk.

Societal acceptance of risk also provides guidance as to the economic

* It should be stressed that the numerical values shown here are intended to be representative only. Each company will need to develop its own set of data for matrices such as this.

value of safety. The acceptable level of risk to society (for events that are outside an individual's control[3]) can perhaps be most conveniently illustrated with the deaths associated with automobiles.[4] In the United States, there were 46,386 traffic-related deaths in 1987. For a population of 240 million, this means that the fatality rate is approximately 1.93×10^{-4}/yr. Although there are many programs to reduce this death rate, society seems, on the whole, to find this value more or less acceptable. This approach is also reflected by use of the fatal accident rate (FAR) in the process industries (the number of fatalities per 10^8 h of exposure to the activity or hazard being considered).

The frequency of 1 in 10,000 years for a serious accident is often suggested as being an appropriate acceptable value for serious injury or death,[5,6] or for a large accident at a process plant. For example, a recent study[7] analyzed 132 federal regulatory decisions and came up with the following guidelines. (The guidelines are based on extended exposure—the assumption that exposure is for ten years is made here, not in the source material).

- If the risk of death or serious injury is greater than 4×10^{-4}/year, action *must* be taken.
- If the risk is less than 1×10^{-6}/year, action need not be taken.
- If the risk lies between these two limits, action should be taken if the cost is below $2 million per life saved.

Another well-known study, the Rijnmond report,[8] suggests a threshold value of 1×10^{-4}/yr for acceptable risk. Additional references on this topic based on European work are provided by Lans and Bjordal.[9] These references generally suggest that a values of 1 in 10,000 years for a major accident is a reasonable goal. At this time, none of the United States agencies (such as OSHA, EPA, or the state legislatures) have promulgated a standard for acceptable risk. (Legislative issues and the codes issued by various professional bodies are discussed in Chapter 9.)

It may be thought that the insurance industry would have a good understanding of the financial value of human life. However, insurance companies do not really assign a value to life. They simply set premiums using actuarial tables so that they maintain profitability; they do not place a value on human life as such.

In conclusion, if there is a probability of serious injury or death to an individual of greater than 1 in 10,000 years, the consensus would appear to be that some action is required. If the probability is lower than this, the justification for a reliability project as a means for improving safety can be obtained using guidelines such as those shown in Table 1-1.

Environmental Impact

A plant shutdown, especially an unplanned shutdown, often leads to large and unexpected discharges of process materials to the environment. Indeed, if a plant is in compliance with environmental regulations during normal operation, then environmental problems can often be equated with reliability problems. Therefore, increased reliability will generally lead to better environmental performance.

Customer Satisfaction and Company Image

A plant that operates reliably will create satisfied customers because fewer problems with off-spec product and missed delivery dates will be encountered.

An additional qualitative benefit of improved reliability is an enhanced company image. The company that operates a smooth, steady operation looks impressive to customers, staff, competitors, regulators, and the investment community. Similarly, the manager who is running that same operation looks impressive to his superiors, peers, and subordinates.

Cost of a Reliability Improvement Program

Although increased reliability is always desirable, there is usually a cost associated with its attainment. Therefore, investments in reliability should only be continued until the incremental revenue generated is no greater than the expenditure required for its generation [illustrated in Fig. 1-1, in

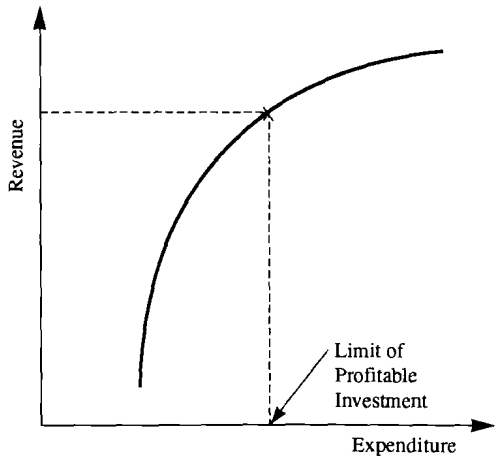


FIGURE 1-1. Justification for Reliability Investments.