Introduction to System Safety Engineering

Introduction to System Safety Engineering

William P. Rodgers

System Safety Engineering Consultant
Rodgers Management
Norman, Oklahoma

System Safety Engineering Manager
TRW Systems
Redondo Beach, California

John Wiley & Sons, Inc.
New York • London • Syndey • Toronto

Library of Congress Catalog Card Number: 72-171914

ISBN 0-471-72933-7

Printed in the United of America.

10 9 8 7 6 5 4 3 2

Introduction to System Safety Engineering

Wiley Series on Systems Engineering and Analysis
HAROLD CHESTNUT, Editor

Chestnut

Systems Engineering Tools

Wilson and Wilson

Information, Computers, and System Design

Hahn and Shapiro

Statistical Models in Engineering

Chestnut

Systems Engineering Methods

Rudwick

Systems Analysis for Effective Planning:

Principles and Cases

Wilson & Wilson

From Idea to Working Model

Sunde

Communication Systems Engineering Theory

Rodgers

Introduction to System Safety Engineering

To my wife Iva who has faithfully supported me with understanding and prayers during my engineering career

SYSTEMS ENGINEERING AND ANALYSIS SERIES

In a society which is producing more people, more materials, more things, and more information than ever before, systems engineering is indispensable in meeting the challenge of complexity. This series of books is an attempt to bring together in a complementary as well as unified fashion the many specialties of the subject, such as modeling and simulation, computing, control, probability and statistics, optimization, reliability, and economics, and to emphasize the interrelationship between them.

The aim is to make the series as comprehensive as possible without dwelling on the myriad details of each specialty and at the same time to provide a broad basic framework on which to build these details. The design of these books will be fundamental in nature to meet the needs of students and engineers and to insure they remain of lasting interest and importance.

Preface

This book is written to accomplish just what the title implies, to introduce students to System Safety Engineering. Like any new professional discipline, there is a lack of knowledge concerning what system safety is, what it can do, and how to use it. These three questions were a primary influence during the writing of this book. As a result, a very practical approach, written in relatively non-technical language is employed. The material presented should give the reader an appreciation for the function of system safety engineering integral in the design and development of products and systems. The reader will also understand the type of information needed to support the system safety effort: the value of safety experience retention; the decision documentation effected which assists the legal people in product liability suits; and the relationship of system safety with other program disciplines such as reliability, system engineering, test engineering, etc.

The author has, for the first time, put into one book a chronological sequence of events from which system safety engineering evolved. By presenting a historical understanding of this new discipline, a foundation is established upon which the strong and weak points of the practical application of system safety can be discussed. The various analytical methods are discussed in Chapter 4 with typical examples of each analysis presented.

The author has presented a fundamental and practical approach to system safety engineering which can be used both as a textbook and a management reference book. By applying the principles presented and following the basic system safety product development program presented in Chapter 3, an efficient and cost effective system safety engineering effort may be carried out.

William P. Rodgers

Redondo Beach, California
August 1971

Contents

1

Safety Within Product Development

A most difficult task to accomplish when explaining a subject is to ensure that the definitions of the terms used are understood. This is especially true with the word *safety*. Practically everyone will say they understand safety until asked to write a specific definition. One very quickly finds that although the word safety is commonly used, it has an infinite number of definitions dependent upon the subjective evaluation of the person using it. For example, piloting a private airplane is considered relatively *safe* to a trained pilot; but, to someone who has never taken flying lessons, it would be a very dangerous and almost certain fatal venture. Or take another case. The individual who commutes to and from work everyday on the Los Angeles freeways accepts his way of life as being *safe* as evidenced by his willingness to expose himself to it twice each day for 5 or 6 days each week. However, for an individual who has only driven in the sparsely populated two-lane roads of Rural America, to be placed on the Los Angeles freeways, especially during rush hours, would be a very harrowing and dangerous experience.

Safety is defined in a subjective and relative manner. Webster defines safety as "the condition of being safe; freedom from danger or hazards, a keeping of oneself or others safe, especially from danger of accidents or disease." Unfortunately, a definition is nebulous at best when the word itself has to be used to define it. Again this illustrates the fact that safety is a relative and subjective term. The Department of Defense (DOD), in their Military Standard for System Safety, Mil-Std-882, dated 15 July 1969, defines safety as: "Freedom from those conditions that can cause injury or death to personnel, damage to or loss of equipment or property." This definition has caused considerable controversy over the interpretation of damage to or loss of property. When interpreted literally, this would include wear-out failures and out-of-specification anomalies. A definition that more concretely describes safety is: "The surety that the environment that personnel or items are subjected to is free from inadvertent or unexpected events which may result in injury to personnel or damage to the

items exposed." This is the definition that will be used for safety through the remainder of this book.

It has only been in the last 60 years that employers have given much attention to safety. Until recently, the protection of one's self was a responsibility left to the individual much the same as supplying the necessary tools of the trade. The dominant factor for hiring people prior to the early 1900's was production. It was left up to each individual to supply his own clothes and hand tools. Personal safety was the responsibility of each employee and very seldom did an employee get paid when he missed work because of a physical injury. In fact, many times an employee was penalized if he got hurt and overall production was affected.

In the past 60 years, the responsibility for safety has shifted from the employee to the employer. It is now the responsibility of the employer to provide a safe working environment and necessary tools and equipment to maintain that safe environment. In fact, with court decisions favoring the injured employee, it can be a very costly error for an employer not to take all possible precautions in providing for the safety of his employees. The shift of safety responsibility has been the result of unions, employee groups, and the public in general, demanding legislation and control which forced industry management to accept this responsibility. For example, a few years ago the Interstate Commerce Commission Regulations for Transportation of Explosives and Other Dangerous Articles By Land and Water, in Rail Freight Service and by Motor Vehicle (Highway) and Water Including Specifications for Shipping Containers, was compiled for safety reasons to protect the general public, as well as the employees handling the materials. For a company not to comply with these regulations was in violation of Public Law 86-710 passed by the 86th Congress. Fines of $10,000 and imprisonment up to 10 years could have been imposed for violating these regulations.

Safety programs have been established in the past on an after-the-fact philosophy. That is, when an accident occurred an investigation was conducted to determine what was needed to prevent a similar accident from recurring. A short review of product development philosophy will help in understanding the origin of the after-the-fact safety approach.

Fifty years ago or more, a young man entering a new profession was expected to start in the shop and learn how to make the produced product with his own hands. By doing this, the new man learned to appreciate the problems of the machinist, the assembler, the tester and the operator or user. The years required for this type of apprentice training were expected and allowed for in the career cycle of an employee. In the early part of the century, a man could expect to devote his entire career to the manufacturing of one or two products. However, this is no longer the case. In studies prepared for the National Commission on Technology, Automation and Economics Progress, The Employment Impact of

Technological Change, Appendix Volume II, Technology and the American Economy, The Report of the Commission, February 1966, Page II-33–"An Investigation of the Rate of Development and Diffusion on Technology in our Modern Industrial Society," (prepared for the Commission by Frank Lynn, INTEC, Inc., Chicago, Ill.), it was found that:

> "The average lapsed time between initial discovery of a new technological innovation and the recognition of its commercial potential decreased from 30 years for technological innovations introduced during the early part of this century (1880-1919) to 16 years for innovations introduced during the post-World War II period, the time required to translate a basic technical discovery into a commercial produce or process decreased from 7 to 5 years during the 1960 to 1970 time period investigated."

Not only is the time required to translate a basic technical discovery into a commercial product or process decreased to a few years, but also the number of new products or processes is increasing at an exponential rate. This rate increase is proportional to the population increase as shown in Figure 1. When one realizes that two-thirds of the people born since the origin of man are alive today, it is not hard to understand the tremendous increase in the number of new products.

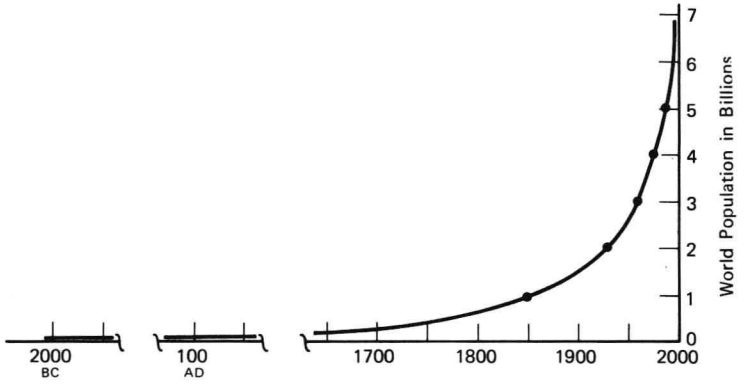

Figure 1. World Population Increase. (Note: Information Taken From World Book Encyclopedia Year Book 1963, pages 188-189)

Two other examples that indicate the increase of new products are the total research and development expenditures and the number of research scientists and engineers in the United States. See Figure 2.

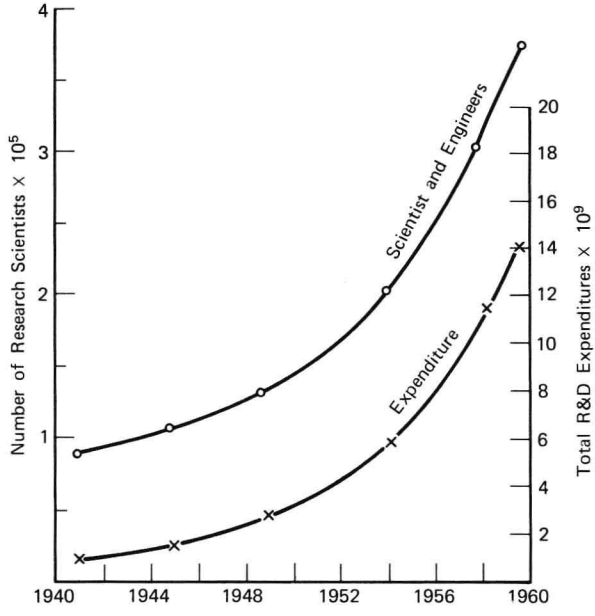

Figure 2. Development Expenditures and Number of Scientists in U.S.

The increase in the number and complexity of consumer products and the decrease in the development cycle time has forced a change in the management control of new products. There used to be sufficient time in a product life cycle to build one or two end items, test them, make necessary improvements, retest, etc., prior to committing to a production schedule. By this time, each manufacturing step and cost was well defined and production plans could be made with a high degree of accuracy. Now, however, this is no longer true. Today we live in an atmosphere of change. Technological progress has been massive and phenomenal. People's minds must be active, progressive and adaptable to a constantly changing way of life forced upon us by such things as: instant communications; high speed transportation; massive computerized analysis; information storage and retrieval capabilities; control and use of high energy sources, such as atomic fission, laser beams, etc. One of the results of this atmosphere of change is the specialization introduced into product development.

Today, an employee generally must specialize in one very narrow field that is used in producing many end products. For example, an automotive engineer may specialize in carburetion and know very little about the rest of an engine or

automobile. A machinist may be very capable on a turret lathe, but know nothing about a drill press or milling machine.

What does all of this mean in relationship to safety?

1. The specialization way of life has often hidden the overall potential dangers to the individual employee. This, in turn, places the responsibility of the employee's safety in the hands of the employer.

2. The increased complexity and costs of new products have made it very uneconomical and disastrous to follow the after-the-fact accident/investigate/fix philosophy.

3. The change in legal liability responsibility causes product safety programs to be concerned with the customer and/or consumer, as well as the employee.

4. The discovery of high energy sources such as exotic fuels, high pressure systems and atomic fissions has increased the magnitude of the potential catastrophic effects of an accident. In fact, in the case of atomic explosions, even one accident cannot be tolerated.

Table 1 lists some examples of how costly, in both lives and dollars, some accidents have been in recent years. Table 2 gives the occupational accident statistics for the United States federal employees and the overall national annual rate between 1958 and 1964. It is no wonder that in recent years more and more emphasis is being placed on before-the-fact identify/analyze/prevent safety programs, rather than the old after-the-fact accident/investigate/fix concepts. As will be seen in the next chapter, the increase in number and complexity of systems has also forced a change in attitudes toward safety.

Table 1. *Some Disasters Involving Propellants and/or Explosives (Excluding Mine Explosions)*

1917, December 6—Halifax, Nova Scotia, Canada
Explosion of war materials and fire; over 1,500 killed; 4,000 injured; 20,000 homeless; property loss $35,000,000.

1921, September 21—Oppau, Germany
Explosion of ammonium nitrate kills about 600 persons.

1937, March 18—New London, Texas
Natural gas explosion destroys schoolhouse; 413 children and 14 teachers killed.

1939, March 1–Osaka, Japan
Huge munitions dump explodes, wiping out village; 500 killed and injured, 300 houses destroyed, 8,313 homeless.

1939, July 10–Penandara de Bracamonte, Spain
Approximately 100 killed; 1500 injured; town demolished in explosion of munitions factory.

1941, June 8–Smederevo, Yugoslavia
Ammunition plant explodes; killing 1,000 and demolishing most of the town.

1942, May 1–Tessenderlo, Belgium
Explosion in chemical works kills 250 workers, injures 1,000.

1944, April 14–Bombay, India
128 die in ship fire which causes explosion in ammunition dump; 1,000 injured.

1944, July 17–Port Chicago, California
Explosions at two ammunition dumps kill more than 300.

1947, April 16–Texas City, Texas
Explosion of French vessel GRANDCHAMP destroys most of city; more than 500 dead or missing.

1947, August 20–Cadiz, Spain
300–500 killed in explosion of shipyards.

1948, March 9–Tsingtao, China
Explosion of ammunition storehouse kills at least 200; several hundred injured.

1948, July 28–Ludwigshafen, Germany
Explosions and fire wreck chemical works of I. G. Farben Company; approximately 200 killed and several thousand injured; damage $15,000,000.

1948, September 22–Hong Kong, China
Fire and chemical explosion in warehouse; 135 killed, 57 injured.

1953, October 16–Boston, Massachusetts
Explosion and fire aboard U.S. aircraft carrier LEYTE kills 37, injures 40.

1956, August 7–Call, Columbia
Seven trucks carrying dynamite explode; dead estimated at 1,100.

1958, June 23–Santa Amaro, Brazil
Fireworks explosion causes about 100 deaths.

1960, March 4–Havana, Cuba
French munition ship blows up, killing 75–100 and injures 200.

Note: Information taken from Encyclopedia Americana.

Table 2. *Occupational Accident Statistics*

	Federal 1958-1964	National Annual Rate
Deaths	1,200	13,800
Disabling Injuries	300,000	1,960,000
Lost Man-Days	18,500,000	235,000,000*

*Equivalent to 990,000 man-years.