Components of System Safety

Proceedings of the Tenth Safety-critical Systems Symposium, Southampton, UK, 2002

Edited by
Felix Redmill and
Tom Anderson

Springer

Safety-Critical
Systems Club

Felix Redmill and Tom Anderson (Eds)

Components of System Safety

Proceedings of the Tenth Safety-critical Systems Symposium, Southampton, UK 2002

Safety-Critical
Systems Club

Data Systems
& Solutions

Springer

Felix Redmill
Redmill Consultancy, 22 Onslow Gardens, London, N10 3JU

Tom Anderson
Centre for Software Reliability, University of Newcastle,
Newcastle upon Tyne, NE1 7RU

British Library Cataloguing in Publication Data
Safety-critical Systems symposium (10th : 2002 :
Southampton, UK)
Components of system safety ; proceedings of the Tenth
Safety-critical Systems Symposium, Southampton, UK, 2002
1.Industrial safety – Management – Congresses 2.Automatic
control – Reliability – Congresses 3.Computer software –
Reliability – Congresses
I.Title II.Redmill, Felix, 1944- III.Anderson, T. (Thomas)
1947-
620.8'6
ISBN 1852335610

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress.

ISBN 1-85233-561-0 Springer-Verlag London Berlin Heidelberg
a member of BertelsmannSpringer Science+Business Media GmbH
http://www.springer.co.uk

Printed in Great Britain

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Camera ready by contributors
Printed and bound by the Athenæum Press Ltd., Gateshead, Tyne & Wear
34/3830-543210 Printed on acid-free paper SPIN 10854697

PREFACE

The Safety-critical Systems Symposium has now been held in early February for ten consecutive years, and this book contains the papers presented at the tenth annual event. The Symposium sessions bring together some of the key components of system safety - the investigation of accidents, the definition of safety requirements as well as functional requirements, an understanding of risk, and the recognition of humans and their behaviour as being crucial to safety.

The papers in this book, on these and related topics, are representative of modern safety thinking, the questions that arise from it, and the investigations that result from its application to accident analysis. Nine are written by leading industrialists and five by academics, and all are aimed at the transfer of technology, experience, and lessons, to and within industry. They offer a broad range of views and, not only do they show what has been done and what could be done, but they also lead the reader to speculate on ways in which safety might be improved - for example, through more enlightened management, a systematic application of lessons, process improvement, and a better understanding of risk and how it may be affected by system design. They also indicate new directions in which safety thinking is being extended, for example in respect of information systems whose data is used in safety-related applications, and 'e-safety'.

The papers are presented in the order in which they were given at the symposium and are laid out under six headings that match the symposium sessions:

- Accidents and Their Investigation
- Issues of Low-SIL Systems
- Human Factors
- Safety Requirements
- Risk
- Communication and Electronic Safety

Not only these Proceedings, but those of all ten symposia, have been published by Springer Verlag, and we thank Springer, and in particular Rebecca Mowat, for their supportive partnership during the last decade. But there can be no Proceedings without papers, and we also thank the authors of the papers in this volume for their time and effort, their cooperation, and their responsiveness to our requirements. We also express our gratitude to Data Systems and Solutions for sponsorship of this book of Proceedings.

FR and TA
October 2001

THE SAFETY-CRITICAL SYSTEMS CLUB

sponsor and organiser
of the

Safety-critical Systems Symposium

What is the Club?

The Safety-Critical Systems Club exists to raise awareness and facilitate technology transfer in the field of safety-critical systems. It is a non-profit organisation which cooperates with all interested bodies.

History

The Club was inaugurated in 1991 under the sponsorship of the Department of Trade and Industry (DTI) and the Engineering and Physical Sciences Research Council (EPSRC), and is organised by the Centre for Software Reliability (CSR) at the University of Newcastle upon Tyne. Its Co-ordinator is Felix Redmill of Redmill Consultancy.

Since 1994 the Club has had to be self-sufficient, but it retains the active support of the DTI and EPSRC, as well as that of the Health and Safety Executive, the Institution of Electrical Engineers, and the British Computer Society. All of these bodies are represented on the Club's Steering Group.

What does the Club do?

The Club achieves its goals of technology transfer and awareness raising by focusing on current and emerging practices in safety engineering, software engineering, and standards which relate to safety in processes and products. Its activities include:

- Running the annual Safety-critical Systems Symposium each February (the first was in 1993), with published Proceedings;
- Putting on a number of 1- and 2-day seminars each year;
- Providing tutorials on relevant subjects;
- Publishing a newsletter, *Safety Systems*, three times each year (since 1991), in January, May and September.

How does the Club help?

The Club brings together technical and managerial personnel within all sectors of the safety-critical systems community. It facilitates communication among researchers, the transfer of technology from researchers to users, feedback from users to researchers, and the communication of experience between users. It provides a meeting point for industry and academe, a forum for the presentation of the results of relevant projects, and a means of learning and keeping up-todate in the field.

The Club thus helps to achieve more effective research, a more rapid and effective transfer and use of technology, the identification of best practices, the definition of requirements for education and training, and the dissemination of information.

Membership

Members pay a reduced fee (well below a commercial level) for events and receive the newsletter and other mailed information. As it receives no sponsorship, the Club depends on members' subscriptions, which can be paid at the first meeting attended.

To join, please contact Mrs Joan Atkinson at: CSR, Bedson Building, University of Newcastle upon Tyne, NE1 7RU; Telephone: 0191 221 2222; Fax: 0191 222 7995; Email: csr@newcastle.ac.uk

CONTENTS LIST

ACCIDENTS AND THEIR INVESTIGATION

ISSUES OF LOW-SIL SYSTEMS

HUMAN FACTORS

SAFETY REQUIREMENTS

RISK

COMMUNICATION AND ELECTRONIC SAFETY

ACCIDENTS AND THEIR INVESTIGATION

Accident Investigation – Missed Opportunities

Trevor Kletz
Dept of Chemical Engineering, Loughborough University LE11 3TU

Abstract

After paying the high price of an accident, we often miss the following opportunities to learn from it:

- We find only a single cause, often the final triggering event.
- We find immediate causes but not ways of avoiding the hazards or weaknesses in management.
- We list human error as a cause without saying what sort of error though different actions are needed to prevent those due to ignorance, those due to slips or lapses of attention and those due to non-compliance.
- We list causes we can do little about.
- We change procedures rather than designs.
- We do not help others to learn as much as they could from our experiences.
- We forget the lessons learned and allow the accident to happen again. We need better training, by describing accidents first rather than principles, as accidents grab our attention; we need discussion rather that lecturing, so that more is remembered; we need databases that can present relevant information without the user having to ask for it.

Finally, we ask if legislation can produce improvements.

Introduction

Almost all the industrial accidents that occur need not have occurred. Similar ones have happened before and have been described in published reports. Someone knew how to prevent them even if the people on the job at the time did not. This suggests that here is something seriously wrong with our safety training and the availability of information.

Having paid the price of an accident, minor or serious (or narrowly missed), we should use the opportunity to learn from it. Failures should be seen as educational experiences. The seven major opportunities summarised above are frequently missed, the first five during the preparation of a report and the other two afterwards. Having paid the "tuition fee", we should learn the lessons.

1 Accident Investigations Often Find Only a Single Cause

Often, accident reports identify only a single cause, though many people, from the front-end designers, down to the last link in the chain, the mechanic who broke the wrong joint or the operator who closed the wrong valve, had an opportunity to prevent the accident. The single cause identified is usually this last link in the chain of events that led to the accident.

Just as we are blind to all but one of the octaves in the electromagnetic spectrum so we are blind to many of the opportunities that we have to prevent an accident.

2 Accident Investigations are Often Superficial

Even when we find more than one cause, we often find only the immediate causes. We should look beyond them for ways of avoiding the hazards, such as inherently safer design - could less hazardous raw materials have been used? - and for weaknesses in the management system: could more safety features have been included in the design? Were the operators adequately trained and instructed? If a mechanic opened up the wrong piece of equipment, could there have been a better system for identifying it? Were previous incidents overlooked because the results were, by good fortune, only trivial? The emphasis should shift from blaming the operator to removing opportunities for error or identifying weaknesses in the design and management systems.

When investigators are asked to look for underlying or root causes they may call the causes they have found root causes. One report quoted corrosion as the root cause of equipment failure but it is an immediate cause. To find the root cause we need to ask if corrosion was foreseen during design and if not, why not; if operating conditions were the same as those given to the designer and if not, why not; if regular examination for corrosion had been requested, and if so, if it had been carried out and the results acted upon, and so on. Senior managers should not accept accident reports that deal only with immediate causes.

Most commentators on the disaster at Bhopal in 1984 missed the most important lesson that can be drawn from it: the material that leaked and killed over 2000 people was not a product or raw material but an intermediate. It was not essential to do store it and afterwards many companies did reduce their stocks of hazardous intermediates, often using them as they were made and replacing 50 or more tonnes in a tank by a few kilograms in a pipeline. For ten years since the explosion at Flixborough in 1974, the importance of keeping stocks of hazardous chemicals as low as possible had been advocated. Though reducing stocks saves money as well as increasing safety little had been done. If we can avoid hazards we can often design plants that are cheaper as well as safer.

The report on a serious explosion that killed four men [Kletz 2001b] shows how easily underlying causes can be missed. The explosion occurred in a building where ethylene gas was processed at high pressure. A leak from a badly made joint was ignited by an unknown cause. After the explosion many changes were made to improve the standard of joint-making, such as better training, tools and inspection.

Poor joint-making and frequent leaks had been tolerated for a long time as all sources of ignition had been eliminated and so leaks could not ignite, or so it was believed. Though the plant was part of a large group the individual parts were independent so far as technology was concerned. The other plants in the group had never believed that leaks of flammable gas could not ignite. Experience had taught them that sources of ignition are liable to turn up, even though we do everything we can to remove known sources. Therefore strenuous efforts should be made to prevent leaks and to provide good ventilation so as to disperse any that do occur. Unfortunately the managers of the plant involved in the explosion had little technical contact with the other plants, though their sites adjoined. Handling ethylene at high pressure was, they believed, a specialised technology and little could be learnt from those who handled it at lower pressures. The plant was a monastery, a group of people isolating themselves from the outside world. The explosion blew down the monastery walls.

If the management of the plant where the explosion occurred had been less insular and more willing to compare experiences with other people in the group, or if the directors of the group had allowed the component parts less autonomy, the explosion might never have occurred. The senior managers of the plant and the group probably never realised or discussed the need for a change in policy. The leak was due to a badly made joint and so joints must be made correctly in future. No expense was spared to achieve this aim but the underlying weaknesses in the company organization and plant design were not recognized. However, some years later, during a recession, parts of the group were merged.

The causes listed in accident reports sometimes tell us more about the investigators' beliefs and background than about the accidents.

3 Accident Investigations List Human Error as a Cause

Human error is far too vague a term to be useful. We should ask, "What sort of error?" because different sorts of error require different actions if we are going to prevent the errors happening again [Kletz 2001a].

- Was the error due to poor training or instructions? If so we need improve them and perhaps simplify the task.

- Was it due to a deliberate decision not to follow instructions or recognized good practice? If so, we need to explain the reasons for the instructions as we do not live in a society in which people will simply do what they are told. We should, if possible, simplify the task – if an incorrect method is easier than the correct one it is difficult to persuade everyone to use the correct method - and we should check from time to time to see that instructions are being followed.

- Was the task beyond the ability of the person asked to do it, perhaps beyond anyone's ability? If so, we need to redesign the task.

- Was it a slip or lapse of attention? If so, it no use telling people to be more careful, we should remove opportunities for error by changing the design or method of working.

Blaming human error for an accident diverts attention from what can be done by better design or methods of operation. To quote Jim Reason, "We cannot change the human conditions but we can change the conditions in which humans work."

4 Accident Reports List Causes that are Difficult or Impossible to Remove

For example, a source of ignition is often listed as the cause of a fire or explosion. But, as we have just seen, it is impossible on the industrial scale to eliminate all sources of ignition with 100% certainty. While we try to remove as many as possible it is more important to prevent the formation of flammable mixtures.

Which is the more dangerous action on a plant that handles flammable liquids: to bring in a box of matches or to bring in a bucket? Many people would say that it is more dangerous to bring in the matches, but nobody would knowingly strike them in the presence of a leak and in a well-run plant leaks are small and infrequent. If a bucket is allowed in, however, it may be used for collecting drips or taking samples. A flammable mixture will be present above the surface of the liquid and may be ignited by a stray source of ignition. Of the two "causes" of the subsequent fire, the bucket is the easier to avoid.

I am not, of course, suggesting that we allowed unrestricted use of matches on our plants but I do suggest that we keep out open containers as thoroughly as we keep out matches.

Instead of listing causes we should list the actions needed to prevent a recurrence. This forces to people to ask if and how each so-called cause can be prevented in future.

5 We Change Procedures rather than Designs

When making recommendation to prevent an accident our first choice should be to see if we can remove the hazard – the inherently safer approach. For example, could we use a non-flammable solvent instead of a flammable one? Even if is impossible on the existing plant we should note it for the future.

The second best choice is to control the hazard with protective equipment. preferably passive equipment as it does not have to be switched on. As a last (but frequent) resort we may have to depend on procedures. Thus, as a protection against fire, insulation (passive) is usually better than water spray turned on automatically (active), but that is usually better than water spray turned on by people (procedural). In some companies, however, the default action is to consider a change in procedures first, sometimes because it is cheaper but more often because it has become a custom and practice carried on unthinkingly. Figure 1 (at the end of the paper) describes an example.

6 We Do Not Let Others Learn from our Experience

Many companies restrict the circulation of incident reports as they do not want everyone, even everyone in the company, to know that they have blundered but this will not prevent the incident happening again. We should circulate the essential messages widely, in the company and elsewhere, so that others can learn from them, for several reasons:

- *Moral:* if we have information that might prevent another accident we have a duty to pass it on.
- *Pragmatic:* if we tell other organizations about our accidents they may tell us about theirs.
- *Economic:* we would like our competitors to spend as much as we do on safety.
- *The industry is one: every accident effects its reputation.* To misquote the well-known words of John Donne,

No plant is an Island, entire of itself; every plant is a piece of the Continent, a part of the main. Any plant's loss diminishes us, because we are involved in the Industry: and therefore never send to know for whom the Inquiry sitteth; it sitteth for thee.

7 We Forget the Lessons Learned and Allow the Accident to Happen Again

Even when we prepare a good report and circulate it widely, all too often it is read, filed and forgotten. Organisations have no memory. Only people have memories and after a few years they move on taking their memories with them. Procedures introduced after an accident are allowed to lapse and some years later the accident happens again, even on the plant where it happened before. If by good fortune the results of an accident are not serious, the lessons are forgotten even more quickly. This is the most serious of the missed opportunities and will be considered more fully than the others. [Kletz 1993] describes many examples but here is a more recent one [Anon 2000]:

During cold weather a water line froze and ruptured inside a building. Damage was fortunately not very serious. Three years later the same line froze and ruptured again. The heating in the building was not operating and the water line was near the door. The basement was flooded and two 15 m^3 tanks floated, reached the ceiling and pushed it up by 0.5 m. The incident occurred at a nuclear site. Can we blame the public for doubting the nuclear industry's ability to operate reactors safely when they let the same water line freeze and rupture twice?

The following actions can prevent the same accidents recurring so often:

- Include in every instruction, code and standard a note on the reasons for it and accounts of accidents that would not have occurred if the instruction etc had existed at the time and had been followed. Once we forget the origins of our practices they become "cut flowers"; severed from their roots they wither and die.
- Never remove equipment before we know why it was installed. Never abandon a procedure before we know why it was adopted.
- Describe old accidents as well as recent ones, other companies' accidents as well as our own, in safety bulletins and discuss them at safety meetings.
- Follow up at regular intervals to see that the recommendations made after accidents are being followed, in design as well as operations.
- Remember that the first step down the road to an accident occurs when someone turns a blind eye to a missing blind.
- Include important accidents of the past in the training of undergraduates and company employees.
- Keep a folder of old accident reports in every control room. It should be compulsory reading for new employees and others should look through it from time to time.
- Read more books, which tell us what is old, as well as magazines that tell us what is new.
- We cannot stop downsizing but we can make sure that employees at all levels have adequate knowledge and experience. A business historian has described excessive downsizing as producing the corporate equivalent of Alzheimer's disease [Kransdorf 1996].
- Devise better retrieval systems so that we can find, more easily than at present, details of past accidents, in our own and other companies, and the recommendations made afterwards. We need systems in which the computer will automatically draw our attention to information that is relevant to what we are typing (or reading), as described below.

Of course, everyone forgets the past. An historian of football found that fans would condense the first hundred years of their team's history into two sentences and then describe the last few seasons in painstaking detail. But engineers poor memories have more serious results.

8 Weaknesses in Safety Training

There is something seriously wrong with our safety education when so many accidents repeat themselves so often. The first weakness is that ***it is often too theoretical***. It starts with principles, codes and standards. It tells us what we should do and why we should do it and warns us that we may have accidents if we do not follow the advice. If anyone is still reading or listening it may then go on the describe some of the accidents.

We should start by describing accidents and draw the lessons from them, for two reasons. First, accidents grab our attention and make us read on, or sit up and listen. Suppose an article describes a management system for the control of plant and process modifications. We probably glance at it and put it aside to read later, and you know what that means. If it is a talk we may yawn and think, "Another management system designed by the safety department that the people on the plant won't follow once the novelty wears off". In contrast, if someone describes accidents caused by modifications made without sufficient thought we are more likely to read on or listen and consider how we might prevent them in the plants under our control. We remember stories about accidents far better than we remember naked advice. We all remember the stories about Adam and Eve and Noah's Ark far better than all the "dos and don'ts" in the Bible.

The second reason why we should start with accident reports is that the accident is the important bit: it tells us what actually happened. We may not agree with the author's recommendations but we would be foolish to ignore the event. If the accident could happen on our plant we know we should take steps to prevent it, though not always those that the report recommends.

A second weakness with our safety training is that it usually consists of ***talking to people rather than discussing with them***. Instead of describing an accident and the recommendations made afterwards, outline the story and let the audience question you to find out the rest of the facts, the facts that they think are important and that they want to know. Then let them say what ***they think*** ought to be done to prevent it happening again. More will be remembered and the audience will be more committed than if they were merely told what to do.

Jared Diamond writes, "Contrary to popular assumptions cherished by modern literate societies, I suspect that we still learn best in the way we did during most of out evolutionary history – not by reading but through direct experience… For us the lessons that really sink in aren't always those learned from books, despite what historians and poets would like us to believe. Instead, we absorb most deeply the lessons based on our personal experience, as everybody did 5400 years ago." [Diamond 2000]