Available online at www.sciencedirect.com
ScienceDirect
Safety Science 45 (2007) 61–73
SAFETY SCIENCE
www.elsevier.com/locate/ssci

Statistics of design error in the process industries

J. Robert Taylor

Rambøll Danmark A/S, Bredevej 2, DK-2830 Virum, Denmark

Abstract

The paper addresses questions on how frequently incidents and accidents are caused by design errors and how significant design reviews are in removing design errors before a system is put into operation. It is based on a review of earlier studies mainly from the chemical and nuclear industries. The studies report that from about 20% to 50% of the studied incidents and accidents have at least one root cause attributed to erroneous design. The number of design errors actually occurring during the design process is much higher, but 80–95% of them are removed by thorough design reviews. To improve the design process further, it is necessary to analyse the nature and causes of design errors through first hand knowledge about the design process.

Keywords: Safety; Incidents and accidents; Design error; Design review; Chemical industry; Nuclear industry

1. Introduction

Design error is one of the most frequent causes of system failure and of accidents in the process industries, but has nevertheless been largely overlooked in risk analysis of process systems and control systems. Evidence for this is given in this paper. It is based on a series of studies by the author as participant in the design process over a period of 35 years, covering both studies of design errors and methods for reducing the incidence of such errors.

Collection of data on design error is not straightforward. Evidence of design error appears in accident reports and in trouble reports from customers to manufacturers. As will be shown, only a small percentage of errors actually reach the stage where they cause

E-mail address: rrt@ramboll.dk

0925-7535/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2006.08.013

accidents or operations problems. By far the majority of errors are removed from systems and plants before they are put into operation. For this reason, it is necessary to participate in the actual design process, in order to be able to collect the data on which improvements in the design process can be based.

Methods such as hazard and operability and functional failure analyses are partially effective in detecting design errors. The actual effectiveness is reviewed here on the basis of practical studies of large-scale systems and on experiments intended to elucidate specific problems. One of the classical methods, Hazard and Operability (Hazop) analysis, is found to give more than an 80% chance of discovering those errors which lie within its domain of application.

2. Definition of design error

A design error may be defined as a feature of a design which makes it unable to perform according to its specification. It is rare that a design fails under all circumstances, and the definition generally means that there are some circumstances, within the scope of the specification, under which the system does not match its specification.

There are some problems with this definition. For many systems, the specification is inadequate, and needs to be supplemented by general statements, such as "additionally the systems should work in a European climate" or "in addition to performing according to the specification, the system should not produce hazardous outputs". For most systems, there are a very large number of requirements which are included in the specification by reference, or are implicit. Many of the requirements which are not stated in the design documents are nevertheless explicit in legal requirements, or standards which are legally binding. To understand design error, and even to determine whether a design error has occurred, it is necessary to understand this implicit or indirect background. To complicate matters even further, specifications may contain errors, which lead them to diverge from the designer's, or the purchaser's true intentions. For these reasons, a more pragmatic definition may sometimes by used (Taylor, 1975).

> *"During analysis of incident records, a design error is deemed to have occurred, if the design or operating procedures are changed after an incident has occurred."*

3. Statistics of design error

3.1. Accident statistics

Statistics of accident causes are important because they give us an idea of how accidents arise in practice, and help prevent us focussing on the purely anecdotal. One of the first published studies of design error is useful in this way. It was carried out on "abnormal occurrence reports" published by the US Nuclear Regulatory Commission (NRC) in the 1960s and early 1970s (Taylor, 1975, 1976). The criterion for whether a design error occurred was an objective one. If a design change was made as a result of the incident, then a design error or omission was considered to have occurred. In order to make this definition compatible with that in the previous section, we need to add the errors in procedures, making 45% design errors in total. The results of this study are given in Tables 1–3. In all 250 reports were assessed over a 10 year period of operation.