Reliability Engineering and System Safety 151 (2016) 34–45

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Common cause failures in safety-instrumented systems: Using field experience from the petroleum industry

S. Hauge [a], P. Hokstad [a], S. Håbrekke [a], M.A. Lundteigen [b,*]

[a] SINTEF Technology and Society, Safety Research, Trondheim, Norway
[b] The Norwegian University of Science and Technology (NTNU), Norway

ARTICLE INFO

Available online 8 October 2015

Keywords:
Common cause failures (CCFs)
Safety instrumented systems (SIS)
Safety integrity level (SIL)
Reliability data
Data collection
Field experience

ABSTRACT

Safety instrumented systems often employ redundancy to enhance reliability, but the intended effect may be reduced when common cause failures are taken into account. It is often assumed that a certain fraction of component failures will occur close in time, due to a shared cause. Unfortunately, few attempts have been made to systematically investigate field experience on common cause failures, with the exception of the nuclear industry which has been in the forefront of research in this area. This paper presents selected results from a research project carried out in the Norwegian oil and gas industry to collect and analyze reported failures. This includes the presentation and derivation of generic (i.e. industry average) values of beta-factors for typical components in the oil and gas industry, and the demonstration of how failure data may be used to construct checklists for updating the value of beta in operation. The results are based on a review of some 12.000 maintenance notifications from six different onshore and offshore petroleum facilities. It is found that the new beta-values are higher than what is seen in many data sources, and some possible explanations are discussed.

1. Introduction

Many of the safety barriers that control the risk in hazardous process industries are implemented by safety instrumented systems (SIS). A SIS is designed to bring the process or protected system to a safe state in response to critical events at the facility. Examples of such events are process upsets, releases of hazardous materials, and fires. The SIS is usually split into three main subsystems; initiating elements such as sensors and push buttons, logic solver such as programmable electronic controller (PLC), and actuating devices, such as valves and circuit breakers. Redundancy is often introduced to enhance reliability, but this positive effect may be reduced if components are prone to the same (shared) cause of failure. Such failures, often referred to as common cause failures (CCFs), may result in a major disabling or complete loss of safety instrumented functions (SIFs). An important part of SIS management is therefore to assess and implement measures to reduce the influence of CCFs on the reliability.

CCFs have received considerable attention over several decades, but the main attention has been on development of models rather than collecting data to support the models, see e.g. Hokstad and Rausand [10] for an overview. Reliability modeling of CCFs was introduced in the nuclear industry for about 40 years ago, and early results were presented e.g. in NUREG-75/014 [24] and Edwards and Watson [2]. The Three Miles Island accident in 1979 (caused by CCFs) resulted in a further advancement of this work, and a number of papers [1,2,12,19,21,30,31,33,36,37] and reports [26,27] were published. Also the aviation industry has given a close attention to CCFs, and more recently the standard IEC 61508 [14] has pointed out the importance of controlling these failures in order to maintain the integrity of SIFs.

The most widely adopted model is the standard beta-factor model [6,15,17,26], with the parameter β (also referred to as beta-factor, or just beta), defined as the fraction of a component's failure rate that represents CCFs. A crucial assumption in this model is that when there is a CCF, all components of the specified CCF group (i.e. a group of similar components for which a CCF event can be registered) will fail. The PDS method [6] uses a variant of this approach called the multiple beta-factor model [9], where also the multiplicity of the CCF (i.e. number of components affected) is explicitly treated.

In the standard beta-factor model the CCFs are implicitly modeled, meaning that a collection of shared causes are catered for by the beta-factor. Also explicit modeling of CCFs is relevant and should be used when sufficient information is available to perform this [21,26]. In this case explicit CCF causes are identified and included in the system failure model. The focus of the present paper has been on implicit modeling, considering estimation of

[*] Corresponding author.
E-mail address: mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

http://dx.doi.org/10.1016/j.ress.2015.09.018
0951-8320/© 2015 Elsevier Ltd. All rights reserved.

the beta-factor. However, common components, such as common utility system, power supply, common logic etc., and common external events, including fire, flooding and earthquakes, should be modeled explicitly, and not be included in the beta factor modeling. Thus, when estimating new values of beta, the contribution from these types of events has been excluded.

It is often assumed that CCFs account for 1–10% of a component's failure rate; e.g. see the range of values given in the checklists for determining beta-factors proposed in IEC 61508 [14]. Earlier versions of such checklists, such as the one in Humphreys [12] even suggested 30% as the maximum value of the beta factor. These checklists are primarily based on expert judgments, and few attempts have been made to link them to operational data.

The nuclear industry is the only industry sector that has run a major project on collecting CCF data. The results were published in several open reports [22,23,35], but these data are not necessarily applicable to other industries. The occurrence of CCFs is highly impacted by local conditions [34], and experience from nuclear plants is not necessarily transferable to other sectors, due to the differences in design and engineering practices, environmental exposure, and the way of organizing and managing operation and maintenance.

The most extensive database for the oil and gas industry, the OREDA database and the OREDA handbooks [28,29] only mention CCFs in relation to fire and gas detectors, and the data are also rather old. Hauge et al. [7] carried out a survey in 2005–2006 of CCF experience among manufactures and oil companies, but the study was of a qualitative nature. The PDS data handbook [5] proposes values of beta for typical SIS equipment in the oil and gas industry, but these are mainly based on expert judgements and to a minor extent on reported failures.

The lack of detailed insight into historical CCF data in the oil and gas industry, led to a research project initiative by SINTEF with a broad participation from the industry through the PDS forum[1]. The project, with main funding from the Norwegian Research Council, carried out operational reviews for six oil and gas facilities; in total some 12 000 notifications for reported failures were reviewed. All failures were identified and further analyzed and classified into failure categories used in IEC 61508 [14] and IEC 61511 [15]. Three main objectives were formulated in relation to the project: (1) Gain deeper understanding of common causes of dangerous undetected (DU) failures and in what context they occur, (2) update generic values of beta for typical SIS components, to reflect an industry average with basis in field experience, and (3) develop new equipment specific checklists that may be used to adjust generic values with conditions and experience relevant for a specific facility. Checklists are already regarded as a good engineering practice for determining beta-factors in many of the key standards for SIS, such as IEC 61508 [14] and IEC 62061 [16]. In addition, the checklists are useful in pointing to specific measures to reduce the likelihood of having CCFs. However, the checklists provided in the standards are not well explained (in terms of underlying assumptions), and they are also too general and too design related to fully capture the effects from local, operational impacts and the variations between the various component types.

This paper describes the main results of this research project. It refers to initial results as presented at the ESREL conference in 2014 [4] and to the final report of the PDS research project [3]. The remaining part of the paper is organized as follows: Chapter 2 reviews some definitions related to CCF and specifies how the relevant concepts are used in the present paper. Chapter 3 discusses the estimation of the beta-factor, focusing on the NUREG estimators and the PDS estimator. Chapter 4 describes the operational reviews that have been carried out to collect CCF data, and presents new suggested beta-estimates based on the reviews. Chapter 5 discusses the equipment specific checklists being developed, and provides the checklist for shutdown valves. Finally, some concluding remarks are given in chapter 6.

2. Definitions, interpretations, and practical challenges

It was recognized early in the project that a precise definition of CCFs was needed to support the operational reviews. The foundation for CCF modeling was therefore devoted considerable attention and also discussed with the PDS forum participants. The following sub-sections summarize some of the reflections and discussions, based on experience from the operational reviews and on the feedback received from the PDS forum participants.

2.1. CCF related terms and definitions

Smith and Watson [36] conducted a rather detailed survey of CCF definitions already in 1980, and concluded that a CCF has the following characteristics: (1) The components affected are unable to perform as required, (2) multiple failures exist within (but are not limited to) redundant configurations, (3) The failures are “first in line” type of failures and not the result of cascading failures (i.e. where a failure of one component has triggered the failure of another component), (4) the failures occur within a defined critical time period (e.g., the time a plane is in the air during a flight or the time between two test intervals), (5) the failures are due to a single underlying defect or a physical phenomenon (the common cause of failures), and (6) the effect of failures must lead to some major disabling of the system's ability to perform as required. This definition is often regarded as rather exhaustive, but more recent research may suggest some clarifications. In particular, it has been proposed, e.g. by [20,32] that it may be reasonable to also add human errors to the common causes in condition (5) of Smith and Watson [36].

The generic standard on SIS, the IEC 61508 [14], defines a CCF as a “failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure”. Unfortunately, it is not straight forward to apply this definition directly [3]:

- The requirement that a CCF shall lead to a system failure is not considered to be very appropriate. If two components in a 2oo4 voting configuration fail due to a common cause, it should in our opinion be considered a CCF event (due to being a multiple failure and a major disabling of the function), even if the system is still functioning (e.g. in a 2oo2 mode).
- The distinction between a CCF and a CCF event is unclear in the IEC 61508 definition, ref. statement referred above “… failure that is the result of one or more events”. A more consistent wording would in our opinion be that a CCF event is an event where two or more components fail simultaneously due to a common cause.
- A limitation of the definition of CCF in IEC 61508 is the focus on multi-channel systems. The concept of CCF has a wider application area, and CCF may also involve multiple failures of several single channel systems. This aspects is recognized in other and more recent definitions of CCF in ISO/TR 12489 [18] and IEC 60050-192 [13], and are more in line with the interpretation of CCF in this paper.

[1] PDS forum is a co-operation between 26 participating companies, including oil companies, drilling contractors, engineering companies, consultants, safety system manufacturers and researchers, with a special interest in SISs, see www.sintef.no/pds.