CHAPTER 28

DEPENDENT FAILURE ANALYSIS

CONTENTS

1 INTRODUCTION

1.1 General

1.1.1 This Chapter gives an overview of the various causes of dependency failures, with a list of reference documents that cover the subject in more detail.

1.1.2 Fault Tree Analysis (FTA) and Success Tree Analysis (STA) provides an objective basis for analysing system design, performing trade-off studies, analysing 'Common Cause (or Mode) Failures', assessing compliance with safety requirements and justifying design improvements or additions (see PtCCh29).

1.1.3 The reliability of a system cannot be improved or even evaluated unless there is a thorough understanding of how each of its elements function and how these functions affect system operation. The accurate representation of these relationships is an integral part of this understanding and is particularly important for meaningful predictions, apportionment's and assessments. A Reliability Block Diagram (RBD) provides a method of representing this information in a form, which is easy to comprehend because it is simple and has visual impact. Due allowance for the effect of common cause failures should be allowed for in the RBD. When such failures occur all the elements affected by the common mode event will fail (see PtCCh30).

1.1.4 DEF STAN 00-41/3[1] states that, as part of Reliability Modelling '*…common mode failures, i.e. failures which can simultaneously affect elements in parallel should be identified and allowed for in the analysis.*'

1.2 Definitions

1.2.1 A set of standardised definitions are given in the Procedures Guide[2] thus:

a) ' Dependent Failure (DF): The failure of a set of events, the probability of which cannot be expressed as the simple product of the unconditional failure probabilities of the individual events.

b) Common Cause Failure (CCF): This is a specific type of dependent failure where simultaneous (or near-simultaneous) multiple failures result from a single shared cause.

c) Common Mode Failure (CMF): This term is reserved for common-cause failures in which multiple equipment items fail in the same mode.

d) Cascade Failures: These are propagating failures.

The term 'dependent failure as defined above is designed to cover all definitions of failures that are not independent. From this definition of dependent failures it is clear that an independent failure is one where the failure of a set of events is expressible as the simple product of individual event unconditional failure probabilities.

2 CAUSES OF DEPENDENT FAILURES

2.1 The causes of dependent failures may be categorised under two broad headings:

a) Common Component Failures; or

b) Supply Failures.

2.2 Both categories can arise due to deficiencies during:

a) design;

b) manufacture;

c) installation;

d) maintenance and testing, including calibration; or

e) operation including modifications to the plant and/or the process.

2.3 The main contributory factors for dependent (and independent) failures include:

a) Acts of a God., i.e. the classic external and internal hazards;

b) use of inappropriate people, (i.e. people with inadequate knowledge or experience)

c) inadequate training;

d) inappropriate or inadequate procedures;

e) inadequate controls and/or supervision;

f) use of inappropriate materials

g) use of inadequate components or supplies, including spare parts;

h) use of the systems beyond their design life; or

i) the operational environment.

2.4 Generally speaking, potential dependent failures that arise from the design, manufacture, and installation stages of a project can be detected during the commissioning and field testing stages. Consequently, there are fewer instances arising from these phases than those arising directly during the operational phase. While deficiencies in the design (e.g. incorrect choice of materials) can give rise to common failures, it is less likely that these will be concurrent although component reliability will be markedly reduced. Contrary to the general situation, by their nature, software dependent failures are less likely to be detected during commissioning.

2.5 Maintenance and testing is a most likely cause of dependent failures, with poor procedures and training the prime reasons for such failures. This is especially applicable if accompanied by inadequate checking and supervision. Calibration errors are an obvious cause of common component failure to perform as intended.

2.6 Dependent failures that occur as a result of a supply fault may be more readily comprehended than those form concurrent common component failures. Such failures and potential failures can occur as a result of errors or defects occurring at all stages of a project.

2.7 It is important that the correct consideration be given to improvements in reliability by replication or diversification, and to minimising common mode supply failures.

3 SOLUTIONS

3.1 Acts of a God are generally beyond the control of the design engineer, who should attempt to mitigate their effects by the application of good engineering practice. The second line of defence is to make the equipment resistant to the cause of dependent failure, e.g. using components resistant to radio frequency interference, or that can withstand the surrounding conditions, e.g. splashing with water. The last line of defence is to protect the equipment from the external hazard, e.g. protective barriers, or administrative protection, e.g. checks to limit the amount of combustible materials held on site.

3.2 Design and installation errors can be largely eliminated by good engineering practice. For example:

a) An independent review of all work should be carried out.

b) Check and agree all the assumptions, the starting data and the criteria for acceptability.

c) The high level specifications and design rules should be agreed and circulated, especially across the various engineering disciplines.

d) Produce detailed low level specifications that should include comprehensive and detailed sequence of operations, hazard/fault documents, protection requirements, and interlock definitions.

e) Ensure an effective change control procedure is implemented and used.

3.3 Operational decisions have the potential to be the cause of a dependent fault based upon human error. Human error dependency analysis is discussed in PtCCh32.

LEAFLET 28/0

RELATED DOCUMENTS

1. DEF STAN 00-41 Issue 3. 25 June 1993. *Reliability and Maintainability MOD Guide to Practices and Procedures.*

2. SRD R418. *SRD Dependent Failures Procedures Guide.* UKAEA. 1989.

3. SRD R146. *A Study of Common-Mode Failures.* UKAEA. 1979.

4. NUREG-0492. *Fault Tree Handbook.* US Nuclear Regulator Commission. January 1981.

5. A E Green & A J Bourne. *Reliability Technology*. Wiley. 1972.

6. D J Smith. *Reliability Maintainability and Risk*. Butterworth Heinemann. 1993.

Intentional blank page