CHAPTER 7

FAILURE CONSEQUENCE ANALYSIS

CONTENTS

		Page
1	Introduction	2
2	Purpose and Benefits	3
3	Problems	3
4	Availability Techniques	3
5	Specifying	4
6	Reporting the Analysis	4

1 INTRODUCTION

1.1 Failure Consequence Analysis (FCA), one of the activities associated with the initial system design and modification thereof, establishes the effect of equipment failures on operation, safety, etc. It extends the data on the basic R&M parameters determined by other activities, operational and support objectives and design details.

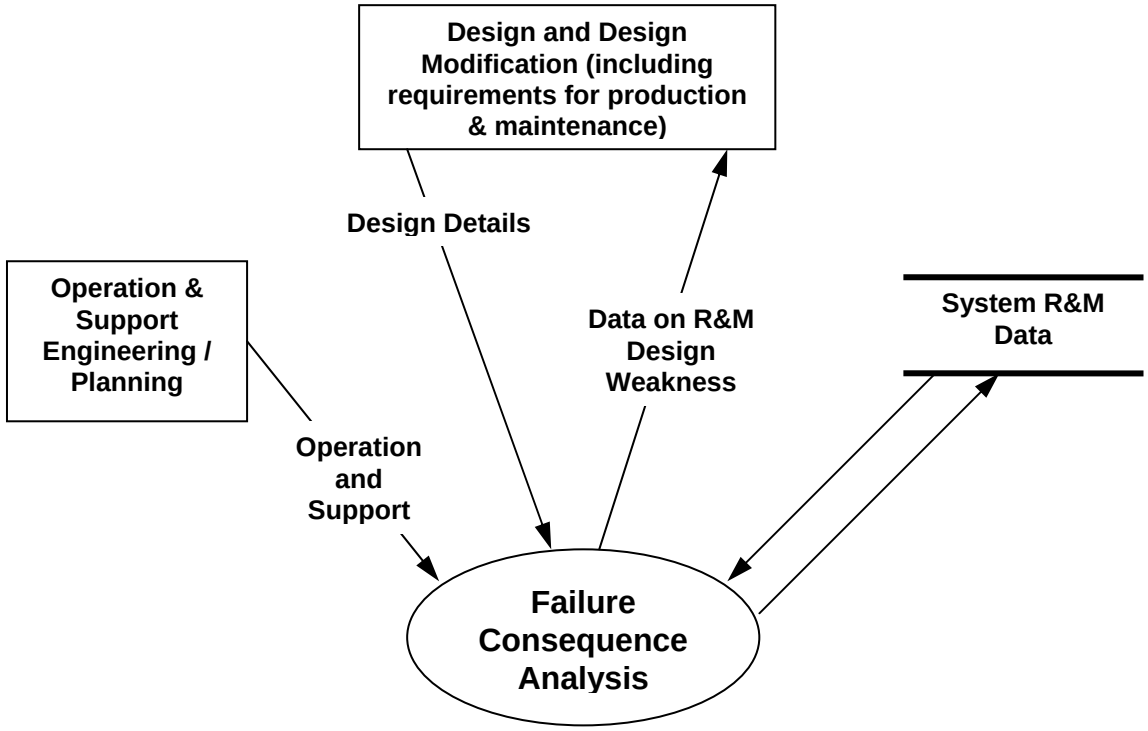

Figure 1: Data and material flow in and out of the Analysis

1.2 This chapter addresses:

a) what Failure Consequence Analysis is;

b) why it is carried out;

c) the benefits to be gained;

d) the drawbacks;

e) the available techniques; and

f) their specification.

2 PURPOSES AND BENEFITS

2.1 Failure Consequence Analysis provides a good assessment of the proposed design or modification against the R&M requirements. The analysis may be used:

a) to assess compliance with contractual requirements; and

b) to assess whether the equipment is fit for production.

2.2 FCA is essentially an engineering analysis that provides an input or feedback to the design and operational processes. The analysis involves much detailed and time consuming work but the resulting reliability and safety improvement will lead to savings in development and in-service costs which more than offset the cost of the evaluation. It is always much cheaper to amend a drawing at the design stage then to manufacture and embody modifications later.

3 PROBLEMS

3.1 Effective Failure Consequence Analysis requires:

a) a properly planned programme that is fully integrated with the requirements of other relevant departments, e.g. design, production and quality assurance;

b) a thorough understanding of the design requirements and the design principles adopted to meet those requirements;

c) appraisals planned to examine critically every aspect of the design that may influence reliability and safety; and

d) close liaison with design and other departments to ensure that any proposed improvements are introduced quickly.

Throughout the design evaluation, the accent must be on attention to detail because often unreliability results from an accumulation of relatively minor points that have been overlooked, rather than from some major omission.

3.2 FCA can be expensive. The techniques employed can require significant resource and time. A justification should therefore be made when they are introduced into the specification or programme. It is not intended to suggest that justification is difficult but that the cost implications should be considered. Often the life cycle cost benefits of reducing the risk of accepting equipment with a poor R&M performance will readily override the costs of the analysis.

4 AVAILABLE TECHNIQUES

4.1 The Failure Consequence Analysis must assess whether the proposed design or modification will meet its specified (or apportioned) R&M targets at all levels of assembly and in all modes of operation. The FCA should also assess whether there are any major sources of unreliability and whether the inherent reliability or safety of the design might be improved.

4.2 Cause analysis uses techniques to determine what causes higher level effects, i.e. a 'Top Down' approach. The techniques normally employed for cause analysis are:

a) Dependent Failure Analysis (see PtCCh28);

b) Fault / Success Tree Analysis (see PtCCh29);

c) Reliability Block Diagrams (see PtCCh30);

d) Monte-Carlo Simulation (see PtDCh4).

4.3 Consequence analysis is used to establish the effects of individual events upon the next higher level of assembly, and eventually upon the overall system. This is a 'Bottoms Up' approach and would employ one or more of the appropriate techniques, such as:

a) Fault Tolerance Analysis (see PtCCh27);

b) Task Analysis (Human Factors) (see PtCCh31);

c) Human Reliability Assessment (see PtCCh32);

d) Failure Mode, Effect & Criticality Analysis (see PtCCh33);

e) Event Tree Analysis (see PtCCh34).

4.4 Figure 1 shows the data flow into and out of the activity. In all cases the specified criteria are needed from the specification in order to determine the appropriate technique. The accept/reject result will also be sent to the R&M evidence collation.

5 SPECIFYING

5.1 The design specification should make very clear what the scope of each R&M parameter relates to. Common terms are often used in slightly different ways. With MTBF and Availability, clarity is needed as to whether a specific functional failure is being referred to, or the general need for corrective maintenance. With MTTR it should be made clear whether the requirement addresses the time for which the equipment is unavailable for operation or just the active corrective maintenance time. Definitions differ from one source to another to an extent that requires definitions to be provided with the specification.

6 REPORTING THE ANALYSIS

6.1 A formal documentary output should be produced as the principal output from the failure Consequence Analysis. The detailed contents will vary from project to project, but in general terms should include:

a) statement of the scope and purpose of the analysis;

b) a system description, including a definition of the build standard of the systems analysed, system boundaries, inputs and outputs, operating state etc.

c) the methods and assumptions. (All assumptions need to be justified and explained in particular sources of reliability data need listing);

d) the results obtained, expressed in terms which are directly related to the objectives;

e) discussion of results, including identification of areas where reliability, maintainability or safety could be improved;

f) conclusions and recommendations; and

g) detailed worksheets and calculations.