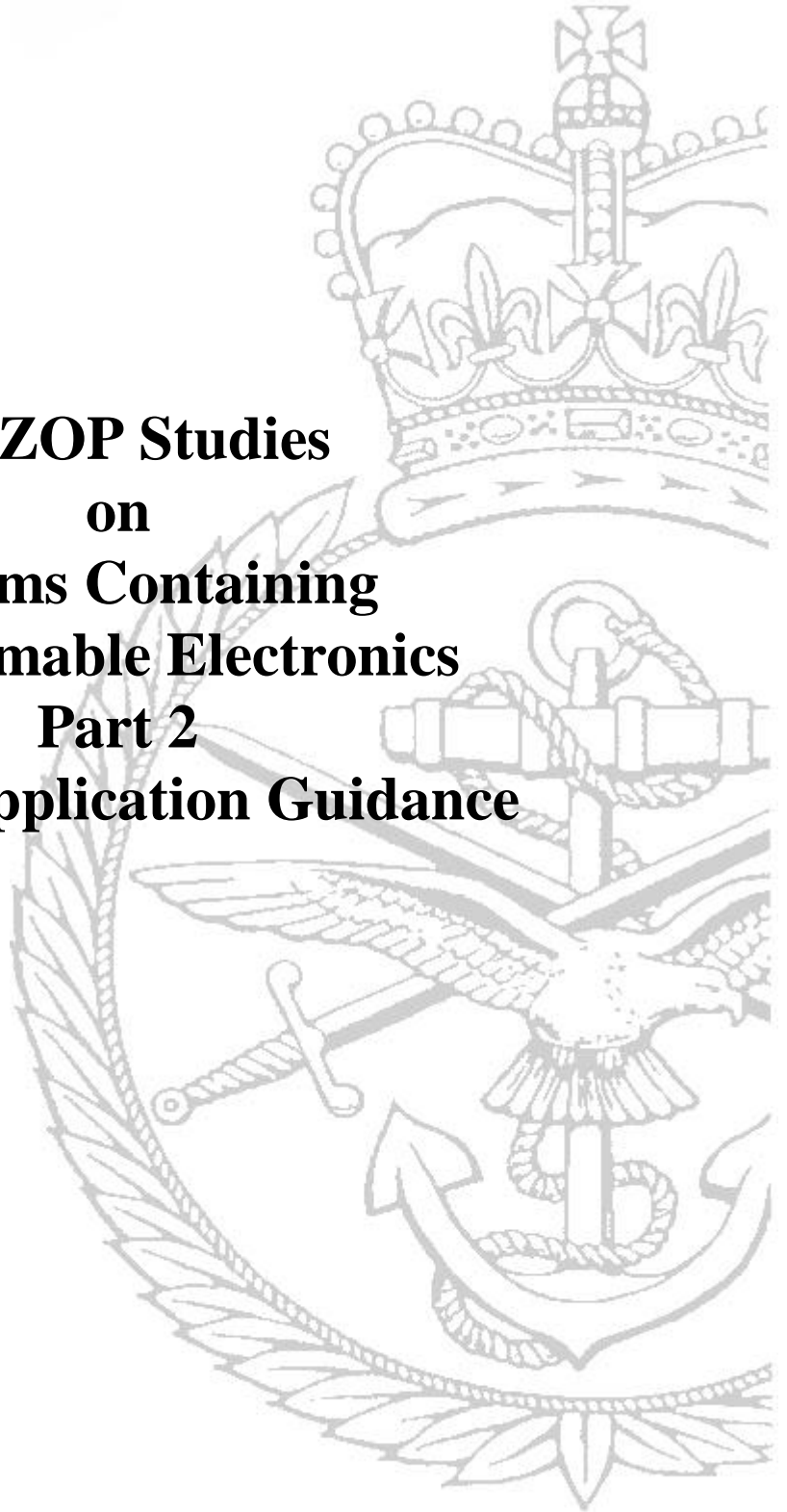




**Ministry of Defence
Defence Standard 00-58**

Issue 2 Publication Date 19 May 2000

**HAZOP Studies
on
Systems Containing
Programmable Electronics
Part 2
General Application Guidance**



AMENDMENT RECORD

Amd No	Date	Text Affected	Signature and Date

REVISION NOTE

This standard is raised to Issue 2 to update its content.

HISTORICAL RECORD

This standard supersedes the following:

Defence Standard (Def Stan) 00-58 Part 2 Issue 1 dated 26 July 1994

CONTENT

Description	Page
Content	1
Preface	3
Main Text	4
SECTION 1 GENERAL REQUIREMENTS	
0 Introduction	4
1 Scope and Applicability	4
2 Warning	5
3 Related Documents	5
4 Definitions	5
5 Abbreviations	5
SECTION 2 CARRYING OUT A HAZOP STUDY: THE GENERAL ISSUES	
6 Overview of the HAZOP Study Process	6
7 HAZOP Studies Throughout the Life of a System	6
8 Initiation of the Study	7
9 Definition of the Scope and Objectives of the Study	7
SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES	
10 Design Representation	9
11 Attributes	12
12 Guide Words: Exploring Deviations from Design Intent	13
13 Interpretations of Attribute-Guide-Word Combinations	14
SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES	
14 Roles of Team Members	16
15 Selecting the Study Team	19
16 Preparatory Work	20
17 The Conduct of a HAZOP Study Meeting	21
18 Recording the Results of the Study	25
19 Follow-up Work	27
20 Auditing	28
Table 1 Guide Word Interpretations	14
Table 2 Guide Word Interpretations for 'value'	15
Table 3 Roles of HAZOP Study Team Members	16
Table 4 Example Attribute-Guide-Word Interpretations for Flow Diagrams	32
Table 5 Example Attribute-Guide-Word Interpretations for State Transition Diagrams	33

CONTENT

Description	Page
Table 6 Example Attribute-Guide-Word Interpretations for Timing	34
Table 7 Example Attribute-Guide-Word Interpretations for Repetition and Response Time	34
Table 8 Example Attribute-Guide-Word Interpretations for Entity Relationship	36
Table 9 Matrix of Example Attributes and Guide Word Interpretations for a Communication System	41
Table 10 Matrix of Example Attributes and Guide Word Interpretations for Digital Hardware	42
Table 11 Matrix of Example Attributes and Guide Word Interpretations for the Mechanical Parts of a System	43
Table 12 Sample HAZOP Study Sheets	46
Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics	55
Table 14 Example HAZOP Study for a Collision Avoidance System	66
Fig 1 Data Flow/Control Flow Diagram	30
Fig 2 The Convention for State Transition Diagrams	33
Fig 3 Simple Example Showing Relationship Between man and Dog	35
Fig 4 Entity Relationship Diagram	35
Fig 5 Example Object Communication Model	37
Fig 6 Example Object Access Model	38
Fig 7 Train Carried ATP Equipment	45
Fig 8 Object Oriented Design Notation Example	52
Fig 9 Top-level View of Helicopter On-board System	53
Fig 10 Part of On-board System in More Detail	54
Fig 11 Extract from Fig 10 Relevant to Item 2	61
Fig 12 Extract from Fig 10 Relevant to Item 23	62
Fig 13 Context for Collision Avoidance System	64
Fig 14 Top-level Decomposition for Collision Avoidance Showing Data Input to Low Speed Logic	64
Fig 15 Low Speed Logic State Transition Diagram for Collision Avoidance System	65
Fig 16 Extract from Fig 15 Relevant to Item 24	71
Fig 17 Extract from Fig 15 Relevant to Item 29	72
ANNEX A Example Guide Word Interpretations	29
ANNEX B Example HAZOP Study at System Block Diagram Level	44
ANNEX C Example HAZOP Study for Helicopter On-board Diagnostics	48
ANNEX D Example HAZOP Study for Collision Avoidance System	63

PREFACE

Standards for Defence

**HAZOP Studies on Systems Containing Programmable Electronics
Part 2: General Application Guidance**

- a.** This standard contains guidance on the requirements contained in Part 1. This guidance serves two functions: it elaborates on the requirements in order to make conformance easier to achieve and assess, and it provides procedural background.
- b.** This Standard is one of a family of standards dealing with safety, being developed or adopted by the MOD, taking into account international standardization activities and supporting research and development and has been produced for MOD with assistance from interested industrial contributors. Its technical content has been commented on by members of the Hazard Analysis Interest Group, which arose out of the Department of Trade and Industry's SafeIT initiative, and by others.
- c.** This standard has been agreed by the authorities concerned with its use and is intended to be used whenever relevant in all future designs, contracts, orders etc. and whenever practicable by amendment to those already in existence. If any difficulty arises which prevents application of the Defence Standard, the Directorate of Standardization (DStan) shall be informed so that a remedy may be sought.
- d.** Any enquiries regarding this standard in relation to an invitation to tender or a contract in which it is incorporated are to be addressed to the responsible technical or supervising authority named in the invitation to tender or contract.
- e.** Compliance with this Defence Standard shall not in itself relieve any person from any legal obligations imposed upon them.
- f.** This standard has been devised solely for the use of the Ministry of Defence (MOD) and its contractors in the execution of contracts for the MOD. To the extent permitted by law, the MOD hereby excludes all liability whatsoever and howsoever arising (including, but without limitation, liability resulting from negligence) for any loss or damage however caused when the standard is used for any other purpose.

TEXT

Standards for Defence

HAZOP Studies on Systems Containing Programmable Electronics
Part 2: General Application Guidance

SECTION 1 GENERAL REQUIREMENTS

0 INTRODUCTION

0.1 This part of the Standard provides additional guidance and information on the requirements of Part 1. The information provided here is for the assistance of those who do not have significant experience in the conduct of HAZOP Studies or only have experience on non-programmable equipment. From Clause 1 onwards, it is organised in accordance with the main headings used in Part 1. Wherever practical, the subclauses numbers relate to the corresponding subclauses in Part 1. In some cases, in order to allow sub-subclause numbering to follow this pattern, dummy subclause numbers have been included; some with an appropriate title, others with a colon to indicate the following sub-subclauses.

0.2 Where additional guidance is not appropriate or applicable to a Part 1 clause, this is marked as 'No further guidance' against the corresponding Part 2 clause.

1 SCOPE AND APPLICABILITY

1.1 This Standard is a self-contained guide for MOD contractors and others carrying out HAZOP Studies. It extends previous guides by providing specific advice on applying HAZOP Studies to systems which include a PES.

1.2 There are a number of existing guides on the conduct of HAZOP Studies. However, guides which are widely available focus on the chemical and oil industries, and do not address the specific needs or peculiarities of PES-based systems.

1.3 No further guidance.

1.4 No further guidance.

1.5 No further guidance.

1.6 No further guidance.

SECTION 1 GENERAL REQUIREMENTS

2 WARNING

The Ministry of Defence (MOD), like its contractors, is subject to both United Kingdom and European laws regarding Health and Safety at Work, without exemption. All Defence Standards either directly or indirectly invoke the use of processes and procedures that could be injurious to health if adequate precautions are not taken. Defence Standards or their use in no way absolves users from complying with statutory and legal requirements relating to Health and Safety at Work.

3 RELATED DOCUMENTS

3.1 The publications shown below are referred to in the text of this standard. Publications are grouped and listed in alpha numeric order (refer also to documents listed in **Part 1** of this standard).

Designation	Title
CCPS Guide	Guidelines for Hazard Evaluation Procedures (ISBN 0 8169 0491 X)
CIA Guide	A Guide to Hazard and Operability Studies
-	HAZOP and HAZAN, Kletz, T.A. (ISBN 1 56032 276 4)
IEC Publication 812	Analysis Techniques for System Reliability - Procedure for Failure Modes and Effects Analysis (FMEA)

3.2 Reference in this standard to any related document means in any invitation to tender or contract the edition and all amendments current at the date of such tender or contract unless a specific edition is indicated.

3.3 In consideration of **3.2** above, users shall be fully aware of the issue and amendment status of all related documents, particularly when forming part of an invitation to tender or contract. Responsibility for the correct application of standards rests with users.

3.4 DStan can advise where related documents are obtained from. Requests for such information can be made to the Dstan Helpdesk. How to contact the helpdesk is shown on the outside rear cover of Def Stans.

4 DEFINITIONS

No further guidance.

5 HAZARD AND SAFETY ANALYSIS

No further guidance.

SECTION 2 CARRYING OUT A HAZOP STUDY: THE GENERIC ISSUES

6 OVERVIEW OF THE HAZOP STUDY PROCESS

No further guidance.

7 HAZOP STUDIES THROUGHOUT THE LIFE OF A SYSTEM

7.1 It is recommended that several HAZOP Studies should be carried out during the project life cycle of a system, except for systems in the lowest risk class. It should be noted, however, that a guarantee can never be given that all hazards have been found. The initial Study should be a high-level one and should be carried out to identify the fundamental hazards of the system, with the system being represented within its environment as a black box.

7.2 Systems in a Higher Risk Class

7.2.1 If implementation of the system can lead to modifications of its design, a HAZOP Study needs to be carried out on the 'as built' system.

7.2.2 There needs to be some consistency in the team across the successive Studies, or hazards may be missed. This consistency should be provided by a core team - preferably including the leader and one or more experts. Team selection should strike a balance between allowing change in order to bring in the right expertise (technical efficiency), maintaining a core team (continuity), and keeping the size down to a cost-effective and manageable level (effectiveness).

7.2.3 The above guidance assumes that successive HAZOP Studies will be complementary. However, there are times when it is desirable to have contrasting rather than complementary Studies, for instance if there is reason to doubt the results of a previous Study. Then, the Study team for the second Study may need to be different from those of the first, and the results of the first would not be used as input to the second.

7.3 It is recommended that the HAZOP Study results should be reviewed and updated when the system is phased out, disposed of, or otherwise removed from service. There are hazards associated with the phasing out or disposal of many equipments (the problem of de-commissioning nuclear submarines is an obvious example). In many cases a review of earlier HAZOP Study results, and of potential generic hazards associated with disposal, will identify the need for specific HAZOP Studies covering de-commissioning and/or disposal.

7.4 HAZOP Studies and Design Detail

7.4.1 When High-Level System Representation Exists:

- a. It is recommended that the overall design is approached in layers, which is facilitated if the design documentation is hierarchical.
- b. The layered approach facilitates the evaluation of the effectiveness of risk reduction measures which have been taken and the identification of any new hazards which might have been introduced.

SECTION 2 CARRYING OUT A HAZOP STUDY: THE GENERIC ISSUES

- c. In successive Studies, there is an increasing amount of technical detail and it is also likely that the design notations will be different at the various stages of the development life cycle. HAZOP Studies are recommended for the higher and intermediate levels of design.
- d. It is recommended that when a HAZOP Study is being carried out at one level and a more detailed level of design exists, the Study leader should ensure that the Study remains at the level defined in the scope of the Study so as to avoid the use of excessive time.

7.4.2 Detailed Level of Study:

- a. For some systems under development, much design detail may be available without safety analysis. The temptation to begin safety analysis by a HAZOP Study at the most detailed design level available should be avoided. Any HAZOP Study should approach the design in a top-down fashion as in 7.4.1 a. above. This ensures that effort is concentrated on the potentially hazardous parts.
- b. There are two main reasons for not carrying out a HAZOP Study at a detailed level unless higher levels have previously been addressed. First, the process is only likely to be cost-effective for those parts targeted by a systematic identification of hazards at a higher level. Carrying out a full HAZOP Study at a detailed level of design can be extremely time-consuming, and effort should be concentrated on those areas that higher level analysis has shown are most likely to lead to hazards. Second, a HAZOP Study may not be appropriate to the examination of some types of failure (such as, those failures more easily addressed by an FMEA). For example, use of a HAZOP Study to identify hazards at the software source statement level of a software configuration item is unlikely to be cost effective.

8 INITIATION OF THE STUDY

8.1 No further guidance.

8.2 The authority of the Study initiator may also be required for securing the appropriate team members for the Study and in dealing with the follow-up actions recommended during the Study, as the necessary resources are frequently at the disposal of the Study initiator rather than the Study leader.

9 DEFINITION OF THE SCOPE AND OBJECTIVES OF THE STUDY

9.1 **Scope** Issues which should be considered by the Study initiator when determining the scope include the following:

- a. the stage of the system's life cycle;
- b. the level of detail of the design to be studied;
- c. the physical boundary of the system to be studied;

SECTION 2 CARRYING OUT A HAZOP STUDY: THE GENERIC ISSUES

- d.** the nature of the risks to be managed;
- e.** the nature of the design representation;
- f.** the number of design representations to be studied;
- g.** the number and outcomes of previous HAZOP Studies and other safety analyses carried out on the system.;
- h.** any legislation which applies to the project or product liability;
- i.** the purpose to which the results of the Study will be put, for example:
 - 1.** choosing the location of the system;
 - 2.** refining the PES architecture;
 - 3.** designing for safety;
 - 4.** defining questions to ask a supplier;
 - 5.** improving the safety of a new or existing operation.
- j.** whether the Study is complementary to other Studies or a contrasting Study to check or confirm previous results;
- k.** where the system under investigation is being integrated with existing systems, the scope should at least include the types of hazards associated with the new system and those associated with the interactions between the new system and existing systems.

9.2 Objectives

9.2.1 The objectives of a HAZOP Study depend on a number of factors, for example:

- a.** the stage of the life cycle at which the HAZOP Study is to be carried out;
- b.** the required safety level of the system;
- c.** the types of hazard of importance in the Study.

9.2.2 Objectives of subsequent Studies would typically include determining that safety measures are in place to mitigate previously identified hazards and to identify any new hazards which might have been introduced.

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

10 DESIGN REPRESENTATION

10.1 Nature of the Representation

10.1.1 :

- a. A diagram may not be to scale, and a line representing the logical interconnection of two components may not indicate their physical locations or distances apart. Yet, the existence of a hazard may depend on these factors, so it should be made clear whether the representation is of the logical or the physical design.
- b. It is recommended that a design representation for use in a HAZOP Study should not be derived from another design representation specifically for use in the HAZOP Study. The process of translation can introduce misinterpretations which mask hazards.

10.1.2 :

- a. Each type of representation has its own set of conventions; the symbols on each have predefined meanings. Thus, there is a certain type of information which each presents naturally. For example, a block diagram naturally expresses the logical relationships between components and a data flow diagram naturally expresses the flows of information between components. Neither explicitly expresses attributes of the flow such as 'timing', 'bit rate' or 'sequence'. The attributes relevant to the functioning and safety of the system, and thus to the Study, which are expressed by the representation, should be listed clearly, either on the appropriate interconnections on the representation or on a separate list to be used by the Study leader. Relevant attributes which are not expressed by the representation should also be listed.
- b. There are times when one design representation is more appropriate than another. **Annexes B, C and D** provide examples of the use of state transition diagrams, object oriented design diagrams and system-level block diagrams in HAZOP Studies.
- c. There are occasions in PES design representations where a single interconnection represents the flow of a number of entities. An example is a data highway carrying both information data and control signals. In all such cases, each entity should be clearly identified.

10.1.3 Some users may not be familiar with some electronic and software representations. It is recommended that such users receive sufficient training in the representation notation so they can make a full contribution to the Study.

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

10.1.4 A wide variety of PES design representations are in use and it is possible for any of them to be the basis of a HAZOP Study. Clearly, some representations are easier to use than others and pictorial representations have proven convenient for many practitioners. **Annex A** gives some examples of common representations and associated guide word interpretations. The use of mathematically formed representations for safety-related software systems is increasing and these too can be used for a HAZOP Study. However, care must be exercised in ensuring that preparatory work is carried out thoroughly and that all team members understand the representation. Examples of PES design representations are:

- a. block diagrams;
- b. flow charts;
- c. data flow diagrams;
- d. object oriented design diagrams;
- e. state transition diagrams;
- f. timing diagrams;
- g. logic diagrams;
- h. electrical circuit diagrams.

10.2 Completeness of the Representation

10.2.1 :

- a. The representations used should cover all aspects of the system which could relate to hazards. If a single design representation does not, or cannot, cover all the relevant attributes or credible failures, then one or more other forms of representation should be used.
- b. The following issues are relevant in the decision of whether or not a further design representation is necessary:
 - 1. where a HAZOP Study makes use of the results of an earlier Study of the same system, one test of the adequacy of a representation is whether it allows the identification and study of the hazards discovered in the previous Study, particularly if it was the initial highest-level hazard identification study;
 - 2. a complete representation requires logical, infrastructure (such as operating system and library functions), and physical information (but a HAZOP Study at an early design stage in the system life cycle may not have physical information available);
 - 3. if dynamic behaviour is critical, such that hazards may result from incorrect sequencing, a representation such as a state transition diagram may be necessary;
 - 4. if the system has multiple states (such as start-up, normal operation, and shut-down) then representations of all of them should be available;
 - 5. if the timing of events is crucial, such that hazards could arise from timing deviations, a timing diagram is necessary;

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

6. if during a Study a question arises regarding the possibility of a hazard, and this cannot be answered by considering the attributes available on the design representation being studied, there is a likelihood that a further representation is necessary;
 7. operating instructions or procedures should be included in the representation to be studied;
 8. when a further design representation is to be introduced, care should be taken to ensure that it adds value (such as throwing up different attributes) and does not simply provide what the previous representation provided. The two should be consistent and complementary. Some design methodologies provide integrated representations which ensure consistency.
- C. There are occasions when it may not be possible to acquire a complete design representation, for example in the case of off-the-shelf software or hardware components. If such an off-the-shelf component is to be used in the safety-related part of a system, the ideal option would be to acquire a complete design representation from its designers, along with the results of any safety or hazard analyses which had been carried out on it. When this is not possible, the effects of its failures should be assessed in the context of the system's safety requirements. This can be done by treating the product as a 'black box' during the hazard identification process, with its inputs and outputs known. If deviations in its outputs are shown to have an adverse effect on safety, then a hazard identification of a more detailed design representation may be required. Efforts should be made to obtain evidence of its achieved safety integrity from the supplier and to check that evidence. If the necessary information is not obtained, a risk should be identified and recorded in the Hazard log.

10.2.2 It should also be remembered that the environment can be the source of hazardous events which can lead to accidents (for example, via lightning or electro-magnetic interference). As it is unlikely that these hazardous events will be included on a design representation, a list of them should be prepared.

10.3 Continuity

10.3.1 If during a HAZOP Meeting it is recognised that an additional design representation is required, then:

- a. the new representation should not be introduced into the current Meeting, even if it is available, because its preparation for study by the planning of its entities, attributes, guide words, and attribute-guide-word interpretations would not have been carried out;
- b. the current Meeting should continue with its planned design representations;
- c. a further schedule of Meetings may be required to address the additional representation;

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

- d.** a log should be made of issues to be addressed in further Meetings. This should include all questions raised and recommendations made.

10.3.2 When a further HAZOP Study is being planned, continuity between the two Studies should be ensured. The following are relevant:

- a.** a list of the attributes identified as relevant but not considered in the first Study should be used in assessing the new design representation;
- b.** the log of issues raised during the original schedule of Study Meetings should be used at the subsequent Study;
- c.** before it is used in a Study, the new design representation should be compared with the previous one to ensure that their scope is the same;
- d.** the Study leader should keep a log of issues which need to be resolved, should mark them as they are resolved, and should ensure that before the end of the Study every entry has been accounted for;
- e.** if it is not possible or appropriate to assemble the same team, then there should be at least two of the Study team members from the first Study team, preferably including the Study leader, in the second Study team.

11 ATTRIBUTES

11.1 Entities and Their Attributes

11.1.1 It is the responsibility of someone familiar with the design, at the planning stage of a HAZOP Study, to identify and document, for each component and interconnection on each design representation, the entities and their attributes, and also the attributes of any components to be studied. It is the Study leader's responsibility to distribute the documented information on the attributes to be used in the HAZOP Study to the Study team in advance of the first Study Meeting.

11.1.2 In a PES, it is common for there to be several types of data flow between two points. For example there may be both information and control data. Thus, when the interconnection between two points is being studied, each type of flow should be identified as an entity in its own right, and every attribute relevant to each entity should be listed and studied.

11.2 No further guidance.

11.3 Deviations from Design Intent

11.3.1 A HAZOP Study may often concentrate on the interactions and only address components in detail if an understanding of their failure modes is essential to the assessment of deviations from design intent on interconnections.

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

11.3.2 If components are to be studied, then their associated attributes need to be identified. It should be noted that 'components' is meant in the broadest sense and includes hardware, software, mechanical, electrical and electronic elements. The examination of components is not unique to HAZOP Studies, but this technique provides a systematic means of reviewing their possible failure causes and consequences. The deviations from design intent on the interactions are, however, the novel feature of HAZOP Studies. Indeed, a Study of the interactions between components is useful as a preliminary technique if the failure modes of the components are not known or are very complex.

12 GUIDE WORDS: EXPLORING DEVIATIONS FROM DESIGN INTENT

12.1 The principle of the use of guide words is as follows. Once a component or interconnection on the design representation has been selected for study, an entity on it (there may be one or more) and an attribute of the entity are chosen. Then a guide word is applied to the attribute. For example, if the guide word 'more' is applied to the attribute 'data value', it generates the questions 'What are the possible causes of the value of this data entity being greater than the design intent?' and 'What are the consequences?' Inquiries are made into these questions and the results recorded. This process is repeated for each guide word in turn, and the whole process is then carried out for each other attribute of the entity being studied.

12.2 No further guidance.

12.3 List of Guide Words and Interpretations

12.3.1 The choice of guide words should be considered carefully, as a guide word which is too specific may limit ideas and discussion, and one which is too general may not focus the HAZOP Study efficiently. The interpretation of the guide words in the context of the representation and the attributes is described further in clause **13** of **Part 2**, and in **Annex A**. Some generic guide words may be inappropriate to a particular Study, and these should be removed from the Study list during the planning stage.

12.3.2 The guide words in **Table 1** are normally adequate for a given Study. It is the responsibility of the Study leader to produce the proposed list of guide words, confirm its adequacy and distribute it to the Study team in advance of a Study.

12.3.3 Guide words may be interpreted differently in different industries, at different stages of the system life cycle, and when applied to different design representations. When guide words are chosen for a HAZOP Study, their interpretations should be defined. Each guide word may have more than one interpretation in the context of its application to the design representation. The Study leader should list all relevant interpretations. It is important that all interpretations are listed during the planning of the Study, distributed to team members and reviewed at the beginning of the Study. Discussion and debate about the interpretations should not take place during the Study Meetings as this leads to confusing results and inefficiency.

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

12.3.4 On occasions it may become apparent during a Study that a thorough investigation requires the addition of a guide word or a new interpretation not in the Study list. Then the guide word should be justified and introduced at the discretion of the Study leader. Introducing a new guide word or interpretation in the middle of a Study means that it has not been applied during the earlier part of the Study, so it is recommended to apply the new guide word retrospectively to the interconnections already studied.

13 INTERPRETATIONS OF ATTRIBUTE-GUIDE-WORD COMBINATIONS

13.1 :

13.1.1 A matrix may be a convenient way of expressing attribute-guide-word combinations and examples of a matrix and other ways of expressing combinations are given in **Annex A**. This provides examples and possible interpretations of the guide words in the context of some common forms of design representation and the attributes appropriate to those representations.

13.1.2 Combinations of specific guide words and attributes need interpretation. Interpretations should be guided by the generic meanings given in **Table 1** of **Part 1** in the context of the particular design representation. For example the guide word 'more' applied to the attribute 'data value' may be interpreted as 'greater'. Similarly, if 'more' is applied to the attribute 'bit rate', it needs to be interpreted as 'higher'.

13.1.3 The example of interpretations in **Table 1** below, gives a comparison between common interpretations used in the chemical industry and those that might be appropriate for use with a dataflow diagram as a design representation. In this, there are entities of both data flow and control flow. Considering the attribute 'flow' (for either data flow or control flow), and applying the guide words given in **Table 1** of **Part 1**, the interpretations might be:

Table 1 Guide Word Interpretations		
Guide Word	Standard Interpretation for Chemical Industry	Example Interpretation for PES
No	No part of the intention is achieved	No data or control signal passed
More	A quantitative increase	More data is passed than intended
Less	A quantitative decrease	Not used here because this is already covered by 'part of'
As well as	All design intent achieved but with additional results	Not used here because this is already covered by 'more'
Part of	Only some of the intention is achieved	The data or control signals are incomplete
Reverse	Covers reverse flow in pipes and reverse chemical reactions	Normally not relevant
Other than	A result other than the original intention is achieved	The data signals are complete but incorrect

SECTION 3 CARRYING OUT A HAZOP STUDY: THE TECHNICAL ISSUES

Table 1 Guide Word Interpretations (Continued)		
Guide Word	Standard Interpretation for Chemical Industry	Example Interpretation for PES
Early	Not used	The signal arrives too early with reference to clock time
Late	Not used	The signal arrives too late with reference to clock time
Before	Not used	The signal arrives earlier than intended within a sequence
After	Not used	The signal arrives later than intended within a sequence

13.1.4 As the example of the guide word 'reverse' shows (in **Table 1**, above), there will be some of the generic guide words which do not have a meaningful interpretation for a particular attribute. There may be others, however, that need more than one interpretation.

13.1.5 For the attribute 'value' for a single data entity, guide words that are considered relevant are 'more' and 'less'. Their interpretations are as in **Table 2**.

Table 2 Guide Word Interpretations for 'value'	
Guide Word	Example Interpretation
More	The data value is too high
Less	The data value is too low

13.1.6 See examples in **Annex A**.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

14 ROLES OF TEAM MEMBERS

14.1 A HAZOP Study is a creative process. It is key to the success of a Study that the team dynamics work, and the role of the Study leader is important to enable creative exploration of deviations.

14.2 Processes and Skills

14.2.1 For each consideration of an attribute-guide-word interpretation, there is a process of:

- a. postulation of a possible deviation from design intent;
- b. exploration of how it could occur and what its possible causes and consequences might be;
- c. explanation of the protection and alarm mechanisms in place or planned, of the behaviour of the system, of problems known with similar systems, and of other relevant factors;
- d. drawing conclusions about whether a hazard exists;
- e. recording the results.

14.2.2 Each stage of the process requires a particular skill, and there need to be team members with the appropriate skills. Two or more roles may be combined in one person, particularly on simple systems. However, it is not recommended that the HAZOP Study leader role be combined with that of recorder.

14.2.3 The typical roles of the team members in carrying out the process are summarized in **Table 3**. However, it is more important that there is a team member capable of carrying out each role of the process than that each role should be the responsibility of a particular team member.

	Postulate	Explore	Explain	Conclude	Record
Leader	Yes	Possibly	Possibly	Yes	
Expert		Yes	Yes		
Designer		Possibly	Yes		
User		Possibly	Yes		
Recorder		Possibly			Yes

14.3 Role of the Study Leader

14.3.1 In planning a HAZOP Study, the Study leader should attend to practical arrangements such as agreeing the details of the Study with the Study team and securing accommodation for the full schedule of Study Meetings.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

14.3.2 In conducting the HAZOP Study Meetings, the Study leader should ensure that:

- a. team members are informed of the Meeting conventions;
- b. meetings are controlled according to the agreed Meeting conventions;
- c. the technical aspects of the Study are carried out thoroughly. This includes:
 1. covering the system systematically;
 2. clearly stating the attribute, guide word and interpretation being considered at any time;
 3. controlling the Study to ensure that it remains focused on the matter in hand;
 4. summarising the conclusions on each item for the recorder.
- d. effort is applied effectively, for instance, by ensuring that team members are not becoming tired or bored;
- e. effort is applied efficiently, for instance, by ensuring that all team members are contributing to the process;
- f. the results are documented;
- g. the documented results are agreed by the full team, or, if consensus cannot be achieved, that all sides of a disagreement are recorded;
- h. the Meeting documentation is signed off;
- i. there is consistency across the full schedule of Study Meetings;
- j. the Study documentation is distributed to appropriate persons.

14.3.3 In checking that follow-up work has been done, the Study leader should ensure that the results of all questions raised are reported back and raised at a later Study Meeting.

14.3.4 In controlling the Study Meetings, the Study leader:

- a. should be able to assist the other team members to understand the design representation, if this becomes necessary;
- b. may delegate to the recorder the duty of ensuring that the results of previous hazard analyses on the system being studied are available during the planning of the Study and at the Study Meetings;
- c. may delegate to the recorder the duty of finding out about previous hazard analyses of connected systems and ensuring that the relevant results are available both at the planning of the Study and at the Study Meetings.

14.3.5 The Study leader has the authority and the duty to terminate or suspend the Study Meeting at any time if it becomes unproductive - for example, if it is recognised that the design representation has not previously been reviewed, or if the team members or the Study leader have lost concentration.

14.3.6 The Study leader should exclude any team member from the Meeting, at any time, if the member is obstructive, or is in any way compromising the effectiveness or efficiency of the Meeting.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

14.3.7 It is recommended that, in order to minimise the chance of problems occurring during the planning or execution of a HAZOP Study, an organisation carrying out HAZOP Studies should have a standard checklist of the Study leader's functions.

14.4 Role of the Recorder

14.4.1 The responsibilities of the recorder are to:

- a. be familiar with the HAZOP Study process;
- b. understand the design representation used and have an appreciation of the application's operating environment;
- c. at the direction of the Study leader, ensure the availability of data and subsidiary documentation needed for the HAZOP Study and any results of previous hazard analyses on the system being studied or connected systems;
- d. understand the nature of the documentation to be prepared, as defined in the objectives of the Study;
- e. follow the discussion and participate in the Study;
- f. document, in concise prose and in the appropriate style, the hazards identified, their possible causes and consequences, any recommendations made, any action for follow-up work, and any cross-references to other documents.

14.4.2 It is recommended that the recorder creates the Study documentation at the Meeting. It should be recognised that the recorder's role is crucial to the success of the Study.

14.5 Role of the Designer

14.5.1 Ideally, the designer should come from the system design team. At the Study Meetings, the designer should be able to answer questions about the design, the design representation, and the design intent.

14.6 Role of the User

14.6.1 The choice of the most appropriate user should be guided by the scope and purpose of the HAZOP Study. This means that in some cases a single person cannot cover the complete user's role.

14.6.2 The user may be someone who has used, operated or maintained the system; or, if the system is still in development, someone who will use, operate or maintain it and who understands and can explain its proposed operational environment and context.

14.6.3 The user's role is to advise on the effects, on system operation, of deviations from design intent, and to help in deciding whether or not there is likely to be a safety issue.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

14.7 Role of the Expert Members

14.7.1 Expert members need to be capable explorers of cause and effect who possess relevant operating environment knowledge and expertise.

14.7.2 The key role of an expert member is to explore the postulated deviations from design intent, determining whether a hazard exists and, if it does, what its causes and consequences are likely to be.

14.7.3 Designers and users can often be good explorers, if they can overcome the temptation to be defensive about the system..

15 SELECTING THE STUDY TEAM

15.1 Team Selection Criteria

15.1.1 It is the Study leader's responsibility to choose the team membership for each HAZOP Study, but it may be necessary for the Study initiator to make the necessary arrangements for the availability of the team members.

15.1.2 The Study leader should determine what expertise is necessary for a successful Study and select the expert members accordingly. Typical areas of expertise which may be useful or necessary are: supplier, applications software developer, operator, maintainer, independent expert. Reviewing the design prior to the Study might be a good way of deciding what skills are necessary, especially when knowledge of subsystems is required.

15.1.3 The Study leader should also consider the need to choose members who between them possess the abilities to postulate, explore, explain, conclude, and record.

15.1.4 The viewpoints of designer and user are always required on the Study, although different personnel may be needed to represent these viewpoints, depending on the particular stage of the life cycle at which the Study is carried out.

15.1.5 Expert members must be competent explorers of cause and effect. They should be chosen for their wide experience of systems such as the one being studied and of the functions and hazards that may be associated with them.

15.1.6 The role of the recorder is important. It should be given to someone who understands the representation and the system under review and who has the capability of participating in the exploration of deviations.

15.1.7 When inviting team members, the Study leader should be specific in naming the persons required, having taken appropriate advice. Representatives of invited members should not be accepted unless it is demonstrated that they can contribute to the Study as effectively as the invited member.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

15.2 Team Size

15.2.1 A Study team of five members allows each of the identified roles to be represented separately, and a team of seven allows for extra expertise where needed without excessively decreasing the cost-effectiveness of the Study.

15.2.2 When a number of HAZOP Studies are carried out on different representations or stages of the same system, hazards may be missed if there is a lack of team consistency between the various Studies. There therefore needs to be a core team which should include the leader and one or more experts. The team may grow and shrink as specific designers, users, maintainers or experts are called in to answer given questions or for analysis of given parts of the design. Once systems are in operation, the role of the maintainer will become increasingly important. Maintainers are likely to be either 'users', who carry out repairs to the system, or 'designers', who change the design of the system in response to operational feedback. There needs to be a balance between allowing change in order to bring in the right expertise, maintaining a core team, and keeping the size of the team to a cost-effective and manageable level.

15.3 It is recommended that training for a Study leader should include being a recorder at a number of HAZOP Studies.

16 PREPARATORY WORK

16.1 Preparatory Work on the Representation

16.1.1 The Study leader should ensure that appropriate, reviewed design representations are available. If significant flaws are discovered in the design or a representation, the Study Meeting should be postponed until the design representations are of adequate quality.

16.1.2 Preparatory Work on Technical Issues:

- a.** The Study leader should ensure that the results of previous hazard identification work are available for the Study and are used to guide the choice of attributes and the level of detail of the representation;
- b.** the Study leader should work with the designer to identify and list the entities and attributes for components and interconnections in the design representation;
- c.** the Study leader should choose the guide words and define their interpretations for each attribute in the context of the present HAZOP Study, taking advice from designers as appropriate;
- d.** the Study leader, in the light of experience and the defined scope of the Study, should assess the adequacy of the attributes and guide words for a thorough analysis. If they are inadequate, a further design representation should be provided.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

16.1.3 Preparatory Work on Planning the Study:

- a. The Study leader should plan the Study (which may comprise a number of Meetings) in consultation as necessary with the designer and the Study initiator;
- b. in planning, the question of whether more than one design representation is needed should be taken into account;
- c. it should be decided what level of recording is required - the recording of everything which transpires at the Meeting, or only exception reporting; also whether what is recorded is a full report of the activities and their results, or only a summary;
- d. it should be decided what rules will apply (for example, see clause **17.1.1** of **Part 2**) so as to ensure efficiency and effectiveness of Study Meetings;
- e. the availability of all team members should be assured for the full schedule of Study Meetings. Substitute members with the appropriate credentials should be identified to cover unexpected absences.

16.2 Briefing the Team

16.2.1 It is recommended that the distribution of a briefing pack should take place at least two weeks prior to the first Study Meeting.

16.2.2 It is recommended that an organisation using HAZOP Studies should design a standard form for the Study leader to use in preparing the plan and issuing a call to the team members.

16.3 Room Layout and Facilities

16.3.1 In planning the Study, attention should be paid to the room layout and facilities. In particular:

- a. the room should have sufficient space for the easy movement of all team members;
- b. the design representation being examined needs to be in such a position that all team members are able not only to see it, but also to use it for reference in discussion;
- c. there should be means for public generation of text and diagrams (such as a flip chart or white board) to clarify points or focus discussion.

17 THE CONDUCT OF A HAZOP STUDY MEETING

17.1 Discipline for Maintaining Progress and Achieving Efficiency

17.1.1 The progress of a Study Meeting is impaired by prolonged discussion or argument. The Study leader should therefore enforce the following discipline:

- a. discussion should stick to the point;

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

- b.** discussion should not stray towards the design or redesign of the system: the purpose of a HAZOP Study is to find hazards and their causes, not to solve problems;
- c.** only one person should speak at a time;
- d.** a maximum of 10 minutes should be spent on the discussion of any one point. After that, a question should be raised and the matter listed for follow-up work. (Note that it should be rare to spend 10 minutes on a single point.);
- e.** the Study leader should stop the Meeting, or call a break, if it has become ineffective, for example, through people becoming tired or bored or if the representation being studied is revealing no new hazards.

17.1.2 Because the success of HAZOP Study Meetings depends on alertness and concentration, the following discipline should apply:

- a.** there should be a time limit of three hours on a Study Meeting, but Meetings of two hours may prove more effective;
- b.** there should be a break of about five minutes at the end of each hour, and the time of this break will need to be controlled by the Study leader;
- c.** there should be a maximum of two Study Meetings in a day;
- d.** two Meetings in the same day should be separated by at least one and a half hours;
- e.** two Meetings per day should be held for a maximum of three consecutive days, after which there should be a break of at least two days.

17.2 The Study Process

17.2.1 Initial Activities:

- a.** At the start of a HAZOP Study Meeting, the Study leader should:
 - 1.** conduct introductions of all the team members and ensure that their names are recorded;
 - 2.** briefly review the Study plan to ensure that all team members are familiar with the system and its background, with the nature of a HAZOP Study, with the relevant technical issues, and with the conduct of the particular Meeting.
- b.** Additional tasks which the Study leader should perform at the start of a HAZOP Study Meeting are to review the technical and recording issues:
 - 1.** describe the conventions used on the design representations and ensure that team members have a common understanding of them;
 - 2.** briefly describe the attributes on the design representation, the guide words to be used, and the attribute-guide-word interpretations to be applied;
 - 3.** define whether recording will be done in total or by exception.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

- c. When the Study team is unfamiliar with carrying out a HAZOP Study on the type of design representation being studied, it is recommended that a brief training HAZOP Study be carried out on a simple but complete example of that type of design representation.
- d. Having set the scene for the Study Meeting, the Study leader should ask the designer to give an overview of the design, its context, and its intent.

17.2.2 Progress of the Study Meeting

- a. The hazard identification process derives its power from a step-by-step procedure.
- b. It is suggested that the analysis proceeds forward from inputs to outputs, choosing interconnections in a logical sequence.
- c. One form of marking which has been found useful is to trace over the component or interconnection with a highlighting pen of one colour when it is chosen and to go over it again with one of a different colour when its study has been completed. Alternatively, on-line support for the representation may be helpful here and during the subsequent steps of the Study. Display should be visible to all team members.
- d. When more than one representation is being used, it may be efficient to study a given component or interconnection on all of them at the same time.
- e. From the list of entities (there may only be one) on a component or interconnection, the Study leader chooses one and marks it as being under study. Then the Study leader chooses one of the attributes of that entity and marks it. The Study leader next identifies which guide word is to be applied and identifies the applicable attribute-guide-word interpretations.
- f. Using an attribute-guide-word interpretation as a prompt, the Study team leader postulates a deviation. This is then explored by the team, usually by the expert team members and possibly by the Study leader, the designer or the user. If it is considered a credible deviation, its causes and consequences are explored, usually by the designer, the user or an expert member.
- g. If the Study leader considers that an identified hazard would be better addressed under a different guide word, the team leader should note this in writing and ensure that it is covered when the appropriate guide word is raised.
- h. The Study team should identify those elements of the system which help to prevent, detect, or give an indication of the hazard.
- i. The Study leader may choose to make notes of the summary on the displayed design representation, thus facilitating subsequent comparison and discussion with the recorder.
- j. The Study leader then either proposes a recommendation or raises a question to be answered outside the Meeting. The Study leader may invite the team to propose the recommendation or question, and this is refined until consensus is reached and it is documented.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

- k. In exceptional circumstances, consensus may be impossible to achieve. In such a case, the Study leader should direct the recorder to document the various opinions, raise a question or recommendation, and then proceed with the Study.
- l. It should be noted that it is not unusual for the first day (one or two Study Meetings) of a HAZOP Study with a new team to proceed slowly. Efficiency improves as the team members come to understand the process and each other, and learn to minimise extraneous discussion.

17.2.3 The first applicable attribute-guide-word interpretation is then applied in order to see if there is a credible deviation of the attribute from the design intent. If a credible deviation is identified, it is examined for possible causes and consequences.

17.2.4 Any previous hazard identification studies should be made use of at this stage.

17.2.5 The presence of protection or indication mechanisms must not stop identified hazards being explored and listed. If such mechanisms exist, the team may explore their efficacy in reducing the probability or mitigating the consequences of the hazard, if this is appropriate. The conclusion or recommendation shall be noted in the HAZOP Study documentation.

17.2.6 Risk assessment of the hazards identified should not be carried out during the HAZOP Study, but as a separate activity as specified in DEF STAN 00-56.

17.2.7 The Study leader concludes the examination of the chosen attribute-guide-word interpretation by summarising the results, which are documented by the recorder.

17.2.8 The process is then repeated for all the attribute-guide-word interpretations for that guide word; then for each other guide word; then for each other attribute of the entity under study. Finally, each other entity on that component or interconnection is treated in the same way. Then the component or interconnection is marked as having been studied and the Study leader chooses another on which to repeat the whole process (see **Fig 2**).

17.3 HAZOP Study Process

17.3.1 A HAZOP Study should not be used as a design review. If the design or the design representation is inadequate or incorrect, the Study may be compromised. The success of a HAZOP Study depends on a thorough design review having previously been carried out.

17.4 Team Dynamics

17.4.1 A HAZOP Study is only as good as the team taking part. Like most team activities, the personal knowledge and skills of the team members are important to success. The way the team members work together is crucial. One of the advantages of the process is that the team can build on a comment by one team member and explore unusual interactions. A HAZOP Study is therefore a creative activity. In order for this creative resonance to be achieved, the Study leader's control and leadership is vital.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

17.4.2 It is often useful for learners of the HAZOP Study process to attend HAZOP meetings as silent observers. Experiencing the creative interaction of the team is an excellent way to reinforce information received in formal training.

17.5 Study Examples

17.5.1 Annex B gives an example of a HAZOP Study of a simple high-level system design. **Annex C** and **Annex D** give examples of two small, but real, HAZOP Studies of software designs.

18 RECORDING THE RESULTS OF THE STUDY

18.1 Recording Style

18.1.1 The full recording style is to record every transaction during the Study - that is to say, the results of applying every attribute-guide-word combination to all the various components and interconnections on the design representation. This style provides the basis of proof that a HAZOP Study has been thorough. If done well, it is likely to satisfy most audit requirements.

18.1.2 The alternative style is to record by exception only, which implies recording only the discovered hazards and their causes, and the actions for follow-up work. This results in more easily manageable documentation, and it does not necessarily diminish the value of the Study. However, it does not demonstrate the thoroughness of the Study and is therefore less useful for audit purposes or for future proof of what was done. It should therefore be used with care.

18.1.3 In setting the objectives for a HAZOP Study, the Study initiator should decide which style is to be used. Examples of factors which are relevant to this decision are:

- a. relevant corporate policy;
- b. regulatory requirements which might apply (the Study initiator should therefore be aware of the relevant regulations in force);
- c. contractual obligations;
- d. the likely auditing requirements;
- e. the possible future need for proof of what was done in the Study;
- f. the magnitude of risks from the system.

18.2 Study Output

18.2.1 At each Study Meeting, the Study leader should ensure that the necessary documentation is produced by selecting a capable recorder, briefing the recorder before the Study, ensuring the recorder's familiarisation with any software package which is to be used for recording or display, and checking the work of the recorder from time to time during the Meeting.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

18.2.2 The Study leader, working with the recorder, should decide on the most appropriate method of recording. This will reflect personal experience as well as any organisation guidelines that may be in place.

18.3 Recorded Information

18.3.1 There are instances when it is not clear whether a hazard could occur, for example when the designer is unsure about certain aspects of the design. Then the Study cannot either dismiss the possibility of a hazard or conclude with a recommendation, so it may be appropriate to raise a question. As a HAZOP Study should not end on a question, the issue should be studied subsequent to the Meeting at which it is raised. The Study leader should review the results given as replies to questions and decide whether the question may be closed, a recommendation raised, or the results presented at a future Meeting.

18.3.2 The following apply to recorded information:

- a. when protection or alarm mechanisms exist in the system, there may be a recommendation for further work to explore their efficacy in the light of the hazards found. The hazard is recorded notwithstanding the protection or alarm mechanism;
- b. every question raised for study after the Meeting by the team should be recorded, with the individual responsible for carrying out the work being identified, as well as the date of completion;
- c. unique and exhaustive numbering of all Study result items allows later traceability of items in audits, in the hazard log, and when follow-up work is checked;
- d. it is recommended that an organization carrying out HAZOP Studies should have a standard form on which to record results.

18.4 All identified hazards should be recorded in the hazard log. Whereas it is important to have a defined documentation method within the Study, all safety-related systems should have associated with them a mandated method of recording all identified hazards.

18.5 Documentation Review

18.5.1 Some HAZOP Study practitioners have found it an advantage if the recorder is a competent typist and inputs the Study documentation to an electronic medium during the Study Meeting. There now exist software packages and other tools for immediate recording and display. These may be considered for use in HAZOP Studies because the signing off of the recorded information requires the agreement of all team members present. If they can read the documentation and agree it before the end of each Meeting, time and effort are saved.

18.5.2 The following are examples of the way in which the Meeting documentation may be prepared and presented to the Study team for its agreement:

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

- a. having recorded the information on paper, the recorder reads it out, sheet by sheet, to the team at the end of the Meeting;
- b. if the information is being recorded on an electronic medium, it may be projected onto a screen throughout the meeting. This can achieve immediate agreement, but it often gives rise to trivial editing which is time-consuming. The Study leader needs to ensure that time is used effectively;
- c. having recorded the information onto an electronic medium during the Meeting, the recorder projects it onto a screen at the end of the Meeting. With a good recorder this method saves a great deal of time;
- d. the Study leader checks and edits the documentation overnight and presents it to the Study team at the beginning of the next day's Meeting. This method may also require an additional Meeting arranged only for achieving agreement to the documentation of the final Study Meeting. (The Study leader needs to remain alert during Meetings so should not use the break between two Meetings on the same day for the checking of documentation.).

18.5.3 It is preferable to obtain the agreement of the Study team to the Meeting documentation before the team disperses at the end of a Meeting.

18.5.4 The Study documentation should be stored permanently and referenced by the hazard log.

18.5.5 An electronic medium may be used both for the initial recording of the information and for obtaining agreement on the documentation, but signing-off by the Study leader will normally require a print out of all sheets.

18.5.6 When consensus has been impossible to achieve (see **17.2.2 k.** in **Part 2**) the various opinions should be recorded.

19 FOLLOW-UP WORK

19.1 Follow-up Meeting

19.1.1 The Study leader may need to arrange a follow-up Meeting of the Study team to continue the Study in the light of the feedback from the follow-up work. At this Meeting, the same responsibilities and rules apply as at the Study Meetings in the original schedule.

19.1.2 As answers are often found between Study Meetings, and thus taken into consideration during the original scheduled Meetings in the Study, the outstanding questions should be reviewed by the Study leader at the end of the original schedule of Study Meetings to assess the need for a follow-up Meeting to complete the Study. As described in **18.3.1** of **Part 2**, the Study leader may close questions between Meetings.

SECTION 4 CARRYING OUT A HAZOP STUDY: THE CONTROL ISSUES

19.2 It is not usual for the Study leader to have the direct authority to ensure that the Study team's recommendations are acted on, and the help of the Study initiator may be needed (see **8.2** in **Part 2**). However, the system safety certification will make use of the HAZOP report thus giving 'authority' to the Study leader by implication. In addition, all hazards identified in the Study will be entered into the system Hazard Log and the procedure called for in DEF STAN 00-56 will help ensure that recommendations are acted on.

20 AUDITING

20.1 Auditing Criteria

20.1.1 Having an independent safety auditor (ISA) to observe and audit some HAZOP Studies should be considered. This provides not only independence of the audit but also encouragement to the Study leader to ensure an auditable Study.

20.1.2 In laying down criteria against which to audit a HAZOP Study and its results, the following are relevant:

- a.** personnel issues:
 - 1.** do adequate procedures exist for carrying out HAZOP Studies?
 - 2.** were there suitable team members at the Study to support the defined team roles?
 - 3.** were the appropriate team members (with the right knowledge) chosen?
 - 4.** was the leader trained?
 - 5.** was the preparatory work carried out thoroughly?
- b.** were there adequate procedures in place to ensure that:
 - 1.** all attributes were identified?
 - 2.** all relevant guide words were applied to all attributes?
 - 3.** the Study was carried out in a technically appropriate manner?
- c.** documentation and follow-up issues:
 - 1.** was a Study plan distributed to the Study team in advance of the Study?
 - 2.** was the design representation verified before use in the Study?
 - 3.** was recording carried out in accordance with the instructions?
 - 4.** were all hazards, questions and recommendations clearly labelled and numbered?
 - 5.** was every sheet of results signed off by the Study leader?
 - 6.** were the results of all questions for Study by the Study team fed back to a Meeting of the team?
 - 7.** was a follow-up Meeting held?

20.2 The above are examples only and do not comprise an exhaustive checklist for the auditing of the Study process. Thorough checks of the technical aspects of the Study are recommended.

20.3 No further guidance.

ANNEX A

ANNEX A

EXAMPLE GUIDE WORD INTERPRETATIONS

A.1 INTRODUCTION

A.1.1 This Annex gives example interpretations of the HAZOP Study guide words in the context of the attributes arising from the application of HAZOP Studies.

A.1.2 Where considered necessary to explain the context for the choice of guide word and interpretation, the notation for the design representation is also described.

A.1.3 In the context of this Annex, design is used as a generic term to cover the development process. In particular, it is possible, and often appropriate, to use a HAZOP Study to identify hazards at the requirements capture stage of a project.

A.1.4 Guide word interpretations are given for the software design representations of data flow diagrams, state transition diagrams and object oriented design. Suggested attributes and guide word interpretations for electronic hardware, communication networks and electromechanical systems are included. Also given are some considerations for the choice of attributes and the interpretation of guide words when timing information is available.

A.1.5 Interpretations of guide words should be made in the context of the system being studied and its representation. It is important that the set of attributes, guide words and interpretations is understood by the team using it, applied consistently, and sufficient to explore plausible deviations from design intent.

A.1.6 The set of guide words and interpretations given in this Annex are examples which have been found to work on particular HAZOP Studies. Other guide words and interpretations are not precluded and, in fact, may be more appropriate for particular studies. This is an important point. The purpose of the guide word is to facilitate the creative exploration of deviations by a team.

A.1.7 In clauses **A.2** to **A.5**, the attributes, guide words and interpretations are given in tables. In the later sections, they are given as matrices. Individual organisations should choose an appropriate and convenient method.

A.1.8 For ease of reference the set of guide words given in clause **12** of **Part 1** is repeated here. The generic list of guide words is:

No: This is the complete negation of the design intention. No part of the intention is achieved and nothing else happens.

More: This is a quantitative increase.

Less: This is a quantitative decrease.

DEF STAN 00-58 PART 2/2

ANNEX A

- As well as: All the design intention is achieved together with additions.
- Part of: Only some of the design intention is achieved.
- Reverse: The logical opposite of the intention.
- Other than: Complete substitution, where no part of the original intention is achieved but something quite different happens.
- Early: Something happens earlier than expected relative to clock time.
- Late: Something happens later than expected relative to clock time.
- Before: Something happens before it is expected, relating to order or sequence.
- After: Something happens after it is expected, relating to order or sequence.

A.2 GUIDE WORD INTERPRETATIONS FOR DATA FLOW/CONTROL FLOW DIAGRAMS

A.2.1 Data flow diagrams are well established and have been found easy to understand by those who are not familiar with software design techniques. The diagram given below is a common convention, using a sub-set of the Hatley-Pirbhai methodology [1], modified to show the entities of data flows and control flows on the same diagram, rather than on separate ones.

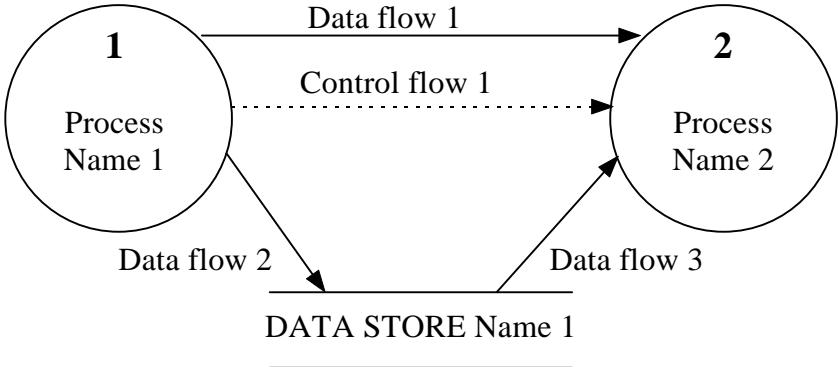


Fig 1 Data Flow/Control Flow Diagram

ANNEX A

A.2.2 A design using data flow diagrams will usually be presented in a hierarchical manner with high-level processes being decomposed into lower-level processes, with associated greater levels of detail for some of the data flows. Thus a HAZOP Study of lower levels of a design will, in fact, begin to 'look inside' the processes defined at the higher level.

A.2.3 It is convenient to think of data flows as being intermittent or continuous. Control flows are data flows with a control context and are modelled as separate entities in many methodologies. Because of their context, in the Hatley-Pirbhai methodology they are always intermittent flows. During a HAZOP Study it may be useful to distinguish between these different types when examining credible deviations.

A.2.4 Data flows may be anything from a single item, to a group of any number of items. The name at a group level is usually descriptive of that whole group. Group flows decompose into sub-group flows and eventually into primitive, single-item flows: this decomposition often happens as the group passes from a parent to a child diagram. With group flows, there may be a need, sometime during the HAZOP Study, to look at the primitive flows. This may be when the decomposition reaches a level at which the primitive flows become apparent, or earlier at the discretion of the HAZOP Study leader. For example, if the exploration of deviations of group flows leads to discussion of the primitive flows, this may indicate a need to look at the primitive flows rather than the group flows.

A.2.4 When a group flow splits between processes, such that one part of the group goes to one receiving process and the remainder to another receiving process, the HAZOP Study should address them as separate data flows between the sending process and the two receiving processes. Similarly, a two-way flow between processes should be addressed as flows in each direction.

A.2.6 **Table 4** gives the attributes that might be explored for deviations as well as some possible interpretations for the guide words associated with those attributes. Note that for many of the attributes, only a few of the standard guide words are considered to have meaningful interpretations. Also note that the table is applicable to generic data flows. It is possible to derive more detailed interpretations for particular data types.

ANNEX A

Table 4 Example Attribute-Guide-Word Interpretations for Data Flow Diagrams		
Attribute	Guide Word	Interpretation
Flow (of data or control)	No	No information flow.
	More	More data is passed than expected.
	Part of	The information is passed incomplete (for group flows).
	Reverse	Flow of information in wrong direction (normally not credible).
	Other than	Information complete, but incorrect.
	Early	Flow of information occurs before it was intended.
	Late	Flow of information occurs after it was required.
Data rate	More	The data rate is too high.
	Less	The data rate is too low.
Data value	More	The data value is too high (within or out of bounds).
	Less	The data value is too low (within or out of bounds).

A.3 GUIDE WORD INTERPRETATIONS FOR STATE TRANSITION DIAGRAMS

A.3.1 Finite state machines [1] recognize that many processes may be in a number of states (an aircraft, say, could be in the states of 'stationary', 'taxi-ing', 'taking-off', 'in-flight' or 'landing'). Finite state machines (often using state transition diagrams) give the 'rules' for how transitions between states occur. In any given 'state', when an 'event' occurs that is associated with a transition from that state, the machine will go to the state indicated by that transition and will perform the associated 'action'. With the Mealy model [1] for state transition diagrams, the actions are associated with the transition and so are convenient for exploration using a HAZOP Study.

A.3.2 Fig 2 shows a typical convention for a state transition diagram (taken from Hatley-Pirbhai). 'States' are shown as rectangular boxes containing the state names. 'Transition arcs' are lines with arrowheads showing the directions of the transitions. 'Events' are the initiating conditions for transitions shown by name as labels on the arcs of the transitions they cause. 'Actions' are shown by name, adjacent to the events that cause them with the two separated by a line e.g. event/action. One event is shown as the start state.

A.3.3 Table 5 shows example interpretations for state transition diagrams, using the two attributes of event and action. If additional information on timing issues is available, then deviations may be explored as in A.4 of this Annex.

ANNEX A

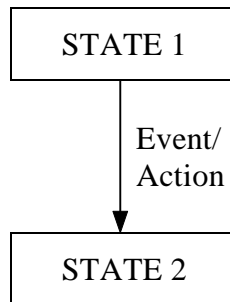


Fig 2 The Convention for State Transition Diagrams

Table 5 Example Attribute-Guide-Word Interpretations for State Transition Diagrams		
Attribute	Guide Word	Interpretation
Event	No	Event does not happen.
	As well as	Another event takes place as well.
	Other than	An unexpected event occurs instead of the anticipated event.
Action	No	No action takes place.
	As well as	Additional (unwanted) actions take place.
	Part of	An incomplete action is performed.
	Other than	An incorrect action takes place.

A.4 GUIDE WORD INTERPRETATIONS FOR TIMING INFORMATION

A.4.1 Timing of Events and Actions

A.4.1.1 When timing information is available together with the state transition diagram then the additional attribute of timing may be associated with the attributes of event and action, giving rise to the possible interpretations in **Table 6**.

ANNEX A

Attribute	Guide Word	Interpretation
Timing of Event or Action	No	Event/action never takes place.
	Early	Event/action takes place before it is expected.
	Late	Event/action takes place after it is expected.
	Before	Happens before another event or action that is expected to precede it.
	After	Happens after another event or action that is expected to come after it.

A.4.2 Repetition and Response Time

A.4.2.1 Timing issues in many designs are given in terms of the attributes of repetition time and response time. Repetition time is the time between successive updates of external primitive outputs. Response time is the time from input to output. An example of repetition time is the need to update commands to the control surfaces of an aircraft every 100 msec. An example of response time is the time to initiate closure of a valve after an operator presses a close switch. **Table 7** below gives example interpretations for relevant guide words for the two attributes.

Attribute	Guide Word	Interpretation
Repetition time	No	Output is not updated.
	More	Time between outputs is longer than required.
	Less	Time between outputs is shorter than required.
	Other than	Time between outputs is variable.
Response time	No	Never happens (time is infinite).
	More	Time is longer than required.
	Less	Time is shorter than required.
	Other than	Time is variable.

A.5 GUIDE WORD INTERPRETATIONS FOR OBJECT ORIENTED DESIGNS

A.5.1 The use of object oriented design methods has increased rapidly in recent years. There are many different notations and approaches used: in this section the notation proposed by Shlaer-Mellor [2] is used. A complete design using the Shlaer-Mellor approach comprises four basic models:

ANNEX A

- a. an Information Model (also called an entity relationship diagram);
- b. State Transition diagrams for each object with dynamic behaviour;
- c. an Object Communication Model to show the event communication between objects;
- d. an Object Access Model to show the synchronous communication between objects.

Note that here the word 'entity' has its specific object oriented meaning, not that used in the remainder of this Standard.

A.5.2 Information Model (or entity relationship diagram)

A.5.2.1 Representation. A simple example of the convention used for the entity relationship diagram is shown in **Fig 3**. An object is an abstraction of a set of real-world things where all the things in the set (the instances) have the same characteristics.

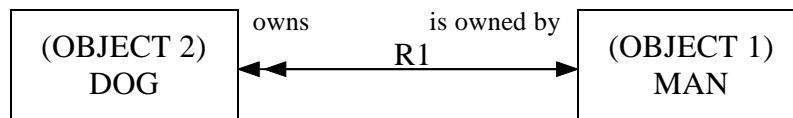


Fig 3 Simple Example Showing Relationship Between Man and Dog

A.5.2.2 A slightly more complex example is shown in **Fig 4**, where there are the entities of a company control department, the group leaders within it and the group members.

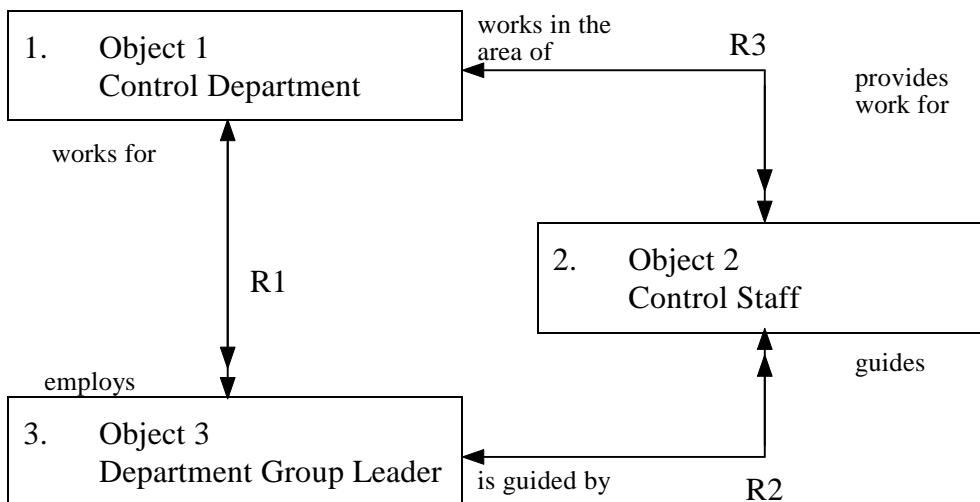


Fig 4 Entity Relationship Diagram

ANNEX A

A.5.2.3 From the point of view of a HAZOP Study relationships are what can cause deviations. Relationships are unconditional where every instance of an object is required to participate in the relationship as in the examples below. In a conditional relationship, there are instances of objects that do not participate. Relationships may be of the following forms:

- a. one-to-one, where a single instance of an object is associated with a single instance of another (e.g. husband and wife);
- b. one-to-many, where a single instance of an object is associated with one or more instance of another, and each instance of the second is associated with just one instance of the first (e.g. the man and dog relationship of **Fig 3**);
- c. many-to-many, where a single instance of an object is associated with one or more instances of another and each instance of the second object is associated with one or more instances of the first (e.g. house and owner).

A.5.2.4 Interpretation of Guide Words Possible guide word interpretations for the attribute of relationship are shown in **Table 8**. Note that here there are two different interpretations for two of the guide words.

Attribute	Guide Word	Interpretation
Relationship	No	Relationship does not take place.
	More/less	Wrong cardinality in a relationship (for example it is one-to-one instead of one-to-many).
	Part of (i)	The set of relationships held by an entity shows incompatibilities between individual relationships.
	Part of (ii)	There is a required relationship that is not shown on the design.
	Other than (i)	The wrong relationship is defined between objects (i.e. there should be a relationship between the objects but not the one given).
	Other than (ii)	Relationship is wrong (i.e. there should not be a relationship between the objects even though one is given).

A.5.3 STATE TRANSITION DIAGRAMS.

A.5.3.1 The Shlaer-Mellor approach uses the Moore state model [2] (as opposed to the Mealy one used in **A.3** above). The main difference from Mealy is that the actions are accomplished when an instance arrives in a state, rather than being associated with the transition between states.

ANNEX A

A.5.3.2 From a purist point of view, in this case the actions are 'hidden' in the states and so a HAZOP Study might not consider them if it is concentrating on the interactions. However, in practice, a HAZOP Study would be likely to explore deviations of the actions as well as the events.

A.5.3.3 Exploring deviations may be addressed as described in **A.3** above (and **A.4** if additional information on timing is available).

A.5.4 Object Communication Model

A.5.4.1 When a state model generates an event, the target state model receives the event some time after the action in which the event was generated is complete. The object communication model gives a summary of such event communication between state models and external entities, i.e., the asynchronous communication between state models in the system. Each state model is represented by an oval labelled with the name of the state model. Each external entity (such as switches or actuators) that can generate or receive events is depicted by a box.

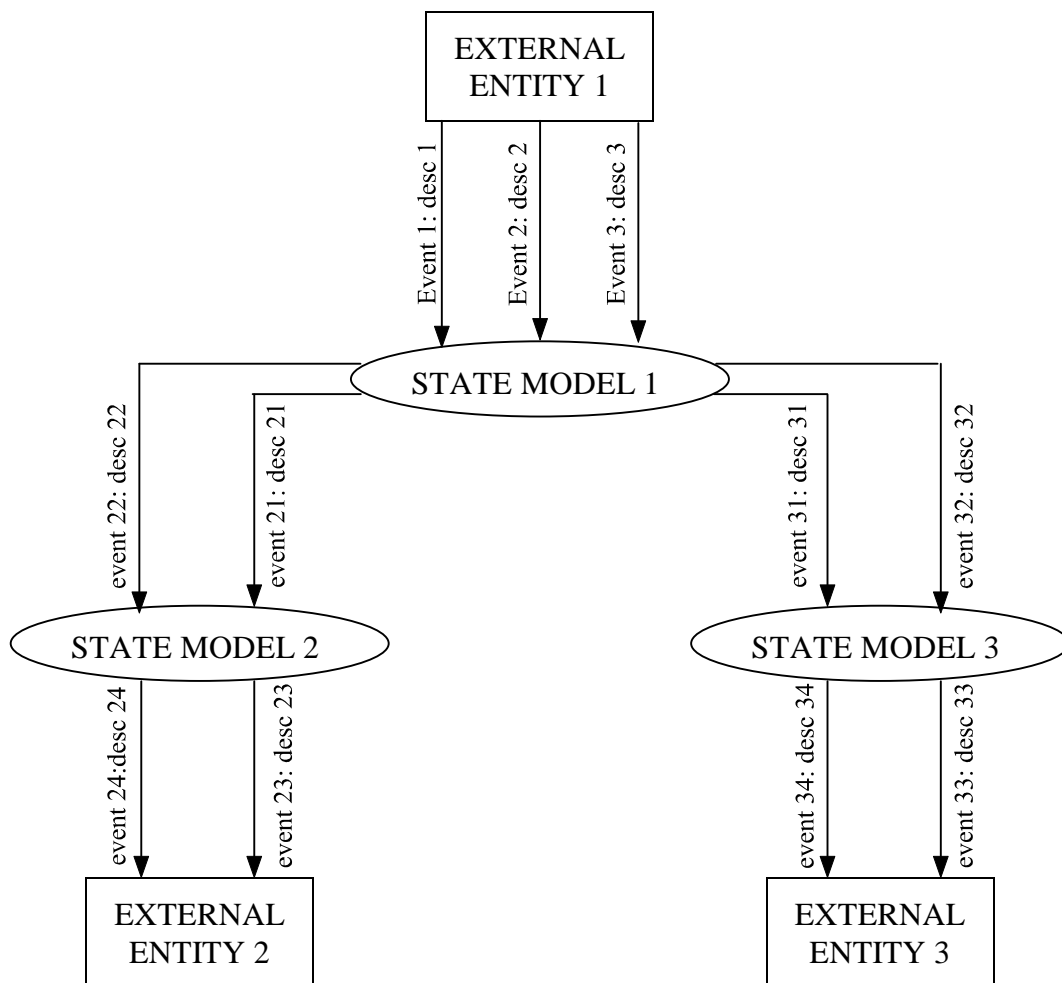


Fig 5 Example Object Communication Model

ANNEX A

A.5.4.2 An event that is generated by one state model or external entity and received by another is shown by an arrow from the generating component to the receiver, annotated with the event label, meaning and (optionally) event data. An example is given in **Fig 5**.

A.5.4.3 The object communication model has the attribute of 'event' that can be addressed during a HAZOP Study. Exploring deviations of events may be addressed as described in **A.3** above (and **A.4** if additional information on timing is available).

A.5.5 Object Access Model

A.5.5.1 The object access model gives a summary of the synchronous communication between state models and data of object instances. When a state model accesses the data of an instance of another object through an accessor process, the data access takes place during the time that the action is running. An object is represented by a flattened oval labelled with the name of the object. The oval represents both the data describing the instances of the object and the state model.

A.5.5.2 If a state model (say state model A) makes use of an accessor assigned to another object (object B), an arrow is drawn from object A to object B, labelled with the process identifier of the accessor as shown in **Fig 6**. The diagram provides a summary of the synchronous communications between state models and object instance data.

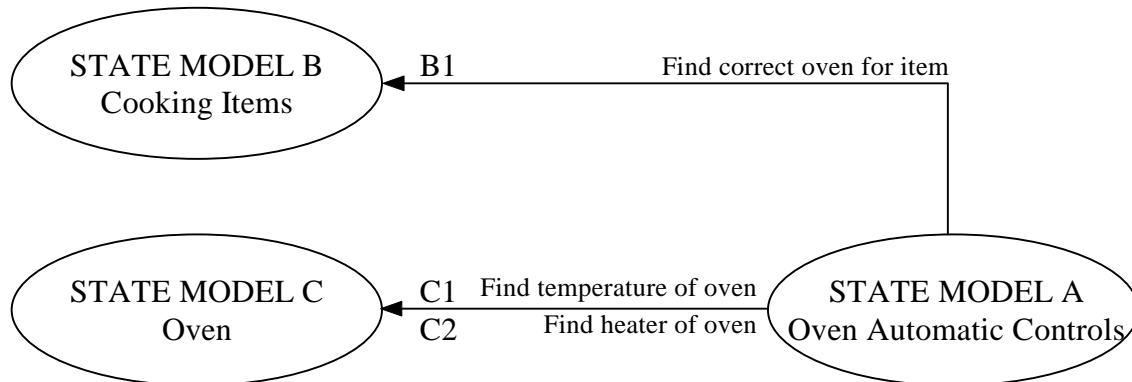


Fig 6 Example Object Access Model

A.5.5.3 A HAZOP Study of this model can treat each interaction as a data flow, with the same set of potential deviations as described in **A.2** above.

A.6 GUIDE WORD INTERPRETATIONS FOR COMMUNICATION SYSTEMS

A.6.1 In looking at a communications network or a specific communications link, there are attributes to examine such as the topology of the network, the encoding of the data and the data rate.

ANNEX A

A.6.2 **Table 9** shows a matrix of attributes and guide word interpretations appropriate for use in a HAZOP Study of the communications of a system.

A.6.3 The matrix has the standard guide words as the headings for each column, the attributes being examined at the left hand of each row, and the interpretations filling each element.

A.6.4 A communication system has a topology, that is the connectivity between a set of nodes, and also encompasses whether a node is a transmitter, a receiver or both. This topology may range from static, through dynamic due to failure, to fully dynamic where nodes can be freely connected or disconnected. The communication system will have one or more masters which control activity on the network. The other masters may be present to increase reliability by redundancy or the system may support multi-masters, e.g. Ethernet.

A.6.5 The data transferred will be encoded to improve the reliability of the system by providing error detection or error correction capability. The protocol defines how the data is transferred between nodes, for example, whether transmission starts following a request from another node, or from an internal event. The system has a bandwidth or data capacity which at a simple level will affect response time, which will in turn vary according to the message priority.

A.6.6 Whether the communication system is synchronous (locked to a central clock) or asynchronous, the data rate is a key attribute.

A.7 GUIDE WORD INTERPRETATIONS FOR DIGITAL ELECTRONIC HARDWARE

A.7.1 In carrying out a HAZOP Study on a representation of the design of digital electronics there is a need to define appropriate attributes and interpretations of the guide words. Taking a simple example of an electrical connection between two component parts of an electrical design, a matrix of possible attributes and interpretations is shown in **Table 10**.

A.7.2 In this example there are two parts of an electrical design. These parts may be discrete components or complex digital systems.

A.7.3 The first attribute is the relationship between the ground (0V) potentials of the two parts. On a printed circuit board with a ground plane this is not an issue. However, it becomes important in systems, for example, with separate ground regimes, large physical separation or high data rates.

A.7.4 The connection between these parts gives the remainder of the attributes. The physical connection attribute looks at the number of connections, the possibility of wrong connection and the likelihood and effects of crosstalk and shorting between carriers.

ANNEX A

A.7.5 The voltage and current attributes compare the drive capability of one end, with the loading and impact requirements of the other. The protocol attributes cover which end may drive the link for bi-directional signals, and how the signal is transferred relative to a timing reference. Finally, the capability of the carrier is questioned.

A.8 GUIDE WORD INTERPRETATIONS FOR ELECTRO-MECHANICAL SYSTEMS

A.8.1 Frequently, PES are included in systems together with electro-mechanical parts and a HAZOP Study will need to address those aspects. A typical mechanical sub-system might include components such as motors, shafts and gearboxes. In **Table 11** some sample attributes are given for the mechanical parts of such a system, together with example interpretations of guide-words to explore deviations.

References:

- [1] Hatley D and Pirbhai I. Strategies for real-time system specification. Dorset House, 1988. ISBN 0-932633-11-0
- [2] Shlaer S and Mellor S. Object lifecycles: Modelling the world in states. Yourdon Press, 1992. ISBN 0-13-629940-7

Table 9 Matrix of Example Attributes and Guide Word Interpretations for a Communication System

	NO	MORE	LESS	AS WELL AS	PART OF	REVERSE	OTHER THAN	EARLY	LATE	BEFORE	AFTER
Generic Meanings	No part of the intention is achieved.	A quantitative increase.	A quantitative decrease.	All design intent but with additional results.	Only some of the intention is achieved.	The logical opposite of the intention.	Result other than original intention is achieved.	Relative to clock time.	Relative to clock time.	Relative to order or sequence.	Relative to order or sequence.
Physical Topology	N/A	There are more nodes than required.	There are fewer nodes than anticipated or required.	N/A	Ability to transmit or receive but not both, e.g. duplex becomes simplex.	N/A	Rogue node misbehaving <hr/> Wrong architecture	N/A	N/A	N/A	N/A
Master	No master node is identified	More active masters than planned.	Less masters active than planned.	N/A	N/A	N/A	Master is other than the one expected to be in control.	N/A	N/A	N/A	N/A
Encoding for Reliability	Encoding missing.	Greater reliability at bandwidth.	Less reliability than required.	N/A	N/A	N/A	Corruption of the encoding.	N/A	N/A	N/A	N/A
Protocol	No protocol implemented.	N/A	N/A	Other handshakes or other control signals.	Partial command or response.	Transmits when should be receiving or vice versa.	Protocol signals present but wrong.	Relative to clock time.	Relative to clock time.	Relative to order or sequence.	Relative to order or sequence.
Bandwidth of Signals	N/A	More than expected (slower or no response).	Less data than expected (faster response).	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Data rate	No data is transferred.	Data rate is too high.	Data rate is too low.	Inappropriate loading of a shared channel.	N/A	N/A	Variable	N/A	N/A	N/A	N/A

Table 10 Matrix of Example Attributes and Guide Word Interpretations for Digital Hardware

	NO	MORE	LESS	AS WELL AS	PART OF	REVERSE	OTHER THAN	EARLY	LATE	BEFORE	AFTER
Generic Meanings	No part of the intention is achieved.	A quantitative increase.	A quantitative decrease.	All design intent but with additional results.	Only some of the intention is achieved.	The logical opposite of the intention.	Result other than original intention is achieved.	Relative to clock time.	Relative to clock time.	Relative to order or sequence.	Relative to order or sequence.
Voltage Difference Between Grounds	Undefined.	Too high a difference.	N/A	N/A	N/A	N/A	Grounds thought to be static that are moving.	N/A	N/A	N/A	N/A
Number of Connections	Missing or broken connection.	N/A	Less connections than signals needed.	Crosstalk.	N/A	Twisted bus e.g. (0-15) ->(15-0).	Shorting.	N/A	N/A	N/A	N/A
Voltage Drive vs Loading	No signal.	Over voltage.	Under voltage.	N/A	N/A	Inverted logic (i.e. in the opposite range).	Outside valid range but not sufficient to cause change.	N/A	N/A	N/A	N/A
Current Drive vs Loading	No signal.	Excessive current.	Insufficient drive for load.	N/A	N/A	Current in reverse direction.	Outside defined range of currents.	N/A	N/A	N/A	N/A
Bi-directional Signals	No drive at all hence no signal.	N/A	N/A	More than one output.	N/A	N/A	The incorrect output driving.	N/A	N/A	N/A	N/A
Timing Relative to a Reference	Missing reference.	N/A	N/A	N/A	N/A	N/A	N/A	Relative to clock time.	Relative to clock time.	Relative to order or sequence.	Relative to order or sequence.
Wire Capability	Missing or broken wire.	Too high voltage. Too high current.	Too low a current.	Interference or EMI.	N/A	Acting as a transmission line.	Wrong wire leading to wrong signals at far end.	N/A	N/A	N/A	N/A

Table 11 Matrix of Example Attributes and Guide Word Interpretations for the Mechanical Parts of a System

	NO	MORE	LESS	AS WELL AS	PART OF	REVERSE	OTHER THAN	EARLY	LATE	BEFORE	AFTER
Generic Meanings	No part of the intention is achieved.	A quantitative increase.	A quantitative decrease.	All design intent but with additional results.	Only some of the intention is achieved.	The logical opposite of the intention.	Result other than original intention is achieved.	Relative to clock time.	Relative to clock time.	Relative to order or sequence.	Relative to order or sequence.
Torque	No torque appears.	Higher than expected.	Lower than expected.	N/A	N/A	Torque is reversed.	Torque is cyclic (fluctuating).	N/A	N/A	N/A	N/A
Load	No load.	Higher than expected.	Lower than expected.	N/A	N/A	N/A	Load is in unexpected direction. Fluctuating.	N/A	N/A	N/A	N/A
Speed	No	Overspeed.	Underspeed.	N/A	N/A	N/A	Fluctuating.	N/A	N/A	N/A	N/A
Force	No	More than expected.	Less than expected.	N/A	N/A	N/A	In wrong direction.	N/A	N/A	N/A	N/A
Temperature	No temp measurement.	Higher than expected.	Lower than expected.	N/A	N/A	N/A	Increasing. Decreasing.	N/A	N/A	N/A	N/A
Material	Complete failure.	N/A	Less of material (wear).	Corrosion is present.	Fatigue	N/A	Creep. Failure.	N/A	N/A	N/A	N/A
Containment	Complete failure of containment.	N/A	N/A	N/A	Partial loss of containment.	N/A	N/A	N/A	N/A	N/A	N/A
Torque Rate	Torque is static.	Increasing.	Decreasing.	N/A	N/A	N/A	Unexpected.	N/A	N/A	N/A	N/A
Load Rate	Load is static	Increasing.	Decreasing.	N/A	N/A	N/A	Unexpected.	N/A	N/A	N/A	N/A
Acceleration	Constant speed.	Higher than expected.	Lower than expected.	N/A	N/A	Changing in wrong direction.	Unexpected. Fluctuating.	N/A	N/A	N/A	N/A
Change of Force	Constant force.	Higher than expected.	Lower than expected.	N/A	N/A	Changing in wrong direction.	Unexpected. Fluctuating.	N/A	N/A	N/A	N/A
Change of Temperature	Constant temperature.	Higher than expected.	Lower than expected.	N/A	N/A	Changing in wrong direction.	Unexpected.	N/A	N/A	N/A	N/A

ANNEX B

ANNEX B

EXAMPLE HAZOP STUDY AT SYSTEM BLOCK DIAGRAM LEVEL

B.1 GENERAL

B.1.1 The purpose of this Annex is to give a small example of a typical HAZOP Study at the System Block Diagram level to illustrate some of the points in this Standard.

B.1.2 The example in this Annex will be presented in two sections:

- a. a brief description of the system and a block diagram;
- b. sample HAZOP worksheets exploring some of the potential deviations, reported 'by exception only' (see **Table 12**).

B.1.3 It should be noted that the design used in this example is of a system at a high level of abstraction. The design and the sample HAZOP Study worksheets are illustrative only and are not taken from a real system. They are included to show the process and are not claimed to be complete.

B.1.4 The example illustrates how a HAZOP Study can explore deviations of some attributes of the system components themselves, as well as of the entities flowing on the connections between them.

B.2 THE APPLICATION

B.2.1 System Purpose The application concerns train-carried equipment for automatic train protection (ATP). This is a function implemented on many Metro trains and some mainline trains. ATP monitors the speed of the train, compares that speed with the planned safe speed of the train and automatically initiates emergency braking if an overspeed condition is recognised. On all ATP systems there is equipment on both the train and track-side whereby information is transferred from the track-side to the train. There are many different ATP systems in existence, all differing in the detail of how they fulfil the basic requirement.

B.2.2 System Description On board the train there are one or more antennae which receive signals from the trackside giving information on safe speeds or stopping points. This information goes through some processing before being passed to a PES. The other major input to the PES is from tachometers or other means of measuring the actual speed of the train. The major output of the PES is a signal to safety relays such as the one controlling the emergency brake. **Fig 7** gives a simple block diagram of this.

ANNEX B

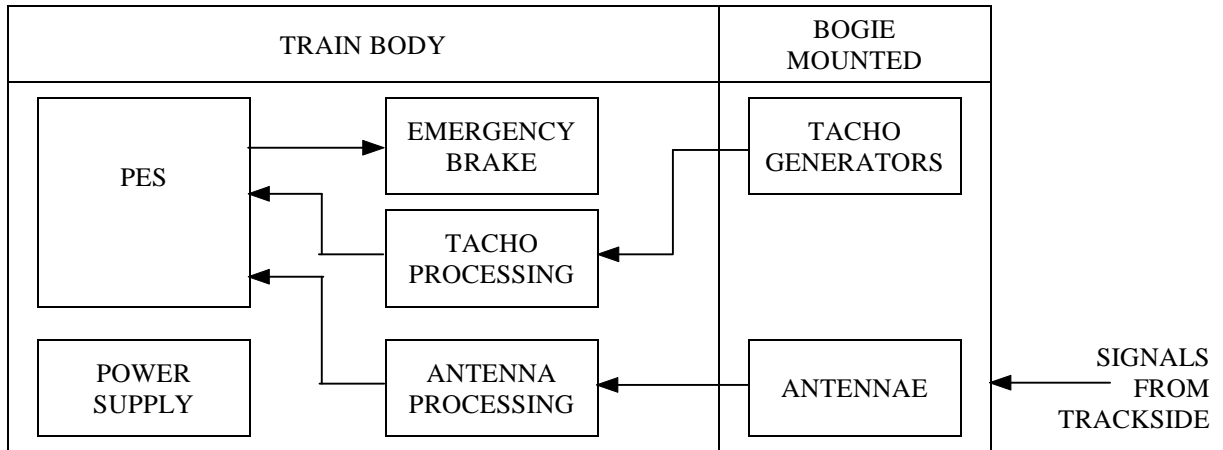


Fig 7 Train Carried ATP Equipment

HAZOP ITEM	PART	ATTRIBUTE	GUIDE WORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION
1	Input to Antenna.	Amplitude.	More	Mounted too close to rail.	May damage equipment.	Installation checks.	R1: Add check to installation procedure.
2	Input to Antenna.	Amplitude.	Less	Mounted too far from rail.	Signal may be missed.	Installation checks.	R2: Add check to installation.
3	Input to Antenna Processing.	Frequency.	Other than	Pick-up of signal from adjacent track.	Incorrect value passed to processor.		Q3: Is action taken to protect against this?
4	Antenna Cabling.	Signal to ATP.	Other than	Pick-up from nearby cabling.	Valid but incorrect signal may be acted on.		R4: Ensure cabling interference is guarded against.
5	Antenna.	Voltage.	More.	Antenna shorts to live rail.	Antenna and other equip becomes live.		Q5: Is there protection against this?
6	Antenna.	Position.	Other than	Failure of mountings.	May hit track.		R6: Ensure that cable will keep Antenna clear of track.
7	Tachometer	Output voltage.	No	Axle locked.			R7: Check implications of this.
8	Tachometer Output.	Signal.	As well as.	Other signals mixed in.			Q8: Is this a credible failure?
9	Tachometer Output.	Frequency.	More.	Design fault.	May indicate wrong speed.		R9: Check maximum frequency.
10	Tachometer Output.	Speed.	As well as	Sudden changes in output caused by wheel spin.	May show wrong speed.		R10: Check this is not a problem in practice.

Table 12 Sample HAZOP Study Sheets (continued)

HAZOP ITEM	PART	ATTRIBUTE	GUIDE WORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION
11	Tachometer Output.	Speed	No	Sudden wheel lock.	May show zero speed.		R11: Check protection against this.
12	Tachometer Output.	Speed	No	Sudden release of locked wheel gives confusing signal.	May show wrong speed.		R12: Check protection against this.
13	Signal to Emergency Brake.	Voltage	More	Stuck at fault in electronics.	May prevent brake initiation.		R13: Check protection against this.
14	Signal to Emergency Brake.	Voltage	More	Failure of part of electronics.	May prevent brake initiation.		R14: Check protection against this.
15	Signal to Emergency Brake.	Voltage	More	Cable fault.	May prevent brake initiation.		R15: Check wiring integrity.
16	Power supply to train equipment.	Voltage	More	Short circuit in drive transformers.	Overvoltage on other equipment.		Q16: Confirm drive transformer isolation?
17	Power supply to PES.	Frequency	As well as	Oscillating frequency of PSU.	Interference leading to unreliable operation.		R17: Check that oscillation frequency will not cause interference.

ANNEX C

ANNEX C

EXAMPLE HAZOP STUDY FOR HELICOPTER ON-BOARD DIAGNOSTICS

C.1 GENERAL

C.1.1 The purpose of this Annex is to show some of the source material and the outputs of a small but real HAZOP Study as an example illustrating some of the points in this standard.

C.1.2 The example in this Annex will be presented in three sections:

- a. a description of the application and of the design of the system;
- b. the HAZOP worksheets as produced by the HAZOP recorder;
- c. some samples of typical dialogue associated with particular items from the HAZOP.

C.1.3 It should be noted that the designs used in this example is of a system at the prototype stage. The HAZOP sheets are taken from real HAZOP Study sessions and are included to illustrate the process, not to be the 'perfect' solution.

C.2 THE APPLICATION

The application concerns on-board fault diagnosis in a helicopter. Various events and symptoms (pieces of 'evidence') occur, deriving from instrument readings or pilot actions. They are used to reason about the state of the helicopter and to identify faults. Faults are notified to the pilot by highlighting a Fault Central Warning Panel (FCWP) and displaying a text description. If a fault is suspected but is not unambiguously identified then a warning panel will be highlighted. The pilot may be asked to perform some Actions to assist in the diagnosis; for example, 'Reduce collective'. Some actions might be recommended as a consequence of a completed diagnosis; for example, 'Land as soon as practicable'. The pilot can ask for the explanation of a fault by clicking on the FCWP.

C.3 DESCRIPTION OF THE DESIGN

C.3.1 Object Orientation Object-orientation aims to overcome the separation of data from operations which process the data. It divides up the functionality required of a system according to the types of entity which have been identified in the system. Data structures and (parts of) function definitions are therefore combined into the definition of a 'class', which acts as a template for creating 'instances'. An object is a module that combines state information with processing capability. The terminology used to describe the basics of object-orientation varies. The state information is held in 'instance variables', or 'attributes', or 'slots'; the processing capability is provided in 'methods', or 'operations' and so on. An object does not, strictly speaking, directly access the data or invoke the functions of another. Instead it 'sends a message' to another object which names the information or processing that is required. Details of how the information or the processing is provided are hidden, leading to a more modular implementation that is easier to revise.

ANNEX C

C.3.2 Shlaer-Mellor Object Oriented Development The Shlaer-Mellor approach to object oriented development consists of two activities:

- a. object oriented analysis (OOA);
- b. a technique for object oriented design (OOD) called 'recursive design' (RD).

C.3.2.1 A more detailed account of the Shlaer-Mellor approach can be found in [1].

C.3.2.2 The OOA activity produces three main types of model:

- a. information models describing objects, their attributes and their relationships;
- b. state models consisting of state machine descriptions of object life cycles, together with object communication models exhibiting the asynchronous communication between object;
- c. process models consisting of data flow diagrams detailing object actions, together with object access models exhibiting the synchronous communication between objects.

C.3.2.3 The OOD activity largely consists of defining implementable classes from objects identified in the OOA. Object oriented design language (OODLE) is used to describe four types of model:

- a. inheritance diagrams;
- b. dependency diagrams;
- c. class diagrams;
- d. class structure charts.

C.3.3 The Design Description Describing the design of the helicopter fault diagnosis system in OODLE would produce a representation which is too complicated for the purposes of the Study. Instead, simplified versions of class diagrams and dependency diagrams have been produced. (The design does not exploit inheritance relations, while accurate class structure charts would be too complicated for present purposes).

C.3.3.1 Classes **Fig 8** illustrates a design notation for classes with reference to the key Evidence class:

- a. hexagons indicate object attributes or state variables ('instance variables');
- b. oblongs indicate operations the object can perform.

C.3.3.2 Dependencies And Connections **Fig 9** is a top-level view of the system, showing the connections between objects. (The objects Helicopter, Pilot and Developer are viewed as external objects, or objects of another operating environment).

C.3.3.2.1 The object connections are of three types:

- a. invoking of an operation on another object, where the invocation (given the current implementation) involves a transfer of control;

ANNEX C

- b. accessing the attribute values of another object;
- c. sending a message to an object, where the receiving object treats this as an event to be dealt with at a later date.

C.3.3.2.2 Apart from the cases of **c.**, which are indicated in the diagram, the figure can be considered a dependency diagram, as described in reference [1].

C.3.3.3 Detailed Interactions **Fig 10** elaborates on the picture contained in the top-level diagram. They show the operations used by the classes involved in the object connections on which the HAZOP focused. The conventions are as follows:

- a. invocation of an object operation is shown by an arrow from an operation of one object to an operation of another object;
- b. object accesses which require a result to be returned are shown with bi-directional arrows;
- c. a dotted line indicates an operation that generates an event to which the target object eventually responds with the target operation;
- d. arrows are given a label which names the parameter, or group of parameters, passing between the objects.

C.3.4 Intended Operation of the System

C.3.4.1 The following describes the role of each object in producing the behaviour of the system. **Fig 9** shows the top-level view of the system. The names of the object classes are capitalised. The HAZOP analysis concentrated on a small number of connections between objects (see **Fig 10**). For those connections, the operations are indicated in *italics*:

- a. the external Helicopter object sends instrument readings and status reports (*send_value*) into the fault diagnosis system to be received by the Data Channel objects (*store_value*);
- b. the Data Channel object responds to these values (with *handle_value*) by:
 - 1. updating the internal description of the helicopter (Aircraft Parameters, with *update_parameters*);
 - 2. arranging for the creation of a piece of evidence (Evidence, with *instantiate_evidence*, which returns an object reference);
 - 3. arranging for a new piece of evidence to be posted where it is visible (in Evidence Pool).
- c. the Context object provides an extra layer of control to the diagnosis process;
- d. the Aircraft Parameters object tells (*notify_changes*) the Diagnosis Rules object of the changes it has handled;
- e. the Evidence object tells (*notify_changes*) the Diagnosis Rules object of the piece of evidence it has constructed;

ANNEX C

- f. the Diagnosis Rules object performs the diagnostic reasoning. It responds to the reported changes with its processing operations (for example, *process_evidence*). This response is enabled by an event from the System Object (invoking the *run* operation on Diagnosis Rules). It results in a complex operation which invokes operations on many other objects:
 1. a new 'control record' (Context) may be created;
 2. the 'control record' may be switched;
 3. evidence may be created (Evidence, with *instantiate_evidence*, returns an object reference);
 4. evidence may be associated with a fault hypothesis;
 5. evidence may be posted (into Evidence Pool);
 6. a new fault diagnosis record (Fault Hypothesis) may be created;
 7. the fault diagnosis record may be updated;
 8. a fault hypothesis record may incorporate new evidence;
 9. a request for pilot action might be displayed (on Pilot Display);
 10. a diagnosis record may be posted (into Expert Pool).
- g. the Fault Hypothesis object records the progress of the diagnosis. It invokes operations on Reason Display and Pilot Display to display information on the record, and feeds back changes to the record into Diagnosis Rules;
- h. the Pilot Display takes the parameters passed by Diagnosis Rules or Fault Hypothesis when they invoke its operations. It also handles events deriving from actions by the (external) Pilot object. It analyses the messages it receives, divides the parameters it receives and sends different parts to appropriate displays:
 1. Fault Text Monitor handles the text underneath the 'Fault' caption;
 2. Action Monitor handles the text underneath the 'Actions' caption;
 3. FCWP Monitor controls the highlighting of fault indicators;
 4. Warning Monitor controls the highlighting of the Warning strip;
 5. Explanation Monitor handles the EXPLAIN indicator and the text underneath the Explanation caption.
- i. the Reason Display takes the parameters passed by Evidence and Fault Hypothesis when they invoke its operations. It analyses the messages it receives, divides the parameters it receives and sends different parts to appropriate displays;
- j. the Expert Pool object acts as an area where the Diagnosis Rules object posts information on the diagnosis record;
- k. the Evidence Pool object acts as an area where the Data Channel and Diagnosis Rules objects posts information on pieces of evidence;
- l. the System Object responds to an instruction from the (external) Developer object, invokes operations on Evidence Pool and Expert Pool to check for changes in those data areas, and enables the Diagnosis Rules object.

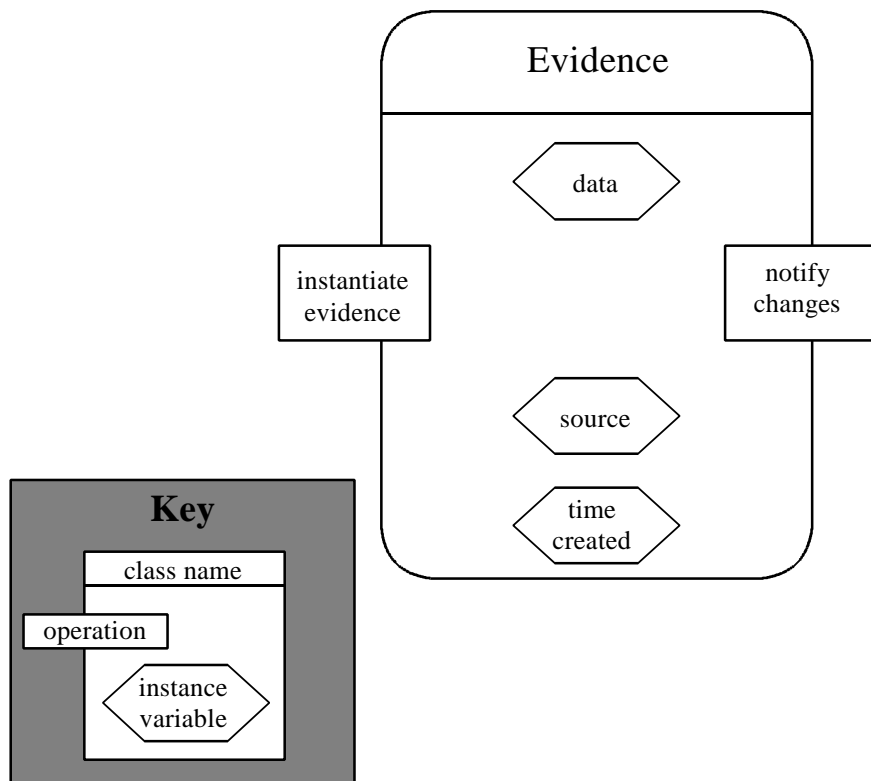


Fig 8 Object Oriented Design Notation Example

C.4 HAZOP STUDY SHEETS

These are shown in **Table 13**.

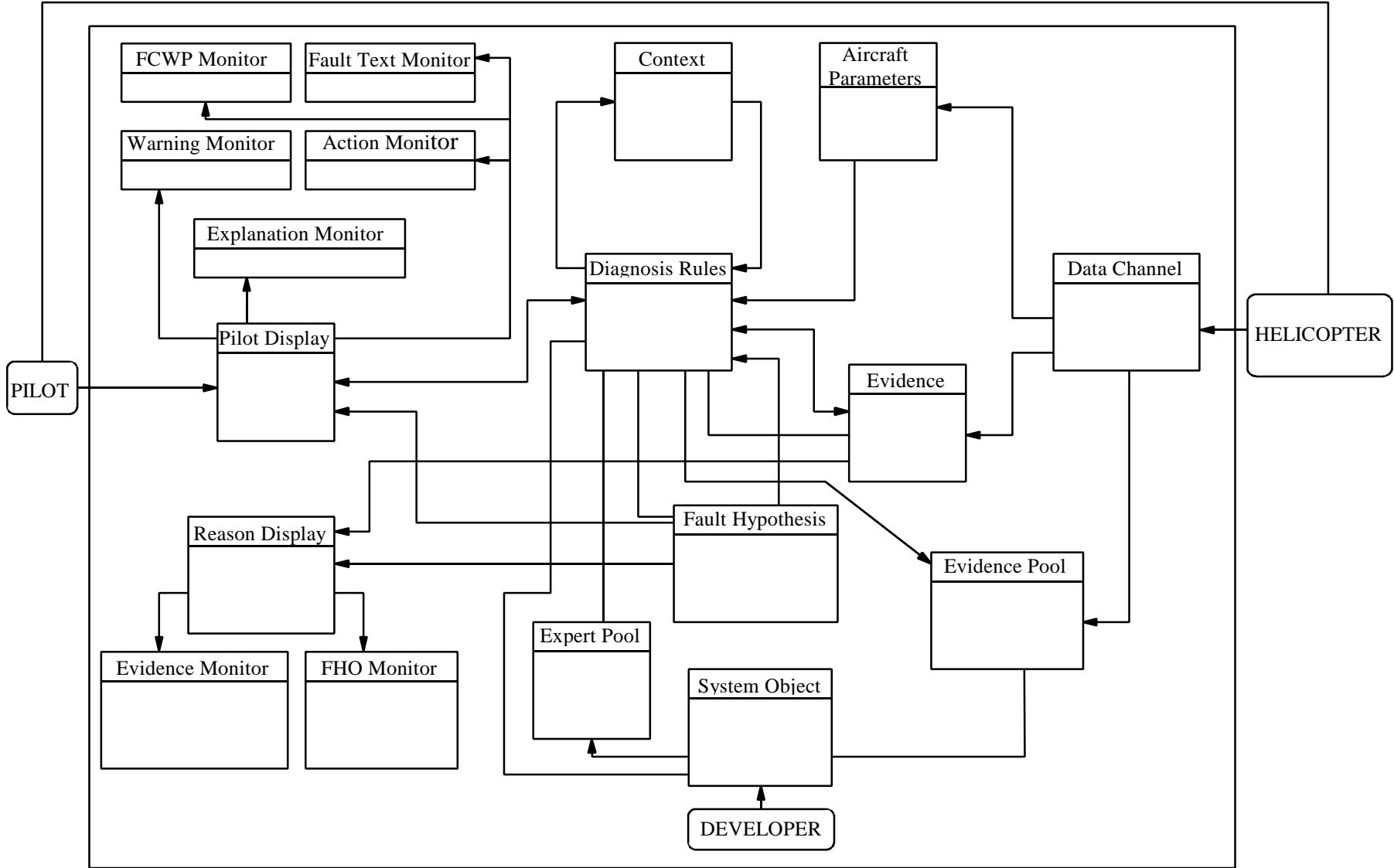


Fig 9 Top-level View of Helicopter On-board System

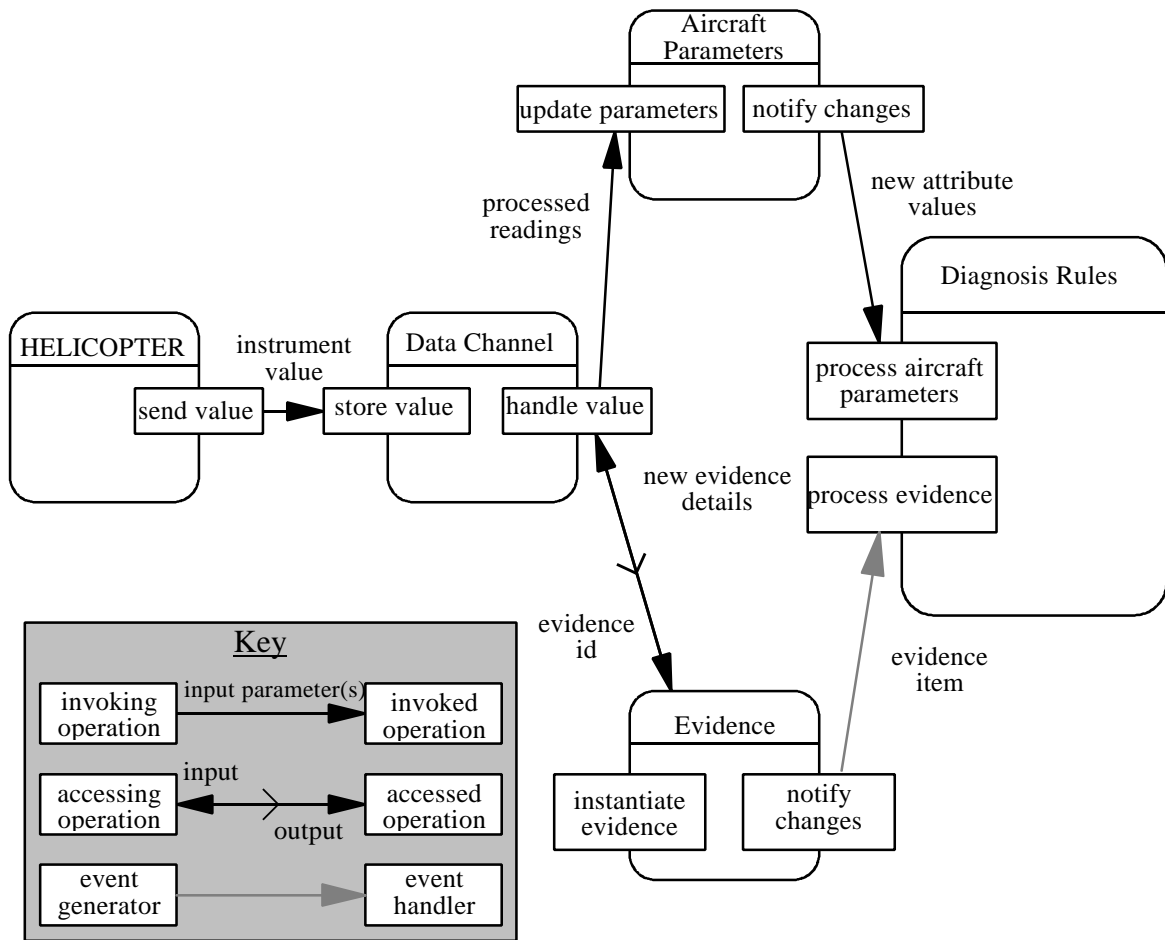


Fig 10 Part of On-board System in More Detail

Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics

HAZOP: Diagram: Date: Leader: Recorder: Team Members:		Helicopter Fault Warning System Figure 10 11-Aug-94 ABC XYZ Z, Z2, Z3, Z4			Description:	HAZOP of object oriented design for a fault warning system for helicopter pilots		
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
1	Helicopter send value to data channel store value.	Data flow	No	Failure of send value method or instrument sensor.	System will not know that this has occurred and may make misdiagnosis, fail to diagnose fault, etc. as it will not receive updated values.		R1 Means should be provided to warn the pilot that the system is not receiving the instrumental values it requires to function as designed.	
2	Helicopter send value to data channel store value.	Data flow	As well as	Other interference from the operating environment.	Data values are corrupted by interference.		R2 This is beyond the scope of this particular study but it is recommended that it is examined in another study.	
3	Helicopter send value to data channel store value.	Data flow	Other than	Value is received in the correct form but is incorrect value, i.e. out of range.	Diagnosis may be based on incorrect values.	Some data is checked within data channel to ensure it is within legal values (plausibility check).	R3 Ensure that all critical sensor values are included in the plausibility check.	
4	Helicopter send value to data channel store value.	Data flow	Other than	A value is received which is in the valid range but is incorrect.	Diagnosis may be based on incorrect data.	Plausibility checks will not realise that this data is erroneous.	R4 Consider checks to eliminate spurious changes, for example, a rate of change check.	

continued on page 56

Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics (continued)								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
5	Helicopter send value to data channel store value.	Data flow	Other than	Corruption in the data channel reference source.	The correct value may be sent to the wrong object. If there is a permanent change in reference this would lead to loss of data.	Recommendations 3 and 4 would help prevent incorrect data being used. Recommendation 1 would help if no data were sent.	N5 See previous recommendations R1, R3 and R4.	
6	Helicopter send value to data channel store value.	Data flow	Other than	Helicopter may not have checks on the data which is sent to the system.	Erroneous data may be passed to the system.		R6 Carry out a study to identify the safety critical aspects of the sensor values and to ensure an adequate degree of integrity of sensor and data channel.	
7	Helicopter send value to data channel store value.	Data flow	Before/after	Incorrect sequencing of data values received.	System will use incorrect evidence in making diagnosis.		R7 Data sequencing should be considered as part of the study carried out under R6.	
8	Helicopter send value to data channel store value.	Data rate	More	Data rate is too high and so data items may be missed out.	System will make diagnosis based on out of date data.		R8 Consider incorporating data rate verification and warning in data channel object, and also include data synchronization in helicopter study under R6.	

continued on page 57

Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics (continued)								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
9	Helicopter send value to data channel store value.	Data store	No	Rate of input is too high and data store becomes full.	System would not be able to process new values and diagnosis would become out of date	System is designed to keep on reasoning with available data	R9 A study should be conducted to determine the implications of each fault on helicopter safety and the consequences of late or missing diagnoses. The system should issue a warning to the pilot if this occurs.	
	Drawing Number #A7 Dat Cha Msg.							
10	Data Channel handle value to Instantiate evidence	Data flow	No	Failure of the handle value method.	No evidence created so no or incorrect diagnosis will be made.	Relies on the integrity of the code	R10 The handle value code should be subject to sufficient verification and validation.	
11	Data Channel handle value to Instantiate evidence.	Data flow	All deviations	Failure of the handle value method.	Integrity of code in handle value method in data channel object is key for a correct diagnosis.		R11 A safety critical method and assessment should be used in the development of handle value method. See R10.	
12	Data Channel handle value to Instantiate evidence.	Data flow	Other than	Incorrect implementation of the rules for designating values as evidence. These rules are fixed in the system.	New evidence details are not recognized and transmitted.		R12 When handle value code is implemented, consider how to validate the parameters that are used to define what is new evidence.	

continued on page 58

Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics (continued)								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
13	Data Channel handle value to Instantiate evidence.	Data rate	More	Evidence is passed at too high a rate.	System may become overwhelmed and fall over.		N13 The rate of new evidence updating is not considered likely to overwhelm the fault diagnosis: the critical rate is set by information received from the helicopter.	
14	Data Channel handle value to Instantiate evidence.	Data flow	No	Lack of pilot action or failure of handle value to generate new evidence.	System will wait for action or evidence.		R14 Provide time out on pilot actions and indication if evidence has not changed.	
15	Data Channel handle value to Instantiate evidence.	Data flow	Part of	Generation of messages is event driven and so evidence might be missed.	Algorithms fail to recognize a critical event.		R15 The criticality of evidence should be considered and critical evidence should be received repetitively.	
16	Data Channel handle value to Instantiate evidence.	Data flow	Before/After	Handle value passes values to some but not all objects (should pass values to aircraft parameters, evidence and evidence pool).	Data is not current in all objects and a misdiagnosis may be possible as there is missing or incorrect data, or diagnosis rules is not told to take action.		R16 Implementation of handle value must be verified to ensure the correct sequence, i.e. instantiate evidence before add evidence.	
17	Data Channel handle value to aircraft parameters.	Data flow	After	New evidence was notified to evidence pool but aircraft parameters were not updated in time.	Diagnosis rule will begin to process with incorrect values risking incorrect diagnosis.		R17 Consider ways to check that the aircraft parameters have been updated when new evidence is entered into the evidence pool.	

Table 13 Example HAZOP Study for Helicopter On-Board Diagnostics (continued)								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
18	Data Channel handle value to aircraft parameters.	Data flow	No	Old parameters in aircraft parameters have not been updated and are sent to diagnosis rules.	An inappropriate hypothesis may be generated.		R18 See previous recommendation R17.	
19	Data Channel handle value to Instantiate evidence.	Data flow	Other than	Incorrect object reference returned by Instantiate evidence.	Incorrect object reference is associated with evidence.		R19 Code for Instantiate Evidence should be subject to appropriate verification and validation.	
	Drawing Number #BA evi msg.							
20	Evidence notify changes to Diagnosis rules.	Data flow	No	Evidence change details are not passed to Diagnosis rules.	Diagnostic rules are not updated	If evidence relates to a potentially hazardous situation it will not be communicated.	R20 Apply checks within diagnostic rules to check that evidence and aircraft parameters are consistent, and to take appropriate action if they are not.	
21	Evidence notify changes to Diagnosis rules.	Data flow	Other than	Details relating to an incorrect evidence are passed.	Diagnostic rules may produce a false diagnosis which could be hazardous.		R21 See previous recommendation R20.	
22	Evidence notify changes to Diagnosis rules.	Data flow	Other than	Incompatibility between the evidence that is notified and the new parameter that is notified.	Diagnostic rules may produce a false diagnosis which could be hazardous.		R22 See previous recommendation R20.	

continued on page 60

HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
23	Evidence notify changes to Diagnosis rules.	Data flow	After	Evidence objects queue for processing. Aircraft parameters updated more rapidly.	Evidence and aircraft parameters would be inconsistent.		N23 Data rate is sufficiently slow to prevent too large a queue forming.	
24	Evidence notify changes to Diagnosis rules.	Data flow	Other than	Problem of synchronizing evidence and aircraft parameters as previously, or due to spurious evidence.	A hypothesis is rejected on a false evidence. The system will then not be able to reconsider this hypothesis if new evidence is received and may be unable to reach a conclusion.		N24 Consider means by which diagnostic rule can recover a discarded hypothesis if new evidence is received.	
25	Evidence notify changes to Diagnosis rules.	Data flow	Other	Diagnosis rule considers it has made a diagnosis and awaits pilot action when new evidence discounting hypothesis is received.	New evidence is ignored.		Q25 Is diagnostic rule able to process new information after a diagnosis has reached a completed stage?	A25 System will start a new diagnosis. This may lead to a new fault with new actions being requested. Consider implications on pilot confidence.

concluded

ANNEX C

C.5 EXAMPLE DIALOGUE

C.5.1 Example Dialogue 1

Item 2	
Leader:	Consider the data flow between Helicopter send value method and channel store value method and consider the deviation as well as. How can we get other information in this data flow?
Member:	Any interference from outside the system from the helicopter.
Member:	Do we know anything about that, for example, would the system be protected against this?
Designer:	No, the data may become corrupted by interference which could cause the system to malfunction.
Leader:	Would the interference be caused by anything within the system or external to the system?
Designer:	External to the system in this case, for example, other parts of the helicopter.
Leader:	Then we need not go into detail about the causes or solution to these factors as they are outside the scope of this study. Lets record that they should be investigated and move on.
Designer:	Recommend that a further study be carried out as I think this is important to the system.

[Recorder notes the item and the study moves on]

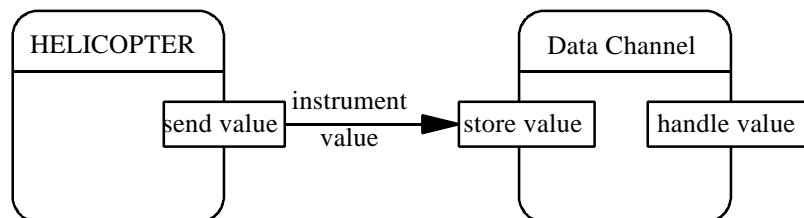


Fig 11 Extract From Fig 10 Relevant to Item 2

ANNEX C

C.5.2 Example Dialogue 2.

Item 23	
Leader	Consider the data flow from evidence, notify changes method to Diagnosis rules and consider the deviation after. How can this occur?
Member:	If there is a lot of evidence what does the system do?
Designer:	The evidence items would be placed in a queue for processing.
Member:	What if aircraft parameters are updated whilst evidence data is queuing?
Member:	Is it possible that the system will work with inconsistent data if is using more up to data aircraft parameters than evidence?
Leader:	Shall we record that as a hazard then?
Designer:	No, the system may act incorrectly if this occurs, but the data rate of evidence is fairly slow so I can't conceive of how a large queue would form that could not be processed in time. I don't think it is a likely occurrence.
Leader:	OK, we'll just record a note then as we have discussed it and then we'll move on.

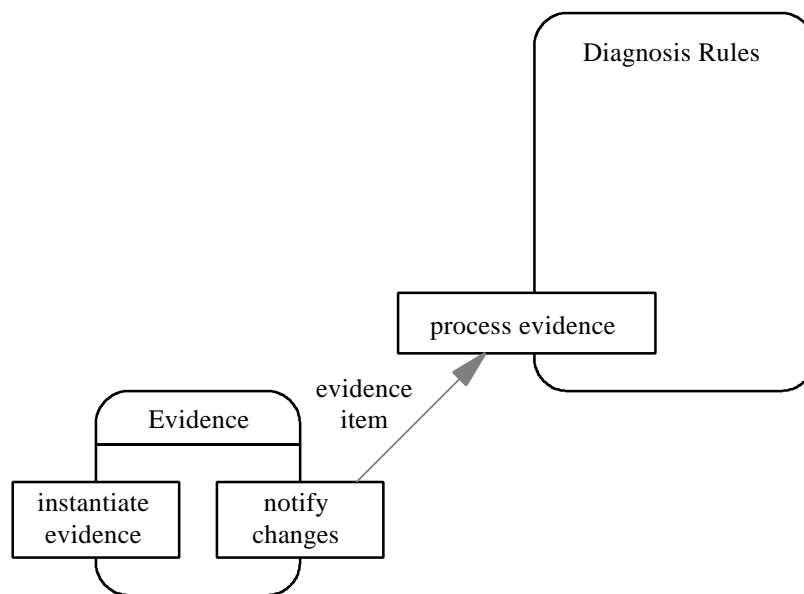


Fig 12 Extract From Fig 10 Relevant to Item 23

Reference

[1] Shlaer S and Mellor S. Object lifecycles: Modelling the world in states. Yourdon Press, 1992. ISBN 0-13-629940-7

ANNEX D

ANNEX D

EXAMPLE HAZOP STUDY FOR A COLLISION AVOIDANCE SYSTEM

D.1 GENERAL

D.1.1 The purpose of this Annex is to show some of the source material and the outputs of a small but real HAZOP Study as an example illustrating some of the points in this standard.

D.1.2 The example in this Annex will be presented in three sections:

- a. a design description of the system using the extended state machine logic (ESML) real time in Yourdon-De Marco notation;
- b. the HAZOP Study worksheets as produced by the HAZOP recorder;
- c. some samples of typical dialogue associated with particular items from the HAZOP Study.

D.1.3 It should be noted that the designs used in this example is of a system at the concept stage. The HAZOP sheets are taken from real HAZOP Study session and are included to illustrate the process, not to be the 'perfect' solution.

D.2 COLLISION AVOIDANCE SYSTEM DESCRIPTION

D.2.1 System Purpose The collision avoidance system is designed to alert the driver of a vehicle of an impending collision at low speeds. The most usual situation is that of a driver of the second or third car at a roundabout. The driver observes the car in front start to move off, looks right to check clearances, the driver in front brakes and a collision occurs.

D.2.2 System Description The system comprises a radar sensor mounted centrally on the front of the car with a fan shaped sensor beam. The geometry of the beam is such as to minimize detection of cars in adjacent lanes. The sensor system will only alert the driver when the speed is below a minimum speed of 5 mph. The system uses road speed sensed from a car's normal sensor and also detects use of brake. The system will alert the driver if he is moving slowly forward (creep) and there is a vehicle in front on which he is closing. If no action is taken then a higher level of alert is used (auditory warning). When an alert is initiated a recorder is also initiated to record car data for use in the event that a collision occurs. **Fig 15** gives the state transition diagram for the system and its relationship to the rest of the system is shown in **Figs 13 and 14**.

D.3 HAZOP STUDY SHEETS

These are shown in **Table 14**.

ANNEX D

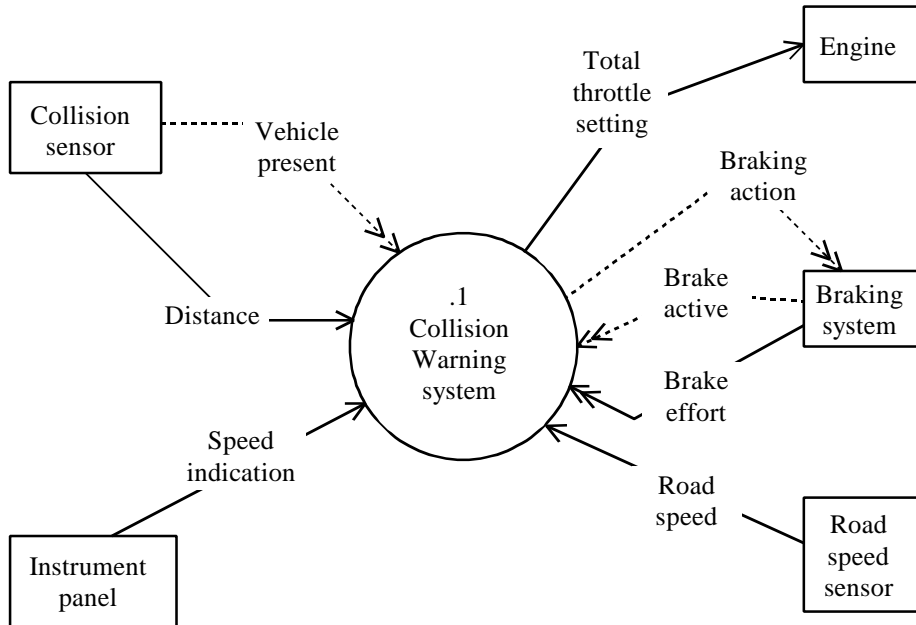


Fig 13 Context for Collision Avoidance System

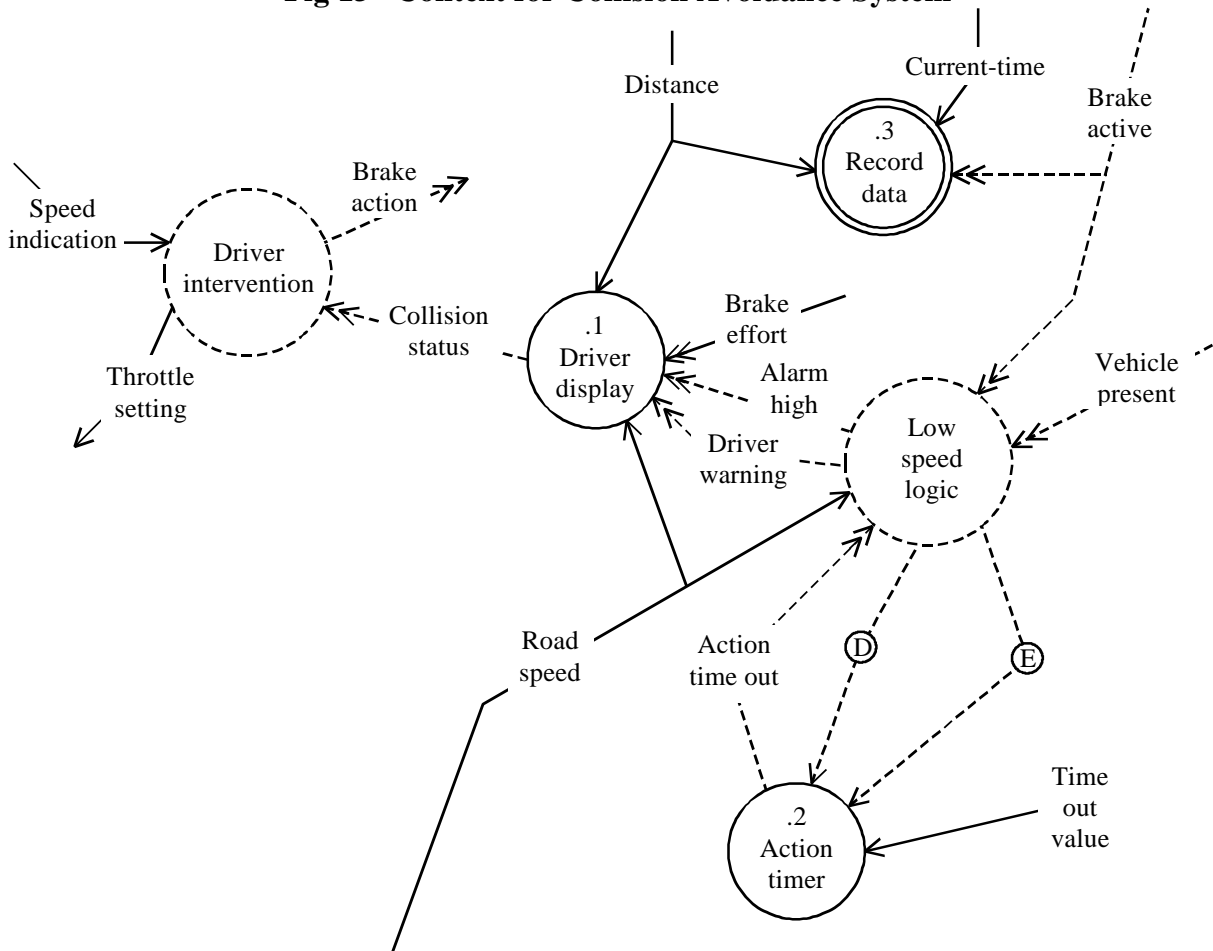


Fig 14 Top Level Decomposition for Collision Avoidance Showing Data Input to Low Speed Logic

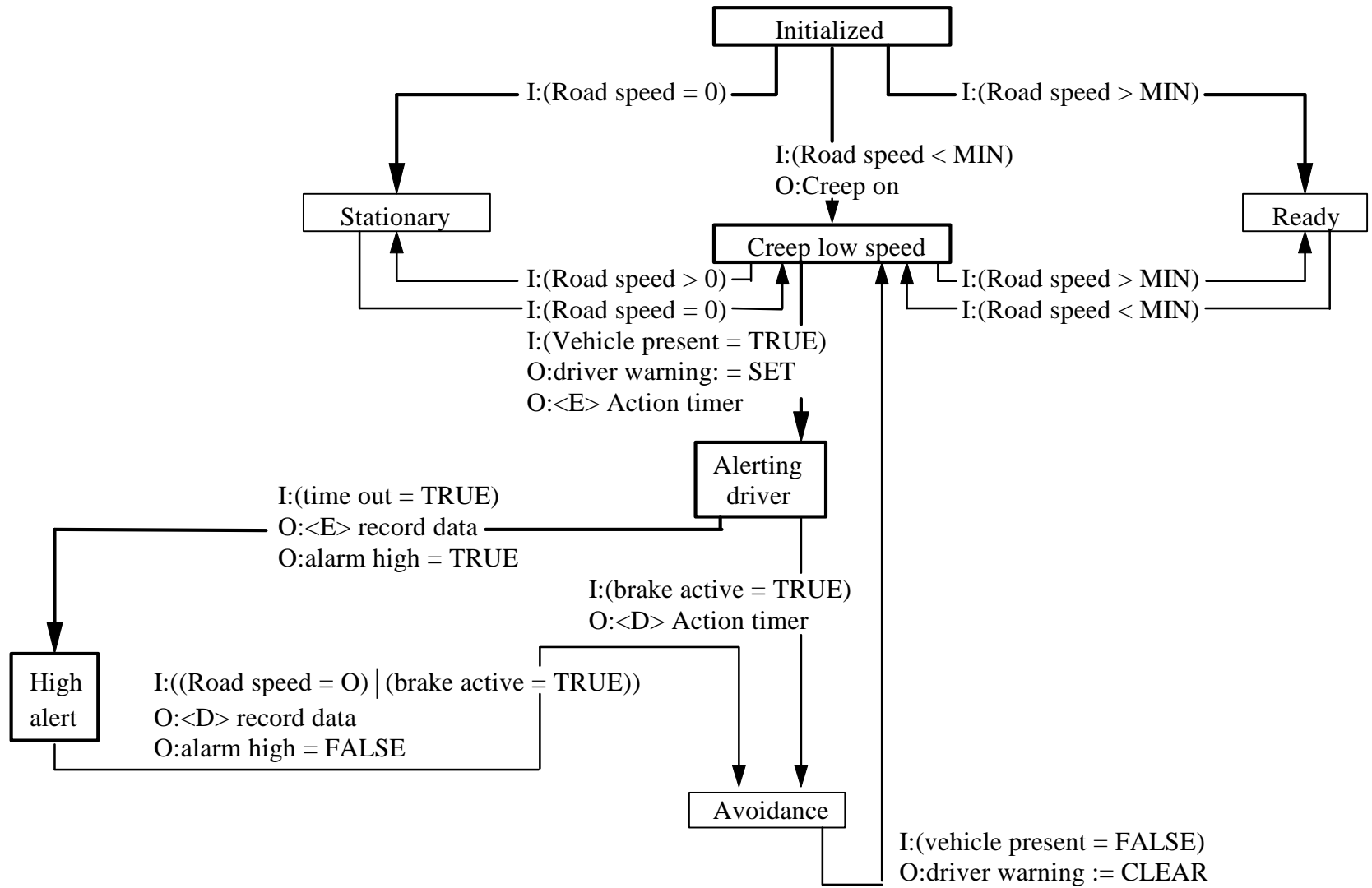


Fig 15 Low Speed Logic State Transition Diagram for Collision Avoidance System

Table 14 Example HAZOP Study for a Collision Avoidance System

HAZOP: Collision Avoidance System		Description:		HAZOP of state transition diagram of main states of collision avoidance system				
Diagram: Figure 15								
Date: 5-Aug-94								
Leader: A Smith								
Recorder: B Smith								
Team Members: C smith, D Jones, E Brown, F White								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/IMPLICATION	INDICATION/PROTECTION	QUESTION/RECOMMENDATION	ANSWERS/COMMENT
1	Initialized to stationary	Event	No	Failure of road speed sensor.	No hazardous consequences			
2	Initialized to stationary	Event	More		No meaning			
3	Initialized to stationary	Event	Less		No meaning in this context			
4	Initialized to stationary	Event	As well as	If the vehicle is stationary then the system will not be operated.	Car ahead can roll back without warning		System is not designed for this type of collision.	
5	Initialized to stationary	Event	Part of		No meaning			
6	Initialized to stationary	Event	Other than		No meaning			
7	Initialized to stationary	Event	Early/Late		No meaning			
8	Initialized to stationary	Event	Before/After		No meaning			
9	Initialized to ready	Event	No		No meaning			
10	Initialized to ready	Event	More		No meaning			
11	Initialized to ready	Event	Less		No meaning			
12	Initialized to ready	Event	As well as		No meaning			
13	Initialized to ready	Event	Part of		No meaning			
14	Initialized to ready	Event	Other than		No meaning			
15	Initialized to ready	Event	Earl/Late		No meaning			
16	Initialized to ready	Event	Before/After		No meaning			

Table 14 Example HAZOP Study for a Collision Avoidance System (continued)

HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
17	Initialized to Creep or Stationary to Creep	Event	No	Road speed sensor faulty.	Vehicle enters Stationary mode not Creep state.	Warning system not activated if there is a target.	R17 Evaluate reliability of road sensor to determine risk of failure.	
18	Initialized to Creep	Event	No	Road speed equals zero meeting condition for transition to both Stationary and Creep.	System may be confused and choice of state will be implementation dependent.		R18 Change the condition so the system has no ambiguity if Road speed = min.	
19	Initialized to Creep	Event	More		No implication.			
20	Initialized to Creep	Event	Less	Coasting with ignition off. Starting the engine just before collision.	Time taken to initialize the system may be insufficient to warn against collision.		R20 Ensure initialization time is in line with the preset speed and distance criteria.	
21	Initialized to Creep	Event	As well as		No hazardous consequence.			
22	Initialized to Creep	Event	Part of	Sensor fault so that road speed indicated is lower than actual speed.	If Creep mode entered at high speed then accelerator vibration at speed may be hazardous.		R22 Consider consequences of warning system being activated at high speed, e.g. while tailgating on the motorway.	
23	Initialized to Creep	Event	Other than	Additional pulses leading to a false high reading of speed.	Fail to creep when should do.			
24	Initialized to Creep	Event	Other than	Wheel spin causes road speed sensor to record higher speed than actual speed.	System is not activated under conditions when it desirable for it to be.		R24 Logic to detect excessive acceleration should be provided.	
25	Initialized to Creep	Event	Early/Late	Variable time for processor to initialize.			R25 Ensure the variability in the initialization of the processor, e.g. engine management system, is acceptable to permit the warning system to be available promptly.	
26	Initialized to Creep	Event	Before/After					

continued on page 68

Table 14 Example HAZOP Study for a Collision Avoidance System (continued)								
HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
27	Creep to Alerting driver	Event vehicle present	No	Vehicle is present but system fails to detect it.	Sensor may have failed.		R27 Provide sensor test facility and warning light to indicate failure.	
28	Creep to Alerting driver	Event vehicle present	No	Vehicle moves into lane from side. Vehicle is too high to be detected.			R28 Test that the sensor can detect a car entering from near side or off side and can detect the wheels on high vehicles.	
29	Creep to Alerting driver	Event vehicle present	No	Target too small, e.g. cyclist or motorcycle.	Collision with vulnerable target not sensed.		R29 Design radar sensor such that motorcycles can be detected.	
30	Creep to Alerting driver	Event vehicle present	More	A transient passage, e.g. passing car or even bird, initiates to alert.	Transit from driver alert only possible if brake pressed.		R30 Filter sensor signal for transients. Consider adding an extra transition so that the alert is cancelled when the sensor signal is no longer detected for sufficient period of time, e.g. a few seconds. Disable timer when alerting Driver is left.	
31	Creep to Alerting driver	Event vehicle present	Less	Filter damps reaction time of system.	Crash is not avoided.		R31 Investigate response profiles and braking profiles of drivers to ensure system response time is adequate.	
32	Creep to Alerting driver	Event vehicle present	Less	Range gate incorrectly set or corrupted so that vehicle present = True is registered too slowly. Distance registered is incorrectly interpreted as greater so that response is too slow.			R32 Investigate range gate setting so that slow response caused by corruption or false echoes is eliminated.	

Table 14 Example HAZOP Study for a Collision Avoidance System (continued)

HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/IMPLICATION	INDICATION/PROTECTION	QUESTION/RECOMMENDATION	ANSWERS/COMMENT
33	Creep to Alerting Driver	Event	As well as	Detection of distant objects as if they were near.	Spurious alert.		R33 The pulse repetition rate and the receive window of the sensor should be set to reduce phantom targets.	
34	Creep to Alerting Driver	Event	As well as	Spurious detection of mini-roundabouts, cattle grids, etc.	Spurious alert.		R34 Optimize beam geometry so as to reduce alerts from low objects.	
35	Creep to Alerting Driver	Event	Less	Minimum speed incorrectly set for performance of car.	Failure to alert.		R35 Minimum value must be set according to the performance of the vehicle.	
36	Creep to Alerting Driver	Event	Part of		No meaning.			
37	Creep to Alerting Driver	Action. Driver warning	Other than	Failure of sensor or B(uilt) I(n) T(est).	No warning given.		R37 Recommend that FMEA is carried out on sensor and Built In Test.	
38	Creep to Alerting Driver	Action	Early/Late	May be too late if cyclic processes rather than interrupts are used to effect transition.	Warning given too late.		R38 A timing analysis is required to ensure the alert state is reached soon enough.	
39	Creep to Alerting Driver	Action	Before/After	Speed exceeds min as vehicle present = true.	Action is not clear in this case and the outcome will be implementation dependent.		R39 Ensure vehicle Present = True takes priority.	
40	Alerting Driver to High Alert	Event. Time out	No	Time out does not occur.	No data is recorded and crash occurs without high alert.		R40 Time out depends on driver response time which needs to be very fast. Consider if High Alert serves a practical purpose. Consider initiating data recording at alerting driver.	
41	Alerting Driver to High Alert	Event	More	Time out too quick so system enters high alert immediately after low alert.	Driver starts to ignore warnings.		R41 Verify timing is adjusted so that repetitive transit to high alert does not occur.	

continued on page 70

Table 14 Example HAZOP Study for a Collision Avoidance System (continued)

HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDEWORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMMENDATION	ANSWERS/ COMMENT
42	Alerting Driver to High Alert	Event	More	Target vanishes, for example accelerates after high alert instigated.	No exit path other than braking.		R42 Consider Target false exit from high alert with a time out on it.	
43	Alerting Driver to High Alert	Event	As well as		No meaning.			
44	Alerting Driver to High Alert	Event	Part of		No meaning.			
45	Alerting Driver to High Alert	Event	Other than	If brake active = true occurs with time out = true action is unclear.	Outcome will be implementation dependent.		R45 Brake active = true should have priority over time out = true.	
46	Alerting Driver to High Alert	Event	Early/Late	The time interval on the timer is important. If this is long in relation to the response time of the driver the recording sequence may not be initiated.			R46 If implementation is a cyclic process the timing of the cycle should be investigated to ensure that it is compatible with response time required of the driver and system.	
47	Alerting Driver to High Alert	Event	Before/After		Not applicable.			

concluded

ANNEX D

D.4 EXAMPLE DIALOGUES

D.4.1 Example Dialogue 1

Item 24	
Leader:	Consider the system moving from initialised state to creep state and consider the attribute action and the deviation as well as. How can we have additional action occurring in this transition?
Member:	What happens if you pull out and get into a wheel spin?
Designer:	The road speed sensor could think that the vehicle is moving a lot faster than it actually is, as it measures from the wheels.
Member:	The system may not be activated when it was designed to be because it could think the vehicle was going faster than 5 mph.
Designer:	Yes, the system will only work below 5 mph.
Leader:	So this is a hazard then which needs to be recorded.
Designer:	Yes, the system needs to measure the rate of acceleration and if this is large to compensate for this against the measured road speed.
Leader:	Let's not solve it now, but record and move on.

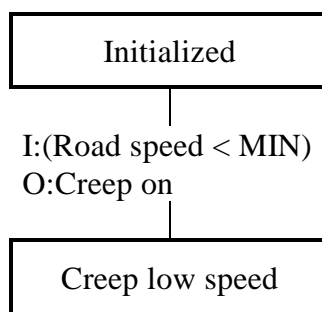


Fig 16 Extract From Fig 15 Relevant to Item 24

ANNEX D

D.4.2 Example Dialogue 2

Item 29	
Leader:	Consider the system moving from Creep state to Alerting Driver and consider the attribute action and the deviation no. How can the system fail to move into alerting driver when it is required to?
Member:	What range has the radar sensor got?
Designer:	It is designed to pick up a vehicle directly ahead, the range is one lane width at 20 metres.
Member:	Would it pick up a small target?
Designer:	Yes, if it was directly ahead.
Leader:	What about a motorbike which was at the side of the vehicle just ahead?
Designer:	Yes, I suppose it could be missed. The system would not warn the driver of its presence then as the condition to move into this state requires vehicle present = TRUE.
Leader:	That sounds like a major hazard, lets recommend that the design of the radar sensor be evaluated.

[Recorder notes item and HAZOP moves on]

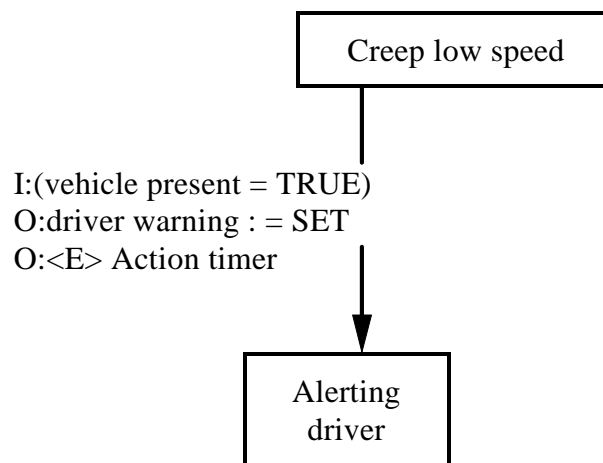


Fig 17 Extract From Fig 15 Relevant to Item 29

Inside Rear Cover

© Crown Copyright 2000
Copying Only as Agreed with DStan

Defence Standards are Published by and Obtainable from:

Defence Procurement Agency
An Executive Agency of The Ministry of Defence
Directorate of Standardization
Kentigern House
65 Brown Street
GLASGOW G2 8EX

DStan Helpdesk

Tel 0141 224 2531/2
Fax 0141 224 2503
Internet e-mail enquiries@dstan.mod.uk

File Reference

The DStan file reference relating to work on this standard is D/DStan/00/58/2.

Contract Requirements

When Defence Standards are incorporated into contracts users are responsible for their correct application and for complying with contractual and statutory requirements. Compliance with a Defence Standard does not in itself confer immunity from legal obligations.

Revision of Defence Standards

Defence Standards are revised as necessary by up issue or amendment. It is important that users of Defence Standards should ascertain that they are in possession of the latest issue or amendment. Information on all Defence Standards is contained in Def Stan 00-00 Standards for Defence Part 3 , Index of Standards for Defence Procurement Section 4 'Index of Defence Standards and Defence Specifications' published annually and supplemented regularly by Standards in Defence News (SID News). Any person who, when making use of a Defence Standard encounters an inaccuracy or ambiguity is requested to notify the Directorate of Standardization (DStan) without delay in order that the matter may be investigated and appropriate action taken.