PASSPORT II

Promotion and Assessment of System Safety and Procurement of Operable and Reliable Road Transport Telematics - II

DRIVE II Project V2058

Deliverable N° 9a

Workpackage: Framework

Framework for Prospective System Safety Analysis Volume 1 - Preliminary Safety Analysis

Authors: K M Hobley (Leeds University)
P H Jesty
K Wolf (TÜV Rheinland)
H Wijnands (TNO)
J Giezen
E Bovelander
F Escaffre (Veridatas)
J-M Astruc
A Kaligeris (ATC)
S Topouzidou
M Favaron (CESI)

Deliverable Type: P

Submission Date : December 1995

Partners: Leeds University, TÜV Rheinland, TNO, Veridatas, ATC and CESI

SUMMARY

The PASSPORT project is concerned with the functional system safety of Advanced road Transport Telematic systems. This document describes a systematic methodology for performing safety analyses on these systems. The framework uses a number of techniques, one of which is novel, and all of which are described in this document. The safety analysis is divided into two phases and should be performed under a Quality Assurance plan. During a preliminary safety analysis the proposed system is modelled using the novel PASSPORT Diagram, which can be checked for completeness and consistency. A hazard analysis is then performed to identify the safety requirements. Preliminary safety integrity levels are assigned, for the future development of the system, by assigning controllability categories to the hazards. The second phase is a detailed safety analysis of the design to confirm the findings of the first phase, and to establish that the safety requirements have been implemented. This phase may be iteratively performed as detail of the design becomes known. A second novel model, the PASSPORT Cross, is produced and formally checked for consistency. Traceability throughout the design is provided by the PASSPORT Identification for Traceability System. The performance of Failure Mode and Effect Analysis and Fault Tree Analysis is assisted by the PASSPORT Cross Model. A fully worked example is provided at the end of the document.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AE	Architectural Element
ALARP	As Low As Reasonably Practicable
ATT	Advanced road Transport Telematics
BSP	Business Systems Planning
CASE	Computer Assisted Software Engineering
CF	Communication Facility
DBMS	Data Base Management System
DRIVE	Dedicated Road Infrastructure for Vehicle Safety in Europe
DSA	Detailed Safety Analysis
EMC	Electromagnetic Compatibility
ERD	Entity Relationship Diagram
FE	Functional Element
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
HAZOPS	HAZards and OPerability Studies
HMI	Human Machine Interaction
IBM	Industrial Business Machines
ICD	Internal Communications Database
ICT	Internal Communication Transfer
ID	Internal Database
IRTE	Integrated Road Transport Environment
IS	Information Set

IT	Internal (data) Transfer
PASSPORT	Promotion and Assessment of System Safety and Procurement of Operable and Reliable road transport Telematics
PHA	Preliminary Hazard Analysis
PITS	PASSPORT Identification for Traceability System
PSA	Preliminary Safety Analysis
PSSA	Prospective System Safety Analysis
QA	Quality Assurance
QM	Quality Management
RAM	Random Access Memory
RDS	Radio Detection System
RSSE	Retrospective System Safety Evaluation
SIL	Safety Integrity Level
TBS	To Be Specified
TCAS	Towards the Certification of ATT Systems - System Safety Aspects
TOE	Target of Evaluation
WHISPER	WHeelchair for Intelligent and Safe Portage in Equipped Regions.

1. INTRODUCTION

The objectives of the DRIVE programme are to improve road safety, transport efficiency and environmental quality. Such benefits are being promised through the use of telematic systems. It is, however, clear that systems sufficient to have the power to advise on or to control road safety, transport efficiency or environmental quality might exercise this power for either good or ill, and the latter condition could be quite disastrous in the worst case. Developers naturally concentrate on the benefits of their system, especially when communicating with their financial supporters, private or public. However, in order to ensure that their systems do indeed only provide the benefits that they desire, and do not cause any undesired effects, a responsible developer should execute a series of processes to confirm the overall safety of the system.

Experience shows that, unless positive action is taken, then at some stage in the life of a system a failure to perform as expected will indeed occur. A recent example of a Transport Telematic system that failed in this manner was the computer aided dispatch system commissioned by the London Ambulance Service, though this was not a DRIVE project.

A system is defined as being safety-related if a fault in any part of the system, hardware or software, could lead to a hazardous situation occurring. There are two principal types of faults: random faults which may occur for many reasons, e.g. component wear, communication breakdown, and systematic faults which may be made in the software or in the overall design of the system. The undesirable effects of component wear, communication breakdown and software faults can be overcome by using a suitable design, but this is only effective if the design is correct. No responsible developer will deliberately produce an incorrect design, nevertheless design faults in both hardware and software do occur, and the reason for them can usually be traced to an incomplete understanding of the system due to its complexity. Transport Telematic systems are usually complex.

For a system design to be as fault free as possible it is necessary to analyse it thoroughly. This analysis should not only show that the system implements the desired benefits but that the risk associated with any possible failure has been reduced to an acceptable level. To gain sufficient confidence that a system has been developed properly it is generally agreed that it should undergo a separate and independent assessment. The need for a safety life-cycle that follows the normal development life-cycle so that the safety of the system can be ensured, is evident for a number of reasons. Among them are the fact that events that may lead to an unsafe situation must be identified during the design phase, since modifications are very expensive, and the fact that many faults are more easily detected at the sub-system level, before the system is integrated. A safety life-cycle is also an important tool for certification.

This document describes the methodology devised by the DRIVE II project PASSPORT (V2058) to perform a Prospective System Safety Analysis (PSSA). The objective of this framework is to give guidance to ATT projects on how to identify their safety hazards. The work is based on the principles laid down by the DRIVE I project DRIVE Safely (V1051)[DRIVE Safely 1992]. The effectiveness of this framework has already been established by applying it to selected DRIVE II projects. The methodology uses a number of techniques which are all described in the appendices. Some of these are well established for use in safety analysis, but the PASSPORT Diagram Model is novel and has been specially designed by members of the project PASSPORT. Appendix F contains a fully worked case study that provides a demonstration of the methodology, and Appendix E discusses the issue of Quality Management (QM) under which the development of any safety-critical system should be performed. Appendix G contains a glossary of the jargon terms used throughout the document. The companion document "Towards the Certification of ATT Systems - System Safety Aspects" (TCAS) [PASSPORT 1995b] describes the work performed in the workpackage Retrospective System Safety Evaluation (RSSE).

2. LIST OF RELATED DOCUMENTS

[Bell 1993]

Bell R and Reinert D, *Risk and System Integrity Concepts for Safety-Related Control Systems*, Microprocessors and Microsystems, Vol. 17 N°1, 1993.

[CIA]

The Chemical Industry Safety and Health Council, *A* Guide to *Hazard and Operability Studies*, The Chemical Industries Association.

[CORD 1994]

CORD, *Recommended Definitions of Transport Telematics Functions and Subfunctions*, DRIVE II Project V2056, 1994.

[DIN V 19250]

DIN V 19250, *Measurement and Control; Fundamental Safety Aspects to be Considered for Measurement and Control Equipment*, DIN, Germany, 1989.

[DRIVE Safely 1992]

DRIVE Safely, *Towards a European Standard: The Development of Safe Road Transport Informatic Systems (Draft 2)*, DRIVE Project V1051, 1992.

[EMCATT 1995]

EMCATT, *Functional System Safety and Electromagnetic Compatibility*, DRIVE II Project EMCATT (V2064), 1995.

[Henley 1992]

Henley E J and Kumamoto H, *Probabilistic Risk Assessment - Reliability Engineering, Design, and Analysis*, IEEE Press, 1992, ISBN 0-87942-290-4.

[HOPES 1993a]

HOPES, *Framework for MMI Safety Analysis*, DRIVE II Project V2002 Deliverable N° 5A, Department of Traffic Planning and Engineering, University of Lund, 1993.

[HOPES 1993b]

HOPES, *Framework for Prospective Traffic Safety Analysis*, DRIVE II Project 2002 Deliverable N°6, Department of Traffic Planning and Engineering, University of Lund, 1993.

[IBM GE/20/02572]

IBM GE/20/02572, *Business System Planning - Information System Guidelines*, Industrial Business Machines.

[IBM GE/20/06300]

IBM GE/20/06300, *Business System Planning - Executive Overview*, Industrial Business Machines.

[IBM GE/20/06551]

IBM GE/20/06551, *Business System Planning - Planning for Distributed Information Systems*, Industrial Business Machines.

[IEC 1508]

IEC 1508, *Functional Safety: Safety Related Systems*, IEC Draft Standard, IEC SC65A (Secretariat) 122/3.

[Jesty 1994]

Jesty P H and Hobley K M, *Integrity Levels - Fact or Fiction?*, Safety Critical Systems Club Newsletter, Vol. 4, N° 1, September 1994.

[Martin 1985]

Martin J and McClure C, Diagramming *Techniques for Analysts and Programmers*, Prentice Hall, 1985, ISBN 0-13-208794-4.

[MISRA 1994a]

MISRA, *Development Guidelines for Vehicle Based* Software, MIRA, Nuneaton, CV10 0TU, November 1994, ISBN 0 9524156 0 7.

[MISRA 1994b]

MISRA, *Integrity*, MISRA Report 2, The Motor Industry Research Association (MIRA), 1994.

[NUREG-0492 1986]

NUREG-0492, *Fault Tree* Handbook, U.S. Nuclear Regulatory Commission, 1986.

[PASSPORT 1994]

PASSPORT, *Quality Assurance Plan*, Deliverable N° 1, DRIVE II Project PASSPORT (V2058), 1994.

[PASSPORT 1995a]

PASSPORT, *Framework for Prospective System Safety Analysis: Volume 2 - Detailed Safety Analysis*, Deliverable N° 9b, DRIVE II Project PASSPORT (V2058), 1995.

[PASSPORT 1995b]

PASSPORT, *Towards the Certification of ATT Systems - System Safety Aspects*, Deliverable N° 8, DRIVE II Project PASSPORT (V2058), 1995.

3. OVERVIEW

A PSSA forms part of a larger set of activities, shown in Figure 3.1 which aim to give guidance to developers of ATT systems on how to apply system safety to their products in a way that can be fully evaluated. This set of activities is divided in three tasks:

i) The Preliminary Safety Analysis (PSA)
This task aims to identify the safety-related systems and to analyse those having safety implications (see Section 5).

ii) The Detailed Safety Analysis (DSA)
This task aims to ensure that system safety is adequately accounted for during the system definition and design phases (see [PASSPORT 1995]).

iii) The Certification Process
This task aims to ensure that the system has been safely and correctly implemented (see [PASSPORT 1995a]).

These tasks are grouped in two distinct end products: the *Framework for Prospective System Safety Analysis* (this document), and the document *Towards the Certification of ATT Systems - System Safety Aspects* (TCAS) [PASSPORT 1995b].

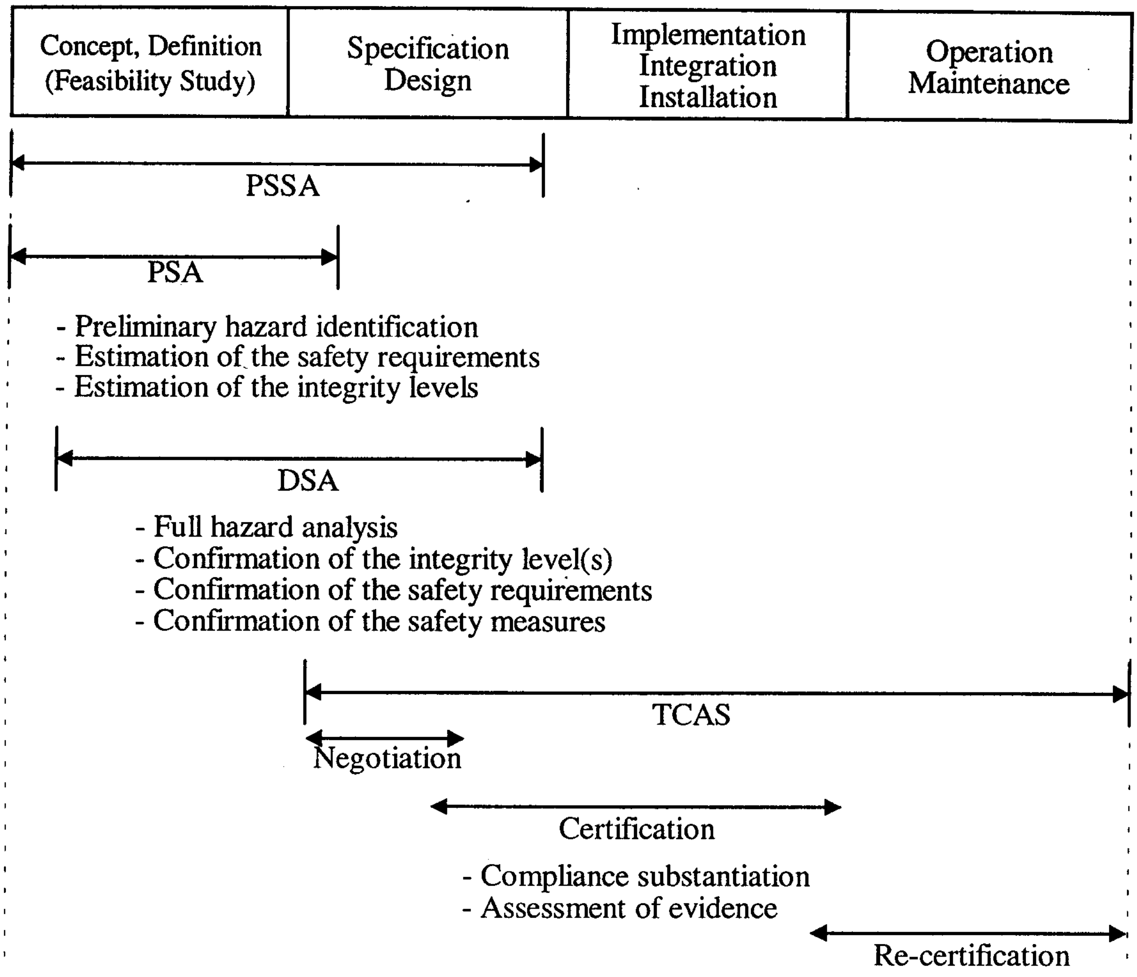

Concept, Definition (Feasibility Study)
Specification Design
Implementation Integration Installation
Operation Maintenance
PSSA
PSA
- Preliminary hazard identification
- Estimation of the safety requirements
- Estimation of the integrity levels
DSA
- Full hazard analysis
- Confirmation of the integrity level(s)
- Confirmation of the safety requirements
- Confirmation of the safety measures
TCAS
Negotiation
Certification
- Compliance substantiation
- Assessment of evidence
Re-certification

Figure 3.1 - Relationship between Safety Analysis Tasks and Assessment Tasks

The context of a PSSA is shown in Figure 3.2. The methodology is based on the philosophy developed by the DRIVE I project DRIVE Safely[DRIVE Safely 1992], and utilises the techniques developed by the DRIVE II project PASSPORT. The PSSA takes models of the Target of Evaluation (TOE), in increasing levels of detail, and by taking account of the safety criteria required by society, natural law and regulations, aims to produce the safety requirements necessary for the TOE, and the SILs needed for the development process. It is essential to appreciate that this work must be performed by a team consisting of both experts in safety matters and experts in the TOE itself (see Appendix A).

3.1 Safety Objectives and Requirements

The safety objectives for the TOE are derived by considering the goal(s) of the TOE and the means by which these goals are to be obtained.

The overall safety objectives for the TOE are formulated to reduce the possibility of the occurrence of undesired effects to an acceptable level. To determine the list of all

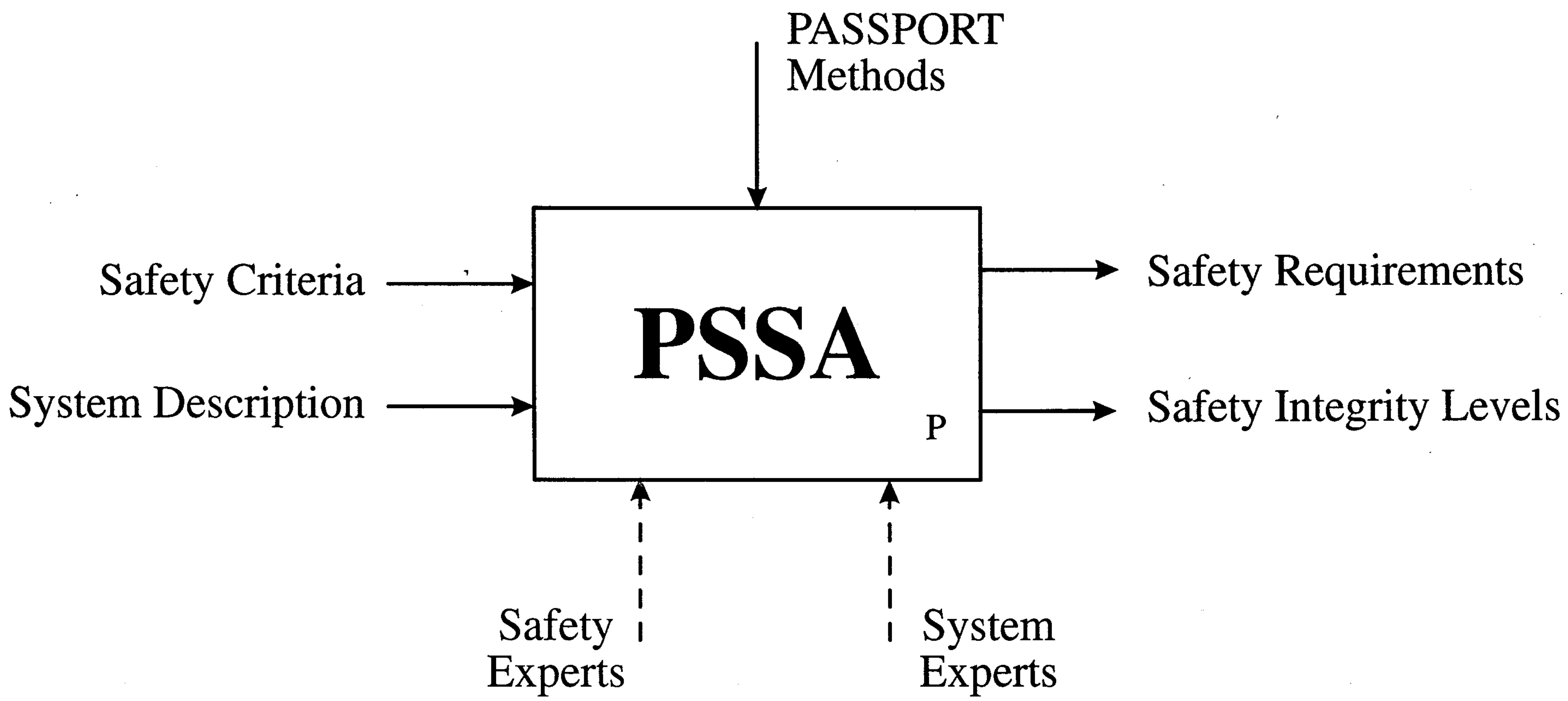


Figure 3.2 - Context of a Prospective System Safety Analysis

the consequences of any failure of the system to perform its specified functions, a hazard analysis is performed. Hazards are identified by considering all the situations which may have undesired effects, with reference to the overall safety criteria.

The safety requirements are derived for the system elements whose failure would have a major impact upon the functionality of the system. The safety requirements which should supplement the list of functional requirements for the system deal with individual hazards, in order to fulfil the safety objectives. The low level safety requirements for the TOE can be defined by identifying the possible events or combinations of events that may lead to a given hazard.

3.2 Safety integrity Levels and Controllability Categories

The degree of care that will be taken to implement each of the safety requirements will depend on the importance of each hazard. The concept of a safety integrity level arises naturally from the fact that some activities are perceived as being more hazardous than others. Their use is desirable because the costs associated with high integrity levels can be very great. A balance must therefore be struck between using too low a level, which will increase risk, and using too high a level, which will result in unnecessary costs.

DRIVE Safely proposed that each hazard should be categorised in terms of the degree of loss of control over the safety of the situation after the failure, which might lead to that hazard, has occurred[DRIVE Safely 1992]. This concept has now been adopted by the UK Motor Industry[MISRA 1994a]. The assessment process considers both the type of control that has been lost, and whether any other control features remain that might help to alleviate the situation in time. Each hazard is placed into one of five controllability classes (uncontrollable, difficult to control, debilitating, distracting and nuisance only). These five controllability categories are then mapped directly onto five safety integrity levels (see also Appendix B).

4. PROSPECTIVE SYSTEM SAFETY ANALYSIS

The flow of information during a PSSA is depicted in Figure 4.1, which is an expansion of Figure 3.2. The activities are initiated with the PSA process (described briefly below, and then in more detail in Section 5) and then followed by the DSA process (described briefly below, and then in more detail in [PASSPORT 1995a]). The methodology for both the PSA and the DSA follows the same basic pattern:

a) Produce a model of the system.

b) Check the model for completeness and consistency.

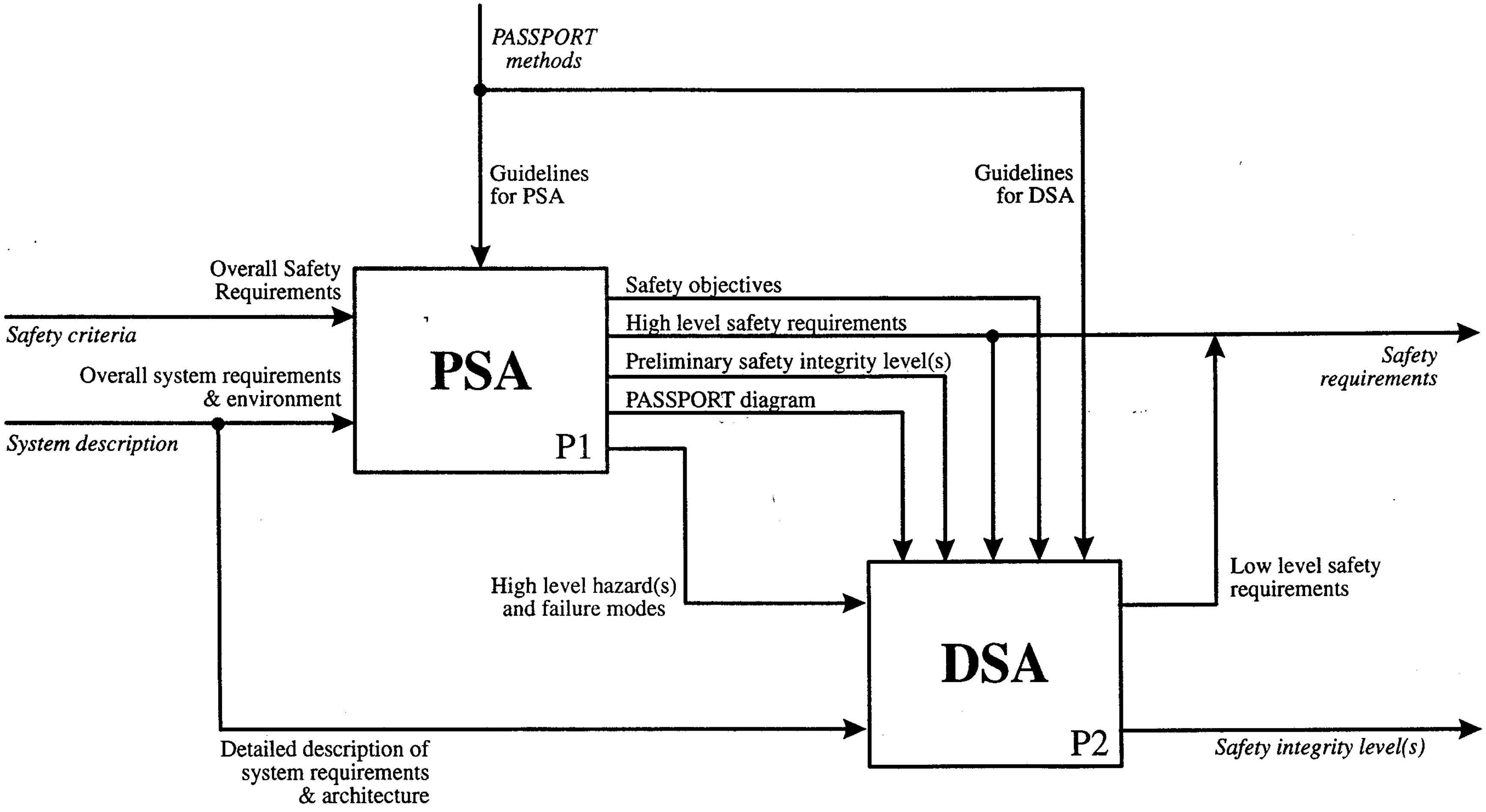

PASSPORT methods
Guidelines for PSA
Guidelines for DSA
Overall Safety Requirements
Safety criteria
Overall system requirements & environment
System description
PSA
P1
Safety objectives
High level safety requirements
Preliminary safety integrity level(s)
PASSPORT diagram
Safety requirements
High level hazard(s) and failure modes
Low level safety requirements
DSA
P2
Detailed description of system requirements & architecture
Safety integrity level(s)

Figure 4.1 - P : Perform a Prospective System Safety Analysis

c) Undertake an hazard analysis.

We must however note the distinction between the less formal PSA process and the very strict DSA process. The PSA process cannot be a formal process because there is usually a lack of detailed information at this stage in the development life-cycle, and it can be a less formal process because everything will be checked again during the DSA process.

4.1 The PSA Process

4.1.1 Purpose of the PSA Process

The primary purpose of the PSA process is to identify whether the TOE has any safety-related aspects associated with it, and if so to identify the high level safety requirements, and the preliminary SILs, associated with them. The PSA process is performed very early in the development life-cycle, and does not require too many details of the proposed design. At this point the environment, boundary, operating goals, overall structure and functionality of the system are known, but the details of its design are still to be determined.

4.1.2 Inputs to the PSA Process

The basic set of inputs to the PSA process should include the following:

- guidelines for performing a PSA,
- the overall safety requirements of the TOE,
- the overall system requirements and the operating environment of the TOE.

4.1.3 The PSA Process

The following are the fundamental activities of a PSA process:

a. A high level system analysis (construction of the PASSPORT diagram).

b. A "what if?" analysis on the PASSPORT diagram to identify the high level hazard(s).

c. A "what causes?" analysis of each of the hazards identified.

d. Conclusions and recommendations.

4.1.4 Output from the PSA Process

The PSA Process should produce the following:

- the overall safety objectives assigned to the TOE,
- a PASSPORT Diagram showing the TOE in relation to its environment,

- the failure modes of system elements, and their relative importance (see also Appendix B),
- the high level hazards associated with the TOE, and their controllability categories,
- the high level safety requirements allocated to the TOE,
- the preliminary SIL(s) necessary for the development of the TOE,

4.2 The DSA Process

4.2.1 Purpose of the DSA Process

The purpose of the DSA process is to analyse in detail the system requirements and the architecture in relation to the safety objectives and the safety requirements identified during the PSA. The DSA is a recursive process, performed in parallel with the system design and ends once there is a sufficient level of confidence that design measures exist to make the system acceptable. The level of confidence required is commensurate with the SIL required of the system and may require liaison with an independent assessor (see [PASSPORT 1995b]).

4.2.2 Input to the DSA Process

The basic set of inputs to the DSA process should include the following:

- guidelines for performing a DSA,
- the overall safety objectives assigned to the TOE,
- a PASSPORT Diagram showing the TOE in relation to its environment,
- the failure modes of system elements, and their relative importance (see also Appendix B),
- the high level hazards associated with the TOE, and their controllability categories.
- the high level safety requirements allocated to the TOE,
- the preliminary SIL(s) necessary for the development of the TOE,
- a detailed description of the system requirements and the architecture of the TOE,

4.2.3 The DSA Process

The following are the fundamental activities of a DSA process:

a. A low level system analysis (construction of the system models and the PASSPORT Cross).

b. A Failure Mode and Effects Analysis (FMEA) to identify the low level hazards.

c. A Fault Tree Analysis (FTA) on each of the low level hazards identified.

d. Conclusions and recommendations.

(a), (b), (c) and (d) are iterated to greater levels of system decomposition until all the safety implications have been fully analysed.

4.2.4 Output from the DSA Process

The DSA process should produce the following:

- the low level safety requirements,
- a confirmation or adaptation of the SIL(s) necessary for the development of the TOE.

5. THE PRELIMINARY SAFETY ANALYSIS PROCESS

The flow of information for the PSA process is shown in Figure 5.1, which is an expansion of box P1 in Figure 4.1. The objectives of the PSA process are:

- establish, for the purpose of the analysis, the overall structure of the TOE and its functionality,
- to establish, for the purpose of the analysis, the boundaries of the TOE, any systems with which it interacts, any human involvement and the application domain,
- establish, for the purpose of the analysis, the characteristics of the interactions and the way that they are transferred,
- identify the hazards of the system,
- identify the potential accidents and mitigating features to the extent practicable at this stage, including any incredible accident sequences that are subsequently discounted,
- identify possible causes (faults) for each failure,
- assign each identified potential hazard with a controllability category (see Appendix B) at this stage, if possible,
- assign to each high level function a SIL, and hence a target failure rate as specified in (see Appendix B) , if possible,
- document any safety features that are to be implemented during the subsequent design and development phases.

The PSA process assumes that the following information is available:

- guidelines for performing a PSA,
- the overall safety requirements of the TOE,

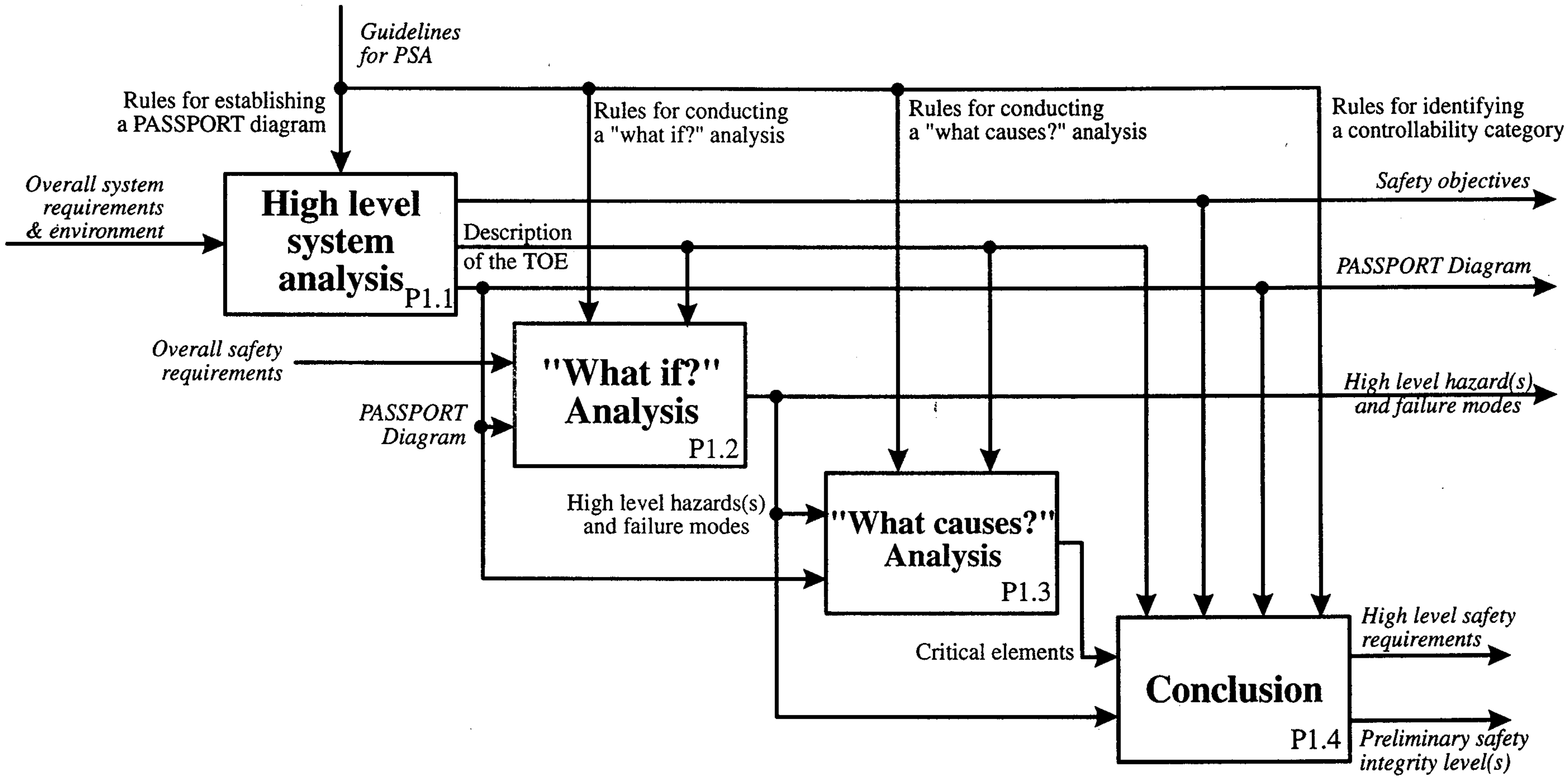

Guidelines for PSA
Rules for establishing a PASSPORT diagram
Rules for conducting a "what if?" analysis
Rules for conducting a "what causes?" analysis
Rules for identifying a controllability category
Overall system requirements & environment
High level system analysis
P1.1
Description of the TOE
Safety objectives
PASSPORT Diagram
Overall safety requirements
PASSPORT Diagram
"What if?" Analysis
P1.2
High level hazard(s) and failure modes
High level hazards(s) and failure modes
"What causes?" Analysis
P1.3
Critical elements
Conclusion
P1.4
High level safety requirements
Preliminary safety integrity level(s)

Figure 5.1 - P1 : The Preliminary Safety Analysis Process

- the overall system requirements and the operating environment of the TOE.

The following are the fundamental activities of a PSA process:

a. A high level system analysis (construction of the PASSPORT diagram).

b. A "what if?" analysis on the PASSPORT diagram to identify the high level hazard(s).

c. A "what causes?" analysis of each of the hazards identified.

d. Conclusions and recommendations.

The outputs of the PSA process are:

- the overall safety objectives assigned to the TOE,
- a PASSPORT Diagram showing the TOE in relation to its environment,
- the failure modes of system elements, and their relative importance (see also Appendix B),
- the high level hazards associated with the TOE, and their controllability categories.
- the high level safety requirements allocated to the TOE,
- the preliminary SIL(s) necessary for the development of the TOE,

5.1 High Level System Analysis

The high level system analysis forms part of the PSA process as depicted in Figure 5.1.

5.1.1 Objectives of the High Level System Analysis

The objective of the high level system analysis is to produce a model that clearly shows the relationship between the proposed system (TOE) and its environment. During this phase, the boundaries of the TOE, its overall structure and functionality, any systems with which it interacts, any human involvement, the characteristics of these interactions and the way that they are transferred are defined (see also Appendix A).

5.1.2 Input to the High Level System Analysis

The basic set of inputs to the high level system analysis should include the following:

- rules for establishing a PASSPORT diagram,
- the overall system requirements and the operating environment of the TOE.

5.1.3 Production and Analysis of the PASSPORT Diagram

The high level system analysis should identify those parts of the system that could violate the overall safety criteria. From this information the safety objectives can be formulated.

The system requirements should be modelled using a PASSPORT Diagram which puts the functionality of the target system into context, and shows the flow of information between the target system and its environment. The basic building blocks of a PASSPORT Diagram Model are the Nucleus of the TOE; a set of terminators which either take input from, or provide output to, the operating environment of the TOE; the information sets that pass between the terminators and the Nucleus of the TOE; and the flow of these information sets. The details of how to create a PASSPORT Diagram Model can be found in Appendix C.

5.1.4 Output from the High Level System Analysis

The high level system analysis should produce the following:

- the safety objectives,
- a PASSPORT Diagram showing the TOE in relation to its environment,
- a description of the TOE.

5.2 Hazard Identification - "What if?" Analysis

The "what if " analysis forms part of the PSA process as depicted in Figure 5.1.

Since the PSA process is performed before many final design decisions have been made and while there is a lack of detailed information, an unbounded "what if?" analysis is performed instead of the formal FMEA. The "what if?" analysis is actually a non-standardised, simplified form of the FMEA since at this stage of the development life-cycle the required detailed knowledge of the failure modes of the system elements at each level is not available and the identification of all possible failure causes associated with each failure mode in order to uncover secondary effects and to devise recommended corrective actions is not possible. A set of guidewords that helps the "what if?" analysis can be found in Appendix D

5.2.1 Objectives of the "What if?" Analysis

The primary objective of the "what if?" analysis is to identify all those elements that are shown in the PASSPORT Diagram model whose failure, in whatever manner, could cause a breach of the safety objectives. This is a Preliminary Hazard Analysis (PHA) which identifies the various possible failure modes of the system, to enable the construction of a preliminary hazard list.

5.2.2 Input to the "What if?" Analysis

The basic set of inputs to the "what if?" analysis should include the following:

- rules for conducting a "what if?" analysis,
- the overall safety requirements of the TOE,
- a PASSPORT Diagram showing the TOE in relation to its environment,
- a description of the TOE.

5.2.3 Establishment of the Failure Modes

A failure mode is defined as the effect by which a failure is observed in a system element (a list of example failure modes are given in Appendix D). Identification of the failure modes may be guided by the following considerations:

- for innovative elements, reference can be made to other elements with similar functionality and structure,
- for commonly used elements already in service, records on their performance, reported failures and/or test can be consulted.

If a system has a protective role, whereby inaction may constitute a hazard, analysis of that system should include the hazards resulting from inaction.

The consequences of each assumed failure mode of a system element on the system function should be determined and reported using worksheet forms as shown in Appendix D

5.2.4 Building up of Preliminary Hazard List

This section provides a brief introduction to the preliminary hazard analysis process and the guidewords it uses in order to construct the preliminary hazard list, a fuller description can be found in Appendix D.

In order to build up the preliminary hazard list for the system, each terminator, information set and the Nucleus of the TOE, as they appear in the PASSPORT Diagram Model, are analysed and the question "what if?" (e.g. what if the information was incorrect; delayed; etc?, or what if the actuator failed to operate; operated with no command; etc?) is asked.

It is desirable for this PHA to be carried out by means of a HAZOP study[CIA] or another systematic method, by a team of people with a variety of expertise (see Appendix A), assisted by guidewords and checklists of potential hazards, to enable the systematic study of the consequences of both intended and unintended functions and malfunctions under all operational conditions. The guidewords that may be used are described in more detail in Appendix D.

In order to avoid masking important hazards with insignificant detail, rules should be developed at this stage to select accident sequences for consideration in this and later analyses. For example, these rules could address the exclusion of rare events (e.g. seismic events) and the exclusion of the effect of multiple (e.g. three or more) independent random component failures occurring concurrently. The cause-effect sequence should be continued until a suitable hazard has been encountered, or there is a belief that no such hazard exists.

The consequences of each assumed failure mode of a sensitive element on the system function should be determined. It is possible that such considerations will produce safety requirements in addition to those produced during the conclusions and recommendations phase. In this case, they should augment this list.

The hazard should be chosen with care; too general and the analysis will become unmanageable; too specific and the analysis does not provide a sufficiently broad view of the system[NUREG-0492 1986].

5.2.5 Output from the "What if?" Analysis

The "what if?" analysis should produce the following:

- a list of failure modes on system elements, and their relative importance (see also Appendix B),
- a list of high level hazards associated with the TOE, and their controllability categories.

5.3 "What causes?" Analysis

The "what causes?" analysis forms part of the PSA process as depicted in Figure 5.1.

Since the PSA process is performed at an early stage of the development life-cycle, a simplified form of the FTA is used, namely the "what causes?" analysis. This informal analysis identifies how each of the hazards in the hazard list might occur, by building up a tree of preliminary events that could lead to an undesirable event. Since at this point, there is a lack of detailed information the tree may be small, may not identify all the causes or combinations of causes that can lead to a specific undesired event, and may include several undeveloped events that need to be further analysed.

5.3.1 Objectives of the "What causes?" Analysis

A "what causes?" analysis should be conducted for each hazard (or undesired event) in the hazard list identified during the "what if?" analysis to discover how the hazard might occur. An analysis of the combinations of possible events that could lead to the given hazard is performed. This will be used, during the conclusions and recommendations phase, to identify the high level safety requirements.

5.3.2 Input to the "What causes?" Analysis

The basic set of inputs to the "what causes?" analysis should include the following:

- rules for conducting a "what causes?" analysis,
- a PASSPORT Diagram showing the TOE in relation to its environment,
- a description of the TOE,
- a list of failure modes on system elements, and their relative importance (see also Appendix B),
- a list of high level hazards associated with the TOE, and their controllability categories.

5.3.3 Creating a Fault Tree

A "what causes?" analysis should be conducted for each hazard, i.e. the high level hazards identified during the "what if?" analysis, in order to determine the combinations of possible events that could lead to the given hazard, and to produce a graphic illustration of these combinations in the form of a fault tree diagram. From an analysis of this diagram it is possible to determine the high level safety requirements.

5.3.4 Output from the "What causes?" Analysis

The "what causes?" analysis should produce the following:

- a list of critical elements that form the leaves of the fault tree.

5.4 Conclusions and Recommendations

The conclusions and recommendations forms part of the PSA process as depicted in Figure 5.1.

Each hazard is assessed according to the process described in Appendix B and a SIL is assigned. The leaves of the fault tree, generated during the "what causes?" analysis, are used as the basis for the construction of the list of high level safety requirements.

5.4.1 Objectives of the Conclusions and Recommendations

The conclusions and recommendations phase should overview the PSA process and identify the high level safety requirements and for each failure assign a preliminary SIL.

5.4.2 Input for the Conclusions and Recommendations

The basic set of inputs to the conclusions and recommendations phase should include the following:

- rules for identifying a controllability category,
- the safety objectives,
- the PASSPORT diagram showing the TOE in relation to its environment,
- a description of the TOE,
- a list of failure modes on system elements, and their relative importance (see also Appendix B),
- a list of high level hazards associated with the TOE, and their controllability categories,
- a list of critical elements that form the leaves of the fault tree.

5.4.3 Identification of the high level safety requirements

The events depicted at the leaves of the fault tree diagram, produced during the "what causes?" analysis, should be discussed in turn. For each, a list of safety requirements should be formulated to prohibit the undesirable event. Also, where relevant, additional safety requirements, identified during the performance of the "what if?" analysis, should be included.

5.4.4 Assignment of Preliminary Safety integrity Level(s)

Each failure mode should be analysed in accordance with Appendix B in order to assign a controllability level to the situation resulting from the failure. These controllability levels should then be discussed to assign an overall SIL to the system.

5.4.5 Output from the Conclusions and Recommendations Activity

The conclusions and recommendations phase should produce the following:

- the high level safety requirements allocated to the TOE,
- the preliminary SIL(s) necessary for the development of the TOE,

Any conclusion and recommendation should be peer reviewed for completeness (see Appendix E). The following intermediate issues should be reported to the project team, using a Configuration Management System (see Appendix E), in order that they might be resolved by the system design process:

- the safety hazards that have been identified,

- the high level safety requirements,
- any additional safety requirements identified during the PSA but not directly associated with the TOE.

5.5 Documentation of the PSA Process

A PSA report should include at least the following sections:

Title Page

Summary

Acknowledgements *

Table of Contents *

List of Abbreviations *

1. Introduction

2. List of Related Documents

3. Procedure used

4. Description of the system concept

5. Identification of the safety objectives

6. Hazard identification - “what if?” analysis

7. Fault identification - “what causes?” analysis

8. Safety requirements

9. Additional safety requirements *

10. Conclusions and recommendations

Appendices *

* - optional

APPENDIX A - HUMAN FACTORS

A.1 Introduction

Whilst this framework is mainly concerned with system safety, accidents seldom occur due to one single factor. The actual combination of factors is often obscure. The success of the development of complex systems is determined by the ability to mobilise and integrate the different areas of expertise involved. This appendix gives a model to facilitate the co-operation between traffic engineers, system engineers, environmental engineers and human factors experts to enhance overall safety.

Currently there are many schools of thought as to how the study of human factors should be approached, and there are often many interpretations that can be put onto a given set of circumstances. This state of affairs can be used to the advantage of those who might be held liable for a failure. Incidents due to the misinterpretation of instruments can lead to allegations of operator error, whilst the instrument ergonomics is also subsequently improved by the manufacturer as a *precaution*. Meanwhile incidents due to traffic layout complexity or driver information overload *may* lead to the use of clearer and simpler messages.

Current design practices for ATT systems involves little co-ordination of the different fields of expertise, whilst case studies of incidents indicate that many of the current problems in safety design involve a combination of these different fields.

In this appendix we highlight the issues surrounding the combination of different areas of expertise. We then propose a methodology to improve the communication between the different fields of expertise. It is not our intention to describe the work to be carried out within each safety area, instead we provide a systematic approach for combining the individual results to optimise the overall safety of ATT systems. Thus we are solely interested in linking the expertise; not in developing the expertise.

A.2 The Entities in the Model

The reduction of human endangerment, injury, and life threatening situations is the main safety goal. Hence, the prime object of interest in accident control and prevention is the human being. Therefore, human involvement should be explicitly described in any safety model.

Figure A.1 is a model of the real world intended to ameliorate the communication between the different areas of expertise. Within this safety model we segregate the different entities which comprise the Target of Evaluation (TOE). The exact boundaries of the TOE should be clearly identified. The model consists of the three entities:

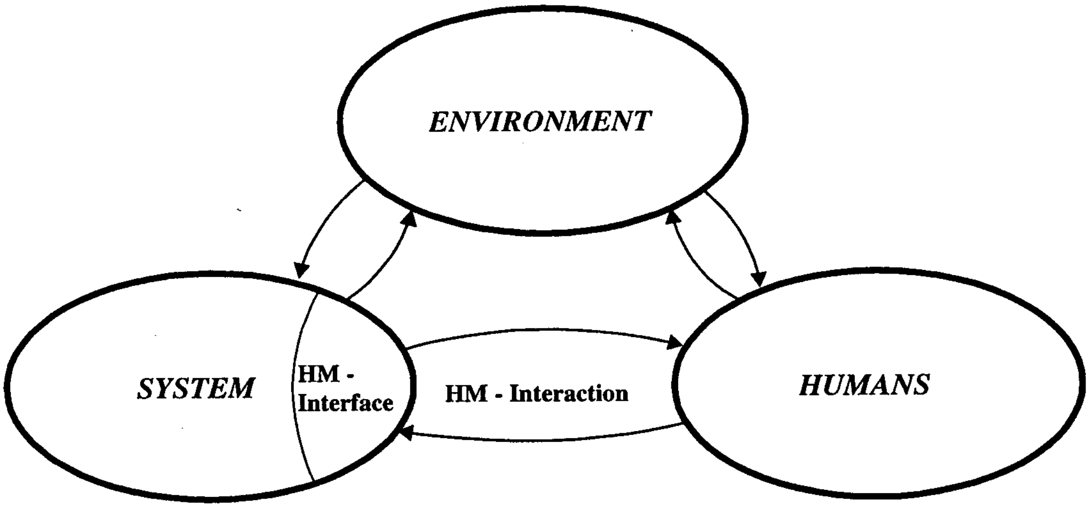


Figure A.1 - A Model for the Binding of Expertise

- *System* - this is the hardware and software which enable the functionality of the TOE. Examples include equipment for vehicles, roads and road and weather monitoring.
- *Humans* - these are all the humans that may be directly, or indirectly, involved in any potential accident involving the TOE. These humans may also be part of the TOE. Examples include road operators, road maintenance personnel, vehicle drivers, passengers and pedestrians.
- *Environment* - this is the set of all inanimate objects external to the TOE. The safeguarding of the environment is an additional safety goal. Objects in the environment include the road infrastructure, road barriers, signs, bridges; together with less obvious items such as the weather and the atmosphere.

A.3 The Interaction Between the Entities

Interactions occur between the three entities system, humans and environment. Some typical interactions that may lead to an accident are given in Table A.1.

The combination of faults which might lead to an accident causing failure are depicted in Figure A.2. There are three causes of human-system interaction error; decision error, where an operator takes the wrong decision; recognition error, where an operator does not recognise the importance of the system information; performance

perceptor actor	System (S)	Humans (H)	Environment (E)
System (S)	Subsystem A disturbs subsystem B, (e.g. a short-circuit blows a common fuse and the rest of system has no power; overloading of a communication channel; etc.).	System gives the wrong warning. Human is hit by the system, or electrocuted	System causes smoke, spills oil, etc.
Humans (H)	Human presses the wrong button.	Passenger distracts a driver. Misunderstanding of site of accident for emergency team.	Vandalism.
Environment (E)	Electrostatic discharge, lightning, weather conditions, etc.	Sunlight disturbs the view of driver.	Bridge Collapse.

Table A.1 - Examples of hazardous interactions between the three safety areas.

error, where an operator is incapable of performing the required task (e.g. due to physical limitations); critical error, where the operator suffers a mental block (e.g. due to information overload).

A.4 The Areas of Expertise

Engineers involved in safety analysis are in general only experts in a specific area. Thus each expert will probably only discover some of the hazards. Furthermore, there might be conflicts between the different safety areas. Negotiations and trade-offs, between the different safety areas, will be required to create an integrated safety solution.

For a balanced assessment of safety all experts must co-operate. In practice such a co-operation can be hard to control and tools for structuring and binding the disciplines can be helpful.

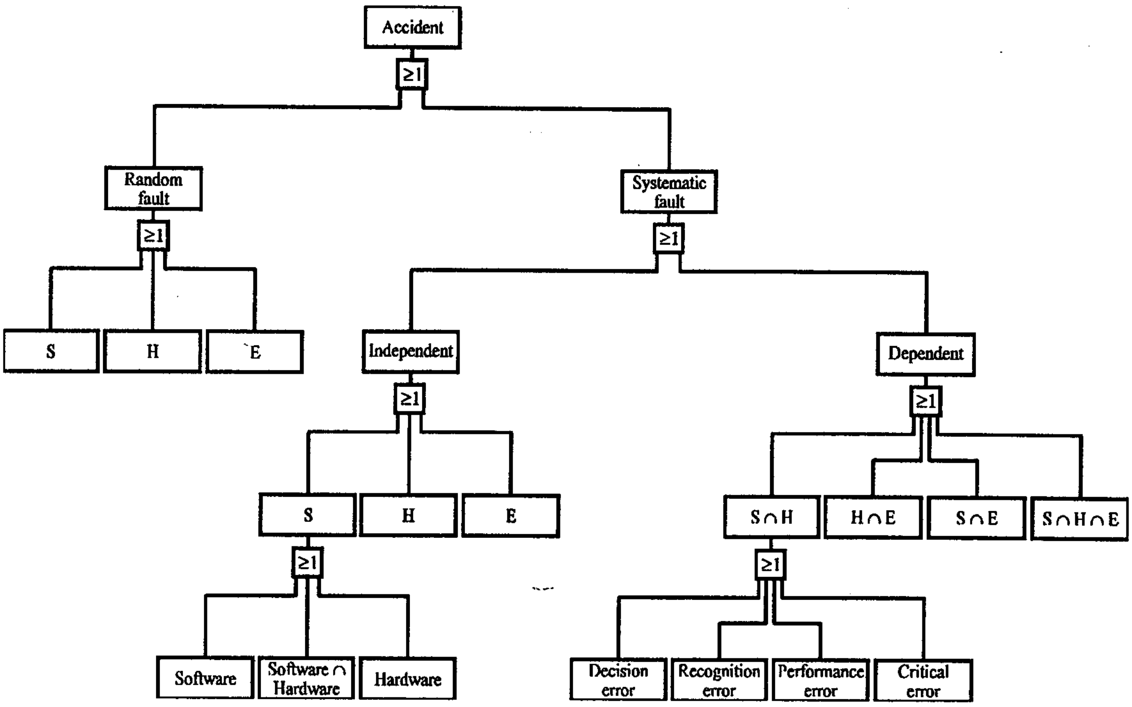


Figure A.2 - Combination of Factors Leading to an Accident

We propose a three stage plan for the co-operation between these three fields of expertise:

- *Team building* - the selection of the team members should be made by the project manager on the basis of expertise, commitment and availability. The project manager should define the project, the TOE, the goals and the resources required.
- *Modelling* - the model developed by the team members should conform to Table A.1 and include the TOE, the human interactions, and the interactions with the environment. The goal of this step is to identify unambiguously:

  a) The boundary of the TOE.

  b) The interactions between the TOE and its operating environment (i.e. the human and environmental interactions).
- *Stepwise assessment* - to produce a safety report it is essential for there to be a meeting between the experts in the individual areas (see Appendix D). In fact, it may be simpler, if the individual safety areas first pool their expertise pairwise and only when any conflicts have been resolved, should the overall safety assessment be produced. This scheme is depicted in Figure A.3, together with an initial stage, whereby preliminary findings of the individual safety experts are fed into the pairwise meetings.

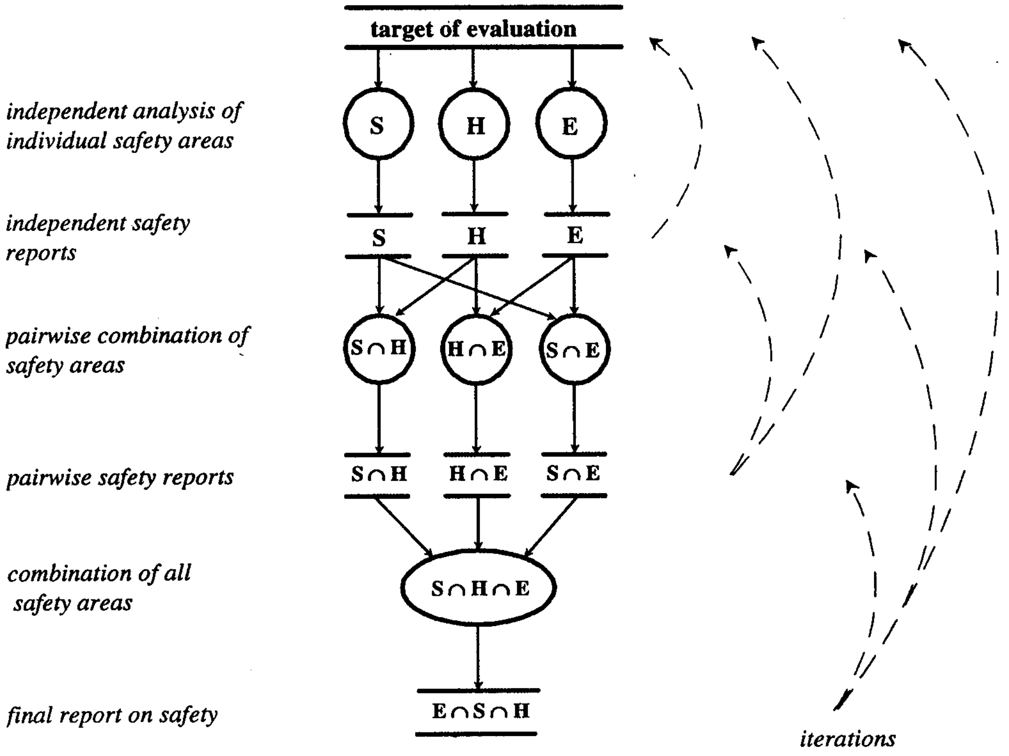

target of evaluation
independent analysis of individual safety areas
S
H
E
independent safety reports
S
H
E
pairwise combination of safety areas
S∩H
H∩E
S∩E
pairwise safety reports
S∩H
H∩E
S∩E
combination of all safety areas
S∩H∩E
final report on safety
E∩S∩H
iterations

Figure A.3 - The Iterative Process for Safety Assessment and Improvement

A.5 Conclusion

A safety modelling approach is proposed for the analysis of potential safety problems in ATT systems, which systematically addresses the interaction of systems, humans and the environment. It is a logical step-wise method for the examination of potentially hazardous ATT systems, which relies upon a creative interaction between experts in the different fields.

While this approach has been successful with regard to the safe operation of some very complex systems, there are still problems in quantifying the influence of the human as an element in an ATT system.

APPENDIX B –
SAFETY INTEGRITY LEVELS AND CONTROLLABILITY CATEGORIES

PLEASE NOTE

As a result of later work on this topic, the following Appendix has been updated in “Guidelines for Safety Analysis of Vehicle Based Programmable Systems”, The Motor Industry Software Reliability Association (MISRA), November 2007 – available from www.misra.org.uk

Appendix B - SAFETY INTEGRITY LEVELS AND CONTROLLABILITY CATEGORIES

B.1 Introduction

The concept of a Safety Integrity Level (SIL) is fundamental to the underlying philosophy of the development of safety-related and safety-critical systems. It arises naturally from the fact that some activities are perceived as being more hazardous that others. Whilst it is true that most physical objects can cause serious injury or even death when mistreated, under normal use the failure of, say, part of a bicycle is likely to have a less serious effect than the failure of, say, part of a nuclear power station. The use of SILs is desirable because the costs associated with the higher integrity levels can be very great. A balance must therefore be struck between using too low a level, which will increase the risk, and using too high a level, which will result in unnecessary costs.

B.2 Hazards, Risks and the Principle of ALARP

A hazard is a physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these. With each hazard can be associated a risk.

Risk is defined as the product of the seriousness of the effect of a failure and the probability of that failure

$$risk = effect \times probability$$

There are three situations (see Figure B.1):

a) The probability is so high or the outcome is so unacceptable that the risk cannot be justified on any grounds.

b) The risk is, or has been made, acceptable or so small as to be insignificant.

c) The risk is between (a) and (b).

Since there is no such thing as zero risk, the law of diminishing returns come into force as greater and greater effort is made to reduce the risk towards zero. Thus once situation (b) has been reached, the risk should be made as small as *necessary*, rather than as small as *possible*.

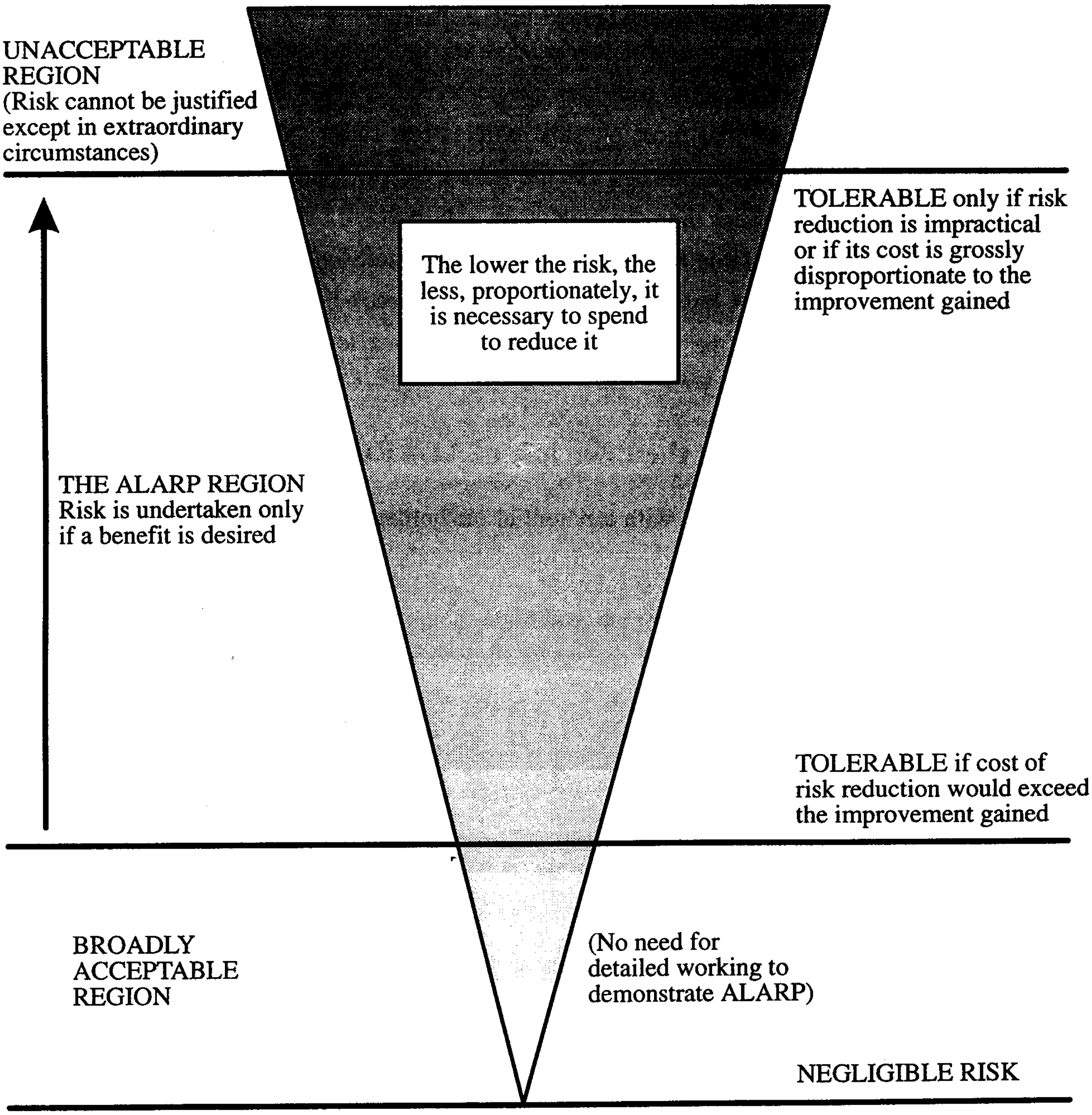

UNACCEPTABLE REGION
(Risk cannot be justified except in extraordinary circumstances)
TOLERABLE only if risk reduction is impractical or if its cost is grossly disproportionate to the improvement gained
The lower the risk, the less, proportionately, it is necessary to spend to reduce it
THE ALARP REGION
Risk is undertaken only if a benefit is desired
TOLERABLE if cost of risk reduction would exceed the improvement gained
BROADLY ACCEPTABLE REGION
(No need for detailed working to demonstrate ALARP)
NEGLIGIBLE RISK

Figure B.1 - Levels of Risk and ALARP

In situation (c) a balance has to be struck between the costs required to reduce the risk and the benefits that will be gained from the functionality of the system. The principle that the risk should be "as low as reasonably practicable" (ALARP) may be used when the function is highly desirable but a risk level that is strictly acceptable, according to the usual criteria, cannot be (reasonably) achieved. (The best examples of the use of the ALARP principle come from the medical industry, which may permit the use of equipment with a relatively high probability of failure when it is the only thing that can help a very sick person.) In general the ALARP principle will be applied in such a way that the higher, or more unacceptable, the risk is, the more, proportionately, those responsible for the risk would be expected to spend to reduce it.

B.3 Safety Integrity Levels for ATT Systems

The current draft of [IEC 1508] attempts to define five levels of safety integrity (including not safety-related) over all industry sectors. However it is important to recognise that its philosophy is based on a number of assumptions which are not always valid, especially for ATT systems.

- There are broadly two types of safety-related system:
  - safety-related protection systems - designed to respond to conditions on the EUC which may be hazardous in themselves or, if no action were taken, could eventually give rise to hazardous events, and to generate correct outputs to mitigate the hazardous consequences, or to prevent the hazardous events.
  - safety-related control systems - designed to carry out active control of the EUC and which has the potential to enter an unsafe state, even if it is not designed to do so.

  The risk model used in [IEC 1508] applies to protection systems, whilst most ATT systems contain safety-related control systems.
- [IEC 1508] assumes that the consequence of a failure is, to a large degree, predictable, i.e. there is a known cause-effect relationship. Whilst this may be true for most static systems, many ATT systems are mobile and their situation, and hence the consequences of failure, vary continuously.

B.3.1 Controllability

In order to resolve the issues described above the DRIVE I project DRIVE Safely developed the concept of "Controllability" [DRIVE Safely 1992]. This takes account of the fact that between a failure (the "cause") and an accident (the "effect") there is a loss of control, and it is this loss of control of the safety of the situation that is categorised. This concept has now also been accepted by the UK motor industry in [MISRA 1994a] and revised slightly in this document. There are five controllability categories defined as follows:

Uncontrollable

This relates to failures whose effects are not controllable by the road user(s), and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.

Difficult to Control

This relates to failures whose effects are not normally controllable by the road user(s) but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to very severe outcomes.

Debilitating

This relates to failures whose effects are usually controllable by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe.

Distracting

This relates to failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.

Nuisance Only

This relates to failures where safety is not normally considered to be affected, and where road user satisfaction is the main consideration.

Examples of how controllability categories can be assigned are given in Section B.3.3.

B.3.2 Integrity Levels

The five controllability categories are related directly to five SILs, i.e. systems associated with failures that result in an uncontrollable hazard must be developed in accordance with an SIL of 4, etc. This is compatible with [IEC 1508] because SIL 0 is not safety-related. Although [IEC 1508] uses numerical target failure measures, it also acknowledges that these can only be applied directly to hardware. Since quantitative techniques and judgements will have to be applied to the software, EMC, etc. factors of an ATT system we therefore prefer not to use numerical target failure measures in our definitions, in order to avoid the possibility of a claim that cannot be substantiated. Thus the definitions of the five SILs are as follows:

Safety Integrity Level 4

A system created to this level of integrity will give confidence to the developer and user that the likelihood of "uncontrollable" failures is extremely improbable.

Safety Integrity Level 3

A system created to this level of integrity will give confidence to the developer and user that the likelihood of a "difficult to control" failure occurring is very remote.

Safety Integrity Level 2

A system created to this level of integrity will give confidence to the developer and user that the likelihood of a "debilitating" failure occurring is remote.

Safety Integrity Level 1

A system created to this level of integrity will give confidence to the developer and user that the likelihood of a "distracting" failure occurring is unlikely.

Safety Integrity Level 0

A system created to this level of integrity will give confidence to the developer and user that the likelihood of a "nuisance only" failure occurring is no worse than reasonably possible.

This process is summarised in Figure B.2.

The "Controllability" technique for identifying SILs is being offered for consideration as an addition to the Standard as part of the official commenting process for [IEC 1508].

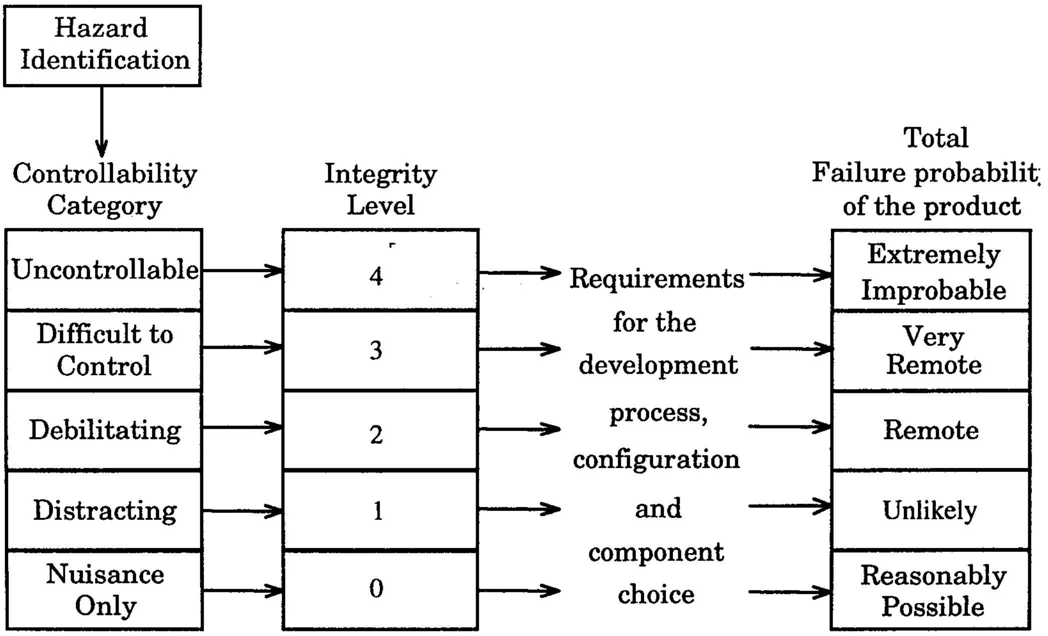


Figure B.2 - Controllability and Integrity Levels

B.3.3 Assigning Controllability Levels

Figure B.3 attempts to illustrate the relationship between ATT hazards and controllability. The complexity of the mapping between hazards, severity factors and other considerations in the determination of a controllability category is clear from the diagram. This section gives two examples of the application of the techniques discussed above.

Each hazard is assessed for the degree of safety of the situation that remains after a failure has occurred, and this "controllability" category defines the safety integrity level required. A systematic argument for finding the integrity level may proceed as follows.

Note: Each of the four sub-headings under "Influencing Factors" has three entries. A qualitative judgement is made for each sub-heading to produce a grade from A-E on the basis that the top entry should have a grade of A, the middle entry a grade of about C, and the bottom entry E.

Initially a judgement is made as to how important to the safety of the situation is the system or the function before the failure.

1. The list of "Ranked Severity Factors" in Figure 3 provides an initial estimate for the Controllability Category. The five grades are allocated as follows:

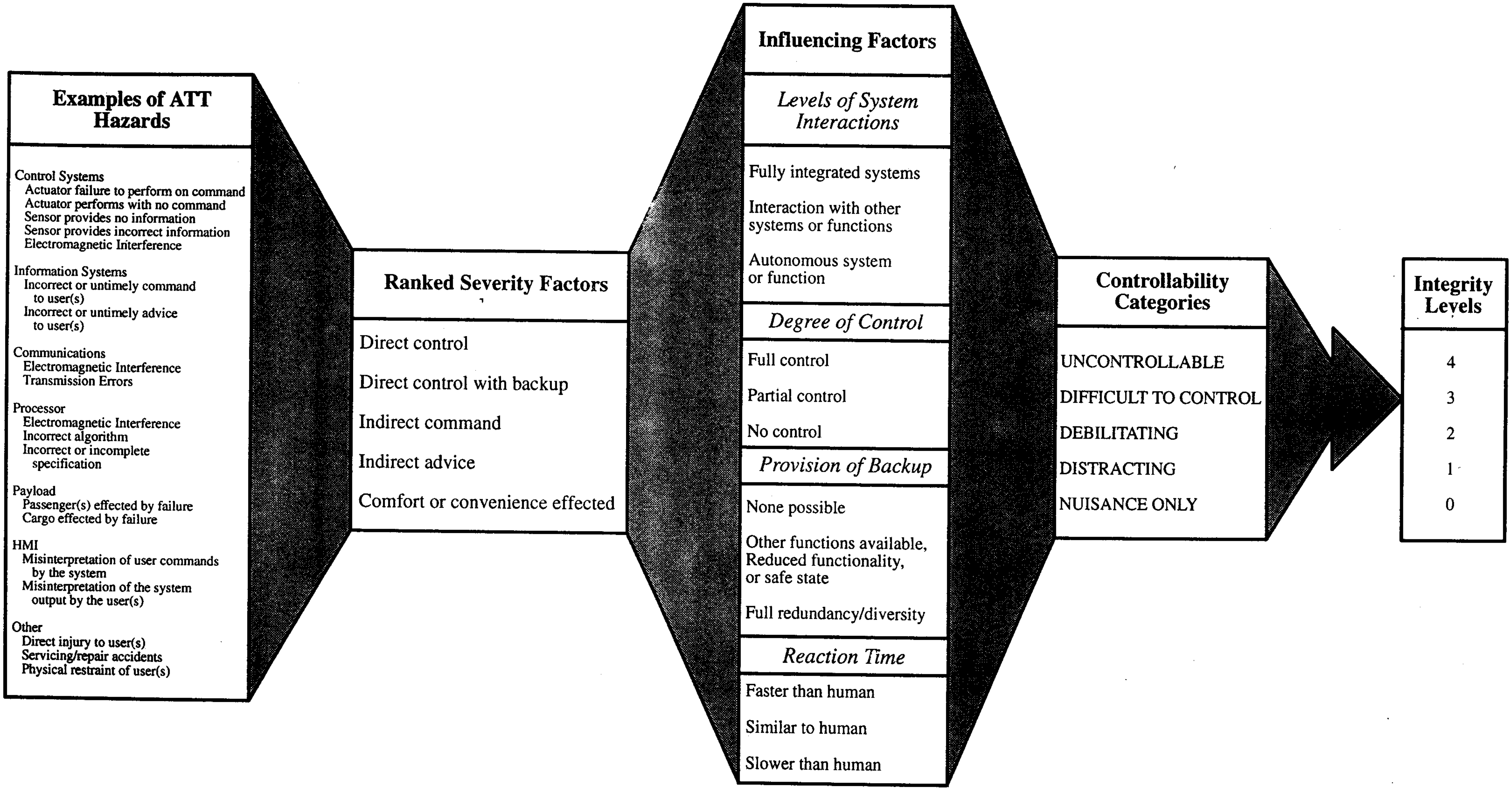
   A. Direct control
   B. Direct control with backup
   C. Indirect command
   D. Indirect advice
   E. Comfort or convenience effected

   This grade may need to be modified by those factors which influence the specific system under investigation.

2. The "Levels of System Interactions" (the degree to which other systems that may be relying on the correct functioning of this system) is considered and a grade allocated as follows:

   A. Fully integrated systems
   B.
   C. Interaction with other systems
   D.
   E. Autonomous system or function

   (If the grade is E then this factor should be ignored because it will not be relevant.)



Examples of ATT Hazards

Control Systems
- Actuator failure to perform on command
- Actuator performs with no command
- Sensor provides no information
- Sensor provides incorrect information
- Electromagnetic Interference

Information Systems
- Incorrect or untimely command to user(s)
- Incorrect or untimely advice to user(s)

Communications
- Electromagnetic Interference
- Transmission Errors

Processor
- Electromagnetic Interference
- Incorrect algorithm
- Incorrect or incomplete specification

Payload
- Passenger(s) effected by failure
- Cargo effected by failure

HMI
- Misinterpretation of user commands by the system
- Misinterpretation of the system output by the user(s)

Other
- Direct injury to user(s)
- Servicing/repair accidents
- Physical restraint of user(s)

Ranked Severity Factors

Direct control

Direct control with backup

Indirect command

Indirect advice

Comfort or convenience effected

Influencing Factors

Levels of System Interactions

Fully integrated systems

Interaction with other systems or functions

Autonomous system or function

Degree of Control

Full control

Partial control

No control

Provision of Backup

None possible

Other functions available, Reduced functionality, or safe state

Full redundancy/diversity

Reaction Time

Faster than human

Similar to human

Slower than human

Controllability Categories

UNCONTROLLABLE

DIFFICULT TO CONTROL

DEBILITATING

DISTRACTING

NUISANCE ONLY

Integrity Levels

4

3

2

1

0

Figure B.3 - Guide to Assigning Integrity Levels

3. The "Degree of Control" to the safety of the situation contributed by this system is considered and a grade allocated as follows:

   A. Full control
   B.
   C. Partial control
   D.
   E. No control

The situation after a failure has occurred is then considered, and a judgement is made as to whether there is anything that can be done in a useful manner to control the safety of the situation.

4. The "Provision of Backup" available after the failure refers to *other* functions that may be used to control the safety of the situation. Note that "Full redundancy/diversity" refers to other systems which can provide the same function but by other means, it does *not* refer to a multi-channel implementation of the function that has failed (that is a design issue and will be one way of achieving the integrity level identified). A grade is allocated as follows:

   A. None possible
   B.
   C. Other functions available, reduced functionality or safe state
   D.
   E. Full redundancy/diversity

5. The "Reaction Time" needed by the road user to apply the backup function(s) is considered, and a grade allocated as follows:

   A. Faster then human
   B.
   C. Similar to human
   D.
   E. Slower than human

Once the five grades have been obtained (or four grades, if "Levels of System Interaction" is E) then the final grade is considered. Starting with the grade for the "Ranked Severity Factor", the other grades will show whether this is actually too high or too low. Whilst a single low value (towards E) might be ignored, it is unwise to ignore a single high value. (*Note*: an average should not be taken since the grades do not have the same dimensions).

Once a final grade has been chosen the full description for the corresponding Controllability Category (E - Nuisance Only: A - Uncontrollable) should be studied to confirm that it does indeed reflect the controllability of the safety of the situation after a failure.

It should be noted that, when all the grades are considered at the end of the process in order to allocate the final controllability category, a balance must be struck between using too low a level, which will increase the risk, and using too high a level, which will result in unnecessary costs.

The following examples show that determination of a controllability category is feasible, although it is a largely subjective process.

B.3.3.1 Total Failure of an Engine Management System

The first scenario to be investigated is the "Total Failure of an Engine Management System". The assumption here is that all other features of the vehicle are not affected significantly in the short term. In particular it is possible to disengage the gears, and the driver is able to operate the brakes and steering as required until the vehicle comes to rest.

- Ranked Severity Factors - The engine management system provides direct control of the vehicle backed up by a number of other functions, a grade of B.
- Levels of System Interactions - The engine management system is Autonomous; a grade of E, which will be ignored from now on.
- Degree of Control - An engine has considerable control over the movement of a vehicle, although this control is managed by the driver; the degree of control is therefore Partial, a grade of C.

Since a total failure of the engine management system will remove the facility for forward acceleration, a primary function of the vehicle, we can expect a medium to high loss of control, though the final value of the controllability category will depend on the next two factors.

- Provision of Backup - Although forward acceleration is lost, the driver will still be able to decelerate with the brakes, and have full lateral control with the steering; the provision of backup is therefore with Reduced Functionality, a grade between C and D.

This would seem to indicate that the driver should be able to avoid an accident under favourable circumstances provided this is supported by the fifth factor.

- Reaction Time - Whilst the driver will have to react immediately to a total failure of the engine management system, this should be within his or her normal capability. The reaction time is thus Similar to that of the driver, a grade of C.

The above argument would seem to indicate that a grade of C would be appropriate. This would give a controllability category of *debilitating* (failures whose effects are usually controllable by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe) for a total failure of the engine management system.

B.3.3.2 Automatic Incident Detection

The second function that will be analysed is Automatic Incident Detection (AID). This is the function that will instruct upstream traffic via Variable Message Signs (VMS) what to do when an incident is detected on the road ahead.

- Ranked Severity Factors - The VMS will provide an Indirect Command, a grade of C.
- Levels of System Interactions - AID does effect other systems (i.e. the VMS signs that give the warning to other drivers, and the other drivers themselves); a grade of D.
- Degree of Control - This function will only have little control over the safety of the situation; a grade of D.
- Provision of Backup - A normal alert driver will have full control over the safety of the situation; a grade of E.
- Reaction Time - A normal alert driver will have sufficient time to react to the situation in the event of a failure of the AID function; a grade of E.

Automatic Incident Detection thus has a grade that lies between E and D. Given that drivers are expected to drive in preparation for the unexpected (i.e. with suitable gaps between vehicles), a controllability category of *distracting* (failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor) would seems to be adequate.

Appendix C - THE PASSPORT DIAGRAM MODEL

C.1 Introduction

Before a system safety analysis can be performed properly it is necessary to define the Target Of Evaluation (TOE). This is to enable the analysis to discover:

- hidden assumptions about the functionality and the characteristics of the TOE,
- differences between the interpretation of the goal(s) of the TOE and the intended implementation,
- any incorrect or misleading view of the system's environment that could lead to incorrect hazard identification,
- any incorrect, misleading or missing set(s) of interactions between the system and its environment, causing faults in the safety analysis of the system,
- any omission in the possible interactions with the environment, which could lead to omissions in the safety analysis of the system.

It is therefore necessary that, before the analysis is started, it must be clear as to what constitutes the system to be analysed.

Special emphasis must be placed upon the completeness and consistency of the description of the TOE; any detail that is omitted in the description may lead to an incorrect safety analysis, and consequently to hidden dangers in the final system. For this purpose the PASSPORT system description method has been designed as a basis for system safety analysis; the most important part of this method, and also the most demanding part, is the creation of the PASSPORT Diagram model. The PASSPORT Diagram model has been developed to enable completeness criteria to be checked as far as possible; this is an enhancement on other system description methods available, most of which avoid the completeness issue altogether.

Moreover, the PASSPORT Diagram model together with the expanded descriptions of its contents are the basis for structured system safety analysis techniques such as "What if?" Analysis, hazard identification, "What causes?" Analysis and the derivation of safety objectives and requirements. "What if?" and "What causes?" analyses are the informal counterparts to Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) respectively. Use of the PASSPORT Diagram model during these analyses also helps to focus attention on the safety analysis rather than on how the system is intended to function. Its use should therefore enhance the quality of the analysis.

C.2 Diagram Construction

The PASSPORT Diagram model is designed to make its interpretation easy; the rules for diagram construction make it simple to begin, and are helpful in performing the remainder of the steps that have to be taken to produce a correct diagram. Peer review is made easy, because the structure of the diagram is always the same; only the characteristics of the TOE change.

C.2.1 Building Blocks of a PASSPORT Diagram model

The following are the basic building blocks of a PASSPORT Diagram model:

- Nucleus of the TOE: This is the nucleus of the system under consideration,
- Terminator : This is an element of the TOE that either takes input from, or provides output to, the operating environment of the TOE. Where relevant the terminator should provide details of the element within the operating environment with which it interacts,
- Information set : An item or set of data,
- Data flow : The movement of data to or from the nucleus of the TOE. This describes the medium for the internal transfer, if this is known.

These have the symbols shown in Figure C.1.

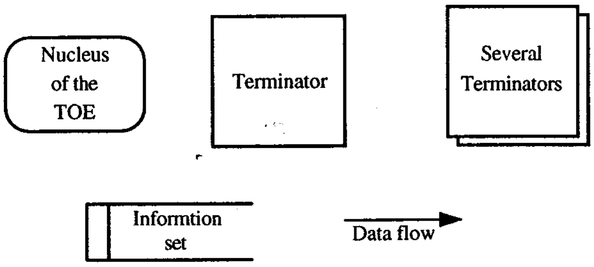


Figure C.1 - Basic PASSPORT Diagram Model Symbols

C.2.2 Construction of a PASSPORT Diagram model

The PASSPORT Diagram model for any system, irrespective of size, should normally fit on an A4-size sheet of paper, with 20 to 30 symbols in total. The level of detail given in the diagram may need to be modified in order to achieve this aim. For very large systems, it may be necessary to perform a number of PSAs for various sub-systems. A typical generic diagram is shown in Figure C.2.

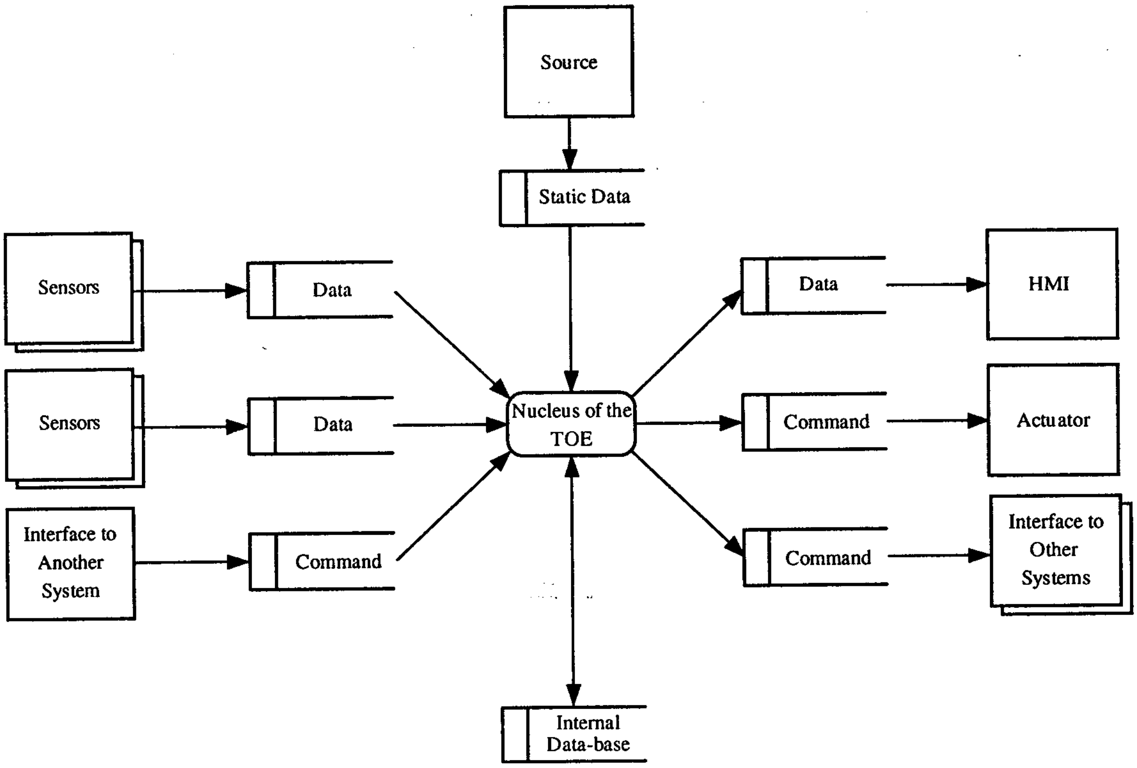


Figure C.2 - Generic PASSPORT Diagram Model

The construction of the diagram follows a sequence of steps.

1. Identify the boundaries of the TOE, in order to determine what is inside the TOE and what is in the immediate environment. Usually the boundary is obvious, ,but on occasions some arbitrary decisions may have to be taken. Once a boundary has been chosen it is essential to maintain that boundary for the remainder of the PSA.
2. Place the nucleus of the TOE in the centre of the page.
3. Identify the goal (the functional objectives) of the system, such as the desired output of the system and those part of the system's environment that is served by these outputs. These system components, which are at the boundary of the TOE, are placed at the right of the diagram.
4. Identify all the dynamic inputs that are required for the TOE to perform its functions and those parts of the immediate environment from which these inputs emanate. These system components, which are at the boundary of the TOE, are placed at the left of the diagram.
5. Identify all the "static" (over a reasonable length of time) inputs that are required for the TOE to perform its functions. (Normally this type of input is neglected in other description methods, because in most cases they are considered to be very obvious. However, their omission can create loopholes in the safety analysis of the

system e.g. initialisation or set-up data, computational parameters. Normally static input will be associated with a system terminator which is responsible for the proper delivery or implementation of the system e.g. manufacturer, system administrator.) These are placed at the top of the diagram.

6. Identify the internal dynamic interactions of the system, i.e. the memory functions e.g. data-bases. These are placed at the bottom of the diagram.

C.2.3 Consistency and Completeness Checks

After the diagram has been constructed checks for its consistency and completeness have to be applied.

Consistency checks are needed for the correct identification and interpretation of the terminators and their associated interactions. These include:

- confirmation that the terminators at the right hand side follow from the functionality of the TOE,
- confirmation that the terminators at the left hand side are necessary to enable the functionality of the TOE,
- confirmation that the terminators at the top are necessary for operational support,
- check the interactions for compliance with the TOE's functionality and the characteristics of the environment.

The (self-)consistency of the PASSPORT Diagram model is centred on the question "What goes in must come out, and what comes out must have gone in". The latter check requires that each output is discussed in turn with all the inputs, and it is confirmed that it is capable of being derived from the static and dynamic inputs in a reasonable way. Failure to pass this consistency check is an indication of a missing input or an incorrect interpretation. Consistency also requires that all the static and dynamic inputs contribute to the functional outputs, any input that is not necessary for any of the outputs should be removed.

The ultimate characteristic of the PASSPORT Diagram model is that it should be complete. Completeness checks are made against the system requirements and thus relies upon an effective requirements capture process. The completeness check is not a mathematical check, rather it must be suited to the level of abstraction used in the diagram.

Appendix D - PRELIMINARY HAZARD ANALYSIS OF ATT SYSTEMS

D.1 Introduction

The objective of a preliminary hazard analysis is to identify the various possible failure modes of a new ATT system so that the safety requirements and the integrity level(s) necessary to assure the safety of that system can be identified. New safety problems can often arise in connection with new technical solutions, which can be caused by interactions with, or within, the equipment that had not been intended or predicted. Whilst some safety hazards are obvious, others may be hidden within the complexity of the system, or of the way that the system interacts with its users, or the environment. This appendix describes a process for performing a systematic hazard analysis based on the hazards and operability studies (HAZOPS) method used in the chemical industry [Henley 1992].

D.2 Hazard Analysis - The Process

The performance of a preliminary hazard analysis of a PASSPORT Diagram should be undertaken by a small team of people with a variety of expertise (e.g. communications, electronic engineering, software engineering, traffic engineering, human factors, environment). The team uses a series of guidewords to stimulate creative thinking about what would happen if the (sub-)system were to deviate from the intended mode of operation in any way. A Hazard Analyst should be appointed, possibly from within the existing team, to lead the analysis. A Secretary must also be appointed to record each hazard as it is identified and the corresponding controllability category assigned to each failure mode. Appendix A describes a systematic approach to handle the interactions between the system hardware/software, the people associated with the system, and the environment.

Each element in the PASSPORT Diagram should be considered in turn and the various possible failure modes discovered. Some failure modes will be so obvious that the Secretary may forget to record them (this must of course not happen!), whilst others will only be discovered after some considerable discussion. In order to assist the latter situation the following set of guidewords have been produced in order that the discussion can concentrate upon all possible operating modes in turn.

It is suggested that the hazard analysis should proceed as follows:

1. The type of the system being studied should be identified (see Section D.3.1).

2. The hazards should then be identified (see Section D.3.2) for all operating conditions (see Section D.3.3).
3. The assignment of controllability categories (see Appendix B) can be performed with the assistance of Section D.3.4.
4. Section D.3.5 can be used to check that the relevant standards and guidelines necessary for the development of the system have been identified.

D.3 "What If?" - Guidewords

D.3.1 System Identification

The following items must be defined before the start of any safety analysis (see also Appendix C).

The boundaries of the system
The interfaces to the system
The environment of the system

D.3.1.1 Primary System Function [CORD 1994]

Road Management and Logistics
Demand Management
Traffic Management
Parking Management
Public Transport Management
Traffic Information
Travel Information
Freight and Fleet Management
Vehicle Control
Internal Services

D.3.1.2 Humans within the System or the Environment

System operators
Trained drivers (e.g. public transport, freight)
Non-professional drivers
Pedestrians
Shopping area
Business area
Industrial site
Agricultural area
Habitation
Recreation area

D.3.1.3 Main Safety Objective

Vehicle control

Traffic flow control

Pedestrian flow control

Pollution control

D.3.1.4 Main Safety Area

Functional system safety

Traffic safety

HMI safety

Environmental safety

D.3.1.5 Safety Impact

Direct control (e.g. Steer by wire)

Direct control with backup (e.g. ABS)

Indirect active safety (e.g. VMS)

- Safety command
- Safety warning
- Safety advice

Passive safety (e.g. vehicle side-bars)

Comfort or convenience effected

D.3.1.6 Safe States

Has the system a safe state?

Can the safe state be reached from all other states?

D.3.2 Hazard Identification

D.3.2.1 General

Loss of function

Function fails on demand

Incorrect command/advice

Absence of command/advice

Delayed command/advice

Road user misunderstands the system

- Does the function require any special training?

Road user has an incorrect mental model of the way that the system works

Road user distracted by the new system (e.g. a new "toy")

Too many commands/too much advice

- Always
- At a critical time

Command/advice not relevant

De-skilling - is it likely that the road user may forget how to behave without the system being available?

Risk compensation - is it likely that the behaviour of the road user might be more risky with the function available than without it?

D.3.2.2 Direct Control - In-vehicle

Loss of function (e.g. steering, acceleration)

Function fails on demand (e.g. brakes)

Jamming of function (e.g. brakes, steering)

Incorrect function (e.g. brakes, steering)

Unintentional function (e.g. brakes, acceleration, unjustified inflation of airbag)

D.3.2.3 Indirect Control - Traffic Control

Traffic lights on simultaneous green

"Ghost" vehicle on dual-carriageway (i.e. vehicle travelling against the flow of traffic)

D.3.2.4 Co-operative systems

Failure of the other system (see Sections D.3.2 and D.3.3)

D.3.3 States of Operation

D.3.3.1 Operational Phases

Commissioning

Running in parallel with system to be replaced

Not operational

Off line

Standby

Start up

Operational

Steady state

Shut down

Abnormal conditions

Maintenance

Periodic inspection

D.3.3.2 Weather Conditions

Day/dusk/night/dawn

Dry/drizzle/heavy rain

Standing water

- Shallow/deep

Mud/dirt on road

Mist/fog/smog

Slush/snow

Ice/black ice

Very hot

Very cold

- Freezing fog

Head/tail/side wind

Dust/sand

Combinations of the above

D.3.3.3 Operational Manoeuvres - Vehicle

Cornering right/left

Braking

Acceleration

Cruising

Speeding

Reversing

Parking

Turning right/left

- At a road junction
- From a gateway/driveway

Cross-roads - straight on

Roundabout

U-turn

Lane changing

Over/under taking

Queuing

Joining dual-carriageway/motorway

Leaving dual-carriageway/motorway

"Following"

D.3.3.4 Operational Manoeuvres - Pedestrian

On the pavement

Crossing the road

- At an authorised crossing point
- Not at an authorised crossing point

Changing mode of travel

D.3.3.5 Human Factors (see also [HOPES 1993a, HOPES 1993b])

Tired

Asleep

Alcohol

Prescribed drugs

Proscribed drugs

Inattentiveness

Lack of training

Inexperience

Slow reaction (e.g. elderly)

Partial sight

Colour blindness

Blind

Hearing deficiency

Deaf

Speech impediment

Dumb

Physical Disability

Wheelchair bound

D.3.4 Backup in Case of Failure

D.3.4.1 Provision of Backup

Is there full redundancy/diversity?

Are other relevant control functions available in all conditions (see Section D.3.3)?

Is there a safe state/fail operational/fail soft/limp home in all conditions (see Section D.3.3)?

Transfer to safe state/fail operational/fail soft/limp home

- Automatic
- Semi-automatic
- Manual
- Failure of transfer mechanism

D.3.4.2 Reaction Time

Is a warning given?

- At the correct time
  - Immediately when the failure is detected
  - Periodically during operation
  - Automatically after a re-start
  - During maintenance/periodic inspection

    - In time to react properly (see also de-skilling)
    - Information overload
        - Always
        - At a critical time
- Is the warning clear?
    - Type of warning (e.g. critical/non-critical)
- Is safety compromised if a failure is not detected in time?
- Will the warning be ignored after too many false alarms?
    - Failure of the warning system

D.3.5 Standards and Guidelines

- Safety regulations
- Safety standards (recommended life-cycle)
- Security
- Quality Assurance
- Environment
    - EMC
    - Pollution control
- Type Approval
- Certification

PASSPORT “What if?” Analysis Worksheet

System ____________ Design by ____________ Date ________

Reference Diagram ____________ Analysed by ____________ Page ________

Element name	Function	Ident N°	Failure mode	Failure cause*	Immediate failure effect	Ultimate failure effect	Justification of failure effects	Provision of Backup	Remarks

Figure D.1- “What if?” Analysis Worksheet

* to be confirmed by the “what causes?” analysis

Appendix E - QUALITY MANAGEMENT SYSTEM

E.1 Introduction

In the final document of the DRIVE project "DRIVE Safely" entitled "Towards a European standard : The development of safe road transport informatic system" it is stated in the Preface Section 2.3. on principles for system development

> For project control and assessment, an ISO 9000 or similar quality system is a minimum requirement.

As far as software development is concerned, this standard states that:

> for non safety-related software, it is highly recommended that such software shall be developed using modern software engineering techniques and tools under a management system that conforms to ISO 9000,
>
> safety critical software should be developed under a management system that conforms to ISO 9004.

This proposal mentions:

- a quality system
- the ISO 9000 standard
- the ISO 9004 standard

What is a quality system, what are the ISO 9000 and ISO 9004 standards and what is a quality system which conforms to ISO 9000?

The purpose of these notes is to present the way for a company to organise itself such that the technical, administrative and human factors affecting the quality of its products and services will be under control.

E.2 Definitions

E.2.1 Quality

ISO 8402 defines Quality as "the totality of features and characteristics of a product or a service that bear on its ability to satisfy stated or implied needs".

In a contractual environment, needs are specified, whereas in other environments, implied needs should be identified or defined.

E.2.2 Quality System

A quality system is the organisational structure, responsibilities, procedures, processes and resources for implementing quality management.

E.2.3 Quality Management

Quality management is that aspect of the overall management function which determines and implements the quality policy.

The management of a company should develop and state its corporate quality policy. The responsibility for and commitment to a quality policy belongs to the highest level of management. This policy should be consistent with other company policies.

Management should take all necessary measures to ensure that its corporate quality policy is understood, implemented and maintained.

E.2.4 Quality Management System

A quality management system is developed and implemented for the purpose of accomplishing the objectives set out in a company's quality policies.

E.3 EN 29000 Standards

The International Standards ISO 9000 were prepared by Technical Committee ISO/TC 176, Quality Assurance. This standard was approved according to ISO procedures.

These Standards were adopted by the European standardisation body CEN under the identification EN 29000. In addition these standards are also called BS 5750 in the UK, and X-50-121 and 122, X-50-131, 132 and 133 in France.

When we mention ISO 9000/EN 29000 we are in fact referring to the ISO 9000/EN 29000 series. This series comprises: (non-exhaustive list)

- ISO 9000-1/EN 29000: Quality management and quality assurance standards. Guidelines for selection and use.
- ISO 9001/EN 29001 Quality systems - Model for quality assurance in design/development, production, installation and servicing (see Figure E.1).
- ISO 9002/EN 29002: Quality systems - Model for quality assurance in production and installation and servicing.
- ISO 9003/EN 29003: Quality systems - Model for quality assurance in final inspection and test.
- ISO 9004-1/EN 29004: Quality management and quality system elements - Guidelines.

EN 29001 : Quality system - Model for quality assurance in design, development, production, installation and servicing

0 Introduction
1 Scope
2 Normative References
3 Definitions

4 Quality system requirements

- 4.1 Management responsibility
- 4.2 Quality system
- 4.3 Contract review
- 4.4 Design control
- 4.5 Document and data control
- 4.6 Purchasing
- 4.7 Control of customer supplied product
- 4.8 Product identification and traceability
- 4.9 Process control
- 4.10 Inspection and testing
- 4.11 Control of inspection, measuring and test equipment
- 4.12 Inspection and test status
- 4.13 Control of non-conforming product
- 4.14 Corrective and preventive action
- 4.15 Handling, storage, packaging preservation and delivery
- 4.16 Control of quality records
- 4.17 Internal quality audits
- 4.18 Training
- 4.19 Servicing
- 4.20 Statistical records

Figure E.1

- ISO 9000-2: Quality management and quality assurance standards - Guide for the application of ISO 9001, ISO 9002, ISO 9003.
- ISO 9000-3: Quality management and quality assurance standards - Guidelines for the application of ISO 9001 to the development, supply and maintenance of software (see Figure E.2).
- ISO 9004-2: Quality management and quality systems elements - Guidelines for service.
- ISO 9004-3: Quality management and quality system elements - Guidelines for processed material.
- ISO 9004-5: Quality management and quality system elements - Guidelines for quality assurance plan.
- ISO 10011-1: Guidelines for auditing systems - Part 1: Auditing.

ISO 9000-3 : Guidelines for the application of ISO 9001 to the development, supply and maintenance of software

- 0 Introduction
- 1 Scope
- 2 Normative references
- 3 Definitions
- 4 Quality system - Framework
    - 4.1 Management responsibility
    - 4.2 Quality system
    - 4.3 Internal quality system audits
    - 4.4 Corrective action
- 5 Quality system - Life-cycle activities
    - 5.1 Contract review
    - 5.2 Purchaser requirement specification
    - 5.3 Development planning
    - 5.4 Quality planning
    - 5.5 Design and implementation
    - 5.6 Testing and validation
    - 5.7 Acceptance
    - 5.8 Maintenance
- 6 Quality system - Supporting activities
    - 6.1 Configuration management
    - 6.2 Document control
    - 6.3 Quality records
    - 6.4 Measurement
    - 6.5 Rules, practices and convention
    - 6.6 Tools and techniques
    - 6.7 Purchasing
    - 6.8 Included software product
    - 6.9 Training

Figure E.2

- ISO 10011-2: Guidelines for auditing quality systems - Part 2: Qualification criteria for quality systems auditors.
- ISO 10011-3: Guidelines for auditing quality systems - Part 3: Management of audit programmes.

This list could be increased by a reference document used by UK assessors for auditing software houses:

- TickIT: Guide to software quality management system construction and certification using EN 29001 (see Figure E.3).

TickIT : Guide to software quality management system construction and certification using EN 29001

Part 1 : Introduction

Part 2 : Application of ISO 9001 to software : ISO 9000-3

Part 3 : Purchasers' guide :

An explanation of the purchasers' expectations of a suppliers quality management system assessed and certified to ISO 9001.

Part 4 : Suppliers' guide :

Guidance to suppliers and in-house developers implementing quality management systems for compliance to ISO 9001.

Part 5 : Auditors Guide :

Guidance to auditors of suppliers seeking certification of their quality management system to ISO 9001.

Figure E.3

E.4 Quality Management System

A quality management system has two inter-related aspects:

- **the company's needs and interests.** For the company there is a business need to attain and to maintain the desired quality at an optimum cost; the fulfilment of this quality aspect should be related to the planned and efficient utilisation of the technological, human and material resources available to the company.
- **the customer's needs and expectations.** For the customer, there is a need for confidence in the ability of the company to deliver the desired quality, as well as the consistent maintenance of quality.

Each of the above aspects of a quality management system requires objective evidence in the form of information and data concerning the quality of the company's products.

An effective quality management system should be designed to satisfy customer needs and expectations whilst serving to protect the company's interests. A well structured quality system is a valuable management resource in the optimisation and control of quality in relation to risk, cost and benefit consideration.

E.5 Quality System Principles

A quality system should function in such a manner as to provide proper confidence that:

- the system is well understood and effective,
- the products or services actually do satisfy customer expectations,
- emphasis is paced on problem prevention rather than dependence on detection after occurrence.

The quality system typically applies to, and interacts with, all activities pertinent to the quality of a product or services. It involves all phases from initial identification to final satisfaction of requirements and customers expectations. The phases and activities form the quality loop:

- marketing and market research
- design/specification engineering and product development
- procurement
- process planning and development
- production
- inspection, testing and examination
- packaging and storage
- sales and distribution
- installation and operation
- technical assistance and maintenance
- disposal after use.

E.6 Quality Manual

The typical form of the main document used in drawing up and implementing a quality system is a “Quality Manual”.

The primary purpose of a quality manual is to provide an adequate description of the quality management system while serving as permanent reference of the implementation and maintenance of that system.

In larger companies, the documentation relating to the quality management system may take various forms, including the following:

- a corporate quality manual

- divisional quality manuals
- specialised quality manuals

E.7 Quality Plan

For projects relating to new products, services or processes, management should prepare written quality plans consistent with all other requirements of a company's quality management system. Quality plans should define:

- the quality objectives to be attained
- the specific allocation of responsibilities and authority during the different phases of the project
- the specific procedures, methods and work instructions to be applied
- suitable testing, inspection, examination and audit programmes at appropriate stages
- a method for making changes and modifications in a quality plan as the project proceeds
- other measures necessary to meet objectives

The International Standard ISO 9004-5 provides guidelines to assist suppliers and purchasers in the preparation, review, acceptance and revision of quality assurance plans intended to be used in support of ISO 9001, and 9003 quality standards (see Figure E.4).

Quality Assurance Plan

0. Commitment of the partners
1. Purpose
    - General
    - Quality objectives
    - References
    - Terminology
2. Management responsibilities
    - Consortium
    - Organisation
    - Task definition
    - Rôle of the partners
    - Decision process
    - Information flow
3. Contract review
4. Design control
5. Document control
6. Purchasing
7. Purchaser-supplied items
8. Product identification and traceability
9. Production
10. Handling, storage, packaging and delivery
11. Installation
12. Inspection and testing
13. Inspection, measuring and test equipment
14. After-delivery service
15. Third party involvement
16. Non conformity
17. Training
18. Quality audits
19. Quality records
20. Statistical techniques

Figure E.4

Appendix F - PRELIMINARY SAFETY ANALYSIS OF THE WHISPER SYSTEM

THE CASE STUDY*

The following is a top level description of a concept that a city is thinking of implementing in its major shopping centre. A PSA has been performed and the remainder of the appendix is a typical report that could be written on the WHISPER system.

Wheelchair for Intelligent and Safe Portage in Equipped Regions

The system under discussion is an intelligent electric (batteries) wheelchair for use by disabled (including blind) people in a busy shopping centre.

- Each chair contains its own route guidance system which enables the passenger to state the required destination and the chair will then proceed to it without further intervention (the HMI details of data input are under discussion). The guidance system primarily calculates its current position by dead reckoning (calculation from a known position), but it can also obtain confirmatory information by reading active transponders embedded in the pavement at strategic locations. These transponders can also inform the chair of any obstructions nearby (e.g. workmen down a hole) by forbidding the chair to proceed into one or more quadrants (centred on the transponder). This information is set on a control panel located near each transponder, to which only authorised personnel have access.
- Whilst most of the areas in which these chairs are intended to travel are pedestrian precincts, they will need to cross some roads on occasions. They will do this at pedestrian crossings controlled by traffic lights. These crossings have a special transponder which is connected to the traffic light controller and informs the chair when it is safe to cross.
- In order to avoid damaging any object or person that the chair might run into, the chair has a bumper all around which is connected to a sensor. When the sensor is activated the chair halts. The chair restarts on the command of the passenger. There is also a devise to warn pedestrians of the wheelchair's approach.

* All ideas concerning, and the concept of, the project WHISPER are exclusive and copyright to the DRIVE II project PASSPORT (V2057/8).

SUMMARY

A preliminary safety analysis has been performed on the project WHISPER. A PASSPORT Diagram has been produced upon which a "What if?" analysis was performed and a number of safety hazards identified. A "What causes?" analysis was performed on an impact by a road vehicle on the wheelchair, and it was proposed that this part of the system should be developed to Integrity Level 2, according to the document produced by the DRIVE I project DRIVE Safely.

F.1 Introduction

The project PASSPORT is concerned with the safe design and development of all types of Advanced road Transport Telematic (ATT) systems. One of its tasks is to provide assistance to DRIVE II projects, and to this end the project WHISPER has been developed as a case study.

During the DRIVE I programme the project DRIVE Safely produced a proposal for the development of all safety-critical ATT systems[DRIVE Safely 1992]. One of the first tasks that must be performed at the beginning of any project is a Preliminary Safety Analysis (PSA) to identify the existence, or otherwise, of any safety hazards that may affect the design. This task has been performed on part of the WHISPER project and is described below.

It should be noted that since the original specification is not clear about some aspects of the system, this PSA report cannot be considered to be complete. Further work will have to be done after consultation with the project engineers.

F.2 Procedure Used

The outline specification of WHISPER was studied and discussed with the project engineers. It was then defined in its relationship to the environment by describing WHISPER with a PASSPORT Diagram model which identified the system terminators.

Based on this diagram a "What if?" analysis was performed in discussion with the members of the project WHISPER. Hazards were identified and evaluated under conditions of correct and incorrect functioning of each terminator defined by the model. During this phase a number of safety objectives were identified for the system.

A "What causes?" analysis was made of the principle hazard identified by the "What if?" analysis, and a number of safety requirements were identified. In addition a controllability category was assigned to this part of the system[DRIVE Safely 1992]. The resulting consequences for the design are then discussed.

F.3 Description of the System Concept

F.3.1 Project WHISPER

The main objectives of WHISPER are:

- the safe transport of disabled (including blind) persons in a shopping precinct,
- the provision of status information to the WHISPER passenger,
- automatic route finding,
- the ability to cross a road safely at a traffic light controlled pedestrian crossing.

There are seven main elements in the WHISPER system and the infrastructure required by the WHISPER system.

1. A route guidance system which calculates how to get from one location to another.
2. A navigation system which calculates the wheelchair's current position by dead reckoning.
3. A number of transponders embedded in the pavement at strategic locations, which the wheelchair uses to confirm its current position.
4. These transponders may also be used to outline (temporary) obstructions. Authorised personnel will use a control panel near to the transponder to indicate one or more quadrants (centred on the transponder) into which the wheelchair is forbidden to proceed automatically.
5. A number of special transponders used by the wheelchair to identify the location of pedestrian crossings, and to inform the wheelchair when it is safe to cross the road.
6. A surrounding bumper which automatically halts the wheelchair if physical contact is made with a person or object.
7. A devise to warn pedestrians of the approach of the wheelchair.

F.3.2 Functional Description of the WHISPER System

The functional description of the WHISPER system is shown in the PASSPORT Diagram of Figure F.1. This shows inputs to the system coming in from the left, and outputs from the system going out to the right. Fixed (read only) data-bases are shown at the top and variable (read/write) data-bases are shown at the bottom.

A brief description of each of the mechanisms by which the WHISPER system reacts to its environment is as follows.

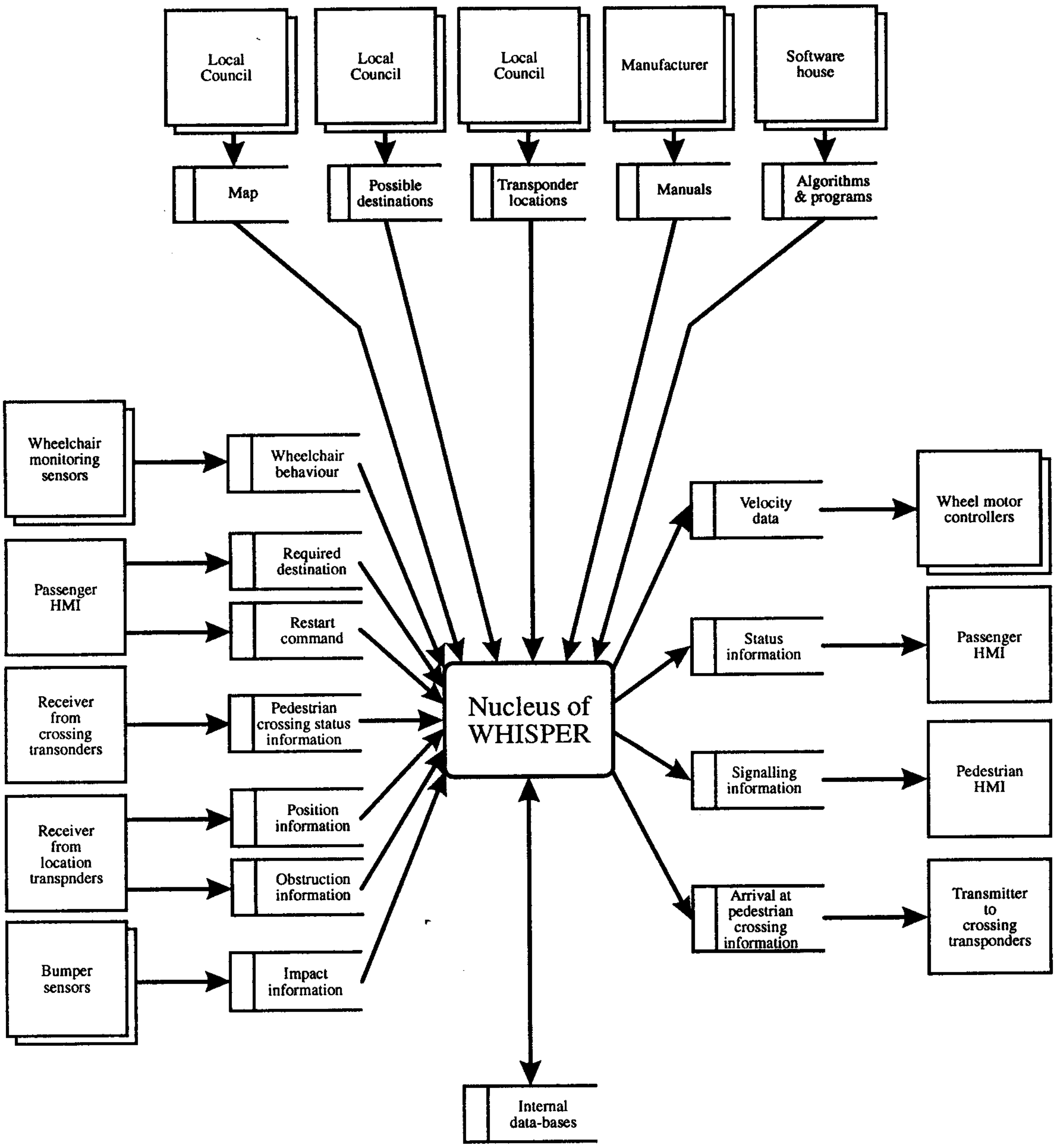


Figure F.1 - PASSPORT Diagram Model for the WHISPER System

F.3.3 Delineation of WHISPER and its environment

F.3.3.1 External Systems

The external systems relevant to WHISPER are:

- *The wheelchair* - there are monitoring sensors in the electric wheelchair that provide information on the behaviour of this electric wheelchair (Wheelchair behaviour). These sensors are located in various places to collect the necessary data. In turn, the wheelchair is directed by motor controllers, one for each main wheel, which instruct the motors to propel the wheelchair in the correct direction (Velocity data).
- *Passenger* - the passenger of the wheelchair states the required destination (Required destination) and restarts the wheelchair when it has been halted (Restart command). WHISPER provides the passenger with information on the status of the wheelchair (Status information).
- *Pedestrian crossing transponder* - this transponder receives information that the wheelchair has arrived at a pedestrian crossing (Pedestrian crossing negotiation) and also informs the wheelchair when it is safe to cross (Pedestrian crossing status information).
- *Location transponder* - this transponder provides confirmatory position information to the wheelchair in the equipped region (Position information), and information forbidding the wheelchair to proceed into one or more quadrants centred on that transponder (Obstruction information).
- *Obstacle* - when the wheelchair runs into any object or persons, this is detected by the bumper sensors. WHISPER is notified (Impact information) and the chair is immediately halted to avoid damage.
- *Pedestrians* - pedestrians are informed of the presence of the wheelchair by signals (Signalling information).
- *Local Council* - the Local Council, or its agent, provides information on the location of relevant items in the shopping centre (Map). This information is necessary for the calculation of the current wheelchair position, its route plan and the provision of route guidance with the Shopping Centre.
- *Local Council* - the Local Council, or its agent, provides a set of possible destinations for the WHISPER passenger (Possible destinations).
- *Local Council* - the Local Council, or its agent, provides up to date information on the location of the transponders in the Shopping Centre (Transponder locations).

- *WHISPER manufacturer* - the manufacturer provides information on the installation, maintenance and use of the WHISPER system (Manuals).
- *Software house* - the software house provides the WHISPER programs with the algorithms for route guidance and position calculation by dead reckoning (Algorithms & programs).

F.3.3.2 Interactions between WHISPER and its external systems

The following interactions (information sets) can be identified between WHISPER and the external systems:

- *Wheelchair behaviour* - this information comes from sensors (Wheelchair monitoring sensors); the following information is likely to be provided:
  - dynamic information (forward/lateral speed and acceleration),
  - wheelchair indicators: lights, signalling,
  - environment light level indication,
  - power supply: batteries level indication.
- *Required destination* - this information contains the identification (e.g. name) of the destination.
- *Restart command* - after the wheelchair has made contact with a temporary obstruction the restart command enables the WHISPER passenger to wait until the obstruction has moved and then instruct the WHISPER system to continue. The details of command and data input are under discussion.
- *Pedestrian crossing status information* - as a minimum this information consists of:
  - pedestrian crossing transponder location information,
  - pedestrian crossing information (e.g. traffic light state).
- *Position information* - as a minimum it consists of:
  - transponder location information.
- *Obstruction information* - as a minimum it consists of:
  - prohibited quadrant(s) identification relative to the transponder.
- *Impact information* - impact detection is true or false.
- *Map* - this information may consist of:
  - a list of the co-ordinates of the destinations,
  - a list of the co-ordinates of the fixed obstructions,

  - a list of the co-ordinates of the location transponders,
  - a list of the co-ordinates of the pedestrian crossing transponders,
- *Possible destinations* - destination name and/or address.
- *Transponder locations* - a list of transponders with a designation of the transponder:
  - type (Pedestrian crossing, Position, Obstruction indicator),
  - location.
- *Manuals* - this information may consist of:
  - description of WHISPER installation (installation manual),
  - description of WHISPER maintenance (maintenance manual),
  - information on how to use WHISPER (users' manual).
- *Algorithms & Programs* - these include the computer programs for the WHISPER Route Guidance System and position calculation by dead reckoning.
- *Velocity data* - this provides details of the motion required of the wheelchair.
- *Status information* - this is the information that the wheelchair passenger needs to know, which is currently under discussion.
- *Signalling information* - this concerns direction signalling and wheelchair lights.
- *Pedestrian crossing negotiation* - this information includes the:
  - crossing request.

F.3.3.3 Internal data-bases required by WHISPER

The following data-bases are likely to be maintained:

- current location and speed information - this includes the following information:
  - current route plan,
  - current location of the wheelchair,
  - current dynamic information (speed and acceleration).
- transponder communication status - a list of transponders which are actually communicating with the wheelchair, with the following information:
  - transponder type,
  - transponder location,
  - transponder information content.

- obstruction avoidance data - a list of transponders where an obstruction has currently been identified, with the following obstruction information (see above):
  - transponder location,
  - prohibited quadrant(s) identified relative to the transponder.

F.4 Definition of the Safety Objectives

There are four objects upon which the WHISPER system performs an action that could be harmful; the WHISPER passenger, a pedestrian, a passenger of another WHISPER system and an obstruction. The overall safety objectives are therefore:

1. The wheelchair must never perform an action that puts the passenger into a dangerous situation.
2. The wheelchair must never perform an action that may harm a pedestrian, or the passenger of another WHISPER system.
3. The wheelchair must never perform an action that may damage an obstruction.

F.5 Hazard Identification - "What If?" Analysis

The hazards associated with the WHISPER system were identified by performing a "What if?" analysis on

Figure F.1. Together with the members of project WHISPER consideration was given to the possible effects of the failure of any part of the WHISPER system which influences the environment, i.e. the terminators at the right hand side of the PASSPORT Diagram Model (see

Figure F.1). These are summarised as follows:

Wheel motor controllers

It is the function of the wheelchair motor controllers to provide all the movement available to the WHISPER passenger. Of all the terminators, it is this that has the most hazards associated with it. This is because it has a direct control over the current situation, whilst the other terminators have indirect effects. There are four items which the motor controllers can have a detrimental effect upon; the WHISPER passenger, a pedestrian, a passenger of another WHISPER system and an obstruction. Thus the hazards associated with the motor controllers are that they may:

1. Move the WHISPER passenger into a dangerous situation, including:
   - crossing a road when it may not be safe to do so,
   - attempting to navigate up or down a flight of stairs.

2. Move the wheelchair into contact with a pedestrian or a passenger of another WHISPER system in a harmful manner.
3. Move the wheelchair into contact with an obstruction in a harmful manner.

Passenger HMI

This HMI will inform the passenger of the current status of the WHISPER system. Because this information is only intended as advice no direct safety hazards can be envisaged, but this must be reconsidered when the final set of information to be given has been decided.

Pedestrians HMI

This HMI is intended to provide a warning of the approach of the wheelchair. This will enable pedestrians and passengers of other WHISPER systems to take evasive actions where necessary. The main failure associated with this HMI is that it could:

- Fail to warn a pedestrian or a passenger of another WHISPER system of the wheelchairs approach.

This failure could enable (2) to occur. Thus this HMI could indirectly cause the wheel motor controllers to:

4. Move the wheelchair into contact with a pedestrian or a passenger of another WHISPER system in a harmful manner.

Transmitter to the pedestrian crossing transponders

This transmitter is responsible for negotiating with the pedestrian crossing lights controller safe passage across the road. The main failure associated with this transmitter is that it could:

- Incorrectly negotiate a safe passage, leading to an incorrect signal to cross.

This failure could enable (1) to occur. Thus the transmitter to the pedestrian crossing transponder could indirectly cause the wheel motor controllers to:

5. Cross a road when it may not be safe to do so.

F.6 Fault Identification - “What Causes?” Analysis

The most hazardous event is identified above is the impact by a road vehicle on the wheelchair.

A “What causes?” analysis was therefore done to identify the possible causes of such a hazard. This is shown in Figure F.2.

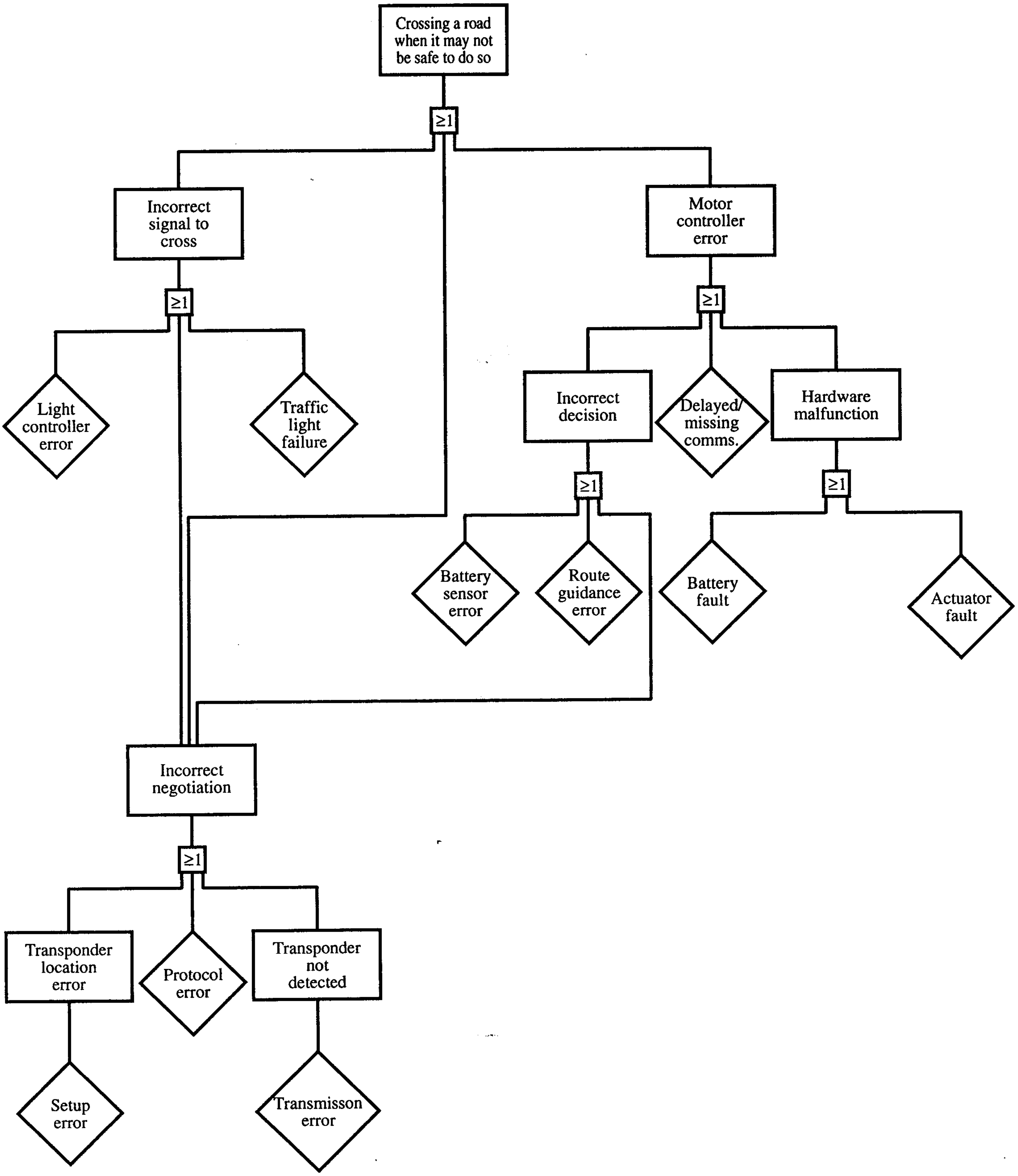


Figure F.2 - "What Causes?" Analysis of Prime Hazard

There are a number of faults which will occur in any "What causes?" analysis and their presence will clutter the resulting tree. These are *software faults, Maintenance faults and faults caused by Electromagnetic Interference (EMI).*

A software fault may be the root cause of any incorrect decision or action taken by any piece of software identified by the "What causes?" analysis, thus in Figure F.2, a software fault may be responsible for the "Incorrect decision" or the "Route guidance error".

All system components may be subject to perfective and/or corrective maintenance. Incorrectly performed maintenance may be the cause of any failure identified by the "What causes?" analysis.

All electronic components may be subject to EMI. This may adversely affect the action performed by that component.

F.7 Safety Requirements

The following safety requirements can be derived from the leaves of the "What causes?" analysis and the discussion of Section F.6 about software, maintenance and EMI. They have been divided into design issues and procedural issues.

Design Issues

1. The traffic lights should have a *safe state* which will not give the WHISPER system an "all clear" signal.
2. The WHISPER system must only react to the transponder nearest to it.
3. The signal transmitted by the transponders must be received correctly or rejected.
4. The wheelchair must receive a positive "all clear" signal from its own pedestrian crossing before commencing to cross.
5. The location of transponders should be such that the wheelchair has its position confirmed just prior to arriving at a pedestrian crossing.
6. The traffic lights monitor must issue a warning of any fault detected.
7. A wheelchair sensor must monitor the charge level of the battery.
8. The wheelchair must not proceed to cross the road unless there is sufficient power in the battery to reach the other side.
9. The route guidance system must provide only passable routes to the navigation system.

10. The wheelchair must commence to cross at a pedestrian crossing within TBS seconds of receiving “all clear”, or else repeat the negotiation to cross (e.g. after waiting for a restart command after bumper sensor activation).

Procedural Issues

1. The location of transponders provided by the Local Council or their agents should be validated.
2. The software should be produced to a suitably high level of quality.
3. Maintenance procedures must exist for:
   - the traffic lights,
   - the battery,
   - the actuators.
4. Whenever the location of a transponder is modified care should be taken to update the internal data-base within the WHISPER system.
5. Whenever the set of possible destinations is modified care should be taken to update the internal data-base within the WHISPER system.
6. Whenever the location of permanent obstacles is modified care should be taken to update the internal data-base within the WHISPER system.
7. All electronic components must be suitably screened against EMI.

F.7.1 Additional Design Requirements

During the performance of the “What if?” analysis a number of safety-related design requirements were identified, but to which no immediate solution could be found. These are listed below.

1. Thought must be given as to what should happen after a wheelchair has stopped due to a bumper contact with an obstacle.
2. Manual control should be available for sighted passengers to proceed in "forbidden" areas.
3. Thought must be given as to how to re-introduce the wheelchair to the WHISPER system after a manual control (may be related to (2)).
4. Thought must be given as to how to permit a fast evacuation in the case of an emergency.
5. Thought must be given to the provision of a manual shut-off switch.

6. If the difference between the current dead reckoning position and the position given by a location transponder is greater than TBS then the wheelchair must stop.

F.7.2 Additional Notes

During the performance of the "What if?" analysis a number of safety-related design requirements of related systems in the environment were identified. These are listed below.

1. In order to avoid frequent collisions with pedestrians the normal routes to be taken by the wheelchairs should be marked on the pavements for all to see and avoid as far as possible (c.f. cycle paths in Germany).
2. All maintenance work within the equipped area should be surrounded by a temporary fence so that if a wheelchair fails to discover a forbidden zone, it will be stopped when the bumper makes contact with the fence.
3. All unsafe locations (e.g. top of steps, side of road) must be protected by physical barriers and, possibly, permanent obstacle beacons, so that it is virtually impossible for a wheelchair to enter them.
4. The system controlling the transponders at each pedestrian crossing is itself safety-critical and needs to be developed according to [DRIVE Safely 1992].

F.7.3 Controllability Category

The scenario to be investigated is "Crossing a road when it may not be safe to do so". A controllability analysis will now be performed in accordance with Appendix B.

- *Ranked Severity Factors* - WHISPER provides direct control, and because blind persons are to be permitted to use the wheelchair no direct backup can be assumed from the passenger. However, the vehicle driver will be able to react to avoid a collision, thus providing a form of backup.
  - we can therefore expect the final score to be about 3.

We will now consider the factors that will influence the controllability of the safety of the situation after the failure in more detail.

- *Levels of System Interaction* - WHISPER is autonomous and reasonably intelligent.
  - a score of 2.
- *Degree of Control* - WHISPER has complete control of its own movements.
  - a score of 4.

We can thus see that the WHISPER system is very important to the correct functioning of the system. We now discuss the features that may be available to mitigate the safety of the situation after a failure.

- *Provision of Backup* - when a blind person is being carried the only means of avoiding a collision is for the vehicle driver to perform an emergency stop, which produces a safe state.
  - a score of 1 or 2.
- *Reaction Time* - since WHISPER is only intended to be used within a pedestrian precinct one can expect that motor vehicles will be subject to a low speed limit.
  - a score of 2.

We thus have a high scoring system (2 and 4) protected by a low scoring backup (1 and 2). Thus, if it is known that the motor vehicles will be kept to a low speed, and that there will be good visibility for vehicle drivers to spot the WHISPER wheelchairs, then a score of 2 would be appropriate. This would give a controllability category of *debilitating* (failures whose effects are usually controllable by a sensible human response and, whilst there is a reduction in the safety margin, can usually be expected to lead to outcomes which are at worst severe). However, if the above conditions do not hold then a final score of 3 should be given, which will lead to a controllability category of *difficult to control* (failures whose effects are not normally controllable by the road users(s) but could, under favourable circumstances, be influenced by a mature human response. They are likely to lead to very severe outcomes.).

F.8 Proposed Design Measures

The interaction of the wheelchair with the pedestrian crossing has been identified as being safety-related and needs to be developed to Integrity Level 2 (the consequence of a *debilitating* controllability category). However whilst more than "normal" care should be taken over its development, it does not require the great expense of time and effort required of the higher integrity levels. The basic requirements are proposed in [DRIVE Safely 1992]. Requirements for developing vehicle based software have been described in [MISRA 1994a] and the certification view of systems development has been described in [PASSPORT 1995]. The proposals outlined in [DRIVE Safely 1992] can be summarised as follows.

During the proceeding hazard analysis the two types of failure, random and systematic, have been considered. Random failures (e.g. sudden failure of hardware) occur as a result of some material degradation in a component during operation, whilst systematic failures are the result of a fault in the design and development process, and are therefore present throughout the operational life of the system (e.g. in software). The measures to tackle hardware and software faults are split into three safety elements:

- Quality - tackles mainly systematic faults.
- Reliability - tackles random faults.
- Configuration - tackles mainly random faults.

These are then divided into measures to control faults and measures to avoid faults. This is discussed in Part B of Draft 2, and the requirements to achieve a level of confidence that corresponds to Integrity Level 2, are described in Section 4.2 of Part E and summarised in Table 4.1.

The above measures are applicable to the complete system, both hardware and software; in addition any software that needs to be developed to Integrity Level 2 should follow its own life-cycle as specified in Part C. The requirements to achieve the necessary level of confidence for software are described in [MISRA 1994b].

It should be noted that the hazard analysis described in this document has only been done on the top level description of the WHISPER system. Once more detailed designs have been created, further more detailed safety hazard analyses should be performed to confirm that these designs do indeed meet their safety requirements.

F.9 Conclusion

The WHISPER system is able to function safely within its proposed environment provided the recommendations for the development of the WHISPER system are followed, or other appropriate measures taken.

Appendix G - GLOSSARY OF TERMS

Accident - An unintended event that causes death, injury, damage to materials or the environment.

Animation - Realistic simulation of a system from its specification, usually for validation.

Auditing - The process of examining software and its related documentation for accuracy, quality, completeness, consistency and traceability.

Authoritative Specification - A specification is authoritative if it can be used to determine whether the system is correct without reference to a higher authority.

Authoritative System Reference - The authority process that determines whether or not a proposed interpretation of a specification, or the specification itself, is in error. It will include such things as the system specification, system proposals, contractual and verbal statements and the judicial system.

Certification - The process of obtaining regulatory agency approval for a function, equipment or system, by establishing that it complies with all applicable statutory regulations.

Common Mode Failure - Failure of apparently independent components or communication links due to an initiating event that affects them all.

Other alternative definitions are:

- Where separate or redundant processes fail because of some event which affects them all.

- The simultaneous failure due to the same error/fault in two or more items forming part of a system.

Complete - Completeness implies that no requirement or need of the customer is overlooked, a system response has been specified for every possible set of inputs, expressions such as 'to be determined' or 'this section is intentionally left blank' have no place, all system requirement specifications must conform to any specified standard and finally, the document should be textually complete.

Component - The degree of structure within the system considered at a particular level of analysis.

Computer - A programmable unit, with its peripheral equipment, controlled by stored programs.

Computer System - One or more computers, software and associated peripherals which uses a common storage for all or part of a program and its data.

Configuration - The specific arrangement of the programmable electronics within a Programmable Electronic System and the type of safety-related systems (i.e. Programmable and Non-programmable Electronic Systems) that make up the total configuration of safety-related systems.

Configuration Control - Ensures that any change, modification, addition or amendment is prepared, accepted and controlled by set procedures.

Configuration Management - Technical and administrative procedures to:

(1) Identify and document functional and physical characteristics of any part of the system;

(2) Control changes to these, and their interfaces;

(3) Record and report change, its process and implementation.

Dangerous Mode of Failure - Those failures of a safety-related system that would impair its safety integrity.

Dynamic Analysis - Execution of a program with test data and the analysis of the results.

Emulator - Software run on a host computer that accepts the same input data, executes the same programs and yields the same outputs as the target computer.

Environment - The part of the external world, including users and inmates of the system, that affects and is affected by the system and may be harmed by an accident caused by it.

Error - If a system is in an erroneous state, then any part of the state which differs from a valid state is an error. A failure therefore occurs because the system is in error, however it should be noted that an error does not always cause a failure.

Another alternative definition is:

- A failure occurs because the system is erroneous: an error is that part of the system state which is liable to lead to failure.

- An error is, in short, a detected deviation from the agreed specification of requirements.

Error Recovery - The use of techniques which aim to transform the current erroneous system state into a safe state from which normal (and safe) operation can continue.

Event - A significant happening that may originate in the environment or the system.

Failure - A system failure occurs when the delivered service deviates from the specified service, where the service specification is an agreed description of the expected service.

A failure is the manifestation of an error in the system or software.

Failure Mode and Effects Analysis (FMEA) - An analysis of the items forming a system and their interconnection made in order to determine the effect on the system of a failure of a specific type of item. The technique requires a knowledge of how an item can fail and how this failure might propagate through the system. The technique used may be:

qualitative:-

for example, item A has a type B failure which leads to a system failure of type C.

quantitative:-

for example, using failure rate information for items and synthesising a failure rate for the system.

Failure Mode, Effect and Criticality Analysis(FMECA) - A type of FMEA which ranks the types of system failure by their criticality to safety, mission, security etc. and groups the items which contribute to each criticality class.

Fault - A defect in a component or the design of a system is fault. The cause of an error is therefore a fault, however it should be noted that a fault does not always cause an error.

Other alternative definitions are:

- The cause of an error is a fault (eg. hardware defect, software defect) which resides, temporarily or permanently in the system.

A fault is a defect that gives rise to an error.

Fault Tolerance - The built-in capability of a system to provide continued correct execution, i.e. provision of service as specified, in the presence of a limited number of hardware or software faults.

Fault Tree Analysis(FTA) - A top down analysis relating each hazard to a logical combination of events and conditions which give rise to the hazard. The logic is represented in the form of a tree structure and develops the system faults down to a level of detail at which there is knowledge of how an item can fail and the probability that it might fail in that system. It is usually used to calculate a probability or frequency of system failure but may be used as a qualitative analysis technique. It has been used, in the latter manner, for safety-critical software.

An alternative definition is:

- Is a top down or deductive method of determining the combination of failures and operating circumstances which could cause a hazard. Basic events, those for which sufficient information already exists, eg. a frequency, failure rate or probability of failure is known, are combined by the laws of boolean algebra to identify which basic events cause a failure mode of a Programmable Electronic System.

Formal Verification - Showing by formal mathematical proof or arguments that software implements its (formal mathematical) specification correctly.

Formal Mathematical Specification - A specification in a formal mathematical notation.

Graceful Degradation - Stepwise reduction of system functions in response to detected failures while essential functions are maintained.

Hazard - A physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these.

Integrity Level - One of "m" possible discrete safety integrity levels which indicates the relative risk to be countered by a safety-related system, and hence also indicates the required relative quality of a safety-related system. (Level m has the highest level of safety integrity; Level 1 has the lowest.)

Mistake - A human fault. A human action (in carrying out any system life-cycle activity) that may result in unintended system behaviour (failure).

On-line Testing - Where equipment or software is tested while it is operating.

Plan - A plan is a description of (part of) a project. It is written in advance and covers the project in its entirety. It gives the philosophy and the relations between the various parts.

Procedure - A procedure is a detailed, step-by-step description of a small part of a programme.

Prototype - A rapidly produced program which is used to validate (part of) a specification.

Redundancy - Provision of additional elements or systems so that any one can perform the required function regardless of the state of operation or failure of any other. Redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

Random Hardware Failure - Failures which result from a variety of degradation mechanisms in the hardware.

Risk - The combination of the frequency, or probability with which a hazard occurs and the consequences of the hazardous event.

Other alternative definitions are:

- The likelihood of a specified undesired event occurring within a specified period or in specified circumstances. Depending on the circumstances, it may be either a frequency (the number of specified events occurring in unit time) or a probability.

- A measure of the likelihood and severity of an accident.

Safety - The expectation that a system does not, under defined conditions, lead to a state in which human life, economic well-being or the environment are endangered.

Note: For system safety, all causes of failures which lead to an unsafe state shall be included; hardware failures, software failures, failures due to electrical interference, due to human interaction and failures in the controlled object. Some of these types of failure, in particular random hardware failures, may be quantified, however system safety also depends on many factors which can only be considered qualitatively.

Safety-Critical Feature - The features that a system must have in order to eliminate the unacceptable hazards associated with it or to reduce the risks from these hazards to an acceptable level.

Safety-Critical Software - Software used to implement a function where failure could risk human life.

Safety Function - A function that must be carried out by the safety-related control system should a hazardous failure occur in the Technical Process or in the safety-related system itself.

Safety Integrity - That characteristic of a safety-related system concerned with its ability to perform its required function, in the desired manner, under all relevant conditions and on the occasions when it is required so to perform.

An alternative definition is:

- The likelihood of a safety-related system achieving its required safety functions under all the stated conditions within a stated period of time.

Safety Life-cycle - The elements of a system life-cycle that are safety-related.

Safety-Related Hardware Reliability - That aspect of the safety integrity relating to random hardware failures in a dangerous mode of failure of the safety-related systems.

Safety-Related Software - Software which ensures that a system does not endanger human life, economic well-being or the environment.

Safety-Related System - A system that:

- implements, independently of any other system, the required safety functions necessary to achieve a safe state for the Technical Process or to maintain a safe state for the Technical Process.

- achieves, on its own or with other safety-related systems, the necessary level of safety integrity for the implementation of the required safety functions.

Safety Requirements - A detailed statement describing the function and performance of a proposed new system and the environment in which it is to operate, with particular reference to safety.

Software Life-cycle - The activities occurring during a period of time that starts when software is conceived and ends when the software is no longer available for use. The software life-cycle typically includes a requirement phase, development phase, test phase, integration phase, installation phase and a maintenance phase.

Standard - A precise and authoritative statement of the criteria necessary to ensure that a material, product or procedure is fit for the purpose for which it is intended.

Systematic Failures - Failures due to faults (including mistakes and acts of omissions) in design, construction or use of a system which cause it to fail under some particular combinations of inputs or under some particular environmental condition. Systematic failures could arise, at any part of the safety life-cycle.

An alternative definition is:

- failures due to faults in the requirements specification, design, construction or use of a system which cause it to fail (every time) under particular combinations of inputs or environmental condition. Software failures are classified as systematic failures.

Systematic Integrity - The non-quantifiable, qualitative aspects of the safety integrity of the safety-related systems.

System - A system is defined to consist of a set of components which interact according to a design. A component of a system can be another system (called a sub-system).

Such components (sub-systems) may be, depending on the level:

- a controlling or controlled system;

- hardware, software, human interface.

An alternative definition is:

- Any mechanism that maintains a pattern of behaviour between itself and its environment.

System Life-cycle - The period of time that starts when a system is conceived and ends when the system is no longer available for use. (c.f. Software Life-cycle)

System Safety Elements - Three defined system characteristics of the safety-related systems. They are Configuration, Safety-related Hardware Reliability and Systematic Integrity.

Technical Process - That part of an RTI system that implements the functional requirements.

Test Case - A set of inputs, execution conditions and expected results.

Testing - The process of executing a program with the intent of finding faults and establishing confidence in correct program operation.

Tolerable Risk Level - The tolerable risk level is the maximum level of risk that is regarded as acceptable in the context of the circumstances in question.

Unambiguous - A requirement is unambiguous if and only if it has only one possible semantic interpretation.

Validation - It is concerned with demonstrating that a system or computer program satisfies its requirements. Informally, validation might be thought of as answering the question “are we building the right thing?”. Validation requires a decision to be made.

Verification - It is the comparison of the output of each individual phase with the output of the previous phase, the objective being to ensure that the output from the new phase fulfils the requirements specified in the outputs of the previous phase. Informally, verification might be thought of as answering the question “are we building the thing right?”. Verification always requires a comparison to be made.

An alternative definition for software is:

- The process of determining whether or not the product of each phase of the software life-cycle development process fulfils all the requirements specified in the previous phase. Verification includes testing.