Urban Traffic Management and Control (UTMC)

Project UTMC22: Safety Issues

Framework for the Development and Assessment of Safety-Related UTMC Systems

Release version 1.0
March 2000

Circulation: Release for public consultation

Foreword

Scope and purpose

Project UTMC22 had two main aims:

- to identify how the safety case for UTMC should be addressed and produce guidance for the UTMC programme and developers on safety-related systems;

- to evaluate the UTMC systems architecture systems and identify and advise on any inherent risks.

The work was carried out in three phases. Phase 1 reviewed available approaches and carried out interviews with a number of representatives of the UTMC developer and user community. There are a number of relevant standards and guidelines resulting from European research and other initiatives. But, the development of safety-related systems remains very much an open question and there are few definitive positions. Equally, the interviews confirmed that there is little detailed awareness of the standards and frameworks that do exist.

Accordingly an expanded role was given to this report, produced in Phase 3 of the project, which addresses the first aim of UTMC. It is intended to explain and inform about existing approaches. It also retreats from setting out *guidance* to UTMC developers and users. Instead, as the report's title suggests, it is now intended as a *safety framework*, proposing how the development and assessment of safety-related UTMC systems might be carried out. It will be up to future UTMC projects (notably the UTMC29 demonstrations) to try out the approach and harden up the advice into guidance based on implementation experience.

Typically, UTMC systems will evolve from existing, perhaps non-safety related systems, into systems which have safety implications. In addition, the boundaries of what a UTMC system comprises are uncertain and changing. UTMC includes 'normal' urban traffic control and traffic information functions, but potentially also advanced active control systems such as automatic vehicle control. So, this Framework has to address all degrees of safety hazard.

The second aim of UTMC22 was specifically covered by Phase 2 of the project. It carried out a preliminary safety analysis of the UTMC Technical Specifications which is available as a separate project report. Not least, this provides a worked example of the assessment approach proposed in this Framework document.

The issues

This Framework is motivated by two fundamental issues. First, the integration of systems like UTMC gives rise to 'emergent' properties which are not present in the original equipment or sub-systems (ie integrated systems are greater than the sum of their parts which is often the motive for integration in the first place). Existing Statutory Type Approval (STA) processes have evolved over many years and cover traffic signal control very well. Traditionally this has been relied upon for urban traffic control systems deployment. Increasingly, roadside equipment is both more complex and diverse, and it is being

integrated in to more complex systems. STA remains very necessary, but it is no longer sufficient.

Second, safety 'best practice' has evolved significantly in recent years in other industries. New international standards such as IEC 61508 on the functional safety of electrical, electronic and programmable electronic systems now exist. In short, the Courts are much less tolerant than before of 'sloppy work'. Developers now need to demonstrate awareness of 'best practice' and to demonstrate that it has been applied.

This Framework tries to address these needs, in relation to the traffic industry and UTMC in particular. It proposes an approach to handle the safety issues of UTMC taking on board existing and evolving standards and procedures. In brief, the position of this Framework with respect to some of these key existing standards and procedures is as follows:

- *Safety Integrity Levels:* SILs are a key concept within IEC 61508. They provide for the categorisation of the reduction in risk required of any safety-related system, or sub-system, into one of four levels (the SILs). The standard defines the life-cycle activities required for each level. IEC 61508 recommends that each industry sector should agree its own method for identifying SILs. Since this has not yet been done for UTMC type systems, this Framework puts forward a method for consideration which was developed during four European and UK projects.

- *The Code of Practice for Traffic Control and Information Systems:* This Code (designated MCH 1869) and the related document on System Certification (MCH 1813) have been developed by the Highways Agency. It is primarily a design methodology for arriving at a point of confidence in a system or an installation. This UTMC Framework adopts similar principles, though there are presentational differences. As already noted, this Framework is intended to be informational rather than practice guidelines, and it places greater emphasis on the technical development of the equipment and sub-systems that comprise UTMC systems.

- *The Design Manual for Roads and Bridges*: Though mainly targeted at trunk roads and motorways, Volume 9, on Network Traffic Control and Communications, does cover some of the types of system that might also appear in UTMC systems. Those parts of this Framework that cover the more general types of application, e.g. control rooms and Variable Message Signs, require the use of similar, and sometimes identical, processes to the ones recommended in the Design Manual.

- *Statutory Type Approval:* For simple equipment which performs a well-defined task, STA is a valid and well-established method to demonstrate, for example, the basic safety of a traffic junction controlled by traffic signals. However, the process needs to be enhanced to validate the full safety of a complex integrated UTMC system. It is very difficult to "Type Approve" systems. The safety of a complex system is usually demonstrated by building up a Safety Case during the development, operation and maintenance of that system and this Framework proposes a possible approach. Another approach has now been published in MCH 1813. It must be noted, however, that neither has been fully validated on a large and/or complex UTMC system.

Approval authority

The interviews during Phase 1 highlighted strong demand for some form of official certification for the safety of a UTMC system, though this goes against the current moves towards self-certification in many other industry sectors. It is for this reason that this Framework includes an "Approval Authority" within the proposed assessment process.

Please note, however, that “Approval Authority” is not intended to be synonymous with the Highways Agency. It could mean equally the organisation responsible for the system in the case of self-certification.

Status of this Framework

This Framework is a proposal on how to handle the safety issues of any possible current and future UTMC systems. It has to cover a large number of issues from both the technical and human factor viewpoints; the first such document that attempts to do this.

Whilst most of the techniques and methodologies mentioned are proven in themselves, it will be necessary (and is planned) to validate their combined use on a variety of types of UTMC system. It is hoped this Framework will also stimulate more general debate about the right way forward for the development of safety-related ITS systems.

There are a number of institutional issues associated with the assessment of the safety of any UTMC system that will need to be resolved. These are listed at the end of this Framework.

Executive summary

The Urban Traffic Management and Control (UTMC) initiative provides the opportunity for traffic management and control systems in an urban environment to incorporate many of the functions planned for future intelligent transport systems using an “open systems” approach. Whilst this should make their deployment easier and cheaper than if it were done in an *ad hoc* manner, the general public will still expect to be protected from potentially dangerous equipment and scenarios.

UTMC systems are integrated systems which exhibit emergent properties that are not present in the individual items of equipment; indeed this is why they have been integrated. This document therefore addresses the issues associated with such systems, and the equipment that they comprise, and proposes a Framework for the development and assessment of safety-related UTMC systems. It is based on the principles and techniques that have been developed for other industry sectors, and codified in various Standards and Guidelines. It also combines the areas of Traffic Safety, Human-Machine Interaction and Functional System Safety, and takes into account the concerns currently being expressed by the various stakeholders, in particular in relation to the requirement for a formal “seal of approval”.

The process of Statutory Type Approval does not provide a means to assure the safety of equipment containing software, particularly where such systems are integrated.. This Framework therefore proposes an extension to the current process that resolves the problems without putting an unacceptable load onto the Approval Authority (currently the Highways Agency).

The basic philosophy behind the approach described in this Framework can be summarised as:

- Identify what needs to be done
- Do it
- Demonstrate that it has been done correctly.

It requires an understanding of the system, a knowledge of the processes and techniques needed to create it, and the ability to demonstrate, to a third party where necessary, that it has all been done correctly, all in accordance with a suitable Quality Plan. Whilst the degree of rigour with which the demonstration process must be done will increase with the severity of the hazards associated with the system, the process should not put create unacceptable costs in a competitive, but regulated, market.

The assessment process is based on the use of the Safety Plan and the Safety Case. The former defines how all the safety issues that have been identified are going to be resolved. The latter contains the results of this work in the form of the justification as to why that UTMC system is considered to be safe for use by the operators and the general public.

Table of contents

Page

List of abbreviations

ALARP	as low as reasonably practicable
BCS	British Computer Society
BSI	British Standards Institution
COTS	commercial off-the-shelf (equipment)
EMC	electromagnetic compatibility
EMI	electromagnetic interference
FMEA	failure mode and effects analysis
FTA	fault tree analysis
HMI	human-machine interaction
HSE	Health and Safety Executive
GPS	Global Positioning System
IEC	International Electrotechnical Commission
IEE	Institution of Electrical Engineers
ISO	International Organization for Standardization
ITS	intelligent transport system
MISRA	Motor Industry Software Reliability Association
NMCS	National Motorway Communications System
PSA	Preliminary Safety Analysis
R&D	research and development
RTCC	Regional Traffic Control Centre
SIL	Safety Integrity Level
STA	Statutory Type Approval
UTC	Urban Traffic Control
UTMC	Urban Traffic Management and Control
VMS	variable message sign

1. Introduction

This Framework was produced as part of the UTMC22 project to study the safety issues associated with Urban Traffic Management and Control (UTMC) systems.

Whilst the introduction of computers and communications into UTMC offers many benefits, the general public has become used to being protected from potentially dangerous equipment; this protection is currently achieved by design standards (e.g. to reduce the ability to of a person to touch live electric circuits) or by a testing process (e.g. vehicle Type Approval and annual safety checks). Since they will expect this protection to continue, there will need to be some form of safety assessment of UTMC systems before they are released for public use.

1.1 The need for a change

There is a general agreement, indeed many European research projects in the field of transport telematics (also known as intelligent transport systems, or ITS) have already demonstrated, that more benefit will be obtained by integrating traffic management and traffic control functions, than by using them in isolation. This changes the very nature of the target of an assessment process in two fundamental ways:

- Traditionally, regulatory agency approval for road transport equipment has been performed using a Statutory Type Approval (STA) process. It was devised when equipment consisted only of mechanical and electrical components, and thus a series of tests was a valid exercise to demonstrate safety. Such systems are now recognised as being “simple”. ITS, however, are normally “complex” systems for which testing alone is not sufficient to validate all operational modes and conditions (see Section 5.5). It will therefore be necessary to provide some form of additional evidence to demonstrate the safety of integrated UTMC systems with emergent properties.
- An integrated system exhibits emergent properties that are not present in the individual items of equipment; indeed this is why they have been integrated. It is therefore necessary to consider the safety hazards that may result from the emergent properties of the system, as well as the specific hazards associated with the equipment of which it is constituted.

1.1.1 UTMC safety hazards

A preliminary safety analysis of the UTMC architecture [UTMC22 2000] has shown that there are a number of safety hazards that will be associated with a typical UTMC system, which are in addition to the obvious hazards at junctions controlled by traffic signals. Most of the new hazards are a consequence of the way that the traffic will behave when it has been given a series of commands and/or information; for example, commands that are intended to produce a smooth flow of traffic can actually increase the likelihood of accidents if they are inconsistent or inappropriate.

1.1.2 Legal issues

The growing emphasis on quality has resulted in an environment in which developers need to be both aware of, and have used, current best practice. The Courts are most unlikely to be tolerant if an accident is shown to be the result of "sloppy work". In addition there are calls for greater openness in the decision making process; in particular on regulators for greater clarity and explanation of their approaches to the regulation of risk. Good principles can be stated as [HSE 1999]:

- The targeting of action — focusing on the most serious risks, or where the hazards are less well controlled
- Consistency — adopting a similar approach in similar circumstances to achieve similar ends
- Proportionality — requiring action that is commensurate to the risks
- Transparency — being open on how decisions were arrived at and what their implications are
- Accountability — making clear, for all to see, who isaccountable when things go wrong but without resorting to unfair retribution.

1.2 A new approach

Since the early 1980s there has been substantial R&D investment to identify workable procedures for the development and assessment of computer-based safety-related systems. One result has been the publication of the International Standard on the *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems* [IEC 61508] in 1999. The Standard, whose creation was led by the UK Health and Safety Executive (HSE), has been designated a "basic safety publication" by the IEC. Although the standard originated in the process control sector and is not produced by ISO, and hence might not be considered by some to be relevant to road transport, it is intended to be applicable to all industry sectors, though they may create their own interpretation of it (an example of which is [EN 50128] for the railway sector). It should also be noted that IEC 61508 is intended for use where no sector-specific standard is in existence, and there are plans to make it a harmonised Euro-Norm (EN).

The civil aviation sector has its own set of guidelines centred on [DO 178B]. Whilst they differ in detail from [IEC 61508] the underlying philosophy is not too dissimilar.

Both [IEC 61508] and [DO 178B] start by identifying the risk associated with each hazard, and hence the degree of risk reduction necessary to bring that risk to an acceptable level. [IEC 61508] classifies this risk reduction using Safety Integrity Levels (SIL), and [DO 178B] uses failure condition categories. These define the degree of rigour that should be used to validate the correctness of the design and implementation of the safety-related electrical, electronic and programmable electronic systems that have the corresponding dangerous failure modes.

1.2.1 New forms of Assessment

The Highways Agency has also recognised the need for a change to the STA process when it issued the *Statutory Approval of Equipments for the Control of Vehicular and Pedestrian Traffic on Roads* [TRG 0500]. It is essentially a four stage process:

1. The supplier must submit a number of documents to the Approval Authority in order to obtain an “agreement in principle” to their intentions.
2. The supplier must agree a test plan for the equipment with the Approval Authority which will be used to demonstrate the conformity of the equipment to appropriate standards.
3. The equipment is submitted for test. For functional performance the supplier is permitted to self-certify. If the functional performance includes safety, the test schedule has to be agreed with the Approval Authority as part of the second stage. The Approval Authority may require to witness any of the approval tests.
4. Upon satisfactory completion of all testing, and receipt and acceptance of final documentation by the Approval Authority, the equipment supplier is deemed to have completed the approval procedure and a STA certificate is issued.

It is however unlikely that the Highways Agency, as the current Approval Authority, will have the resources to support the full working of [TRG 0500] into the future as the number of different types of equipment increase. An alternative approach, “self certification” which is gaining hold throughout Europe, does not have the support of any of the stakeholders in the UTMC arena who still want some kind of “official seal of approval”, each for their separate reasons:

- Manufacturers — to demonstrate that they have achieved compliance
- Local authorities — to guarantee good equipment
- Consultant engineers — to cover liability issues
- Highways Agency — to maintain the regulations.

Whilst STA applies to individual items of equipment, UTMC systems will emerge from the integration of many items of equipment, and the assessment of this combination has to take a different form. The Highways Agency has recently published a *Code of Practice for Traffic Control and Information Systems* [MCH 1869] to assist local highway authorities, consultants and contractors who design and implement such integrated systems. Its companion document on *System Certification* [MCH 1813] describes a mechanism for demonstrating that the Code of Practice has been applied.

However, the preliminary safety analysis of the UTMC architecture has found both Traffic Safety hazards and Human-Machine Interaction (HMI) safety hazards for the emergent properties of integrated transport systems [UTMC22 2000], as well as with the basic equipment. It also found that the degree of risk associated with the various hazards varied considerably. Whilst there are a number of guidelines on how such issues should be treated, there is currently no regulatory requirement that they should be used.

A workable formal assessment process that takes **all** these considerations into account is therefore necessary.

1.3 The Framework

1.3.1 Scope of the Framework

Earlier work in this project showed that many of the people who will be associated with the creation of UTMC systems were not familiar with the new approach to the development and assessment of safety-related computer-based systems that has been developed since the early 1980s. There is therefore a need for a document that both explains the problems and

the reasons for the solutions, since a detailed set of guidelines is not likely to be understood by many people at this stage.

There are few UTMC-like systems currently deployed and so few people have had any experience in analysing and assessing their safety properties. This Framework should therefore be read as a proposal as to how these activities might be done, rather than as a mandate for how they must be done. It is based on the current good practice used in other industry sectors, and on the results of a number of applied research projects which have been specifically considering the safety of transport telematic systems. It does not contain the details of the techniques to be performed, as these are well documented elsewhere. Instead it provides a framework as to how these techniques might be applied during the development of a typical UTMC system.

This Framework will need to be validated before it can adopted as a complete safety policy for all UTMC systems.

A summary of the key supporting documents can be found in Appendix L, which is distributed as a separate document.

In order to illustrate various issues a few examples are presented in shaded boxes, separate from the main flow of the text.

1.3.2 Intended readership

This Framework is aimed at engineers and senior engineers who will be associated with the specification, procurement and development of UTMC systems including:

- Equipment manufacturers
- System integrators
- Highway authorities
- Highways Agency (as the current Approval Authority)
- System operators.

For the engineers it will provide an introduction to the other documents which describe the detailed processes and techniques that should be used. For the senior engineers managing a project it will provide an overview of the type of work and expertise that will be necessary.

In order to ensure that the document is understandable to the intended readership, it has been produced in five stages, with reviews being undertaken by representatives of the various stakeholders.

1. A first draft was written and then reviewed by 15 persons.
2. This was followed by a workshop, attended by 23 persons, during which further comments were received.
3. A second draft was written that took account of the comments on the first draft. This was also reviewed by 5 of the original reviewers.
4. A version of the Framework was then produced that took account of these later comments and this was then reviewed by the Highways Agency.
5. The final version has benefited from its comments.

The partners in the UTMC22 project would like express their sincere thanks to all the reviewers for the considerable work that they did.

1.3.3 Target systems

UTMC systems are one set of applications that will make use of Intelligent Transport Systems (ITS). When it comes to the issue of safety it does not make sense to try and categorise a system as belonging to UTMC or not. Not only might this place *ad hoc* restrictions on what can be deployed, but the safety aspects of an application might be ignored because it is not in the list. In addition, there is a growing need for ITS to work across the urban/inter-urban boundary. Nor does it make sense to distinguish between Traffic Control Systems and Traffic Management Systems; whilst the former is normally obviously safety-related, the latter may also contain some longer term Traffic Safety hazards. It is therefore essential to consider each function in its application, and for this reason this Framework is really addressed at all ITS.

It should, however, be recognised that whilst there is no basic engineering difference between an urban traffic management and control system and an inter-urban traffic management and control system, the regulatory environment in the UK is very different. The assessment process being proposed is for UTMC systems.

1.3.4 Relationship with the Highways Agency Code of Practice

The Highways Agency *Code of Practice for traffic control and information systems* [MCH 1869], is intended to be part of the *Design manual for roads and bridges*. The Code of Practice covers all public roads except motorways, and is concerned with the safe and consistent design methodology of traffic control systems and providing an awareness of the lifecycle procedures. The final version of this document, and its companion on *System Certification* [MCH 1813], was not available for inspection until the very end of this project; it has therefore not been possible to re-organise the material in this Framework accordingly, though a number of changes have been make to the text.

The Code of Practice and this Framework are concerned with similar issues, but they approach them from different angles. Thus, whereas the Code of Practice provides the overall framework for the deployment of ITS, this Framework is concerned, in particular, with the more detailed engineering and human factor requirements of the development part of the lifecycle, and provides explanations as to why the various procedures should be performed.

Although the Code of Practice makes reference to [IEC 61508] it does not address the issue of SILs which are fundamental to its use. This Framework makes some proposals for their application to UTMC systems.

Both [MCH 1869] and, in particular, [MCH 1813] seem to be oriented towards systems whose hazards have a low level of risk. However the UTMC Technical Specification [UTMC 1997] also includes functions whose hazards will have a high level of risk. This Framework therefore includes process that may be used for the development and assessment of such systems.

1.3.5 Relationship with the National Motorway Communications System

The National Motorway Communications System (NMCS) [DMRB Vol. 9] describes how a number of individual applications, e.g. emergency telephones and automatic incident detection, should be integrated onto a single communication system. Whilst much of the

document is concerned with details of deployment, the parts that cover motorway control offices and the use of VMS for strategic traffic management take a very similar approach to the one described in this Framework.

1.3.6 Relationship with other industry sectors

This Framework follows the basic philosophy, though not necessarily the detail, that is being used in a number other industry sectors, notably process control, rail transport and civil aviation. The regulatory environments under which they operate are, of course, different but each sector needs to demonstrate that their products are safe using an assessment process. This can range from pure self-assessment, through self-certification with regular third party inspections (sometimes called “enforced self regulation”, e.g. Her Majesty’s Railway Inspectorate), and up to full third party certification during all phases of the lifecycle.

2. Management overview

This section provides a summary of the Framework for the Development and Assessment of Safety-Related UTMC Systems. It is aimed at senior engineers and/or managers responsible for specifying, procuring and manufacturing UTMC systems or components of them, and provides an overview of the tasks that may need to be done to demonstrate that a UTMC system is safe for public use.

2.1 Producing safe UTMC systems

The need to produce a safe UTMC system is obvious; how to do it economically and effectively is less so. The use of computers means that equipment may no longer be tested exhaustively, and the integration of systems may result in undesired emergent properties. During the last 10–15 years a new approach to the development of safety-related system has been developed, and is codified in [IEC 61508]. This Framework adopts the basic philosophy behind this approach, though it is presented in a manner that caters for the special needs of UTMC systems.

2.1.1 The real cost of safety

There is a perception that rigorous safety engineering of the type described in [IEC 61508] is very expensive. The modern engineering environment is extremely cost-conscious and manufacturers of every type of product or service are under immense pressure from their customers to reduce both the cost and the time-to-market. How can such pressures be reconciled with the rigorous engineering of safety-related systems? There are basically two answers.

- The creation of absolute safety is just not possible. It is therefore necessary to ensure that sufficient resources are applied without “wasting effort”. Engineering frameworks for safety-related systems such as [IEC 61508] are based on the concept of Safety Integrity Levels (SILs). Safety integrity is the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. A SIL is one of four possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related system. The use of SILs ensures that the degree of rigour necessary during the development lifecycle activities are appropriate to the degree of safety required from a system. It is therefore possible to have a level of confidence in a safety-related system being used in a particular application without having to “over-engineer”.

- Apparent cost-savings early in a project’s lifecycle can often lead to much greater expenditure later on should problems begin to appear. It is a well-documented engineering principle that the costs associated with any changes that have to be made to a system due to a problem increase dramatically as more lifecycle phases are completed. The situation is usually exacerbated when safety issues are involved.

The Framework described in this document aims to ensure that the required level of safety is built into a system from the outset. It recommends a mechanism for identifying the appropriate measures and techniques and assisting with a “right first time” design. Although

some of these measures and techniques may involve a seemingly additional cost “up front”, the potential costs of not applying them are much greater.

2.1.2 Safety expertise

A safety hazard is defined as being a physical situation with a potential for human injury. However, whilst this definition only refers to injury to humans, it is necessary to consider possible injury to property, fauna, flora, atmosphere etc. as well. Certain safety hazards are obvious, for example a green light conflict for traffic signals, but others are less obvious and are often concerned with the reason as to how an accident or conflict situation can come into existence. Past experience has led to safety being considered under the three headings of:

- Functional System Safety, which is primarily concerned with the reliability of a piece, or pieces, of hardware and/or software
- Human-Machine Interaction, which is concerned with how a human user interacts with a system via an interface
- Traffic Safety, which is concerned with the safe operation of the traffic system as a whole. It includes the ways in which a system might affect road user behaviour so as to alter the interaction between the driver, the vehicle, the road infrastructure and other road users such that they no longer use road transport in a safe manner.

This Framework is based around a combined lifecycle which shows at which stages of the development of a UTMC system, or units which are part of a UTMC system, activities are required in each of these three areas. This lifecycle reflects the growing recognition that the introduction of ITS such as UTMC is merging the boundaries between the different disciplines, though it is unlikely that the relevant expertise will be found in a single individual. In addition, there is an increasing desire in the wider safety-related systems community at the present time to formalise the competency of individuals to undertake engineering tasks during the development of safety-related systems.

On 28 January 1986 the Space Shuttle *Challenger* exploded during take-off killing all seven crew members. The subsequent Rogers Commission concluded that the root of the accident was an accumulation of organisational problems. It was critical of management carelessness, bureaucratic interactions, complacency, disregard for safety, and flaws in the decision-making process. It also stated that a properly staffed, supported, and robust safety organisation might well have avoided the communication and organisational failures that influenced the decision to launch. [Leveson 1995]

2.2 The overall approach

The basic philosophy behind the approach described in this Framework can be summarised as the three stages shown in Figure 1. This requires an understanding of the system, a knowledge of the processes and techniques needed to create it, and the ability to demonstrate, to a third party where necessary, that it has all been done correctly, all in accordance with a suitable Quality Plan. The degree of rigour with which the demonstration process must be done will increase with the severity of the hazards associated with the system.

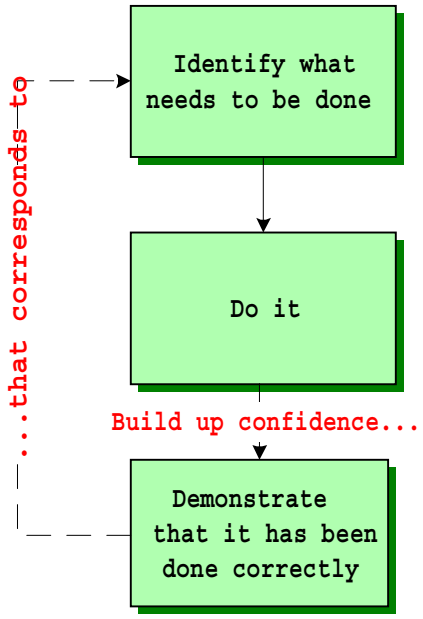

Figure 1: Philosophy of this Framework

The following sub-sections briefly describe the various activities that are necessary to assure the safety of a UTMC system. They are all described in more detail in later sections.

2.2.1 Identify what needs to be done

Prospective safety analysis is concerned with analysing the proposed scheme from the different perspectives of:

- How individual drivers, and the traffic in general, might behave
- How the users might interact with the equipment
- The safety hazards associated with the equipment itself.

These are likely to be interrelated.

The hazards have to be classified in order to discover the degree of risk reduction that is required. This exercise will ultimately determine the degree of rigour needed for the remainder of the lifecycle.

Having gained an understanding of all the safety issues relating to the scheme, a Safety Plan should be created that details how each of the safety issues is going to be resolved. This will also form part of any Certification Plan.

Once agreement for the Certification Plan has been reached the development can continue.

2.2.2 Do it

During the development phases not only must the processes be done correctly, but it must be possible to see that they have been done correctly. The evidence can only be collected during the development process; it cannot be created afterwards. The processes that will

be used to develop the system will therefore depend on the requirements of the methods that will be used to assess their correctness.

2.2.3 Demonstrate that it has been done correctly

Assessment is a fundamental part of the engineering process for a safety-related UTMC system, and it should be done in accordance with the Safety Plan. The processes of verification and validation, including tests, will be done by various different people at various different times. The objective is to build up a satisfactory justification, a Safety Case, as to why the UTMC system is considered to be safe for use by the operators and the general public. Whilst some of this work may be done in-house, if a special expertise is needed, or if the degree of rigour demands it, then an independent assessor will be required.

Once a Safety Case has been approved, the system may become operational. After this the Safety Case continues to be an important document, for example to support a legal argument after an accident, and it must be updated as changes are made to the system.

2.3 Formal assessment of UTMC systems

The present assessment regime for traffic control equipment is STA. This process is entirely adequate for assessing “simple” electromechanical systems, as it is a test-based process. However, for dealing with “complex” integrated systems that contain software, evidence of additional measures beyond testing is required to provide assurance of the safety properties.

This Framework proposes a new process for assessing “complex” UTMC systems which extends the existing process to one that is based on the Safety Plan and the Safety Case. Earlier work showed that all the stakeholders wanted to maintain the “official seal of approval” associated with STA, but this new process will also satisfy the requirements for “self certification” currently being advocated by many as the future European approach.

2.4 Costs and misconceptions

This Framework does not aim to increase the lifecycle costs of a system any more than is absolutely necessary to satisfy the current legal and societal expectations of any safety-related system. Indeed it could be argued that it actually decreases the possible total costs in the case of a safety-related failure by reducing the risk of any hazard.

Each hazard has an associated risk, and the degree of risk reduction necessary to bring it to an acceptable level is classified as a SIL. The use of SILs ensures that costs are targeted at where they are needed. Thus, whilst the preliminary safety analysis of the UTMC architecture [UTMC22 2000] has identified a number of hazards, many of the resulting SILs are at such a level that companies which already work with a quality assurance plan may find that minimal changes need to be made to their current procedures.

It should also be noted that, as specified as the moment, a SIL only has a direct effect on the development of those safety-related electrical, electronic and programmable electronic sub-systems that have dangerous failure modes that may result in the corresponding hazard(s). The remainder of the UTMC system development, for example civil engineering

construction, would proceed as normal provided, of course, that it takes account of the relevant Traffic Safety and HMI hazards in a satisfactory manner; though the SIL will give an indication as to how much thought and effort should be applied.

3. Safety issues in UTMC systems

One of the stated aims for ITS is safety, and therefore the population in general, and politicians in particular, will not expect people to be harmed as a direct result of the introduction of an ITS. Indeed it is fortunate that the infamous London Ambulance Despatch System [SWT_RHA 1993] and [Flowers 1996] has not been associated with ITS in the minds of the public, but its lessons are ignored at our peril.

> On 26 October 1992 a new telematics based ambulance despatch system for the London area became operational. The faults in the system, both technical and human factors, were such that many ambulances arrived extremely late to collect their patients. Subsequently there were claims that the system had contributed to about 20 deaths before most of it was switched off after two days

In normal usage the word safety is considered to have binary attributes: a product, or a system, is either safe or not safe. In fact, of course, nothing is absolutely safe, and every activity carries a risk of danger, however vanishingly small. The continual quest to produce safer and safer cars, aeroplanes, food, toys etc. is the destiny of all engineers, but when certain people, such as politicians, state that anything less than absolute safety is unacceptable, then it is necessary to ask them what they really mean. Any reasoned argument will demonstrate that absolute safety is just not achievable, especially in an activity such as transport which is based upon the motion of physical objects. Whilst the design of the human brain enables people to walk, or even run, without bumping into things, it is perhaps not surprising that, when the speed is increased by an order of magnitude, they occasionally make mistakes. Unfortunately the idealists cannot be ignored because the press, if not the law, tends to be on their side.

3.1 As safe as practicable

Since it is not possible to create anything that can be guaranteed never to fail, perhaps everything should just be made as safe as possible. However, if everything were in that condition then the sale of matches would be severely restricted, cafés would not be permitted to sell hot drinks, and private transport would probably be banned. Thus a strict interpretation of the word “safe” can lead to impractical, if not ridiculous, results. So what should we be aiming for?

In fact our society is prepared to accept certain risks in order to derive benefits, indeed there is almost no activity which not does have some, albeit very small, risk associated with it, even if this is rarely admitted. There is thus a requirement for activities to be as safe as practicable or, in other words a balance must be made between the benefit to be obtained and the risk associated with it. It is interesting to note that at least one country, Sweden, now has the stated objective of aiming for no road transport related deaths at all in its Vision Zero programme.

The concept of being “as safe as practicable” has been developed in the international standard on the functional safety of safety-related systems [IEC 61508] in its use of SILs to target the degree of effort needed during development onto those electrical, electronic and programmable electronic systems that have dangerous failure modes.

3.2 Safety issues

A safety hazard is defined as being a physical situation with a potential for human injury [IEC 61508]. However, whilst this definition only refers to injury to humans, it is wise to consider possible injury to property, fauna, flora, atmosphere, etc. as well. Certain safety hazards are obvious, for example a green light conflict for traffic signals, but others are less obvious and are often concerned with the reason as to how an accident or conflict situation can come into existence. Past experience has led to safety being considered under the three headings of:

- Functional System Safety
- Human-Machine Interaction
- Traffic Safety

though there is a growing recognition that the introduction of ITS is merging the boundaries between them (see Figure 2).

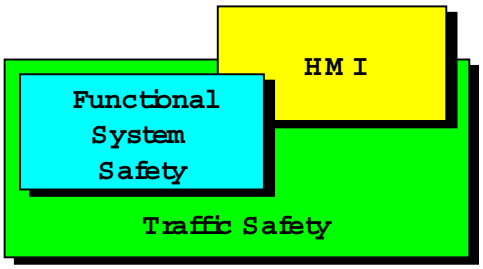

Figure 2: Relationship between the three aspects of safety

3.2.1 Functional System Safety

Functional System Safety is primarily concerned with the analysis of the reliability of a piece, or pieces, of hardware and/or software. This analysis should identify the aspects of design, operation or failure of the system that may generate malfunctions and lead to dangerous and/or unanticipated modes. In the context of ITS in general, and UTMC in particular, a system may consist of many items of equipment which may be interacting, and this interaction is one of the targets of the analysis.

3.2.2 Human-Machine Interaction

Human-Machine Interaction (HMI) is concerned with how a human user interacts with a system via an interface. The targets of analysis are normally the visual, auditory and tactile interfaces within the vehicle, at the roadside and in the control room, and their ability to be used effectively and safely. As user interactions with a system may be prolonged, complex issues such as menu and dialogue design and user under/overload are also assessed to identify potential conflicts between the system design and the behaviour of the user.

3.2.3 Traffic Safety

Traffic Safety is concerned with the safe operation of the traffic system as a whole. It covers the outcome of both Functional System Safety and most, though not all, HMI problems for the system and the user, and the malfunctions that may lead to accidents. It also covers the ways in which a system might affect road user behaviour so as to alter the interaction between the driver, the vehicle, the road infrastructure and other road users (including vulnerable road users such as pedestrians and cyclists) such that they no longer use road transport in a safe manner.

Consider a junction controlled by traffic signals.

- The equipment in general, and the correct operation at all times of the controller should be managed by an expert in **Functional System Safety**.
- The size, luminosity, location etc. of the signal heads so that they will always be interpreted correctly by the drivers should be managed by an expert in **HMI**.
- The layout of the junction, and the timing of the signals, in order to create a naturally safe driving scenario, together with any special arrangements for particular classes of vehicle, e.g. regular HGV traffic carrying hazardous goods, should be managed by an expert in **Traffic Safety**.

3.2.4 "The Safety of the System"

A fundamental issue raised by the advent of ITS is the distinction between a system and the component parts, or units of equipment, of which it is comprised. The reason why initiatives such as the UTMC programme are being introduced is that additional benefits are expected to be gained from the integration of the separate and distinct (sub-)systems. These "emergent properties" are therefore a property of the total system only, and ***not*** of the individual sub-systems, and the safety of these properties must also be considered. Each of the three subject areas described above may therefore influence the others. Safety must therefore always be treated as a system issue, and a true systems engineering approach must be taken to ensure that all the parts are considered together as well as all the aspects, or their combined behaviour.

When a kit-car first arrives it is just a "box of bits". Whilst some of the bits may perform simple functions, the one thing that the box of bits cannot do is travel on the road to the shops. This emergent property only appears when all the bits have been assembled together (correctly!).

3.2.5 Boundaries of responsibility

Whilst it may be obvious that "someone must be responsible for the safety of the system" it has not always been considered explicitly in the past for traffic control systems. The primary reason for this has been that the main safety-related traffic control equipment used so far has been the traffic signal, and its suitability can be assessed by the STA process. Even when their use has been co-ordinated, e.g. using SCOOT, the basic safety of each junction has resided in the corresponding controller. The advent of ITS, however, changes this scenario and the justification for the safety of any system, the Safety Case, will be built up with evidence from a number of different sources, and over some considerable length of

time. It is therefore necessary for there to be clear lines of responsibility for guaranteeing, and then maintaining, the safety of the system.

The deployment of a typical UTMC system is likely to involve many different organisations and companies, many of which will be doing something that has an effect on the safety properties of the system. Whilst one can expect that each one will be responsible for the safety of their own part of the system, it is important that "someone" sets up a management structure to ensure that not only do all the parts come together in a coherent fashion, but that the safety properties of the system are considered holistically as well. The current tendency to rely on many specialist sub-contractors during a deployment only serves to exacerbate the problem whereby something might "fall between the cracks". See also Sections 4.3 and 5.1.1.

3.3 The assessment process

One particularly important feature of this "new" approach, and one that is followed by other recent standards e.g. [DO 178B], is that each new function or system must be considered on its merits within the chosen application. Thus if the same function or system is to be used in two or more different applications then its use in each application must be analysed separately in case the safety implications vary (see also Section 7.3.1). It is for this reason that this Framework does not contain a list of possible functions or systems, together with their safety requirements. Whilst this approach is different to that taken by STA, where each system can only be used in a limited range of applications, it does handle the additional issues that emerge when equipment is integrated and re-used in a variety of complex applications.

4. Lifecycles for safety-related UTMC systems

The word “system” can be used in many senses, and it is important to be able to distinguish between them. Figure 3 shows that a typical UTMC system may be built up from a variety of units. Each unit performs one or more functions, for instance a Global Positioning System (GPS) navigation system, and may be used in more than one application, for example route guidance or hazardous goods monitoring. Some units may be fully Type Approved, such as a traffic signal controller, some may be available in the general market place, such as a computer system, and some may be specifically designed for the application. A (large) manufacturer may offer such a UTMC system as a market package. When a city purchases and installs such a system, a number of parameters will have to be set in order to satisfy the constraints of the city environment, and it then becomes a unique deployment of that system. It is essential that a developer or system integrator is aware of these distinctions, and hence the assumptions that have already been made for a given unit or system, and that need to be made for a given deployment.

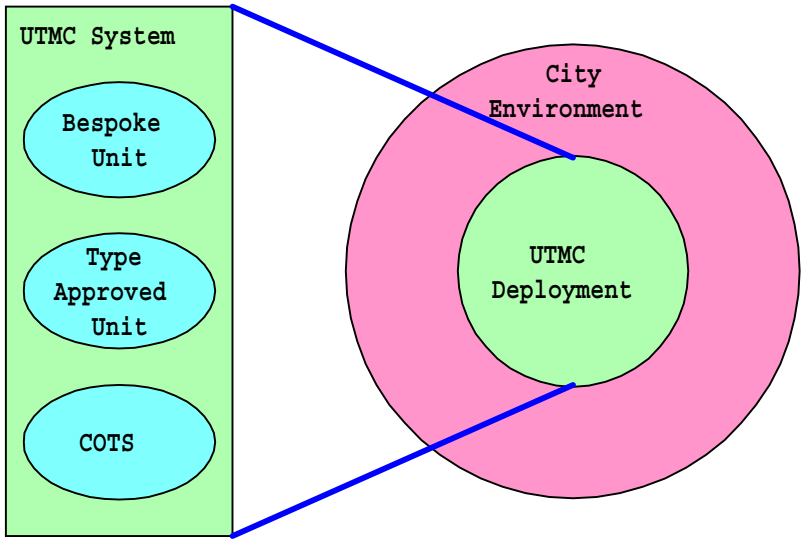

Figure 3: System and deployment

In order to clarify when certain tasks should be done it is common to refer to a system lifecycle. However, the problem with any lifecycle diagram is that it will always be an approximation to what happens in practice. It is with this warning that we present Figure 4, for the development of an integrated system, and Figure 5, for the development of its constituent sub-systems, or units. These figures attempt to highlight all the important stages associated with the tasks that assure the total safety of the final system. The rectangles, briefly described below, show the various phases that are often seen in a system lifecycle. The ellipses contain the tasks that need to be performed during these phases to assure the safety of the final system, these are described briefly below and then in more detail throughout the remainder of the Framework. It should also be noted that expertise on three different aspects of safety are needed at various stages, as described in Section 3.2, and that it is unlikely that this expertise will all be found in one individual person.

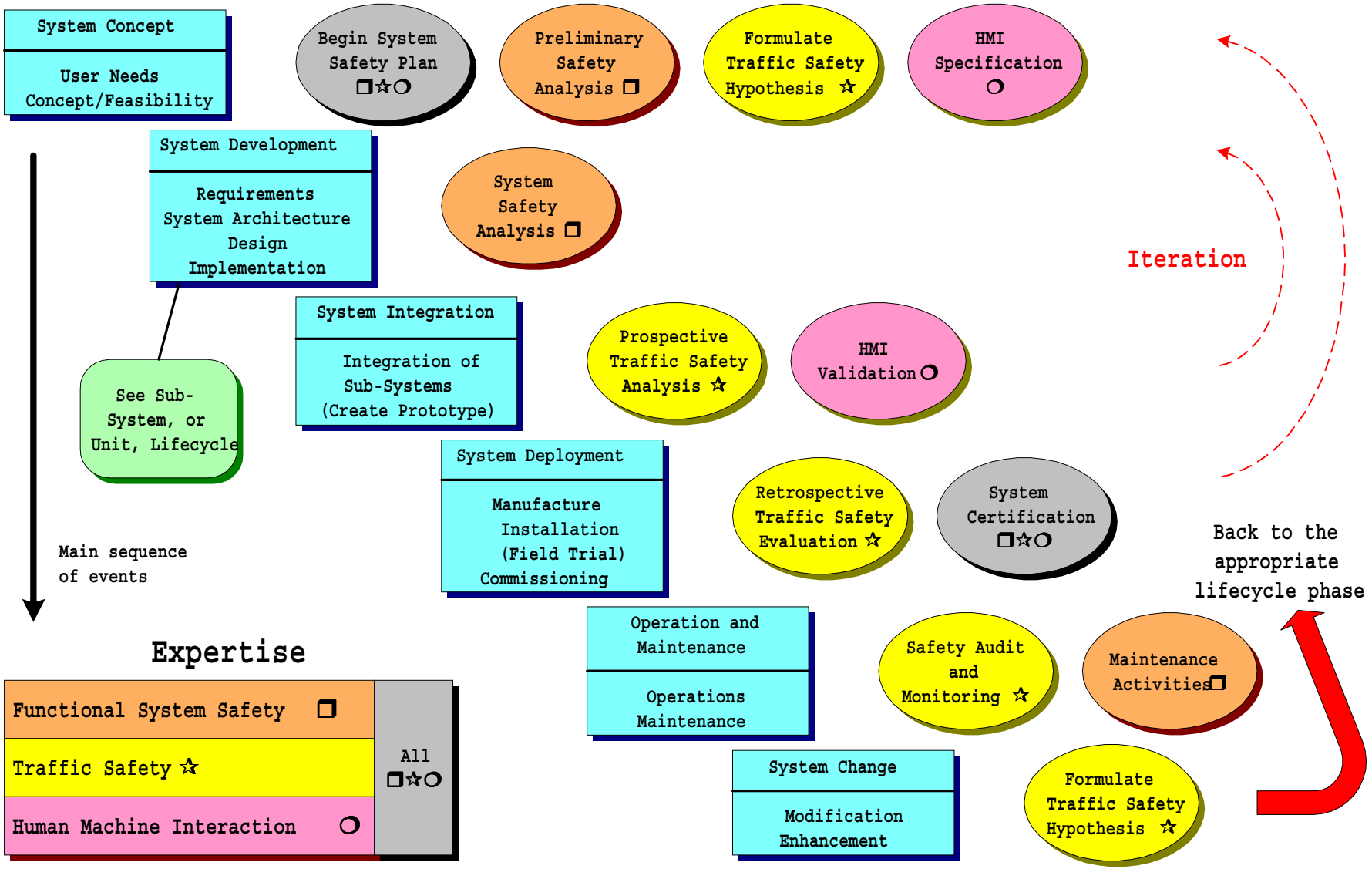

Figure 4: Lifecycle for the safety of a UTMC System (if possible, this diagram should be viewed in colour)

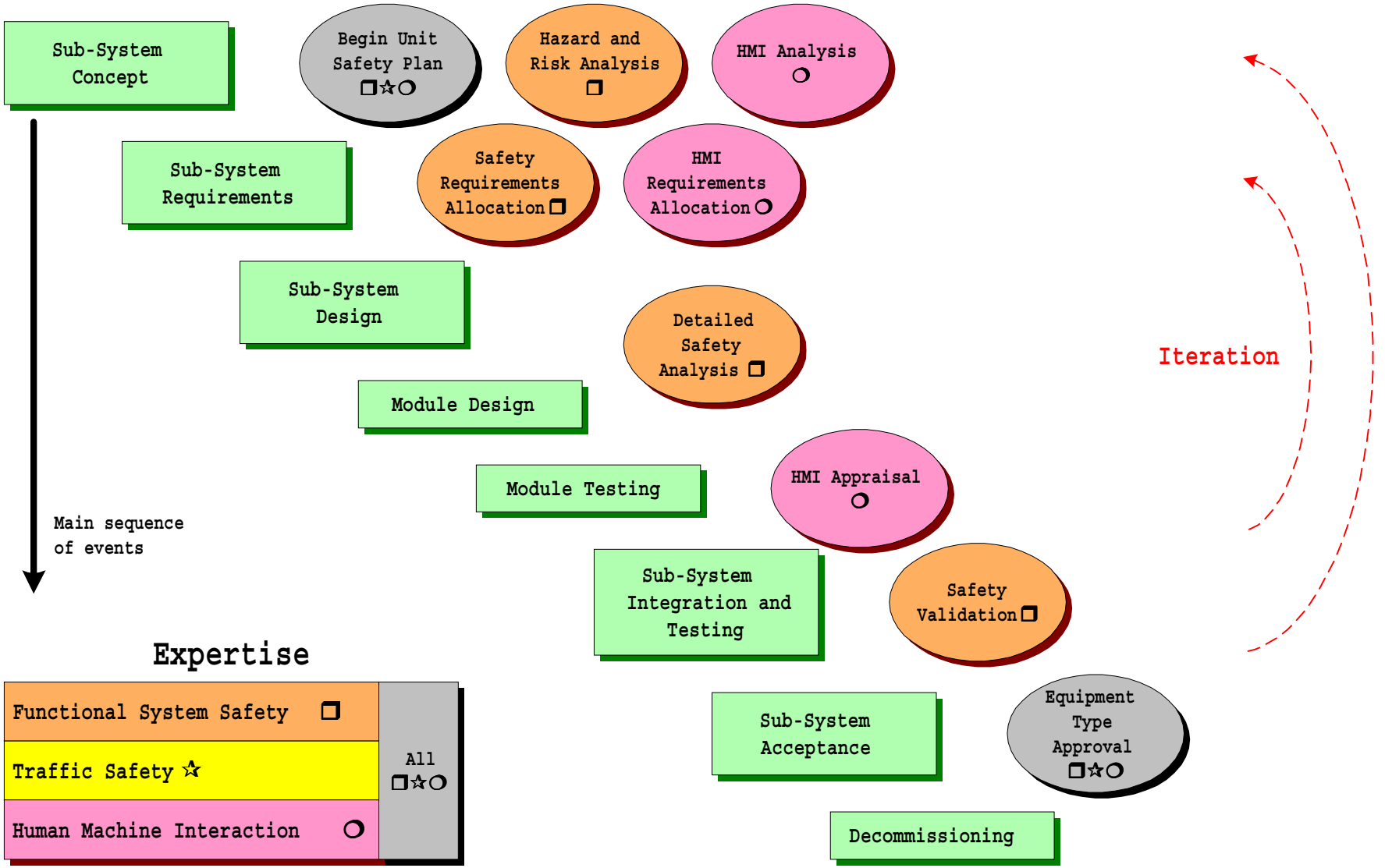

Figure 5: Lifecycle for the safety of a sub-system, or unit (if possible, this diagram should be viewed in colour)

The remainder of this Framework is centred on the extra tasks that are needed to assure the safety of a UTMC system, and whose titles are given in the ellipses. A brief explanation of each task is given below. The tasks associated with formal safety assessment are all described in more detail in Section 7. Section 5 describes the safety-related tasks that should be performed as part of the lifecycle of a system (Figure 4), and Section 6 covers the safety-related tasks for the sub-system, or unit, lifecycle (Figure 5). The titles in each ellipse will all be found as sub-section headings.

4.1 Lifecycle phases for an integrated system

In order to avoid any confusion the following meanings have been assigned to the lifecycle phases of an integrated system. It should be noted that, whilst the phases must be performed in the basic order shown going down the page, in practice it will be necessary to "jump back" to an earlier phase on many occasions, and it is for this reason that neither Figure 4 nor Figure 5 contain any arrows between the boxes.

- **System concept**
  - *User needs*: The collection of desirable attributes from the various categories of potential user of the system
  - *Concept/feasibility*: "I have an idea for how to satisfy the user needs for the system and I want to see if it is sensible and feasible"

- **System development** — see also Section 4.1.1
  - *Requirements*: The systematic collection of all the functional and non-functional features that the system must possess
  - *System architecture*: The high level structures of a class of systems that will satisfy the requirements
  - *Design*: The detailed and deterministic statements on how to create the system
  - *Implementation*: The creation and testing of the various individual units, or sub-systems, of which the system is to be comprised

- **System integration**
  - *Integration of sub-systems*: The combining of the individual units, or sub-systems, into the full system, and the confirmation that it functions and behaves correctly
  - *(Create prototype)*: The first one or more systems may be created as prototypes with which to perform off-road tests to confirm the validity of the design (this phase is normally only necessary when a new type of system is being developed)

- **System deployment**
  - *Manufacture*: The creation of multiple copies of (usually) the same unit
  - *Installation*: The process of setting up the system in its final location
  - *(Field trial)*: The process of performing trials (usually) on the "first of a kind" (this phase is normally only necessary when a new type of system is being developed)
  - *Commissioning*: The process of establishing that the installation complies with all statutory regulations, and contractual agreements

- **Operation and maintenance**
  - *Operations*: The normal day-to-day functioning, and management, of the system
  - *Maintenance*: The activities which are necessary to keep the system operational, e.g. to prevent a failure from occurring, or the repair of failed components

- **System change**
  - *Modification/enhancement*: The process of changing the system, normally by the addition of new equipment and/or functions, so that it is no longer the same as before.

4.1.1 Lifecycle phases for a unit or sub-system

- **Concept**: "I have an idea for how to satisfy the user needs for the unit or sub-system and I want to see if it is sensible and feasible"

- **Sub-system requirements**: The systematic collection of all the functional and non-functional features that the unit or sub-system must possess

- **Sub-system design**: The detailed and deterministic statements on how to produce the sub-system using one or more modules

- **Module design**: The detailed and deterministic statements on how to produce the modules

- **Module testing**: The testing of the modules against the sub-system requirements

- **Sub-system integration**: The combining of the individual modules into the full unit or sub-system, and the confirmation that it functions and behaves correctly

- **Sub-system acceptance**: The process of establishing that the unit or sub-system complies with all statutory regulations, and contractual agreements

- **Decommissioning**: The process of removing and then disposing of a unit or sub-system.

4.2 Lifecycle phases to assure the safety of a system

Safety, like quality, cannot be added onto a system after it has been produced, it must be built in from the beginning. In order to ensure that the all the safety-related tasks are performed correctly the UTMC system development and deployment should be undertaken under a formal Quality Management system, e.g. [ISO 9000]. The basic philosophy of this Framework, which is summarised in Figure 6, is that not only must there be an understanding as to what needs to be done but, once it has been completed, there must also be a demonstration that it has been done correctly. This demonstration must be performed with a degree of rigour that will provide the necessary confidence in the safety of the final system.

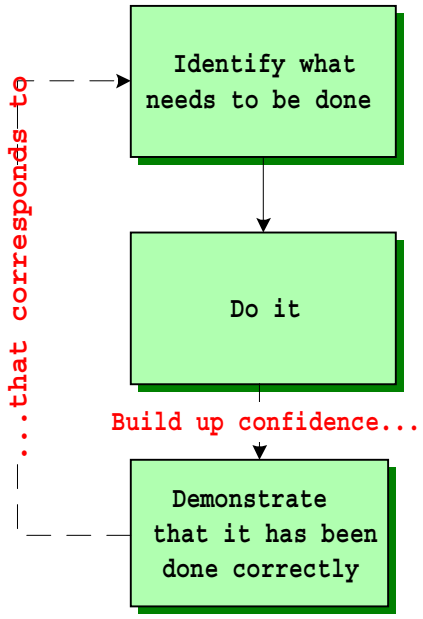

Figure 6: Building confidence

The following sub-sections provide an overview of the processes that should be performed to assure the safety of an ITS. These processes are described in more detail later in the document. Whilst the sub-sections indicate the areas of expertise that will be needed to perform the detailed work, the needs of each expert should be understood by the others, and there should be regular communication between them.

4.2.1 Safety planning and assessment

In order to be able to demonstrate the safety of the final system a plan must be made so that the correct tasks are undertaken from the beginning.

- **Begin System Safety Plan**: The process of creating a plan as to how the safety of the system will be assured. This plan should be continually reviewed and modified as further information is obtained

- **Begin Unit Safety Plan**: The process of creating a plan as to how the safety of the sub-system or unit will be assured. This plan should be continually reviewed and modified as further information is obtained

- **Equipment STA**: The process of approving a unit or sub-system for use in a limited range of applications

- **System Certification**: The process of approving a specific installation in a specific application.

4.2.2 Functional System Safety

In order to assure the Functional System Safety of an ITS there should be a number of processes to identify the safety hazards, decide how to mitigate them, and then to demonstrate that this has been done satisfactorily.

- **Preliminary Safety Analysis**: The process of finding the safety hazards that are associated with the system concept, and the safety requirements needed to mitigate them

- **System safety analysis**: The process of analysing the design, especially the interactions between the various individual units, or sub-systems, of which the system is to be comprised

- **Maintenance activities**: The process of performing the actions that are necessary to keep the system functioning correctly

- **Hazard and risk analysis**: The process of identifying hazards directly associated with the unit or sub-system, or that propagate to becoming a hazard of the system

- **Safety requirements allocation**: The process of allocating requirements to mitigate the effects of any safety hazard.

- **Detailed Safety Analysis**: The process of analysing the detailed design, both to identify any further safety hazards, and to demonstrate that design measures exist to mitigate all the safety hazards

- **Safety validation**: The process of confirming that all tests and other processes have been performed to demonstrate that all safety hazards have been mitigated adequately.

4.2.3 Human-Machine Interaction

Human factors design and development targets should be defined for the HMI aspects which can then be used as benchmark criteria in establishing the success or failure of a system during its development.

- **HMI specification**: The process of analysing the human factors issues associated with planned use of the system, and the expected ability of the users

- **HMI validation**: The process of confirming that the desired HMI performance has been achieved

- **HMI analysis**: The process of analysing the human factors issues associated with planned use of the unit or sub-system

- **HMI requirements allocation**: The process of specifying the HMI attributes of the unit or sub-system

- **HMI appraisal**: The process of testing a prototype to confirm that the desired HMI performance has been achieved.

4.2.4 Traffic Safety

The proposed solution to a traffic problem should be checked to ensure that it does not bring additional safety hazards, and the final installation(s) should be monitored for any unexpected effects.

- **Formulate Traffic Safety hypothesis**: The process of planning a solution to a traffic problem and assessing the safety hazards that might be associated with it

- **Prospective Traffic Safety analysis**: The process of performing small scale off-road trials on prototypes or facsimiles (e.g. driving simulators) of the system in order to confirm, or otherwise, the basic hypothesis

- **Retrospective Traffic Safety evaluation**: The process of performing full "before and after" field trials on the fully deployed system, usually when it is the "first of a kind", in order to assess the safety and other benefits

- **Safety audit and monitoring**: The process of verifying that a specific installation is correct, and then monitoring the system for a long period of time in order to identify any long term problems or unexpected effects.

4.3 Rôles and Responsibilities

Figure 4 and Figure 5 indicate that there are a number of tasks that need to be performed in order to assure the final safety of an ITS; and that a variety of expertise is needed which is unlikely to reside in one individual. They also indicate that in order to create a full ITS (Figure 3) there are likely to be a number of sub-systems or units. The final safety of the ITS is therefore going to be the result of work carried out by a variety of people over a length of time. Thus, not only must this work be co-ordinated in a satisfactory manner but, whenever a manufacturer produces a commercial off-the-shelf (COTS) sub-system, or unit, then sufficient information must be made available to the system integrators.

The overall responsibility for the safety of the final ITS must be allocated to one named person, the Safety Manager, who will co-ordinate all the activities according to a formal Safety Plan (see Sections 5.1 and 7.2). Each of the phases shown in Figure 4 and Figure 5 must be considered, and the tasks allocated to competent personnel; indeed the *Guidelines for the Safety Audit of Highways* states: "The rôles and responsibilities of all those concerned … should be specified in clear terms of reference. This may be either a standard document or one developed for a specific scheme" [IHT 1996]. Rôles include client (highway authority), project manager, manufacturer and auditor. It is often necessary to seek external and independent advice, in particular during a safety evaluation. In the case of sub-systems or COTS units it is normal practice for the relevant manufacturer to be responsible for the safety of that item.

4.3.1 Competence of persons

Whilst it is obvious that all personnel performing one of more of the tasks that will ensure the safety of an ITS should be competent, there are currently few people who can demonstrate that competence in an obvious manner. The main reason for this is that many of the techniques and methodologies that are now recommended have only been available for a few years, and few people have the experience of using them so far. It is therefore

important that the Safety Manager ensures that all the key personnel are both aware of the new features, and problems, associated with the advent of ITS, and that they have received suitable and adequate training in how to deal with them.

It is also important that a "safety culture" pervades all the organisations associated with the development of any safety-related system. Whilst it will be the responsibility of the Safety Manager to see that such a culture exists, they cannot do this effectively without the backing of senior management, and all the Authorities and Government Agencies associated with the creation of any ITS.

With the support of the Institution of Electrical Engineers (IEE) and the British Computer Society (BCS), the HSE has been funding a study on the competencies necessary for those working on safety-related systems. This has now been published [IEE 2000], and states that "all personnel dealing with safety-related systems including purchasers, operators and maintainers as well as designers and implementers should be competent to perform the tasks assigned to them. Competence requires all practitioners to have qualifications, experience, and qualities appropriate to their duties. These include:

- Such training as would ensure acquisition of the necessary knowledge of the field for the tasks which they are required to perform
- Adequate knowledge of the hazards and failures of the equipment for which they are responsible
- Knowledge and understanding of the working practices used in the organisation for which they work
- The ability to communicate effectively with their peers, with any staff working under their supervision, and with their supervisors
- An appreciation of their own limitations and constraints, whether of knowledge, experience, facilities, resources, etc., and a willingness to point these out.

Professionals with the responsibility for design or for supervision of operators may be expected to have in addition:

- A detailed working knowledge of all statutory provisions, approved codes of practice, other codes of practice, guidance material and other information relevant to their work; an awareness of legislation and practices, other than these, which might affect their work; and a general knowledge of working practices in other establishments of a similar type
- An awareness of current developments in the field in which they work."

The enquiry into the London Ambulance Despatch System [SWT_RHA 1993] and [Flowers 1996] found that the main contractor used to develop the system had no previous experience of developing similar systems, let alone safety-related systems. The company had been chosen primarily on the basis of the price for which they had offered to do the work.

4.3.2 Training

It is clearly a requirement for operating a safe UTMC system that all the relevant staff are suitably qualified. Staff need to have appropriate skills and competencies, and the organisations involved need to ensure that there are appropriate procedures in place to provide those skills and competencies. There is no specific qualification in UTMC operation for which individuals can be certified, but there are arguments for creating such a

competence. Certainly it is incumbent on system operators to ensure that their staff are appropriately trained. Additionally, it should be pointed out that training is not merely a question of providing a background competence. Lack of training in system-specific operating procedures for emergencies was one of the factors that exacerbated the Channel Tunnel fire. Such training should be provided on a regular basis to ensure that emergencies are handled, as much as possible, on a proceduralised basis. Appropriate training should also accompany system modification. Here best practice would suggest that operating staff be involved in the design process, for instance as regards control room layout. Simulated prototypes of a new system, enabling operators to actually "use" the new system have been shown to be helpful in the design of air traffic control systems. Whilst a new system is being installed, and before it goes live, it is vital that staff be given "hands-on" training in its operation. Feedback from such testing and training should be used to improve the operating procedures.

The enquiry into the Channel Tunnel fire in 1996 found that "the number and complexity of the existing procedures and insufficient training of the Rail Control Centre Operators led to errors and delays in the implementation of the necessary actions." Recommendation 17 of the enquiry was: "… must improve the training of all … staff in relation to the management of emergencies and develop a structured and practically based training programme to cover these needs." [CTSA 1997]

5. Lifecycle for the safety of a UTMC system

This section describes the safety activities that should be undertaken during the development of an integrated ITS from a number of sub-systems, or units. It expands on each of the safety activities shown in Figure 4. The safety activities associated with the development of an individual sub-system, or unit, are described in Section 6.

5.1 Begin system safety plan

Safety cannot be added afterwards, nor will it happen by accident; it must be designed into the system from the beginning. In addition, in order that the system may be assessed successfully (see Section 7) certain information must be produced that can only be created at specific points in the lifecycle, and not retrospectively. A Safety Plan is therefore essential (see also Section 7.2).

A Safety Plan contains all the activities that need to be undertaken to assure the safety of the final UTMC system, when these activities should be done, and who is responsible for ensuring that they have been done. The detailed contents will be an application of this generic Framework for a specific UTMC system, and should contain:

- The objectives and scope of the plan
- A description of the management structure, including responsibilities, and interfaces for all safety-related activities
- The (safety-related) management and technical tasks to be undertaken, and how issues will be resolved
- The establishment and maintenance of the Hazard Log (all the details pertinent to each hazard)
- The identification of the measures to be imposed on sub-contractors to ensure that they are aware of their responsibilities.

The responsibility for producing and maintaining the Safety Plan resides with the Safety Manager of the project. The document itself will not be static, but will be expanded to reflect new information when it has been obtained. A particularly important milestone will be when the Preliminary Safety Analysis (see Section 5.2) has been completed and the SIL(s) of any safety-related units have been identified (see Appendix C), since this will determine many of the future activities that will be necessary, their degree of rigour, and hence the competencies needed of the personnel undertaking the work (see Section 4.3.1). The existence of the Safety Plan, and the style of its contents, will help to foster the safety culture for the entire project.

5.1.1 Boundaries of responsibility

It is not the task of this Framework to specify how responsibility for safety should be allocated in any given situation, but to point out that unless some individual has the overall formal responsibility for the safety of a system, and knows that he or she has it, then some aspect may get overlooked. Consideration must be given to safety during all phases of the lifecycle, and thus it is quite likely that certain aspects will be delegated for certain periods of time. This is perfectly acceptable provided it is done in a logical and planned manner.

Experience of complex systems has shown that far fewer problems occur if the basic structure of a system follows the basic structure of the management activities needed to run it. This also applies to the development process. The reason for this is that when the structures are similar, the management boundaries of responsibility coincide with logical sections of the system, or phases in the lifecycle.

The allocation of responsibility should be documented in the Safety Plan (see above) and/or the Safety Case (see Section 7.4.3). Whenever an aspect of safety is delegated to another organisation the precise boundaries of responsibility should be included in the contract, which must also ensure that the responsibility remains extant for the necessary time; for example, for a potential legal claim under the Consumers' Protection Act 1988, this may be forever. Particular consideration must be given to those situations where the safety associated with a single item of equipment may be divided, for example the setting of the timing stages for traffic signals, and their basic safety protection system (for instance green light conflict detection).

On 4 June 1996, the maiden flight of Ariane 5 ended in a failure. Only about 40 seconds after initiation of the flight sequence, at an altitude of about 3700 m, the launcher veered off its flight path, broke up and exploded. The failure was traced to a fault in the guidance system which consisted of a number of identical units operating in parallel. These units were based on those that had been used successfully on the Ariane 4 launchers, and were supplied according to specification. However they were never tested with Ariane 5 trajectory data, and when other Ariane 5 tests were performed, they were only ever represented by their simulated output. The report concluded that "close engineering co-operation, with clear cut authority and responsibility, is needed to achieve system coherence, with simple and clear interfaces between partners" [Ariane 5].

5.2 Preliminary Safety Analysis

During the early stages of a project it is important to identify as many of the issues associated with the proposed system as possible, in particular those associated with safety. There are both good financial as well as good engineering reasons for this, since experience during the DRIVE II project PASSPORT showed that many of the transport telematics projects being advised at the beginning of the programme only had a very tenuous idea of what it was they were intending to do. It is also essential that a system should be assumed to be safety-related until it has been shown not to be so, because some hazards are not immediately obvious.

Thus one of the first actions that should be undertaken at the beginning of any project is the performance of a Preliminary Safety Analysis (PSA), sometimes called a Preliminary Hazard Analysis. Whilst techniques do exist for performing a Preliminary Hazard Analysis on the design of a system, e.g. [Def Stan 00-58], the DRIVE II project PASSPORT developed a particularly effective technique for performing a PSA on any ITS as part of a feasibility study during the concept phase. A brief overview of the methodology is given in Appendix B, but the reader is referred to [PASSPORT 1995a] for a full description. The objectives of this process are to:

- Understand the system concept
- Model the system concept and identify the system boundary
- Identify the top level hazards

- Identify the top level safety requirements
- Identify the Safety Integrity Level(s) — see Appendix C.

Whilst this technique is oriented towards the identification of ”Functional System Safety” hazards, since it is based on a purely functional model of the system, it is also possible to identify some “Traffic Safety” and HMI issues as well. However, it must be noted that the PASSPORT technique is unlikely to identify all Traffic Safety and HMI issues, and therefore the tasks described in Sections 5.3 and 5.4 must be performed as well.

The enquiry in to the London Ambulance Despatch System [SWT_RHA 1993] and [Flowers 1996] found that “there had been no attempt to foresee fully the effect of inaccurate or incomplete data available to the system”, e.g. vehicle status/location. Indeed the success of the design would have depended on “the near 100% accuracy and reliability of the technology in its totality”.

The hazards found during the PSA of the UTMC Technical Specification [UTMC22 2000] include that if the messages on VMS cannot be read to be understood easily then they will be a distraction to the driver. They should also provide consistent information when a number are being used in an integrated system. The potential severity of the hazard increases when VMS are used to provide commands to drivers rather than advice or information.

5.3 Formulate Traffic Safety hypothesis

A main task during the concept phase is the formulation of Traffic Safety hypotheses about the system. These hypotheses, which need to take into account the complexities of human behaviour, will help to indicate whether the system is likely to be beneficial or harmful to safety, and will help to guide the subsequent Development and Deployment phases by providing a focus for the “prospective” and “retrospective” evaluations to be conducted.

The *Guidelines on Safety Evaluation of Transport Telematics Systems* [CODE 1998a], developed in the European project CODE, provide guidance on hypothesis formulation. They identify ten main areas in which an ITS can affect Traffic Safety (in addition to those which can occur as a result of system safety problems). They are:

1. Direct effects of an in-vehicle system on the user (modification of the driving task).
2. Direct effects of a roadside system on the user.
3. Indirect behaviour modifying effects of the system on the user.
4. Indirect behaviour modifying effects of the system on the non-user (imitating effect).
5. Modification of the interaction between users and non-users (including vulnerable road users).
6. Modifying accident consequences (e.g. by improving rescue).
7. Modifying exposure (frequency and/or length of travel).
8. Modifying modal choice.
9. Modifying route choice.
10. Modifying speed choice.

For each of these “areas”, the CODE Guidelines provide:

- a short description of the area — how can it influence safety

- systems that are likely to have such an effect — the classification of systems is based on the CORD list of functions [CORD 1994].

Areas (1) and (2) include HMI effects, the former from an in-vehicle system and the latter from a roadside system. These "areas" are intended to serve as reminders of the effects that ITS ***may*** have, not as a list of effects that they ***will*** have. Judgements about whether a particular effect is likely for a given system will have to made on the basis of:

- Knowledge of the system — the more detailed the specification, the easier it is to make an assessment
- Expert judgement
- Past experience.

In many cases it will not be possible to come to conclusive judgements until later phases. Thus in order to ensure the safety of the final system one should be conservative at this phase, and include for further examination effects that are possible, in addition to those that are probable. It is worth noting that many ITS have failed to come to market, or failed to succeed in the market, because of inadequate consideration of potential effects at the concept phase. Alternative versions could have performed far better if there had been a more systematic approach.

5.4 HMI specification

UTMC systems, like many other complex systems, are a combination of components and functions that, when combined, are intended to fulfil a certain target goal. If human beings are part of such a system then it is important that the design of the system takes account of the abilities and limitations of those humans. Most appropriately, this should be in the form of identifying the human rôles and responsibilities within the overall system, and defining how the humans will interact with the system and what the outcome should be. An analysis such as this should aid the definition of the HMI requirements for the *equipment* and, if relevant, for the *environment* where the interaction will occur. If the system design does ***not*** give relative importance to these aspects at the system concept phase then human related performance deficiencies may be built into the system. As a result HMI errors may be generated and the overall performance and safety of the system may be jeopardised.

Human factors issues should therefore be considered carefully at the system concept phase to ensure that adequate account is taken of the human users and/or operators within the system. This should include consideration and analysis of the following aspects for system concept definition:

- Overall rôles and responsibilities of all users and operators
- Assumed capabilities of those users/operators
- Assumed outputs of the system to users/operators
- Assumed range of inputs from users to the system and responses to system outputs.

As a result of carrying out these assessments the HMI should be specified in terms of:

- Functional description, and design requirements for equipment, for all human interactions with the system
- Range of environments under which interaction will occur
- Required level of *performance* of the interaction/interface.

It is important that at this stage in the system concept definition that both assumptions and specifications are defined and agreed by the system design team and, if appropriate, the Approval Authority and/or the end-user(s) or customers. Assumptions by the system designers about human rôles and reactions for any defined system may not be shared by the end-user or customer, and therefore this process should attempt to identify any mistaken assumptions concerning the system's eventual use. It is also important that the physical and environmental characteristics are defined in this process. This should have a direct effect on the specification of equipment characteristics necessary to implement the interaction/interface. In defining such a specification it is important that it is also related to measurable targets for the system developers. If this is achieved then it is possible to utilise such targets as benchmarks for subsequent assessments within the system's development.

As there are potentially a wide diversity of types of UTMC systems, and a wide range of potential human involvement in interfacing with these systems, further guidance is given on issues for UTMC assessment in Appendix A.

Overall the HMI assessment at the System Concept phase should help to refine a concept that takes appropriate note of the human abilities and needs. It should also specify the characteristics and requirements for the human interface aspects of the system. These can then form the basis for future assessment and review as the system design develops. These targets should therefore be expressed in such a manner as to allow later investigations into system performance to be carried out at validation and appraisal phases.

> The enquiry in to the London Ambulance Despatch System [SWT_RHA 1993] and [Flowers 1996] found that "staff, both within Central Ambulance Control (CAC) and the ambulance crews, had no confidence in the system and were not fully trained. The physical changes to the layout of the control room … meant that CAC staff were working in unfamiliar positions."

5.5 System safety analysis

There are many ways in which a system might produce a safety hazard. The most obvious is when a person is put into sudden and immediate physical peril by an item of equipment failing to operate in a safe manner, for example a green light conflict at a set of traffic signals. However there are other, sometimes more subtle, ways in which a system creates an unsafe situation which can build up over a longer time frame, for example a traffic control system that creates anger and frustration for the drivers, or an information system that provides incorrect or misleading data (such as for route guidance). These latter failure modes do not appear in simple systems with short cycle times but many ITS, in particular UTMC systems, will be operating continuously and controlling a large number of separate items of equipment in a manner that may never repeat. It is therefore necessary to consider the safety hazards that may result from the emergent properties of the system, as well as the specific hazards associated with any equipment of which it is constituted.

> In December 1998 a German couple, out for a holiday drive near Berlin, ended up in a river. Their automatic route guidance system indicated that they should cross the river over a bridge, but since it was dark and raining they did not see that the crossing should actually have been undertaken using a ferry.

A current issue in standards is that of “simple” versus “complex” systems. It is covered in IEC 61508, although the most straightforward definition is found in [Def Stan 00-54]. In general “complexity” refers to the degree to which a system or component has a design or implementation that is difficult to understand and verify. The following definitions are adopted in this Framework, based on those in [Def Stan 00-54]:

> **Simple**: a system may be classified as “simple” if its design is suitable for exhaustive simulation and test, and its behaviour can be entirely verified by exhaustive testing.
>
> **Complex**: a system is classified as “complex” if its design is unsuitable for the application of exhaustive test, and therefore its behaviour cannot be verified by exhaustive testing.

5.5.1 Systems engineering and system architecture

“Systems engineering is an interdisciplinary approach and means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem … Systems engineering integrates all the [relevant] disciplines and speciality groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs.” [INCOSE]

The European Telematics Application project CONVERGE-SA considered a systems engineering approach to ITS and has shown how a system architecture can be described using three levels of abstraction [CONVERGE 1998a]. The Level 3 and Level 2 architectures contain the top-level assumptions about the system, in particular the laws, rules, and command and control structures under which the system will operate. The primary functions and sub-functions are identified and organised in a working and workable manner such that these assumptions hold, any conflicts are resolved, and the desired emergent properties are recognisable. Level 3 and Level 2 architectures may be written as a Reference Model and/or an Enterprise Model [ISO 10746], the latter being particularly appropriate to describe the commercial and/or business relationships between the various enterprises or authorities within the system. The Level 1 architectures describe the overall structure of the system in terms of the relationships between the various functions and physical units such that they will produce a working system and exhibit the properties defined in the Level 3 and Level 2 reference model(s). See Appendix F for a further discussion on this subject and how safety issues can be considered.

The London Stock Exchange spent £400M in the development of Taurus, an automated stock transaction system. The entire project was scuttled after it became clear that the system was unlikely ever to satisfy its requirements; its complexity had grown beyond manageability. Much of the criticism centred on the system integration [Neumann 1995]

5.6 Prospective Traffic Safety analysis

Traffic Safety work in the System Integration phase allows the hypotheses raised in the Concept phase to be addressed and should provide assurance that the system finally

delivered for a full-scale field trial will be as safe as reasonably practicable. Work here will often be iterative as modifications are made to the system concept or design, and it may be necessary to re-test the system, or elements of the system. Normally the work will be carried out in the laboratory and/or at an off-road test site. Laboratory work may include trials with users, trials with operators, simulations and so on.

The relevant guidelines have been developed at a European level. The HOPES *Framework for Prospective Traffic Safety Analysis*[1] [HOPES 1993a] provides information on a variety of tools and techniques that can be applied in laboratory and off-road tests. It also discusses how these tools might be applied to one system that is highly relevant to UTMC, namely variable message signs (VMS).

The CODE Guidelines [CODE 1998a] also further expand on how the hypotheses raised at the Concept phase should be addressed in terms of specific tests. The section on Urban Traffic Management Systems (in fact defined as "urban traffic management and information systems") is of particular relevance to UTMC. Both roadside and in-vehicle information to the driver is covered. Particular attention is paid to issues of behavioural adaptation, that is, how road user behaviour might be modified through use of the system.

An appendix to these Guidelines provides advice on experimental design. This is necessarily brief (there is obviously a huge literature on this subject) but there is a special focus on the Poisson process, (the statistical distribution that is normally applied to indicators of safety such as accidents or conflicts).

Among the most significant tools and techniques to apply at this stage are:

- Simulators (including driving simulators) which allow the observation of behaviour under near-real but controlled conditions. Simulators are often combined with the use of rapid prototyping tools to create "working" versions of an ITS while the real versions are under development. This approach can be used to study alternative versions of a system.
- Modelling tools such as traffic assignment models (e.g. to study the effect of a new system on traffic flows) or micro-simulation models (e.g. to study more detailed or more complex behavioural effects of a new system). Micro-simulation could be used, for example, to study traffic flows and disturbance with and without a ramp-metering system.

It is sensible to seek expert advice on suitable methods and metrics for this phase of development. Well-structured work here will help to prevent unanticipated consequences later.

5.7 HMI validation

HMI validation may be defined as the process of confirming that the desired HMI performance for the system has been achieved. As stated in Section 5.4, the HMI attributes of the system should have been defined in the following form:

- Functional description and design requirements for equipment for all human interactions with the system
- Range of environments under which interaction will occur

[1] The term "prospective" is used in the HOPES Framework to indicate analysis during the System Integration phase; the term "retrospective" being applied to the more traditional before and after evaluation carried out on real roads during field trials.

- Required level of performance of the interaction/interface.

For each of these specified system performance targets ideally there should be clear and unambiguous methods of measurement and assessment to establish whether the system under development is yielding the HMI performance required. Such a performance may be expressed in a range of terms specific to the particular system under development and assessment. The methods of measurement used to establish system compliance with target performance goals are therefore important to achieve success. While general safety and usability assessment methodologies are under development for use in design and development of systems, standardisation of these methods is not yet achieved. However some published material is available [e.g. Green 1994, Hale *et al* 1990] related to systems development.

Further consideration of HMI analysis also occurs at sub-system level where the performance of the sub-systems, or units, of the system are assessed separately (see Section 6.3). Supporting discussion to this concept is also given in Appendix A.

The design of in-vehicle devices (HMI) to provide the driver with information and communications is an area of particular concern in relation to potential driver distraction. In order to guide the design and development of such systems several guidance documents have been produced within the standards bodies. Perhaps the most relevant document is that produced in May 1998 by the European Commission, *Statement of Principles — Human-machine Interface for in-vehicle information and communication systems* [CONVERGE 1998b].

5.8 Retrospective Traffic Safety analysis

The field trial phase in Traffic Safety provides the overall confirmation that a system is not unsafe or (even better) that it is beneficial to safety. The normal procedure is to use a “before and after” approach, with the duration of the “before” and “after” periods carefully selected so as to:

1. be long enough to provide statistical reliability
2. not be subject to too many extraneous influences such as seasonality.

In addition to studying the test area, it is often advisable to study a control area, to eliminate time-trend and other extraneous effects.

Guidelines from the European telematics research programmes are available in the form of the *Framework for Retrospective Traffic Safety Analysis*, created by the HOPES project [HOPES 1993b]. The document provides guidance on experimental design issues and on indicators for Traffic Safety.

One major issue is that accident studies, the traditional measure of a change in road safety, are not appropriate because there is often insufficient time or insufficient size of trial for accident numbers to be a reliable indicator of a change in safety. It may therefore be necessary to use other indicators of safety. Of these the best validated are traffic conflicts, but various behavioural indicators are also available such as short headways, time-to-collision, unsafe manoeuvres, and changes in speed.

5.9 Safety audit and monitoring

Provided that the earlier stages of Traffic Safety work have been carried out properly, the main tasks at this phase are:

1. Certification of the proper installation and operation
2. Monitoring of the scheme for a reasonable period after start-up.

Certification corresponds to Stages 2 (Detailed Design[2]) and 3 (Pre-opening) of Safety Audit [IHT 1996]. However, the current Guidelines for the Safety Audit of Highways do not include any appreciation of the complexity or flexibility of ITS. With any such system, including a signal control system, it will be necessary not only to check that the hardware (poles, signs, etc.) have been installed in such a way as not to impede safety, nor that they will be obstructed when trees come into leaf, but also to check that the system ***operates*** in a way that is not detrimental to safety, and preferably enhances safety. It should be noted that seemingly quite small changes to signal timings, staging and offsets can have significant effects on safety levels at a junction, along a route, or in a network. It is vital to ensure that appropriate consideration is given to these issues in the detailed specification of a scheme.

A certain city redesigned a major complex junction controlled by traffic signals, and provided large overhead direction signs across all the lanes. After a number of red light violations had resulted in major accidents, an in-depth investigation was undertaken. It was discovered that all the violators were visitors to the city, who had been concentrating on the overhead signs to such an extent that they failed to spot the traffic signals showing red, because they were not in the same field of view.

5.10 Maintenance activities

The main issues to consider during this phase is that the system should maintain the safety properties that have been designed into it. There are two main activities needed to maintain the integrity of the installation, and to keep its equipment functioning correctly:

- **Preventative maintenance**: this must be carried out at regular intervals on all the hardware of the system; thus items should be inspected, serviced, or replaced as necessary. Whenever this is done, especially during servicing or replacement, care must be taken to leave the system in its original safe state by the use of the correct components, and by the manner in which they are manipulated, e.g. it is possible for the electromagnetic compatibility (EMC) of an item of equipment to be compromised by not replacing connectors properly.

The installation must also be checked to ensure that all the features on which the safety of the traffic depends are still present, e.g. signs not hidden by trees or damaged, “white lines” not worn away. A particular issue is the removal of temporary signs once they have served their purpose.

- **Corrective maintenance**: this must be carried out whenever a fault is identified. For items of hardware the same care must be taken during their replacement as for

[2] This is not the same terminology as used in this document. The Guidelines for Safety Audit are talking about the detailed design of a ***scheme***, as opposed to the design of a system. A scheme can be seen as a specific installation of a generic system (see Figure 3).

preventive maintenance, and for the same reasons. For software the situation is slightly different. As soon as any change is made to a piece of software then its integrity is potentially compromised, and any SIL certification that it may have may become invalid. Experience has shown that it is not uncommon for the fixing of one fault to cause another, and any changes that are made must be carried out under the same management and configuration controls as during the original development (see Section 6.8).

Records must be kept of all the maintenance activities performed on all safety-related equipment. They will not only become a supplement to the Safety Case of the system (see Section 7.4.3), but they will also demonstrate, or otherwise, that the reliability of the system is as it was originally planned.

5.11 System change

A change to a system can occur for a variety of reasons (see also Section 7.1.3), for example the desire to:

- Add more equipment of the same type
- Replace out-of-date equipment
- Add new functionality
- Improve the current functionality
- Change the current functionality
- Remove out-of-date functionality.

Apart from the desire to replace out-of-date equipment, all of these reasons will have been triggered by a high-level desire to make a change to the road transport environment, or to formulate a new Traffic Safety hypothesis (see Section 5.2). In addition any changes that might be made to the way that the sub-system, or units, are configured, or to the way that they are constructed, for example using a new technology, or programmed, have the potential to introduce new safety hazards. It is therefore necessary to go back to the appropriate lifecycle phase.

The amount of work involved will, of course, depend on the nature of the change, but at the very minimum an Impact Analysis must be undertaken to identify possible effects of the proposed change. The results of this analysis must be recorded in the Safety Case for the system, especially if no additional safety hazards are found. If new safety hazards are discovered then it might be sensible to treat the change as if it were a new system. It is essential that all the changes are made under a full configuration and quality management process to ensure that all the decisions taken, and features made, for the old scheme are at least considered for the new one.

Great care must be taken if changes are to be made to software. The seeming ease with which such changes can be made belie the ease with which faults can be added to a previously working system. All changes must be carried out under the same management and configuration controls as during the original development (see Section 6.8).

A system which is making decisions based on the fright being carried on a lorry may not be safety-related if the contents are not hazardous. However, if the data changes to include hazardous goods and this information is, say, transmitted to the emergency services in the case of an accident, then the resulting system will become safety-related.

As part of a research project, a certain European city developed an enhancement to a set of traffic signals that took account of the flow of pedestrian traffic across that part of the road. This was shown to have improved the overall safety of that crossing. However, when the city came to upgrade that signal controller, the technicians failed to reconnect the enhancement. This resulted in a variety of hazardous situations for the pedestrians which had not existed before.

6. Lifecycle for the safety of a sub-system, or unit

6.1 Begin Unit Safety Plan

Safety cannot be added afterwards, nor will it happen by accident; it must be designed into the unit, or sub-system, from the beginning. In addition, in order that the system may be assessed successfully (see Section 7) certain information must be produced that can only be created at specific points in the lifecycle, and not retrospectively. A Unit Safety Plan is therefore essential (see also Section 7.2).

A Unit Safety Plan contains all the activities that need to be undertaken to assure the safety of the unit, or sub-system, when these activities should be done, and who is responsible for ensuring that they have been done. It serves a very similar purpose to the System Safety Plan (see Section 5.1) and, depending on the size of the unit, or sub-system, it will have some similar contents. However, a primary objective will be to plan the verification and validation activities (see Section 6.8).

The responsibility for producing and maintaining the Unit Safety Plan resides with the Safety Manager of the project that is developing that unit. The document itself will not be static, but will be expanded to reflect new information when it has been obtained. A particularly important milestone will be when the hazard and risk analysis has been completed(see Section 6.2) and the SIL(s) of any safety-related sub-units have been identified (see Appendix C), since this will determine many of the future activities that will be necessary, their degree of rigour, and hence the competencies needed of the personnel undertaking the work (see Section 4.3.1). The existence of the Unit Safety Plan, and the style of its contents, will help to foster the safety culture for the entire project.

6.2 Hazard and risk analysis

Even if the sub-system, or unit, is being developed as part of a larger system, for which a PSA should have been performed (see Section 5.2), a hazard and risk analysis should also be undertaken on each item of equipment for which a manufacturer is responsible. The reason for this is twofold:

- It is possible that the PSA for the system was not done at a sufficient level of detail to enable all the safety hazards of the item of equipment to be identified
- Each manufacturer is legally responsible for the safety of the equipment that it produces, and should therefore ensure that its own procedures are in conformance with [IEC 61508].

As in Section 5.2 the objectives of this process are to:

- Understand the system concept
- Model the system concept
- Identify the top level hazards
- Identify the top level safety requirements
- Identify the Safety Integrity Level(s) — see Appendix C

and similar techniques may be used to achieve them, for example [PASSPORT 1995a] (see also Appendix B) or [Def Stan 00-58].

6.3 HMI analysis

At a sub-system level this phase of the design and development process is associated with the analysis of the human factors issues associated with the planned use of the sub-system.

The main concern of a traditional HMI analysis is related to the performance of the interface between the system, the users and their operating environments. As stated in Section 5.4, it is necessary to consider the assumptions made with regard to human involvement with the system at a more global level at the earliest stage of system development. Relevant assumptions made earlier in the system concept definition should be re-established and reviewed when sub-systems performance targets are being defined. This is particularly important when the sub-systems will have a direct influence on the HMI.

It has also been noted (see Section 5.4) that if HMI analysis is not performed throughout the system lifecycle then a concept may be developed that is constrained in its effectiveness, and potentially safety, by the lack of recognition of some real-world operational constraint. This is also true at a sub-system level.

General frameworks for establishing a methodology that take into account the organisational implementation of a system are available [Grandjean 1980, Wilson and Corlett 1995] and should form a reference guide to this aspect of the concept definition process. This may also guide a concept definition of the physical and environmental workspace requirements for control rooms etc. for which many design guides are available [e.g. Def Stan 00-25, Grandjean 1987, Pheasant 1988] (see also Appendix J).

There have been many models developed to assess how the consideration of human factors/ergonomics issues should be best applied. The most relevant in the context of the safety lifecycle described in Section 4 is a design process-oriented approach to ergonomics (see Figure 7). This approach views the design process as a series of repetitive processes where an *analysis* is made of an aspect of the system concept or detailed design, a *synthesis* is made of this work which is then subject to an *appraisal* and a *decision* made. This decision will then confirm some aspect of the design that will then be passed on for further incorporation and development.

This description of a sub-stage of the design process will be a familiar view to most individuals who will have been involved with a product or system development programme. Formal decision points will be planned for the hand over of firmed up concept descriptions, component specifications, sub-assembly performance inspections and so on up to and including system commissioning and hand-over. Subsequent repetitions of this basic sub-stage lead to greater and greater development of elements of a system leading eventually into incorporation of these elements into sub-assemblies or sub-routines until eventually a complete system can be put together as a prototype.

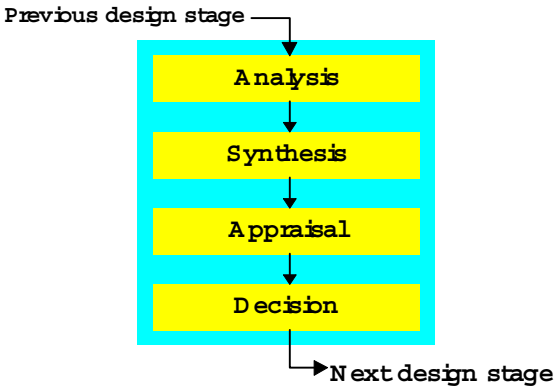

Figure 7: A simplified model of a sub-stage of the design process Adapted from [Wilson and Corlett 1995]

6.4 Safety requirements allocation

Safety requirements are of two types [DRIVE Safely 1992]:

1. **Safety functional requirements**. These are functions that must be carried out by the safety-related system should a hazardous failure occur in the technical process, or in the safety-related system itself. They may also prevent systematic faults violating the safety of the system (see also Appendix G).

2. **Safety integrity requirements**. These are measures to ensure that all the safety functions are performed with sufficient reliability. They are divided into:
   - Measures to avoid faults: these are to avoid systematic faults during the development and production phases (see also Appendix G):
     - **Quality**: by working in accordance to a relevant Quality Plan a developer is assured that all phases of the lifecycle will be performed, and any data that needs to be passed back to an earlier phase (e.g. test results) will be acted upon.
     - **Reliability**: by using components with a known failure rate, the reliability of the underlying hardware of the system can be ensured.
     - **Analysis**: most faults are made during the system lifecycle because of an inability to manage the actual, as opposed to the perceived, complexity of the system requirements. When it is not possible to prove mathematically the correctness of a system design (the usual condition) it is necessary to go as far down this path as is necessary; the higher the SIL the closer to a proof of correctness under all conditions one has to get. This requires greater and greater understanding of the system itself.
     - **Test**: although testing cannot normally demonstrate the absence of faults, it will provide confidence that the system performs correctly.
   - Measures to control faults: these are to control random and systemic faults during the operation phase (see also Appendix G):
     - **Diversity**: Identical redundant systems may contain the same systematic fault. In an attempt to avoid this happening it is sometimes possible to develop one or more of the channels in a different manner, e.g. by using a different technology. Note that care has to be taken in just what can be claimed about diverse channels, since systematic faults can occur for unexpected reasons, e.g. similar styles of engineering training.

- **Redundancy**: Redundancy is the normal technique used to control random hardware faults. In its basic form two (or more) identical channels are used to perform an action and the results are compared.
- **Self Test**: A safety-related system should run a set of self-test routines on a regular basis; the actual frequency will depend upon the reliability required. These tests help to ensure the hardware integrity of the system. When a fault is discovered it may be possible to isolate the relevant channel and maintain operation with the remaining redundant channel(s). In this situation the user may not notice any lack of functionality and hence it is essential that a warning is given that the safety integrity of the system has been reduced, and that corrective maintenance must take place. Alternatively the system can be placed into a safe state, or one with a minimum "limp home" functionality.
- **Monitoring**: A variation on self-test is to have continuous independent monitoring of the safety-related system. There are two basic types of monitoring. The fundamental type is the detection that an error has occurred, but without knowing why. Whilst it is not essential for the monitor to be able to identify the original fault, a monitor that stores details of all errors identified will enable long term maintenance strategies to be optimised.

6.5 HMI requirements allocation

At this phase the HMI attributes of the unit or sub-system must be defined.

At a simple interface level there are also many detailed aspects that must be considered. These can include the allocation and specification of the design of the user workplace, displays, controls and environment. Reference should be made to appropriate design guidance in ergonomics and human factors material and standards, where available and appropriate to the type of interaction and interface assumed at an overall system level, and guidelines exist for equipment/interface design for a wide range of types of environment and operation. Thus, at this phase appropriate HMI specifications for a number of aspects can be defined that might include the allocation of HMI attributes in terms of:

- workplace, (design and layout of interface components and workspace)
- displays (physical characteristics, display format, font, contrast etc.)
- controls (buttons, knobs, handles etc.)
- the users' environment (specify range of lighting, temperature etc.)

As the sub-system moves in isolation at first, and then in combination with other sub-systems to later development phases, these defined attributes for the HMI can be used as benchmarks for the various sub-assemblies of the system to be evaluated.

In this process it may be assumed that detailed engineering of both hardware and software will proceed to develop initial prototype sub-systems and components that can permit partial system functionality to be assessed. The normal process under which this detailed development proceeds mirrors that of numerous iterations of the Analysis, Synthesis, Appraisal, Decision sub-stage in the design process described in Section 6.3 [Wilson and Corlett 1995].

It is also important to note that HMI evaluations at all stages in the development lifecycle should be identified, scheduled and carried out to ensure that the allocation of HMI is appropriately and successfully implemented.

6.6 Detailed Safety Analysis

Once the design has been started it should be subject to a regular safety analysis. The degree to which this should be done will depend upon both the nature of the system and the SIL required. All safety-related systems should be subject to an independent assessment and these activities should be agreed in advance (see Section 7). A brief overview of the methodology is given in here, but the reader is referred to [PASSPORT 1995b] for a full description. The main phases of detailed safety analysis, which should be performed iteratively, are:

- Confirmation of the self-consistency of both the Functional Model and the Physical Model of the sub-system, or unit
- Confirmation of the consistency between the Functional Model and the Physical Model of the sub-system, or unit
- Identification of (additional) safety hazards
- Confirmation that only incredible scenarios have been rejected
- Identification of (additional) safety requirements
- Confirmation that all the safety requirements have been implemented
- Confirmation of the allocation of Safety Integrity Level(s).

Whilst these phases are similar to those of PSA, there will be more detail available, and the design chosen may itself introduce further safety hazards.

The first two phases are necessary because it makes no sense to undertake a safety analysis on a design that is fundamentally incorrect. The hazard analyses should be undertaken using the techniques of Failure Mode and Effects Analysis (FMEA) [IEC 812] and Fault Tree Analysis (FTA) [IEC 1025] as shown in Figure 8.

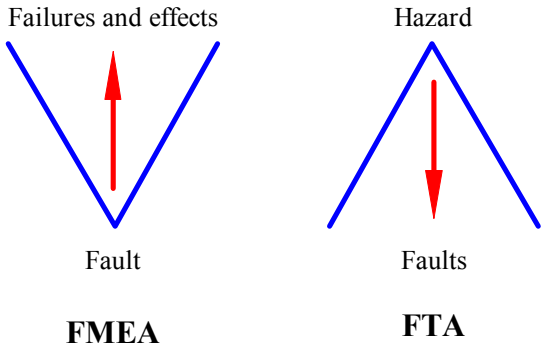

Figure 8: FMEA and FTA

FMEA is a qualitative method of reliability analysis. It is intended to identify failures which have consequences affecting the functioning of a system, within the limits of a given application, thus enabling priorities for action to be set. It is an iterative method of performing a system reliability or safety analysis. Ideally an FMEA will start at the Concept phase of a project and be continually updated as development progresses. An FMEA should be performed, at least, on all elements that implement a safety function or safety requirement, and all physical elements that implement many functions. The objectives of an FMEA are to identify:

- all potential failure modes of a system
- the effects of those failures
- the consequences or severities of those effects

- the priorities and responsibilities for actions to reduce severities or mitigate consequences
- the results of those actions.

FTA is a complementary technique to FMEA. Whereas FMEA starts with faults and identifies effects, FTA starts with a hazard and identifies the fault or faults that could lead to that hazard. An FTA should be performed on each possible system failure in order to:

- identify the (combination of) causes
- demonstrate the independence, or otherwise, of causes
- identify common events and weak links
- derive reliability figures for the system, if those for the components are known.

The combined effect of performing both an FMEA and an FTA will provide a high degree of confidence that all the functional system safety hazards associated with the system have been identified, and that suitable measures have been taken against them.

6.7 HMI appraisal

This is the process under which testing of a prototype is undertaken to confirm that the desired HMI performance has been achieved. Clearly within any specific system there will be identified stages at which a "prototype" system is available when such a review of (HMI) performance can take place. Due to the complex nature of many UTMC systems such a "prototype" stage may not have a complete range of system functionality available. If this is the case then it is possible that a complete appraisal of the HMI issues and targets is not possible. This consideration raises some additional issues with regard to the overall position of HMI appraisal within the development lifecycle and the consequences related to the migration of the system functionality from concept to implementation.

6.7.1 Overall system lifecycle

Earlier sections have emphasised the importance of setting appropriate HMI-related performance targets within the overall definition of the system concept for use in system development. It has also been noted that the setting of relevant HMI evaluation and re-assessment activities should be planned as an integral part of the Development phase as it progresses.

It may be assumed that for any given system there will be appropriate scheduled milestones in the system development lifecycle when evaluations of the emerging system can be undertaken. In the context of HMI and safety assessment these may be considered to establish whether original HMI design goals and targets are still being addressed. Such interim assessments may be carried out by evaluating prototype parts and sub-systems with a representative sample of users in a real or simulated operating environment.

Although the design of any such evaluation would be most appropriate within the context of a specific system there are often common types of issues that can have an impact on a system's HMI. Examples may be seen where some external constraint on the system as a whole is recognised at a stage part-way through development and initial system concepts have to be reviewed and reassessed. Another typical mid-development issue is when, internal to the development programme, a small range of engineering options become available that fit within a system concept and the "best fit" has to be sought. In both of these

examples an additional iteration of the Concept/Development lifecycle may have to be undertaken to either:

1. Re-define part of the concept, and any subsequent performance related target for subsequent re-development, or
2. Re-specify part of the detailed definition of part of the system.

In either case if there are consequences to the design and operation of the HMI then this may require either theoretical re-analysis or practical evaluation. Development of the system should be capable of ensuring that neither form of system re-definition is allowed to be passed without an appropriate safety evaluation.

When the system reaches a sufficiently advanced stage to be capable either in whole or part to be tested then it is possible that the HMI usability, effectiveness and safety can be assessed. Due to the nature of ITS it may not be possible to perform real-world evaluations, in which case such evaluations as can be done may have to be carried out off-line. If formal testing is to be carried out it must also be against an agreed set of performance criteria within a defined test procedure.

If no legal, statutory or standards guidance is available for any part of the system related to HMI then such an evaluation will be reliant on the definition of an HMI approval method being available from the Concept/Development phase. This could be in the form of an assessment of system HMI safety, e.g. an objective assessment of actual performance against target performance, if target performance is defined by agreed metrics with associated test methods. If this is not available then an alternative may be an independent subjective evaluation of actual performance against target performance, supported by an evaluation of actual system specification against the concept definition that set the target performance parameters. In either case it is important also to determine what is the criteria for passing/failing such a testing or approval process. If the target performance is over *x* metrics relative to *y* forms of HMI (for instance in-vehicle, roadside display, control room) then what constitutes a pass? Is it 100% compliance?

6.7.2 System migration issues within the development lifecycle

As a system moves from development and testing towards deployment (implementation and commissioning) it is likely that the need for further HMI assessment decreases. However it is acknowledged that in specific cases there may be a need to carry out full HMI assessment during commissioning or indeed after the system has been put in service. This could occur, for example, where it was impossible to carry out relevant real-world evaluation until installation, and information may be required to modify system performance to provide an enhanced HMI for a later modification of the system.

In such cases it may be useful to provide an evaluation methodology that is compatible to that used in the Development phase to assess how successfully the HMI design was guided, and thus be able to adapt the procedures for later developments.

Indeed, as the status of knowledge increases about human factors in relation to novel concepts of traffic control systems, and the response of drivers and road users, then it may be necessary to revisit the types of evaluation carried out. This may be particularly relevant post commissioning as subsequent evaluations may be some years after initial concept work. Guides to some of the emerging issues are constantly being introduced (for example [Hancock and Parasuraman 1992], [Parkes and Franzen 1993], [Barfield and Dingus 1998]).

6.8 Safety validation

Validation is the demonstration that a product satisfies its requirements, and safety validation is the demonstration that a product satisfies its safety requirements (see Section 6.4), and that it has achieved its SIL. In order to achieve this aim evidence must be gathered throughout the development lifecycle and, for safety-related systems, the higher the SIL the more convincing the evidence must be.

It is important to realise that the validation process is essential to achieving a given SIL. A SIL indicates not only a certain reliability, but also that the development of the system has been carried out in accordance with an appropriate development process, and that the system has been assessed in the safety-related context in which it is to be used. It is expected that the assessment team will be independent from the development team. The degree of independence necessary will depend upon the SIL (see Section 6.8.1).

"Simple" systems can be tested exhaustively in order to demonstrate that they work correctly in all respects (see Section 5.5). However, as soon as a (sub-)system contains software, for example part of a UTMC system, it becomes "complex" and cannot be tested exhaustively. It should be noted that, although software is normally considered to be the major culprit (see Appendix H), modern highly integrated circuits, and complex communication systems, can also demonstrate similar properties (see also Appendix I).

Evidence that will demonstrate the correctness of a system to a sufficient level of confidence may be obtained by a variety of means, all of which should be considered:

- **Analysis**: The use of a technique to demonstrate the properties of particular products of the lifecycle, and may examine in detail the functionality, performance, traceability and safety implications of an item (e.g. of software), together with its relationship to other items within the system, and may include the use of formal mathematical methods.
- **Audit**: The process of examining a product and its related documentation for accuracy, quality, completeness, consistency and traceability, and that its production has been performed in conformance with a specified process.
- **Review**: Reviews can be performed for a variety of purposes and with varying degrees of rigour. A review provides a qualitative assessment of correctness to establish that proper and adequate development procedures have been adhered to, including software design standards appropriate for the project; that the results of the analyses are acceptable, or that identified actions arising from the analyses or tests results are, or have been, carried out correctly; and that the design fulfils the requirements of the Requirements Specification. The possible processes can range almost continuously between:
  - a formal detailed examination of a the conformance between the requirements of a product and the product, with the aim of finding anomalies, and guided by a checklist or similar aid (e.g. Fagan Inspection), c.f. *verification*
  - checking that certain processes have been performed, c.f. *validation*. This is often an official process that leads to the signing of a release note or approval of the reviewed subject.
- **Testing**: The process of supplying a set of inputs, process conditions and expected results with the intention of exercising the product and to find faults.
  - **Black box testing**: Tests used to ensure that the specified functions are performed fault-free under both normal and abnormal conditions (e.g. robustness testing).
  - **White box testing**: Based on a knowledge of the internal structure (e.g. of the software code), test cases are chosen exercise "boundaries", provide adequate coverage of the possible inputs and code paths, etc.

  (Note that testing can only be used to prove correctness in all respects if, and only if, all possible states are tested)

- **Validation**: The demonstration that a product satisfies its requirements. Validation requires a decision to be made.
- **Verification**: The comparison of the output of each individual phase of the lifecycle with the inputs to that phase, the objective being to ensure that the output from the new phase fulfils the requirements specified in the inputs to that phase. Verification always requires a comparison to be made.

The degree of confidence that must be obtained in a product will depend upon its importance, for instance the SIL of a safety-related system, and guidance may be found in [IEC 61508] and [MISRA 1994].

6.8.1 Independent assessment

Not only must safety validation be done, it must be seen to have been done. It is always good practice to use a different set of people to check work than those who created it, but if both groups of people come under the same management, then they can be also be under similar pressures. The higher SILs should require greater independence of assessment in order to ensure that there is no bias from the development team, nor misplaced pressure from management. The degree of independence should be achieved by one or more of:

- different person
- different department or section
- different company or division

Further guidance may be found in [IEC 61508] and [MISRA 1994].

6.9 Decommissioning

Whilst it is most unlikely that a whole UTMC will undergo a complete decommissioning, individual items of equipment will be replaced as they become worn out or obsolete. The decommissioning process is likely to constitute a change to the system and it should be treated as such (see Section 5.11). Environmental regulations also require special care to be taken during the disposal of equipment, especially if it contains toxic material.

7. Safety certification and Statutory Type Approval

This section describes the activities that should be followed in seeking formal approval to install and operate equipment that is either a part of, or comprises, a UTMC system.

7.1 Introduction

7.1.1 Statutory Type Approval, certification and conformity assessment

In general, an assessment process may take one of a number of different forms:

- **Statutory Type Approval**: the process of testing product-intent samples according to some defined strict criteria immediately prior to volume production.
- **Certification:** the process of obtaining regulatory agency approval for a function, equipment or system by establishing that it complies with all the applicable statutory regulations. There are normally two classes of regulations against which a certification process may be performed. The first ensures that the target of the certification process conforms to one or more standards so that it will be able to function correctly. The second ensures that the target will be able to function safely.
- **Conformity assessment or self certification**: a process whereby a manufacturer can demonstrate that a product conforms to certain standards, etc. [90/683/EEC] provides eight different processes for different types of product.

At the present time, regulatory agency approval for control equipment used in road transport is performed using the STA process. It has been used for many years on, for example, the traffic signal controllers that are used to provide the basic safety of road junctions. It was devised when systems consisted only of mechanical and electrical components and thus the successful application of a series of tests was a valid exercise to demonstrate safety. Such systems are now recognised as being “simple”. ITS, however, are normally “complex” systems for which testing alone is not sufficient to validate all operational modes and conditions (see Section 5.5). It will therefore be necessary to provide some form of additional evidence to demonstrate the safety of integrated UTMC systems with emergent properties.

In order to gain the confidence required that a “complex” product does conform properly, a knowledge of the development process is also needed. Such certification is done in the aerospace industry by representatives of the notified body following the entire development process. Whilst such a process is likely to be perceived to be too expensive for the ITS industry in which cost margins are very tight, and SILs are normally low, there is clearly a need for a process which maintains the authority of the STA, or full Certification process. [MCH 1813] provides mechanism to formally certify that certain processes have been performed, and module H of [90/683/EEC] provides a process whereby the notified body can monitor the activities of a manufacturer without have to perform all the verification and validation activities itself.

7.1.2 The current mechanism

The current STA process for traffic control equipment is defined in Highways Agency specification [TRG 0500B]. It is essentially a four stage process.

The first stage, called "agreement in principle", involves the manufacturer submitting a number of documents to the Approval Authority (currently the Highways Agency), including:

- Preliminary engineering proposals or supplier's specification
- Functional description of hardware and software.

All questions involving interpretation of the specification(s), quality assurance, equipment function, safety etc. are resolved at this stage. Techniques proposed for maintaining safety as required by the specification must be clearly described in the functional description. Upon satisfactory completion of these requirements a letter confirming the Approval Authority's agreement in principle with the submitted proposals is issued to the supplier.

The second stage involves the supplier agreeing a test plan for the equipment with the Approval Authority which will be used to demonstrate the conformity of the equipment to appropriate standards. Again on satisfactory completion of this stage a letter is issued to the supplier by the Approval Authority.

During the third stage, the equipment is submitted for test. For certain aspects such as EMC the use of an accredited test house is required; however, for functional performance the supplier is permitted to self-certify. If the functional performance includes safety, the test schedule has to be agreed with the Approval Authority as part of the second stage. For non-safety functional performance the supplier is permitted to draw up the specification although the Approval Authority may require to inspect it. The Approval Authority may require to witness any of the approval tests.

Finally, upon satisfactory completion of all testing, and receipt and acceptance of final documentation by the Approval Authority, the equipment supplier is deemed to have completed the approval procedure and a STA certificate is issued.

7.1.3 Scope

One problem with a formal assessment mechanism, especially one that has legal status, is that it is first necessary to define what is, and what is not, an ITS. However, unlike an aircraft or a nuclear power station, which are unmistakable, there is currently no legal definition of what is, and what is not, an ITS. In addition, and also unlike an aircraft or a nuclear power station, whose boundaries are well defined, many ITS, in particular UTMC systems, will be subject to continual:

- **Extension**: UTMC-like systems are subject to geographical extension as the finance becomes available. This will be done either with identical equipment to that already installed or, more likely, with new hardware that performs the same or similar functions.
- **Expansion**: Functional expansion of UTMC-like systems may be undertaken either with additional equipment or, possibly, by re-programming existing equipment.
- **Evolution**: An ITS can evolve in at least two ways:

  (a) It is possible for a safety-related system to emerge from a previously non safety-related system by the addition of new functions and/or new types of data. For example, an ambulance dispatch system and a taxi scheduling system have very similar top-level

functional requirements, or a commercial fleet of lorries may begin to carry hazardous goods.

(b) It is possible for an application to change its required SIL over time. For example, a route guidance advice system becomes a command system if it is so good that the driver becomes accustomed to not having to check the safety implications of following the directions being given.

As UTMC-like systems increase in complexity the changes may also modify the total system behaviour as new emergent properties appear. It will therefore be necessary to define:

- What must be assessed, both for equipment and integrated systems
- When it must assessed
- When it must be re-assessed.

In addition, there is the issue of system versus unit assessment. Individual pieces of equipment (e.g. a traffic signal controller) can be subject to STA [TRG 0500] at the unit level. In a UTMC environment, these controllers will be part of a larger system which will be subject to the new Code of Practice [MCH 1869]. Previous sections of this document have shown that the safety of a system such as a UTMC cannot be assured by simply assembling a collection of components which have been subject to STA. This section will show how Unit STA could be used within the context of a larger system.

Similarly, there is considerable interest in the use of commercial-off-the-shelf (COTS) equipment. COTS can provide a more cost-effective solution than bespoke development for certain components of a UTMC system. However, the use of COTS raises particular issues which need to be addressed.

7.2 Safety planning — assessment

Safety planning is the first activity to be performed in the lifecycle for a system (see also Sections 5.1 and 6.1). The aim of producing a Safety Plan is to ensure that verification and validation are performed throughout the project and that these activities are performed with a rigour appropriate to the required SIL [IEC 61508]. The Safety Plan for a UTMC system defines the content of the Safety Case for that system and the steps necessary to compile and assess it.

Similarly, preparation for assessment is a task which must begin at the start of a project, otherwise the possibility exists of arriving at some point in the assessment only to find that a vital piece of information has been omitted or overlooked. Early liaison with the assessor is recommended to ensure that the actual process is as smooth as possible, and that everything that the assessor expects to find has been produced.

7.2.1 Issues in certification

Whilst the main reason for certification is the primary safety of the system, there are other ones as well. Typical issues that may need to be addressed for an ITS include:

- **Safety**: To ensure that the equipment or system will not cause harm to any person
- **Environment**: To ensure that the equipment or system will not cause harm to the environment or interfere with other systems

- **Security**: To ensure that the equipment or system, and any data within it, are protected from external attack or interference
- **Conformance**: To ensure that equipment or system will be inter-operable with any other equipment or system necessary, and that it conforms to any other regulation not covered by safety, security or the environment above
- **Health and Safety at Work legislation**: To ensure that a system is installed in a manner that is safe for the installers, and that it is safe to operate and maintain.

Note that this list is not intended to be complete.

Clearly some of these issues are related and a single assessment activity may cover more than one issue. It is therefore necessary for a plan to be produced to enable the total certification of a system to be undertaken in a cost-effective manner.

The remainder of this section mainly covers the safety-specific issues in ITS assessment.

7.2.2 Development of Intelligent Transport Systems

ITS development may consist of many sub-system developments, each of them consisting themselves of multiple equipment developments. Furthermore, nested within each equipment development, there can be multiple hardware development cycles as well as multiple software development cycles.

Because of the iterative nature of all but the simplest design programmes, the development of ITS should be considered to be cyclical rather than sequential. Furthermore, the entry point for any given activity may occur at any point in the cycle. For a new ITS, the process begins with the top level definition of the requirements. For functional additions to an existing ITS, the entry point may occur in the context of changes to a particular piece of equipment.

The development of an ITS can be considered as three connected processes:

- The core development process which produces the ITS itself
- The supporting processes which act across all levels of the development processes. These processes include:
  - Preliminary and detailed system safety analysis (see Sections 5.2, 6.2 and 6.6)
  - Requirements validation
  - Design verification
  - Configuration management
  - Process assurance

  The level of rigour necessary for each of these supporting processes depends on the complexity of the functional implementation, and the SIL
- The assessment process (see also Section 6.8).

7.2.3 The Safety of the System

Whilst the safety of a specific item of equipment such as a traffic signal controller is well understood, the ITS industry will offer many novel products whose side effects are not fully known. In addition the integration of equipment into co-operating systems, such as a UTMC system, will create additional side effects whose characteristics may vary depending on the way that the system is structured and/or used.

It is for these reasons that it is not possible to provide a set of simple instructions on exactly which techniques should be used to guarantee that a system should receive a final certificate for use by the public. Each new piece of equipment, and each new system configuration must be analysed separately. Sometimes Functional System Safety issues will predominate, at other times it will be the Traffic Safety or HMI issues, and occasionally one will be able to demonstrate that there are no safety issues at all. However, the generic nature of road transport being the interaction of people and (fast) moving solid objects means that, normally, all three aspects of safety must be considered for any ITS. It is therefore essential that both the applicant, and the Approval Authority have people with sufficient knowledge that they can produce and agree an adequate cost-effective strategy to certify a given ITS.

7.2.4 Routes to approval

The following two sections outline the procedures that may be followed for equipment (or unit) approval and system approval.

The Safety Plan for a UTMC system will identify when individual units (equipment) need to be assessed, and how these align with the overall assessment of the system. Individual pieces of equipment that are part of the overall system will either be Type Approved following [TRG 0500], or equivalent evidence will be produced which will be included in the Safety Case for the overall system. Note that for systems designated as being “complex” (see Section 5.5) the requirements of STA alone may not be sufficient evidence. Section 7.3 describes the issues associated with unit assessment in the context of a wider UTMC system.

In general terms, the complete UTMC system will need to be approved as an entity following an approach such as that described in Section 7.4. This will include assembling a Safety Case for the complete system. Part of the evidence in the Safety Case will be the STA or equivalent data for pieces of equipment making up this system. Safety Cases are described in more detail in Section 7.4.3 and Appendix K.

7.3 Equipment Type Approval

Equipment STA is the activity performed at the end of the development lifecycle for a piece of equipment (or a “unit”). In general, equipment that is installed as part of a UTMC system should continue to be Type Approved. The Safety Case for the overall system will then contain evidence that the individual items of equipment that have been integrated into the overall system, and upon which the basic safety of the system usually depends, have been duly approved.

Some equipment will be designated as “simple” and others as “complex” (see Section 5.5). For systems designated as “simple”, evidence of equipment STA will normally be sufficient. Note that the fact that a “simple” system can be tested exhaustively does not automatically confer on it the benefits associated with a simple design. It is necessary to provide documentary evidence that an exhaustive test of the design has been carried out.

However, for “complex” systems additional evidence will normally be required. Whilst the equipment should continue to be Type Approved, the Safety Case will contain additional

evidence about the equipment and the degree of rigour followed in its development and validation (see Section 6.8). This is especially relevant for software-based equipment.

7.3.1 Equipment Type Approval and COTS

There are two types of COTS equipment that have to be considered in a UTMC context. The first is equipment such as a traffic signal controller which is purchased "off the shelf" and already carries STA. The second is equipment which has not been designed specifically for Urban Traffic Control (UTC) or UTMC and which therefore has not been Type Approved as a piece of traffic control equipment. Such items may include computer equipment and communications receivers.

Where COTS equipment already carries STA under [TRG 0500], this approval can be "carried over" into the UTMC context, although additional information may be required as part of the Safety Case for its use in the wider system (see above).

Where COTS equipment does not carry STA, it will be necessary to include in the Safety Case evidence that the equipment is fit for its purpose at the required SIL. The PSA and the system safety analysis (see Sections 5.2 and 5.5) will indicate the requirements that need to be placed on individual pieces of equipment.

> A GPS receiver system may be purchased "off the shelf". Whilst this system may already carry some "approvals" relevant to its target market (e.g. EMC Directive) it is unlikely to have been designed to be used in a safety-related application. If this receiver is now required for use in a safety-related application such as hazardous goods tracking, additional evidence will be required to prove the fitness for purpose of this receiver in a UTMC system.

Developments in the safety-related systems community, for example the UK certification scheme to IEC 61508 [CASS 1999], mean that, in the future, it may be possible to buy a COTS with a certificate to SIL *x*. Whilst such a system will normally be able to be integrated into a UTMC system, and its certificate included as part of the Safety Case, it will be necessary to verify that the interpretation of SIL *x* from the sector producing the equipment is not only compatible with the UTMC interpretation, but that the method of integration will not invalidate the assumptions.

7.3.2 Equipment histories

As an alternative to STA or similar evidence for COTS, equipment can be accepted as part of the Safety Case that has a "track record" of working correctly over a number of years. In this case a formal (documented) history of the correct functioning of the equipment should be included in the Safety Case. The precise length of time over which the equipment is deemed to have worked satisfactorily will depend on the application.

A history-based approval procedure called ETOPS is used in aviation, where twin-jets are not allowed to fly across extended over-water routes unless the type has completed several thousand hours of trouble-free operation. New aircraft typically have to be used on overland routes or fly circuitous routes across the Atlantic until sufficient operational hours have been built up for ETOPS. Note that ETOPS approval for a particular aircraft does not just depend on the type's operational hours, however, but also on other factors such as the rigour of maintenance.

Whilst equipment histories can be useful, particularly in the interim period as systems migrate from UTC to UTMC, it must be remembered that modifications can invalidate them. This is particularly relevant where software is concerned. Developers should be aware that the tendency to "tweak" software means that a new approval may be required for an otherwise unchanged item of equipment.

[IEC 61508] describes a similar concept, "proven in use", as an additional means of demonstrating that a safety-related system is fit for purpose. The requirements of the standard for proven in use are summarised as follows: "A previously developed sub-system shall only be regarded as proven in use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the sub-system (during which time all failures have been formally recorded), and which takes into account any additional analysis or testing, as required. The documentary evidence shall demonstrate that the likelihood of any failure of the sub-system (due to random hardware and systematic faults) in the … safety-related system is low enough so that the required safety integrity level(s) of the safety function(s) which use the sub-system is achieved."

The standard expands further on what these requirements mean in practice. The concept of "proven in use" may prove useful to developers and integrators of UTMC systems, particularly where COTS equipment is being used, but further work is needed to define the precise criteria relevant to this sector.

7.4 System Certification

A new Approval process similar to that defined by [TRG 0500B] is proposed for the assessment or certification of "complex" UTMC systems and their components (see Figure 9). The process is essentially the same as the existing scheme but with additional requirements for "complex" systems. It has also been designed so that the System Certifier can devolve work to accredited assessors at any stage that more detailed analysis is required than can be performed internally. The System Certifier may be:

- a senior engineer in the company that is installing the UTMC system (self certification);
- a third party 'testing house' that is independent of the organisations that are associated with the installation of the UTMC system;
- an organisation appointed by the Government, e.g. the Highways Agency.

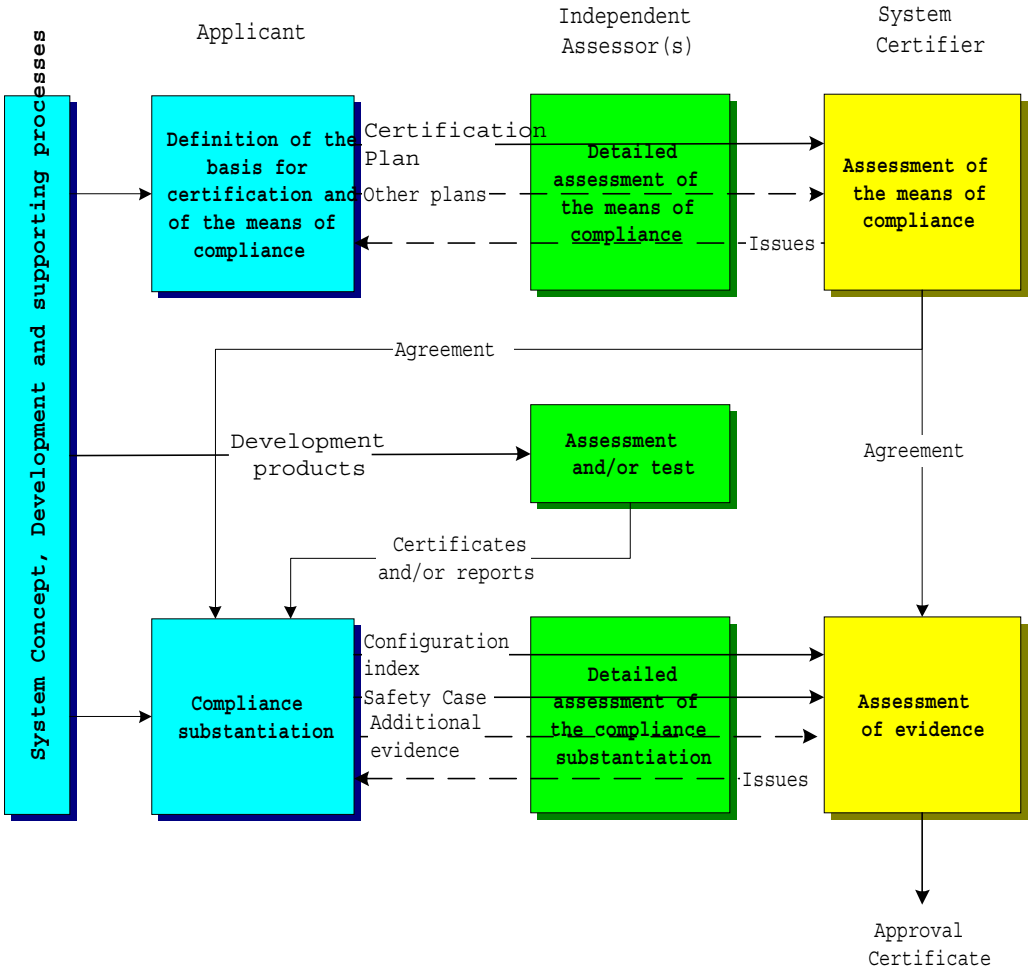

Figure 9: Proposal for the Approval of "complex" systems

UTMC systems can vary in the degree of safety hazards that are associated with them, and hence in the level of safety integrity that they must demonstrate, and it not necessary to produce the same degree of detail of evidence for all systems.

7.4.1 Evidence: Low safety integrity levels

When UTMC only needs to demonstrate a low level of safety integrity it is only necessary to be certain that the correct processes have been performed by qualified persons. The work itself need not be assessed beyond normal quality assurance procedures. A process of this form is described in]MCH 1813] in which a "System Certifier should be a person who is in a position to know what procedures have been carried out, and knowledgeable enough to understand the technical implications of those procedures and with sufficient authority to ensure that they are carried out. This person should normally be the Project Manager or other person responsible for managing the systems aspects of the system."

[MCH 1813] proposes a number of forms on which the System Certifier can keep track of the stages in the project, and to provide a continuous record of progress. It also proposes a certificate that may be used to represent the formal certification of the system.

7.4.2 Evidence: High safety integrity levels

In order to deal with the issues associated with “complex” systems which need a high level of safety integrity, the “agreement in principle” stage is expanded. The applicant, typically a manufacturer or a system integrator, will be required to submit documentation to the System Certifier that includes:

- A **Certification Plan** which defines the system, outlines the product development process, and identifies an acceptable means of compliance with the regulations. It should include a PSA of the system concept, and a preliminary SIL for the equipment or system
- **Other Plans** may also be needed, e.g. for software or hardware qualification, and/or for the demonstration of compliance with a Technical Specification, e.g. UTMC.

Subject to the satisfactory resolution of any issues, the System Certifier will agree the contents of the plan(s) as being suitable for the demonstration of compliance. If the system is too large and/or complex for the System Certifier to check internally, it may require the Applicant to obtain a detailed assessment of the means of compliance from an Independent Assessor.

During the Development phase, products and groups of products will be passed to Independent Assessor(s), who will supply certificates and/or reports as appropriate. All those that relate to the safety of the system should be incorporated in the Safety Case (see Section 7.4.3). Once the Applicant believes that all the work has been performed in accordance with the agreed Certification Plan, the following documents are submitted to the System Certifier:

- **Configuration Index**: the configuration identification of each item of equipment, software, inter-connections between equipment, required interfaces with other systems and sub-systems, and all safety-related operational and maintenance procedures and limitations. When applicable, any permissible interchange of alternative equipment within the ITS should be given
- **Safety Case**: see Section 7.4.3.
- **Additional evidence**: For example, any deviation from the agreed plan should be described together with the rationale to substantiate the deviation. Also any Security, Environmental and Compliance to a Technical Specification data, for evidence that the system satisfies any non-safety-related regulatory requirements.

Subject to the satisfactory resolution of any issues, the System Certifier will determine the adequacy of the data to show regulatory compliance. Once it is satisfied that all is in order, an **Approval Certificate** can be issued. If the system is too large and/or complex for the System Certifier to check internally, it may require the Applicant to obtain a detailed assessment of the compliance substantiation documents from an Independent Assessor.

At the discretion of the System Certifier, the Applicant may be permitted to submit only a **Certification Summary** to describe how it was determined that the ITS, as installed in the environment, complies with the agreed **Certification Plan**. The System Certifier may then only need to inspect part of the total compliance substantiation data.

Many of the processes described above rely on the product and process information being obtained during the development of the ITS. Such data may not always be available for existing ITS, or subsequent modifications, or when COTS equipment is used. In such cases an alternative means of compliance may be necessary. This will need to be agreed in advance with the System Certifier and is likely to need independent verification.

7.4.3 Safety Case

The evidence that will be used to justify the overall safety of a system should be collected together in a Safety Case. A Safety Case shall contain all the information necessary to assess the safety of a system, an application, or a specific installation, to the required SIL - the higher the SIL the greater the level of detail that will be necessary. A good Safety Case will provide information that will make the assessor comfortable with the reliability, availability and maintainability properties [Skogstad 1999]. There are three different types of Safety Case applicable for UTMC systems:

- **Generic Product Safety Case**: generic products that can be re-used in quite different applications
- **Generic Application Safety Case**: valid for a class of applications
- **Specific Application Safety Case**: a specific installation of a specific application. This should be divided into:
  - **Application Design Safety Case**: evidence of safety for the theoretical design of the specific application
  - **Physical Implementation Safety Case**: evidence of safety for the implementation of the specific application.

Appendix K describes some possible contents of a Safety Case.

7.4.4 Re-approval

As described in Section 7.1.3 many ITS, in particular UTMC systems, are likely to undergo extension, expansion and/or evolution many times during their existence. Indeed it is most likely that a whole UTMC will never enter a state that could be called “decommissioned”, but rather it will evolve gradually from one generation to the next. At what stage during one of these changes should it be necessary to obtain re-approval?

There are four main types of change, which are not mutually exclusive:

1. Extension of the same functionality.
2. Expansion with new functionality.
3. A simple change (extension, expansion or evolution) that is easy to understand.
4. A complex change (extension, expansion or evolution) that is not easy to understand.

On the principle that all “new systems” should be approved, then it is clear that in the case of (2) and (4) above re-approval will be necessary. Even if cases (1) and (3) are not re-approved then the system owner must be able to produce the evidence, added to the Safety Case, that it was not necessary (see Section 5.11). In practice it can be envisaged that the rules will themselves evolve as experience is gained.

When introducing a sub-system or ITS modification, the System Certifier should consider the impact that the modification has on the basis for the existing ITS certification. In some cases a supplement to the existing certification basis may need to be added, and the applicant should propose a means of compliance that defines how the revised ITS will satisfy the revised basis of the certification. Whether or not this basis has changed, it will be necessary to assess the anticipated means of showing compliance to ensure compatibility with the agreed basis of certification.

7.4.5 Certification mechanisms

At the present time no recommendation is made on the precise mechanism which should be put in place for supporting the certification and/or assessment process for safety-related UTMC systems described above. Self-certification of the form described in [MCH 1813] may be sufficient for those UTMC system which only need to demonstrate a low level of safety integrity, but it is not suitable when high levels are required.

The nature of a mechanism for high levels of safety integrity will depend on the policy decisions that need to be made concerning the implementation of the recommendations in this Framework (see Section 8). However it should be noted that generic assessment methods based on IEC 61508 have been developed, or are under development. The two most relevant to UTMC are:

- CASCADE, a European transport-sector project [CASCADE] which has developed a "General Assessment Method" based on an earlier draft of IEC 61508
- CASS, a UK project, has developed an assessment scheme based on IEC 61508 [CASS 1999]. It is based on the work of the earlier FRESCO project [FRESCO 1996]. Although driven primarily by the process sector, it is intended that the CASS scheme should be more widely accepted and used.

Either of these schemes would provide an eminently suitable base for developing a UTMC Safety Assessment process. As CASCADE was developed by the transport sector (rail and automotive) it would probably be the more suitable, although it may require some updating in view of developments to IEC 61508. CASS will initially be more process sector oriented, although a CASS certificate for a piece of COTS equipment would be acceptable evidence as part of a UTMC Safety Case as described in Section 7.4.3.

8. Conclusions and issues for the future

This Framework is a proposal as to how the safety of UTMC systems may be assured. It is based on the principles and techniques that have been developed for other industry sectors, and codified in various standards and guidelines. It is also the first document of its type to combine the areas of Traffic Safety, HMI and Functional System Safety. It takes into account the concerns currently being expressed by the various stakeholders, in particular in relation to the requirement for a formal "seal of approval".

Where this Framework overlaps with the Highways Agency Code of Practice the approach is similar or compatible, but this Framework also includes the processes that should be undertaken when the associated hazards have a very high risk. In addition this Framework expands on the Code of Practice both in terms of what should be done and why it should be done. It, or a document based on it, could therefore act as supporting Guidelines to the Code of Practice.

However, since many of the procedures described are new to this industry sector, it will first be necessary to validate the approach with a number of case studies or demonstrators.

8.1 Issues

During the course of preparing this Framework a number of issues were raised that either need further technical investigation, or that affect national and local policy in the way that certain processes and activities are organised. Those issues that are considered to need urgent attention are marked with the symbol "⇒".

8.1.1 General

⇒ It will be necessary to form an agreement in principle on the contents of this Framework by all the various stakeholders. Once this consensus had been reached further work will be needed to generate a full set of guidelines or a code of practice.

8.1.2 Safety Integrity Levels

Whilst the use of SILs is becoming well established in other industry sectors, including the motor industry [MISRA 1994], their use has not yet been endorsed for use in traffic management and control. At the moment the Code of Practice [MCH 1869] and NMCS [DMRB Vol. 9] both refer to the relevant standard [IEC 61508], but they do not offer advice on how it should be applied in this industry sector.

⇒ The process by which the SIL of a system, or an item of equipment, is identified can vary with the industry sector. It will be necessary to agree a process for ITS in general, and UTMC systems in particular.

⇒ Many of the safety tasks described in this Framework can be done with varying degrees of rigour. It will be necessary to identify the amount of work that should be done in a given situation. (Note that the use of SILs for software is already well defined.)

- The “algebra of SILs”, namely how a COTS which has been assessed to SIL *N* can be used in an application of SIL *M* (where *M* > *N*), is still the subject of research.

8.1.3 Safety Cases

⇒ Formal Safety Cases have not been required for UTMC-type systems before. The approach outlined in this Framework has been taken from an analogous industry sector, and so there is a need to produce exemplar Safety Cases for UTMC systems.

8.1.4 Assessment or Certification

- The method of assessment of COTS for use in safety-related applications is the subject of active research, and the approach may have to be modified in the light of the results.

⇒ When is a change not a change? There is a need to provide advice/regulations on how to handle change and evolving Safety Cases — for example the problem of invalidating approval “by stealth”.

- When is a UTMC system not a UTMC system? The Technical Specification for UTMC includes many functions that may not be deployed by a local authority. How will their assessment be handled?

- It should be noted that the assessment process can break down when a developer is unaware that the product is a safety-related ITS which needs a special lifecycle (for example the ill fated London Ambulance Computer Aided Dispatch System [SWT_RHA 1993] and [Flowers 1996]).

8.1.5 Education and Training

⇒ Many of the processes described in this Framework are not currently deemed to be necessary as part of supply contracts. Will potential UTMC owners and users recognise that additional resources may be needed?

⇒ There will be a need to provide training to (most of) the stakeholders in the processes and techniques described in this Framework.

8.1.6 Legislation

⇒ How will the new Approval Process get implemented? Is legislation required? Is a migration strategy required? Is it necessary to have both Independent Assessors and an Approval Authority? It should be noted that the trend within Europe is towards “self certification”.

- Who assesses the assessors? (Note that other non-UTMC UK projects are currently considering this problem)

⇒ How is the link between urban and inter-urban ITS to be handled? STA is handled by the Highways Agency as the Approval Authority. However, for inter-urban ITS (e.g. Regional Traffic Control Centres (RTCC)) the Highways Agency are themselves the "owner" of the system. This seems to suggest the process proposed at present for UTMC cannot apply because there must be a degree of independence between the Approval Authority and the system owner/operator, particularly for safety-related systems that require to be developed to the higher SILs (see Section 6.8.1).

9. References

[89/336/EEC] 89/336/EEC, *Council Directive, On the Approximation of the Laws of the Member States to Electromagnetic Compatibility, Official Journal of the European Communities* (139), 25 May 1989.

[90/683/EEC] 90/683/EEC, *Council Decision, Concerning the Modules for the Various Phases of Conformity Assessment Procedures which are Intended to be Used in the Technical Harmonisation Directives, Official Journal of the European Communities* (380), 13 December 1990.

[ARIANE 5] Lions J L (Chairman), *Flight 501 Failure*, Report by the Inquiry Board, Paris, 1996.

[Barfield and Dingus 1998] Barfield W and Dingus T A (eds.), *Human Factors in Intelligent Transportation Systems*, Lawrence Erlbaum Associates, ISBN 0 8058 1434 5, 1998.

[BS DD 235] BS DD 235, *Guide to In-Vehicle Information Systems*, BSI, 1996.

[CASCADE] CASCADE (Esprit Project 9032), *Generalised Assessment Method (GAM): Guidelines*, September 1996; *Generalised Assessment Method (GAM): Rules*, January 1997.

[CASS 1999] *Certification and assessment of safety (related) systems* {http://www.eutech.co.uk/cass}.

[CODE 1998a] Draskóczy, M, Carsten, OMJ., and Kulmala, R (eds.), *Road safety guidelines*, Deliverable B5.2, TR 1103 CODE support project of the Transport sector of the TELEMATICS APPLICATIONS Programme, Fourth Framework Programme (1994-98), 1998, {http://www.trentel.org/index.htm}.

[CODE 1998b] Jesty P H, Giezen J, Fowkes M, *System Safety Guidelines*, Deliverable D5.4, TR 1103 CODE support project of the Transport sector of the TELEMATICS APPLICATIONS Programme, Fourth Framework Programme (1994-98), 1998, {http://www.trentel.org/index.htm}.

[CORD 1994] Ryd P-O (Ed), *Recommended Definitions of Transport Telematics Functions and Sub-functions*, DRIVE II project CORD (V2056), Deliverable D004 - Part 3, 1994 {superseded by [CONVERGE 1997]}.

[CONVERGE 1997] Gaillet J-F, *A proposal for a Revised Transport Telematics Functions List,* Deliverable DSA7.2, TR 1101 CONVERGE support project of the Transport sector of the TELEMATICS APPLICATIONS Programme, Fourth Framework Programme (1994-98), 1997, {http://www.trentel.org/index.htm}.

[CONVERGE 1998a] Jesty P H *et al*, *Guidelines for the Development and Assessment of Intelligent Transport System Architectures*, Deliverable DSA2.3, TR 1101 CONVERGE support project of the Transport sector of the TELEMATICS APPLICATIONS Programme, Fourth Framework Programme (1994-98), 1998, {http://www.trentel.org/index.htm}.

[CONVERGE 1998b] Fowkes M *et al*, *Statement of Principles — Human-machine Interface for in-vehicle information and communication systems*, TR 1101 CONVERGE support project of the Transport sector of the TELEMATICS APPLICATIONS Programme, Fourth Framework Programme (1994-98), 1998, {http://www.trentel.org/index.htm}.

[CTSA 1997] Channel Tunnel Safety Authority, *Inquiry into the fire on heavy goods vehicle shuttle 7539 on 18 November 1996*, 1997.

[Def Stan 00-25] Interim Defence Standard 00-25, *Human Factors for Designers of Equipment, Part 6, Vision and Lighting*, 1986.

[Def Stan 00-54] Draft Interim Defence Standard 00-54, *Requirements for safety related electronic hardware in defence equipment*, 1999.

[Def Stan 00-58] Draft Interim Defence Standard 00-58, *HAZOP Studies for Equipment Containing Programmable Electronic Systems*, 1996

[Department of Transport 1996] *A Policy For Using New Telematic Technologies for Road Transport*, Consultation Document, Department of Transport UK, 1996

[DMRB Vol. 9] DMRB Volume 9, Network - Traffic Control and Communications, Design Manual for Roads and Bridges Volume 9, Department of Transport, 1994-9.

[DO 178B] DO-178B / ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, RTCS and EUROCAE, 1992.

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

[EMCATT 1995] EMCATT, *Functional System Safety and EMC*, DRIVE II Project EMCATT (V2064), 1995.

[EN 50128], EN 50128, *Railway Applications — Software for Railway Control and Protection Systems*, CENELEC, 1995.

[Flowers 1996] Flowers S, *Software Failure, Management Failure: Amazing Stories and Cautionary Tales*, Wiley, ISBN 0 471 95113 7, 1996.

[FRESCO 1996] FRESCO, *Final report Section 3: An Overview of the FRESCO Assessment Method (FRAM)*, May 1996.

[Green 1994)] Green P, *Measures and Methods Used to Assess the Safety and Usability of Driver Information Systems*, Technical Report, No. UMTRI-93-12. University of Michigan Transport Research Institute, USA, 1994.

[Grandjean 1980] Grandjean E, *Fitting the task to the man: A textbook of Occupational Ergonomics*, Taylor & Francis, ISBN 0 85066 379 2, 1980.

[Grandjean 1987] Granjean E, *Ergonomics in Computerised Offices*. Taylor and Francis, ISBN 0 85066 350 4, 1987.

[Hale *et al* 1990] Hale A R, Stoop J and Hommels J, "Human Error Models as Predictors of accident scenarios for designers in Road Transport Systems", *Ergonomics*, **33**, pp. 1377–1388, 1990.

[Hancock and Parasuraman 1992] Hancock P A and Parasuraman R, "Human Factors an Safety in the Design of Intelligent Vehicle-Highway Systems (IVHS)", *Journal of Safety Research*, **23**, pp. 181-198, 1992.

[HINT 1999] Carsten, O, Franzén, S, Draskóczy, M and Carver, E, *Monitoring and control of human implications of new technology*, Deliverable D11 of Fourth Framework Transport Research Programme project HINT (Human Implications of New Technology), Institute for Transport Studies, University of Leeds.

[Hitchins 1992] Hitchins D K, *Putting Systems to Work*, Wiley, 1992.

[HOPES 1993a] Carsten, O.M.J., ed. *Framework for prospective traffic safety analysis*, Deliverable 6 of DRIVE II project HOPES, Department of Traffic Planning and Engineering, University of Lund, 1993.

[HOPES 1993b] Oppe, S., ed., *Framework for retrospective traffic safety analysis*, Deliverables 7a and 7b of DRIVE II project HOPES, Department of Traffic Planning and Engineering, University of Lund, 1993.

[HSE 1999], Le Guen J, *Reducing risks, Protecting People*, HSE Discussion Document, 1999, {http://www.open.gov.uk/hse/condocs/dde11.htm}.

[IEE 2000] *Safety*, *Competency and Commitment: Competency Guidelines for Safety-Related System Practitioners*, IEE Publications, ISBN 0 85296 787 X, February 2000.

[IEC 1025] IEC 1025, *Fault Tree Analysis*, International Electrotechnical Commission, 1985.

[IEC 812] IEC 812, *Analysis Techniques for System Reliability — Procedure for Failure Mode and Effects Analysis (FMEA)*, International Electrotechnical Commission, 1985.

[IEC 61508] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, 1999.

[IHT 1996] *Guidelines for the safety audit of highways*, Institution of Highways & Transportation, 1996.

[INCOSE] International Council on Systems Engineering (INCOSE) {http://www.incose.org}

[ISO 10746] ISO 10746-1 (Draft), *Reference Model of Open Distributed Processing*, 1994.

[ISO 9000] ISO 9000, *Quality Management and Quality Assurance Standards — Guidelines for Selection and Use*, 1987.

[ITSEC 1991] ITSEC, *Information Technology Security Evaluation Criteria (ITSEC); Provisional Harmonised Criteria*, Version 1.2, CEC DG XIII, 1991.

[ITSEM 1992] ITSEM, *Information Technology Security Evaluation Manual (ITSEM), (Draft) Version 0.2*, CEC DG XIII, 1992.

[Leveson 1995] Leveson N G, *Safeware — System Safety and Computers*, Addison Wesley, ISBN 0 201 11972 2, 1995.

[MCH 1813] MCH 1813, *System Certification*, Highways Agency, 1999.

[MCH 1869] MCH 1869, *Code of Practice for Traffic Control and Information Systems*, Highways Agency, 1999.

[MIL-HDBK 217] MIL-HDBK 217, *Reliability Prediction of Electronic Equipment*, US Department of Defense, 1995

[MISRA 1994] MISRA, *Development Guidelines for Vehicle Based Software*, MIRA, ISBN 0 9524156 0 7, 1994.

[McCormick and Sanders 1992] *Human Factors in Engineering and Design*, 7th Edition, McGraw Hill, ISBN 0 07 054901 X, 1992.

[Neumann 1995] Neumann P G: *Computer Related Risks*, Addison-Wesley, ISBN 0 201 55805 X, 1995.

[Parkes and Franzen 1993] Parkes A M and Franzen S (eds.), *Driving Future Vehicles*, Taylor and Francis, ISBN 0 7484 0042 7, 1993.

[PASSPORT 1995a] Hobley K M *et al*: *Framework for Prospective System Safety Analysis Volume 1 — Preliminary Safety Analysis*, Deliverable N° 9a, V2058 PASSPORT project of the Advanced Transport Telematics (ATT/DRIVE II) sector of the TELEMATICS APPLICATIONS Programme, Third Framework Programme (1991-94), 1995.

[PASSPORT 1995b] Hobley K M *et al*: *Framework for Prospective System Safety Analysis Volume 2 — Detailed Safety Analysis*, Deliverable N° 9b, V2058 PASSPORT project of the Advanced Transport Telematics (ATT/DRIVE II) sector of the TELEMATICS APPLICATIONS Programme, Third Framework Programme (1991-94), 1995.

[PASSPORT 1995c] Astruc J-M *et al*: *Towards the Certification of ATT Systems — System Safety Aspects*, Deliverable N° 8, V2058 PASSPORT project of the Advanced Transport Telematics (ATT/DRIVE II) sector of the TELEMATICS APPLICATIONS Programme, Third Framework Programme (1991-94), 1995.

[Pheasant 1988] Pheasant S, *Bodyspace: Anthropometry, Ergonomics and Design*. Taylor and Francis, ISBN 0 85066 352 0, 1988.

[Preece *et al* 1994] Preece J *et al*, *Human Computer Interaction*. Addison-Wesley, ISBN 0 201 62769 8, 1994.

[Redmill 1998] Redmill F, *IEC 61508 - Principles and Use in the Management of Safety*, Computing and Control Engineering Journal, Vol 9 Nº 5, IEE, 1998.

[Skogstad 1999] Skogstad Ø, *Experiences with Safety Case Documentation According to the CENELEC Railway Safety Norms*, in “Towards System Safety”, Proceedings of the Seventh Safety-Critical Systems Symposium, Springer-Verlag, Feb 1999.

[SWT_RHA 1993] SWT_RHA, *Report of the Inquiry into the London Ambulance Service, South West Thames Regional Health Authority*, ISBN 0 90513370 6, 1993, {also available from http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html}.

[TickIT] TickIT, *A Guide to Software Quality Management System Construction and Certification using ISO 9001* (Issue 2), TickIT, 1992.

[UTMC 1997] Urban Traffic Management and Control (UTMC) Systems, *Technical Issues*, Department of the Environment, Transport and the Regions, 1997

[UTMC22 2000] UTMC22, *Preliminary Safety Analysis of the UTMC Architecture*, Department of the Environment, Transport and the Regions UTMC Programme, 2000.

[Wiener 1993] Wiener L, *Digital Woes: Why We Should Not Depend on Software*, Addison-Wesley, 1993.

[Wilson and Corlett 1995] Wilson, J R and Corlett E N (eds.), *Evaluation of Human Work: A practical ergonomics methodology*, Second Edition. Taylor and Francis, ISBN 0 7484 0084 2, 1995.

9.1 Bibliography

This section lists other texts which may be of use or interest to the developers of safety-related ITS.

Davis D, “Legal Aspects of Safety Critical Systems”, *Proceedings of the 14th International Conference on Computer Safety, Reliability and Security (SafeComp ’95)*, ed. G Rabe, Springer-Verlag, pp. 156–170, ISBN 3 540 19962 4, 1995.

Perrow C, *Normal Accidents*, Basic Books, 1984.

Petroski H, *To Engineer is Human: The Role of Failure in Successful Design*, St. Martin’s Press, ISBN 0 312 80680 9, 1985.

Reason J, *Managing the Risks of Organisational Accidents*, Ashgate Publishing, ISBN 1 84014 104 2 / 105 0, 1997.

Tenner E, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, Knopf, 1996.

Thomé B (Ed), *Systems Engineering: Principles and Practice of Computer-based Systems Engineering*, John Wiley and Sons, 1993.

Rechtin E, *Systems Architecting: Creating and Building Complex Systems*, Prentice Hall, 1991.

Appendix A
Other HMI and human factors issues

A.1 Objective

The system lifecycle described in the main body of this report gives a structure as to how UTMC-like systems may be brought forward from concept, through development, to implementation. The relevance and importance of Functional System Safety, Traffic Safety and HMI considerations that should be addressed to develop ***safe*** systems are identified, and the relevant considerations and content of various sub-tasks in the development of such systems are also described.

This Framework has therefore identified the importance of HMI issues in the successful implementation of future UTMC systems. The contents of this appendix are intended to develop further some of the background issues and aspects of relevance in this area.

A.2 HMI definition and system development

The need for specific emphasis on HMI target setting and regular assessment within the UTMC design and development lifecycle has been stressed. This is based upon the understanding that such an emphasis has not always been historically given in system development projects and that systems have subsequently been delivered with a compromised performance. This compromised performance being in part attributable to inadequate specification and assessment of the HMI issues. In the most extreme case this can affect the safety with which a system, including its users and operators, perform.

Therefore it has been considered that it is not always recognised that re-evaluation of the system against pre-defined and agreed HMI criteria should be regularly and formally incorporated in the Analysis/Synthesis/Appraisal/Decision process. It has been argued that if this is not formally planned then it can result in later complications in the design and development process. As sub-phases of the design process can often be carried out in parallel then it is possible that some design decisions can be made whose implications for the eventual HMI are not seen until a later stage of design integration where HMI assessment is carried out.

Therefore if human needs are not fully assessed, and appropriate design guidelines derived at the System Concept phase, then HMI mismatches and inefficiencies may become inadvertently built into the system at the outset. If this unfortunate deficiency is not identified until later in the lifecycle then remedial re-design will become increasingly costly to implement. HMI assessment at the System Concept phase should therefore be seen as a fundamental part of the process of defining the system that has embodied within it an understanding of the needs and capabilities of the future users. The safety assessment of a concept from an HMI perspective may also be integrated into the PSA described in Section 5.2.

The assessment of the human related aspects of design should therefore have its strongest emphasis in the System Concept phase. It should help to place a systematic analysis of the

perceived rôles and responsibilities of any human “interface” with the system envisaged. It should review these rôles and responsibilities against an analysis of the organisational and physical environment in which the UTMC system will be implemented, taking into account in particular the needs of, and constraints upon, control room staff. It should also assess the human interface to the UTMC perceived at the road to drivers, and other road users (including pedestrians and cyclists), and their own range of abilities and environmental constraints. It should take into account the wide variation in skills, capacities and training among road users, including for example the need to cater to child and elderly pedestrians. It should carry out this analysis with the support of appropriate skilled staff and access to supporting references. It should at this stage resolve the key human factors issues into performance targets that the eventual system should achieve in relation to its human users. These targets should directly enable later assessments of the system to be undertaken at all relevant development and deployment stages.

As the lifecycle moves into the Development phase then HMI assessments can be carried out on initial prototype parts of the system/interface to establish whether the detailed design process is producing an interface and performance that is complying with target performances established within the Concept phase. This may be carried out by evaluating prototype parts and sub-systems in a simulated operating environment with a representative sample of users. The focus and detailed design of any such evaluation would be most appropriately selected within the context of a specific system. However it is clear that within this stage of a complex system development there are often choices to be made from a number of design options for sub-systems. Where such trade-offs between particular alternative approaches affect any aspect of HMI then this may be subject to trial evaluation.

During testing, the HMI input to the safety assessment may be reduced to a pre-specified target performance evaluation for the system based upon definitions arrived at within the Concept phase. If a new HMI is to be deployed on the roads, it may be necessary to test that HMI, perhaps against appropriate alternatives, or against a more traditional HMI, in real-world conditions. It is notable that this has not always been done in the past and that systems have been put on the streets without adequate testing to ensure that all road users can understand and use the system properly. It should be noted that elderly road users, for example older pedestrians, will have more difficulty in adjusting to change than their younger counterparts, and that most existing road users will not receive any special training in system use. Assuming that the system arrives at appropriate levels of HMI performance at the end of iterations within the development stages, then the system should be provided for deployment without the need for further HMI assessment.

The relevance of HMI analysis and assessment is therefore highest at the Concept phase in the safety lifecycle and decreases in emphasis as the system moves through the Development and Deployment phases. It must still be present within these more detailed phases as often changes in design caused by some unforeseen constraint or compromise can result in a new effect on the user HMI and operational safety. It is therefore important to emphasise that HMI assessment is an aspect that should remain as part of the overall system approval framework.

A.3 UTMC and human interaction — other general issues

It is assumed that any future UTMC system will be intended to affect the behaviour of traffic with an “emphasis on the active management of traffic rather than reactive control” [Department of Transport 1996]. It is also clear that any such concept will involve a range of human involvement with the system. This may cover a wide range of levels of interaction

but perhaps the rôles of operator/controller and end-user (namely road user) are most easily visualised in this context.

Taken from this perspective it is clear that the operational effectiveness of any such system will rely on the performance of both the machine (system) and its human "components". Therefore if a UTMC system is to be produced that will perform effectively in operation and be designed for safety then it should have specific and continuous emphasis placed upon the human factors needs and requirements that the system must deliver. The design of the HMI aspects of the system should be a priority aspect within the system concept work to define the overall concept. This should ideally involve the participation of human factors or ergonomics practitioners within the design team developing and refining the system concept. This would enable an early, iterative analysis of the HMI issues relevant to that concept.

For example, the humans within the system may be individual road users (drivers or cyclists) responding to roadside signing or displays (interface), passengers of public transport, pedestrians, or traffic control centre operators. In addition the more complex and lengthy the interaction between the user and the system, the more detailed the analysis of the HMI issues will need to be.

Where the issues relate to more complex interactions, particularly in relation to control room type HMI, there may be also be more fundamental questions to be answered about the allocation of tasks between operator/user and the system. Establishing a system concept that makes appropriate and beneficial use of humans operators is crucial in defining a system that is effective and safe. A satisfactory system concept for any particular implementation may be very site-specific and it is therefore appropriate to establish generic questions that seek to establish the system and its relation to its human users or operators (see also Appendix J).

Human factors issues related to the system design may therefore be at an overall system level (allocation of functions and tasks) or at a defined interface level (design of display, controls and environment). Each of these aspects are in need of analysis at the Concept phase.

At the overall level of system concept development there are many questions that may be posed with regard to how the human operator/users interact with the system. Examples of some typical and pertinent questions that may have relevance to UTMC systems are given below [adapted from McCormick and Sanders 1992]. These questions are an abstract from a much larger list of system definition HMI and human factors questions that may be relevant to the assessment and definition of a system concept.

1. What are the functions that need to be carried out to fulfil the system objective?
2. If there are reasonable options available, which of these should be performed by human beings?
3. For a given function, what information external to the individual is required? Of such information, what information can be adequately received directly from the environment, and what information should be presented through the use of displays?
4. For information to be presented by displays, what sensory modality should be used? Consideration should be given to the relative advantages and disadvantages of the various sensory modalities for receiving the type of information in question.
5. For any given type of information, what type of display should be used? The display generally should provide the information where and when it is needed.
6. Are the various visual displays arranged for optimum use?

7. Are the information inputs collectively within reasonable bounds of human information receiving capabilities?
8. Do the various information sources avoid excessive time sharing?
9. Are the decision making and adaptive abilities of human beings appropriately utilised?
10. Are the decisions to be made at any given time within the reasonable capability limits of human beings?
11. In the case of automated systems or components, do the individuals have basic control, so that they feel that their behaviour is being controlled by the system?
12. When physical control is to be exercised by an individual, what type of control device should be used?
13. Is each control device easily identifiable?
14. Are the controls properly designed in terms of shape, size, and other relevant considerations?
15. Are the control devices arranged conveniently and for reasonably optimum use?
16. Is the workspace suitable for the range of individuals who will use the facility?
17. If there is a communication network, will the communication flow avoid overburdening the individuals involved?
18. Are the environmental conditions such that they permit satisfactory levels of human performance and provide for the physical well-being of individuals?

Although this represents only a small part of such a system/operator assessment checklist it indicates that an HMI assessment for safety evaluation must consider wider issues related to human efficiency in operating a system. Some of these issues relate to human needs within the context of a task or job, others relate to longer term effects on human performance (factors such as fatigue, inadequate workplace design etc.) that may eventually lead to a safety hazard.

At an interface level there are also many detailed aspects that must be considered. These can include analysis of the design of the user workplace, displays, controls and environment. Reference should be made to appropriate design guidance in ergonomics and human factors material and standards where available and appropriate to the type of interface. At the system Concept phase this should therefore defined HMI specifications for aspects such as :

- workplace, (design and layout of interface components and workspace)
- displays (physical characteristics, display format, font, contrast etc.)
- controls (buttons, knobs, handles etc.)
- the users' environment (specify range of lighting, temperature etc.)

A.4 In-vehicle equipment/UTMC interface

It should also be noted that in the future there is the possible delivery of UTMC-derived information into individual road vehicles for drivers, which raises considerations of the in-vehicle HMI. As in-vehicle provision of traffic and route information is already available there are established guidelines for in-vehicle HMI to prevent driver distraction. Such publicly available guidance as the BSI *Guide to in-vehicle information systems* [BSI DD 235] provides information as to how this aspect of interface design should be handled. Standards or recommended practices such as these may subsequently form a system requirement and/or constraint as to the design of the interface.

Appendix B
Preliminary Safety Analysis

The following is a summary of PSA from the Framework for Prospective System Safety Analysis produced by the European DRIVE II Project PASSPORT (V2058) [PASSPORT 1995a]. A PSA should be carried out before the detailed design is underway and is based on the information that is available at the time. Since most new systems are extensions of, or make use of, existing systems, the information available at even this Concept phase can be quite considerable. The sub-phases of a PSA are:

- Modelling the system
- "What If?" analysis
- Identification of the primary safety hazards
- Identification of the primary safety objectives
- "What Causes?" analysis
- Identification of the top-level safety requirements
- Preliminary assignment of the SIL(s).

A hazard is an undesirable effect by the system on its environment. In this situation the term "environment" encompasses anything with which the system might interact. It is therefore necessary to produce a model that shows the system in relation to its environment. One such model is the PASSPORT Diagram which is an extension of Yourdon data-flow diagrams. A PASSPORT Diagram (see Figure B.1) contains the kernel of the system at the centre, and its boundary elements, which interact with the environment, surrounding it. The system boundary is immediately outside the boundary elements. The data passing between the kernel of the Target of Evaluation is also shown, as are any known databases. The model is specifically designed for ITS which interact with other systems. The diagram can be checked for completeness by ensuring that it will perform the functions specified in the system requirements, and also that all the influences on the system ("Static Data") are present (e.g. development process, standards, given data etc.) The diagram can also be checked for consistency by ensuring that "what comes in must go out" and "what comes out must have gone in".

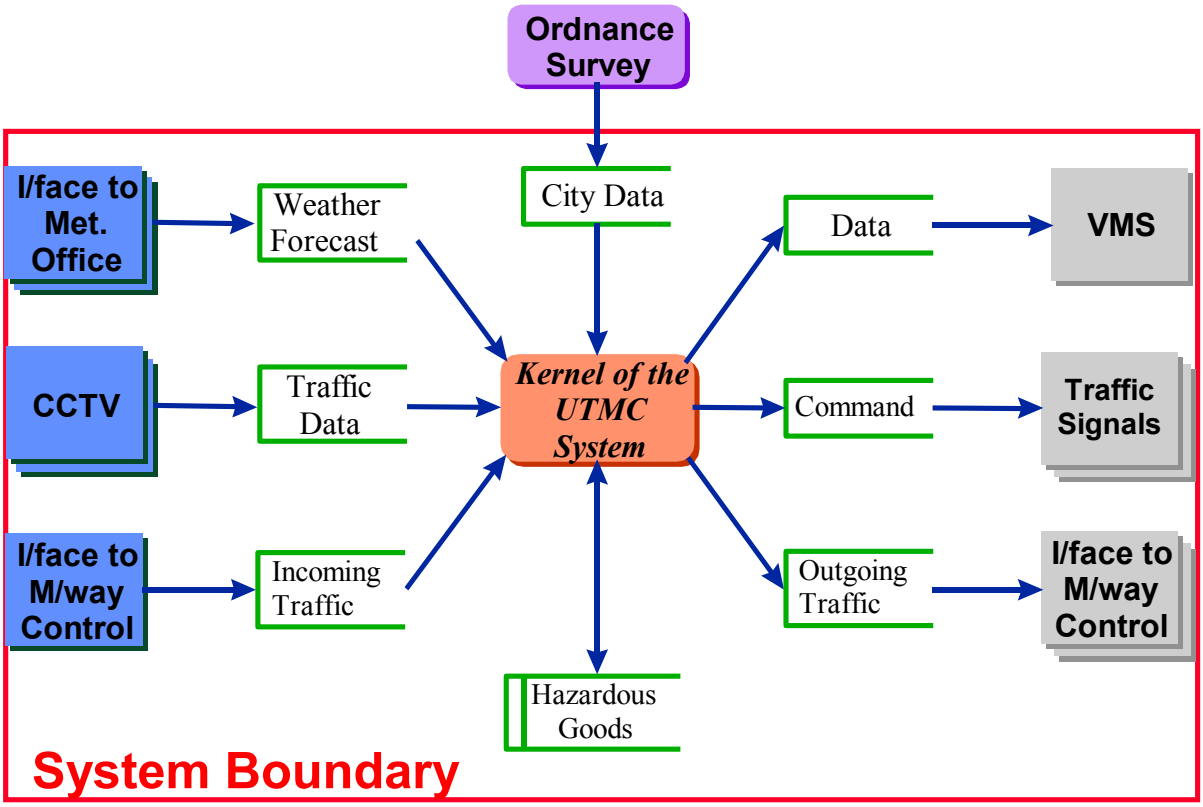

Figure B.1: Example PASSPORT Diagram (incomplete)

A PSA should be performed by a team of persons with a variety of relevant expertise, including HMI and Traffic Safety, and once the team is agreed that the PASSPORT Diagram does indeed provide a true representation of the system the hazard analysis can begin. Initially an informal FMEA, or "What If?" analysis, should be performed on each "box" in the diagram; this will enable the primary hazards to be identified, from which the primary safety objectives can be formulated. Each hazard can then be studied further by using an informal FTA, or "What Causes?" tree analysis, based on the information currently available; this will enable the preliminary safety requirements to be identified. A study of the controllability of each hazard (see Appendix D) will enable a preliminary SIL to be assigned for the design and development of the corresponding sub-system.

Appendix C
Safety Integrity Levels (SILs)

Safety Integrity Levels provides a mechanism whereby a safety-related electrical, electronic or programmable electronic system may be developed in a manner that ensures the final product will both operate in a safe manner, and with sufficient reliability. Their use provides a systematic methodology which results in systems which are as safe as practical. Safety integrity is defined as "the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time", and a SIL is a "discrete level (one of four) for specifying the safety integrity requirements of safety functions" [Redmill 1998].

The basic definition of a SIL is in terms of the degree of risk reduction required to reduce the safety-related hazards associated with an item of equipment to an acceptable level. IEC 61508 uses Figure C.1 to describe this concept.

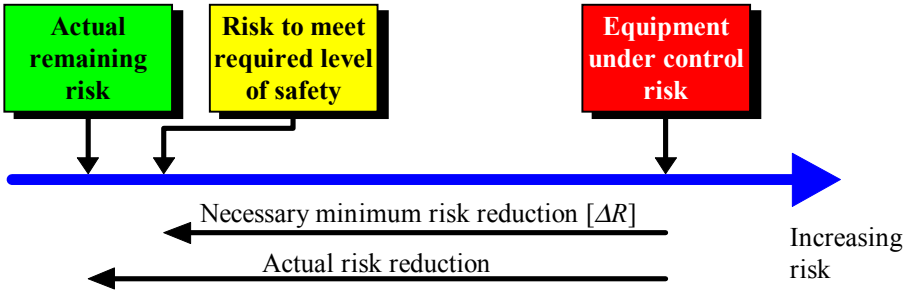

Figure C.1: Risk reduction

Risk is defined by the relationship:

$$risk = probability\ of\ occurrence \times degree\ of\ severity\ of\ harm$$

This definition shows that in order to reduce a risk either the *degree of severity of harm* should be reduced by a suitable design, or the *probability of occurrence* should be reduced by suitable means. Since ΔR can usually only be measured in a qualitative manner, an assessment has to be made of all the relevant factors, before the risk reduction required is placed into one of four bands, or SILs. However, since it is possible to obtain different answers depending upon the basis used to categorise the level of risk, IEC 61508 recommends that each industry sector should produce its own interpretation, and a technique based on finding the "Controllability" of a UTMC system after a failure is described in Appendix D.

Each safety hazard found during the PSA should be assigned a controllability category, and the most serious category found is then assigned to the system under investigation. The five Controllability categories map directly onto the SILs in the manner shown in Figure C.2 (the fifth SIL, 0 (zero), has been added because there is a need to be able to analyse systems that might turn out not to be safety-related). Thus, once a SIL has been allocated to the system, this then defines the nature of the future development of that system (see also Section 6.4). The aim is to reduce the risk of a safety-related hazard, by reducing the

probability of a dangerous failure, to an acceptable level. This is all summarised in Figure C.2.

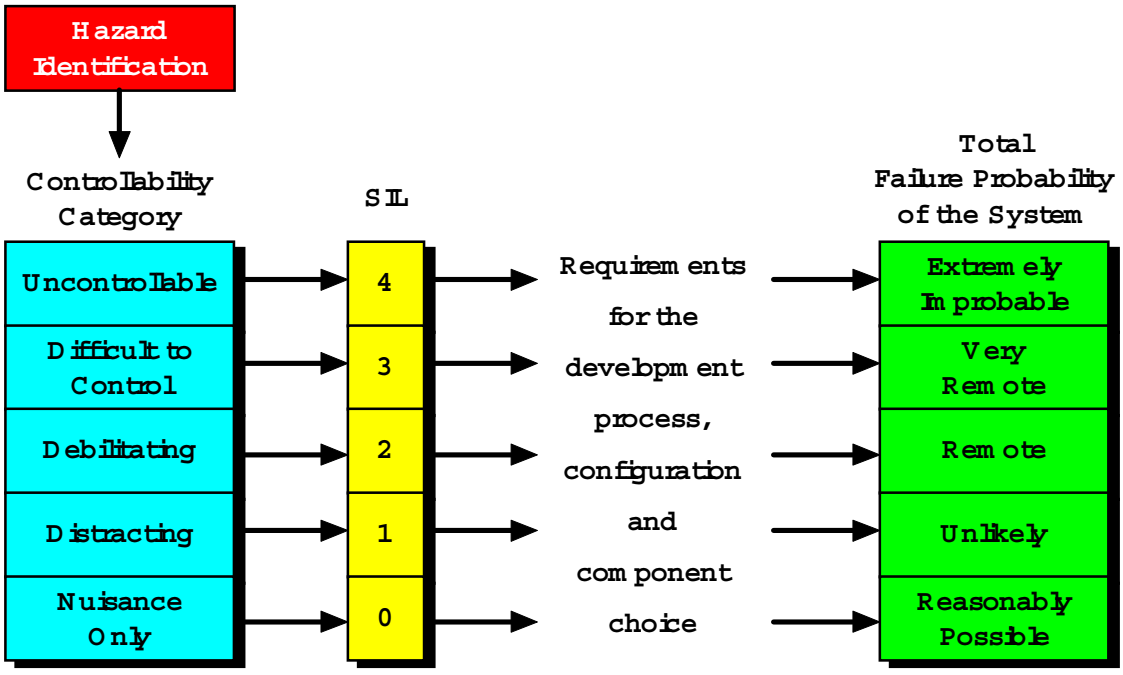

Figure C.2: Controllability and Safety Integrity Levels

IEC 61508 has suggested some figures for the rather imprecise phrases of Figure C.2 (see Table C.1), though they have not yet been tested in the full light of a public debate. These figures, which should apply to the system that is reducing the risk of the safety-related hazard, should normally be taken to be the desirable minimum dangerous failure rates, and some industry sectors or companies may wish to aim for a better figures, especially when working to the lower SILs. For example if a probability of a dangerous failure of 10^{-3} for SIL 2 is given to a system created in volumes of 10^{+6} per year, this could be taken to imply that there are designed to be 1,000 failures per year, which would almost certainly be considered commercially unacceptable. This situation can certainly occur in the automotive industry where millions of certain units are produced each year.

SIL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	Continuous or high demand mode of operation (Probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Table C.1 - Safety Integrity Levels and target failure measures

Unfortunately a problem arises when Table C.1 is applied to systems which might be subject to systematic faults (see Appendix G), for example those associated with software and

EMC, for which there are currently no methods available to demonstrate such figures before a system becomes operational. These issues are discussed further in Appendix H and Appendix I.

It should be noted that the above discussion assumes that all the risk reduction (Figure C.1) will be performed by an electrical, electronic or programmable electronic system. It may be possible to reduce part of the risk with a (sub-)system that uses another technology, or with external facilities, and in this case the SIL of the electrical, electronic or programmable electronic system may be reduced. This approach may be essential when the risk is very high, or when very great reliance needs to be placed on those parts that are subject to systematic faults.

The emergency shut down system in the Seiswell B Nuclear Power Station not only uses redundancy (three identical traditional computer systems based on electrical circuits), but also diversity (a simpler control system based on magnetic circuits). By this means the risk reduction allocated to the software in the computer system was kept to a modest and manageable level.

There may also be occasions when it is still not possible to reduce the risk to the level indicated in Table C.1. In these situations it is necessary to review the situation using a principle called ALARP (As Low As Reasonably Practicable). This is described in Appendix E.

Appendix D
Controllability

The techniques suggested in the informative parts of [IEC 61508] are based on the assumption that it is necessary to increase the reliability of the equipment that is providing protection from a safety-related hazard (see Figure C.1). They also assume a constant and/or predictable environment. Road transport is neither constant nor predictable, and the process described here is being offered as a possible alternative approach, which will need to be validated.

Controllability is a technique to classify the hazards associated with ITS in general, and UTMC systems in particular. It was developed for the automotive industry by the Motor Industry Software Reliability Association [MISRA 1994] from an original concept created in [DRIVE Safely 1992]. An equivalent version for all ITS was developed during the European Framework III project PASSPORT [PASSPORT 1995a], the sequel to the Framework II project DRIVE Safely.

Controllability is a technique to find the SIL of an ITS which is independent of the traffic conditions, and that can take into account the possible reactions of the road user to, and the possible consequences of, any dangerous failure. It is also independent of the number of units deployed so that, say, a high volume equipment manufacturer will use the same SIL for the same system in the same application, as a low volume manufacturer.

Controllability provides a qualitative assessment of:

the ability of any category of user to control the safety of the situation after a dangerous failure.

Note that no attempt is made to specify the final effect explicitly, or to identify the probability of occurrence of the dangerous failure. The technique is based on the fact that in between a dangerous failure and a final event, there is a loss of control which is classified into one of the five categories shown in Table D.1.

Controllability Categories	Definition
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 customer satisfaction is the main consideration.

Table D.1: Definition of Controllability Categories

The degree of loss of control is assessed by considering (See Figure D.1):

- **Ranked Severity Factors**: The overall nature of the system
- **Levels of System Interaction**: Whether there are other systems which may be dependant on data being provided by the sub-system under consideration, e.g. a roadside system that provides safety-related information to vehicles
- **Degree of Control**: The degree of control that the sub-system has on the safety of the system when it is working normally, and that therefore might be lost
- **Provision of Backup**: The number, and type, of other sub-systems available to mitigate the loss of control caused by the dangerous failure
- **Reaction Time**: The speed with which it is necessary for a user or operator to react with the back-up sub-system(s) in order to mitigate the loss of control.

An effective approach is to perform the following tasks:

1. Make a qualitative judgement for each of these five factors 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. (If the grade is E for “Levels of System Interaction” then this factor should be ignored because it will not be relevant.)

2. Once the four or five grades have been obtained 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 that an average should **not** be taken because the grades do not have the same dimensions.)

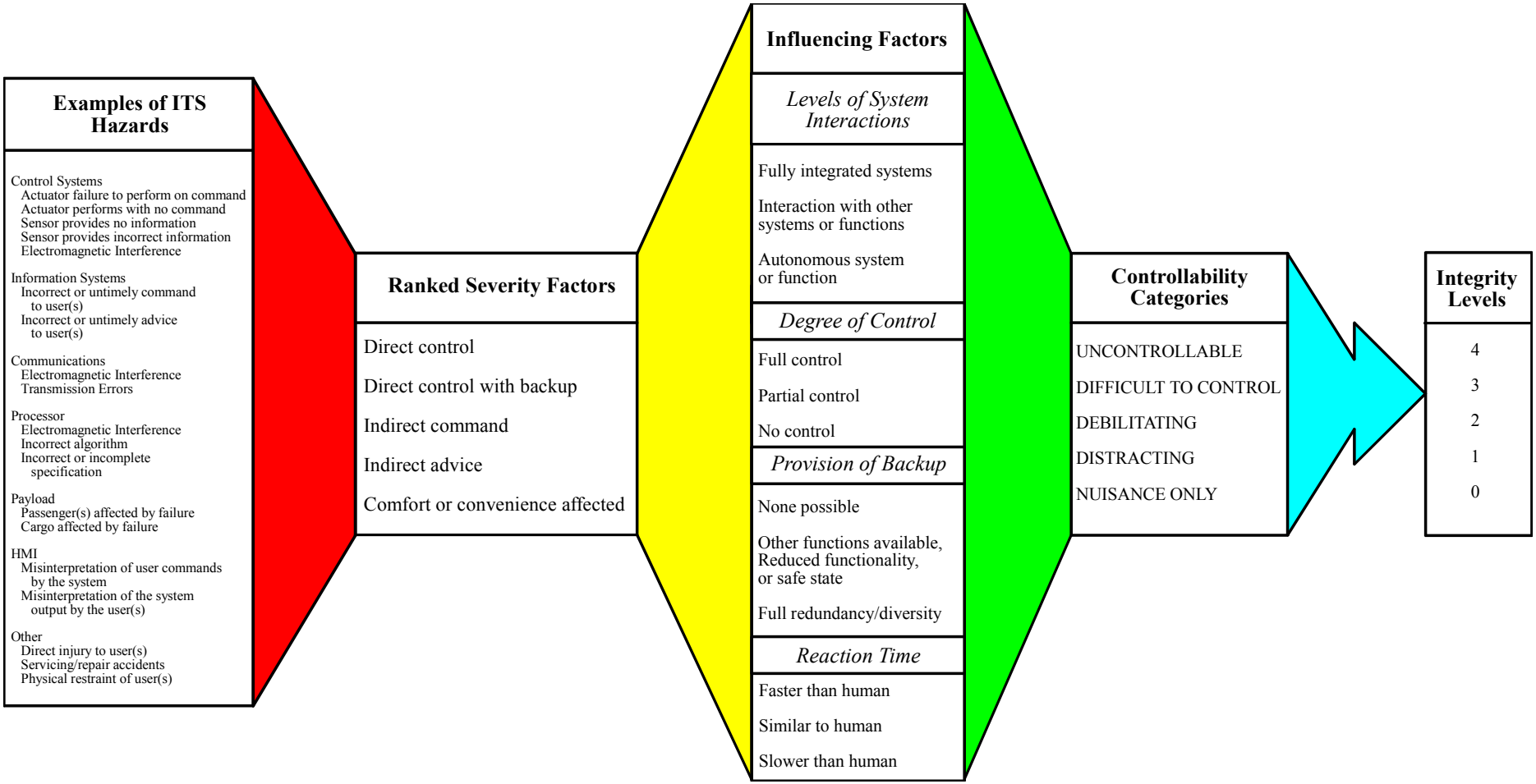

Figure D.1: Guide to assigning Safety Integrity Levels

3. Once a final grade has been chosen the full description for the corresponding Controllability Category in Table D.1 (using E for Nuisance Only up to A for Uncontrollable) should be studied to confirm that it does indeed reflect the controllability of the safety of the situation after a dangerous 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.

D.1 Total failure of an engine management system

The first scenario to be investigated is the "total failure of an engine management system" (as fitted to a road vehicle). 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 their 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.

D.2 Automatic incident detection

The second function that will be analysed is automatic incident detection. This is the function that will instruct upstream traffic via a 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**: automatic incident detection does affect other systems (i.e. the VMS 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 automatic incident detection 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 (that is 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 E
ALARP

The concept of ALARP (As Low As Reasonably Practicable) should be used when the functionality of a system is considered to be very desirable, but the risks associated with it are higher than one would normally wish to have.

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, which is defined as the product of the degree of severity of the harm and its probability of occurrence:

$$risk = probability\ of\ occurrence \times degree\ of\ severity\ of\ harm$$

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

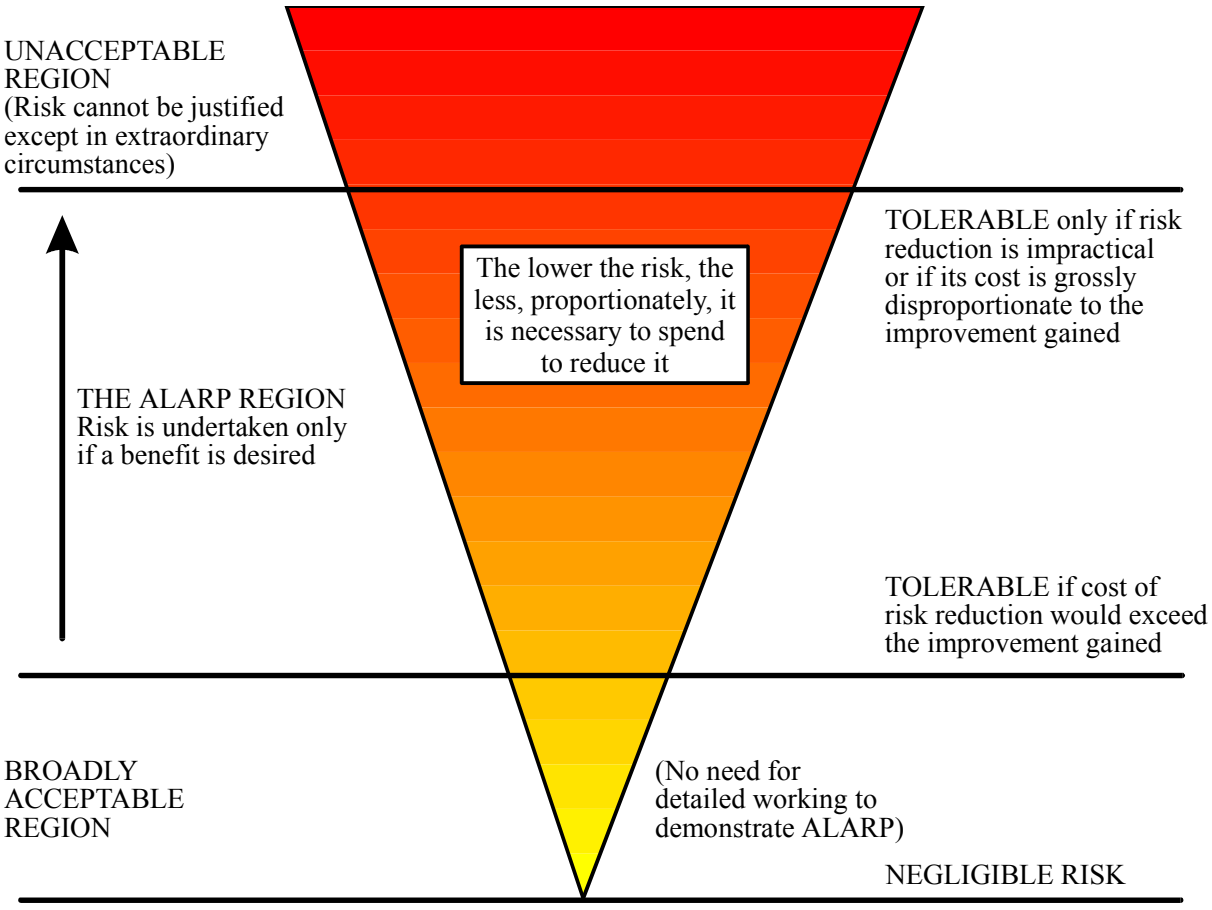

Figure E.1: Levels of risk and ALARP

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

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

3. The risk is between (1) and (2).

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 (2) has been reached, the risk should be made as small as ***practicable***, rather than as small as ***possible***.

In situation (3) 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 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 sector, 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.

[IEC 61508] gives a possible way of how to operate the principle of ALARP. Table E.1 shows the possible consequences of an accident against the frequency with which it might occur. Each cell in the table gives the category of risk that is assigned to that combination according to the definitions shown below. Note that it is intended that each application sector should give precise definitions to the contents of this table, and this will be necessary for UTMC systems if this approach is adopted.

	Consequence			
Frequency	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Table E.1: Risk classification of accidents

- Risk Class I: intolerable risk.
- Risk Class II: undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained.
- Risk Class III: tolerable risk if the cost of risk reduction would exceed the improvement gained.
- Risk Class IV: negligible risk.

In this example Risk Class I is in the “unacceptable region” of Figure E.1, Risk Classes II and III are in the “ALARP region”, and Risk Class IV is in the “broadly acceptable region”. Any use of Risk Classes II or III would have to be justified and their achievement demonstrated with a safety case.

Appendix F
Reference models

The first part of this appendix is based on Appendix C of [CODE 1998b].

One of the prime reasons for the development of an architecture is simplification; this is in order to satisfy the basic engineering principle of KISS, or "Keep it Simple, Stupid!". One of the main reasons for the resultant poor operation of a system, or even its outright failure, is that the complexity grows to the extent that no-one (developers, operators, users or maintenance staff) has a real understanding of what the system is, or does, or how it does it. At best it will not satisfy the various users' needs, and at worst it will be unpredictable or even unsafe [Neuman 1995, Wiener 1993].

It is also important to distinguish between the functions of a system and its behaviour. For example different well-known word-processing packages have the same functionality (more or less), but they behave in different ways; or again the basic functionality needed by a taxi company is the same as that needed for an ambulance service, but their quality attributes (such as reliability, availability, maintainability) will be different. It should be noted that, whilst an unsafe function will usually be as a result of a random failure, unsafe behaviour will often be designed into the system, namely as either systematic or systemic failures (see Appendix G).

One of the prime ways to simplify a system is to define a structure, in which certain aspects of the system can be captured. Traditional software development methods, for example Data Flow Diagrams, Jackson Structure Diagrams or even Object Oriented Modelling, do not start from any higher level structure; they allow the structure of a system to emerge from the methodology. Indeed it is important to note that the term "structured method", which is commonly applied to them, applies to the method itself, not necessarily to the results, and definitely not to the overall system. It might be better to describe them as "systematic methodologies".

A disadvantage of a higher level structure is that the result of the design process will not meet "equifinality". For system development this term, from system theory, means that, starting from the same requirements specifications, design rules, tools etc. a broadly similar outcome should be produced even when it done by different teams of developers from different organisations with different cultures. Whilst this may not matter for simple one-off systems, ITS in general, and UTMC systems in particular are required to be part of an overall family of products which are both interoperable and behave in a similar manners.

It was to cater for these issues in particular, though there are others, that the CONVERGE project recommended the use of layered reference models for the Level 3 and Level 2 Architectures [CONVERGE 1998a]. Consider Figure F.1 which shows the typical result of creating a Data Flow Diagram compared with a layered model [Hitchins 1992]. In the natural decomposition, on the left, the number of connecting lines in the Data Flow Diagram comes to $F(F–1)$, whilst in the layered structure, on the right, the number of connecting lines is $2(F–1)$, where F is the number of functions. The layers containing Functions B and C are augmented with the facilities to pass data straight through to the layers above and below.

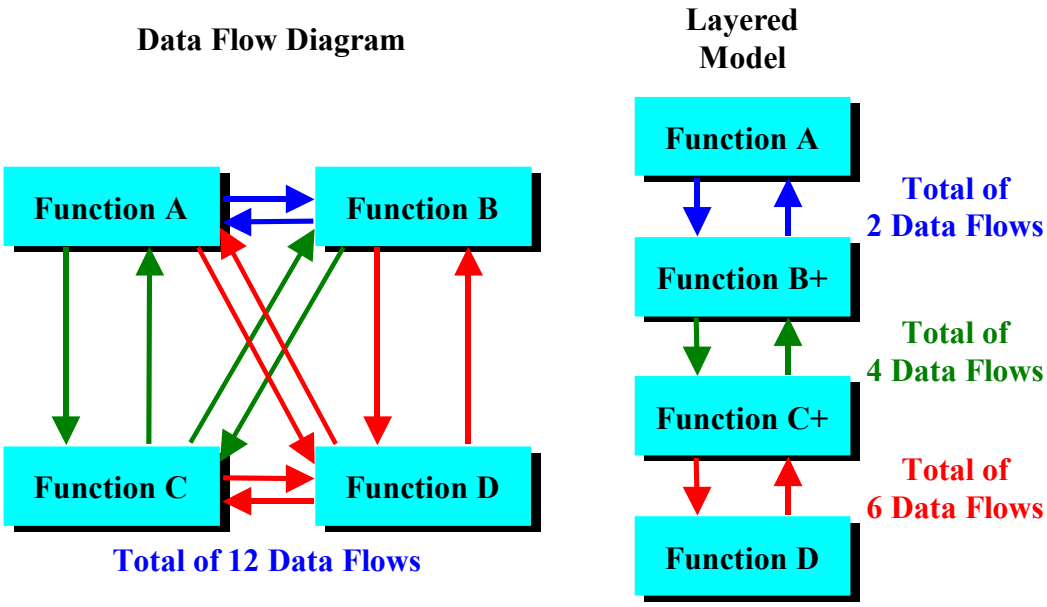

Figure F.1: Data Flow Diagrams vs. layered models

Of course, the situation in the Data Flow Diagram decomposition is not always as aggravating as it is shown here, but it is clear that the number of connections grows rapidly and makes matters very complex, e.g. consider the effort needed to add a new function, or to adapt a function, with consequences to one or more of the data flows.

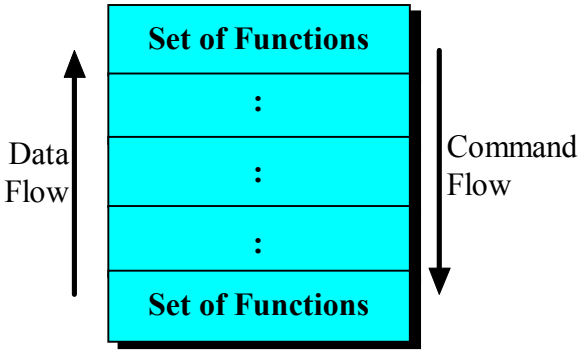

Figure F.2: Layered reference model

A full layered model is created by forming groups of functions into a number of layers, typically between three and seven (see Figure F.2). The layering offers special opportunities and features. These include:

- **Understanding:** The layered model provides a concise picture of the entire system in a manner that all stakeholders and domain experts can understand. It is a very effective way of achieving the "holistic" view of the system, and many of the behaviour, or "ontological" issues can also be analysed from this model.
- **Control:** The layered model offers the tactical advantage of hierarchical control, whereby the higher layers may exert control over, or influence the functioning of, the lower layers.
- **Functional distribution:** An ITS such as a UTMC system is likely have its functions distributed over a wide geographic area, by grouping these functions into layers the inherent property of distributiveness will be shown.

- **Time horizon**: As one goes up in the layers the length of time of the scope lengthens and reaction times can be extended. Thus the performance of the system can be optimised during development.
- **Level of detail:** As one goes up the layers the data is consolidated, leading to information that is more meaningful to humans, who tend to interact with the higher layers.
- **Graceful degradation:** The layered model shown in Figure F.2 has the property that the lower layers may operate without the existence of the higher layers, albeit with reduced functionality. This permits fail-safe conditions, and maintenance operations, to be planned at an early stage.

F.1 Layers of safety

The functions may be allocated to each layer for a number of reasons, one of which is safety. There are at least three different aspects of an ITS for which safety may be an issue.

1. Safety-critical or safety-related applications which are either protecting or controlling something. Their reaction time must be short and the data that they need are not sophisticated. The safety-related functions associated with such applications should be located in one of the lower layers.

2. Safety-related applications which are providing either advice or commands, often directly to the traveller. These will be the result of a (automatic) decision making process which has processed data from a number of sources, and the full control feedback loop is of long duration. The safety-related functions associated with such applications, in particular those confirming that such advice or commands are safe, will have to be located in a layer high enough to receive all the data they need, but low enough to be effective.

3. Any safety-related function needed to protect or control a property that emerges from having a combination of equipment will have to be located in a layer high enough to receive all the data from those items of equipment, probably after it has been processed, but low enough to be effective.

It is good practice to keep safety-related layers distinct (see Figure F.3), and for them to contain the minimum number of functions necessary. It is by this means that any of the special lifecycle activities required to reduce the risk of dangerous failures, especially at the higher SILs can be applied in a cost effective manner.

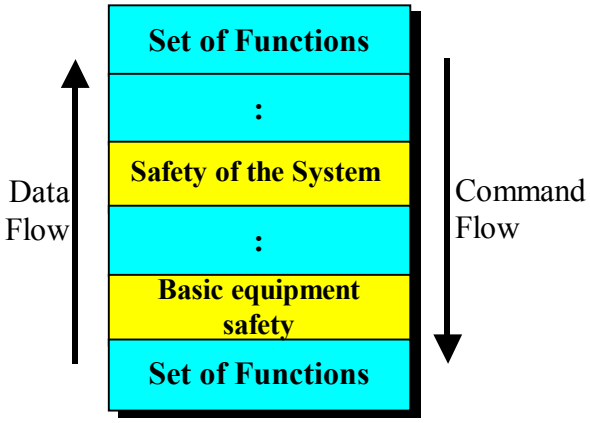

Figure F.3: Layered reference model with safety layers

Appendix G
Random, systematic and systemic faults

Failures are brought about by one of three basic mechanisms:

- random faults
- systematic faults
- systemic faults.

Random faults usually occur as a result of some degradation process in a material, or when a system is operated outside its limits. Typical examples include a piece of metal which will eventually break after is has been bent often enough, or a light bulb which will blow after a number of hours of use. The physics of these devices is well understood and it is possible to produce tables of failure rates from which one can calculate the expected failure rate of a complete product, e.g. [MIL-HDBK 217]. It is then possible to ensure that parts are changed during maintenance, before they are likely to fail. Unfortunately this situation does not hold for systematic faults.

A **systematic fault** is one that will always occur in the same manner in a given set of circumstances or, in other words, one that is designed into the system. This type of fault has become omnipresent in software, and engineers are still learning how to deal with them. Traditional engineering development is based upon the assumption that systems can be fully understood, and that any errors made in the design will be discovered during analysis or testing. The arrival of software has made all aspects of this assumption invalid. A program is a design, thus software faults are, by definition, systematic and should be discovered either by analysis or by testing. However a full and complete test of most computer programs will take longer than the average human lifetime and so whilst testing is useful, indeed essential, the process can only be used to find faults and not to prove their absence.

A **systemic fault** is one that affects or pervades the whole system, or at least a large part of it. For example, an omission or a fault in the specification, or even an incorrect interpretation of the specification, will result in the wrong system being built, and certain desired goals not being met: this can occur when the desired system is not fully understood. In addition, a failure to consider system safety in an adequate manner may result in systemic faults; for example, if a system has to be operated within certain safety limits, yet it is possible for these limits to be exceeded. Whilst systemic faults may occur systematically, they are unlikely to be discovered by normal automatic fault detection methods because they will not have been considered early in the lifecycle. A systematic fault will normally be made later in the lifecycle, often because of a mistake in the design process, e.g. during software programming.

Appendix H
Safety-related software

There are some fundamental differences between software and hardware. Hardware has both a development and a manufacturing phase and, whilst faults may occur at any time, it is often possible to test the correctness of an electro-mechanical prototype (STA) before it enters the manufacturing phase. If this is done under a good quality management system then any failures that do occur during operation are likely to be the result of wear and tear (random faults). The production of software is concentrated into the pre-manufacturing phases of the lifecycle, since the production of multiple copies is trivial and there is no wear and tear during its use. Thus any faults that may appear in software will be due to mistakes in the design (systematic faults: see Appendix G) and, since software tends be to be complex, such mistakes can occur frequently unless certain precautions are taken.

Since software is not subject to random faults there is the problem as to how to demonstrate that an ITS has a dangerous failure rate that conforms to Table C.1 and thus achieves a particular SIL. There has been some research on predicting a failure rate based upon a knowledge of the structure of the software and the development process. This research is promising for certain types of system, unfortunately not many safety-related systems fall into these categories, and when they do the dangerous failure rates that can be predicted only just reach those required for SIL 1.

An alternative approach is to recognise that, although the same fault occurs when the same conditions are repeated exactly, the conditions themselves often have so many possible states that, for all practical purposes, they can be considered to occur at random. A series of tests based upon this premise can produce useful data provided, of course, the input data set does indeed represent reality. Since the best way to achieve reality is to run a system live, operational history is very good evidence, when it has been recorded!

There is, however, another approach. The first point to note is that Table C.1 refers to a safety-related system as a whole, and not just to the software: it is therefore good practice to reduce as far as possible the reliance for the safety of the system on software. The second point to note is that the problem is not so much how to create very reliable software, as how to demonstrate, in advance, that it has been achieved. The use of certain techniques during the development process is known to make the creation of faults more likely, and so it is advisable to avoid them when writing safety-related software if at all possible. The list of undesirable techniques includes the use of pointers, stacks and floating point arithmetic.

The problem with pointers is that their use is rarely fully defined, for example when an item is referenced by a pointer which is subsequently deleted, should the item itself also be deleted? Programmers rarely have any control over what actually happens, or when. This is not acceptable when one of the fundamental assumptions about the development of a safety-related system is that you should know exactly what you are doing.

The uncontrolled use of stacks can lead to the running out of memory (one of the failures in the London Ambulance System [SWT_RHA 1993] and [Flowers 1996]).

Floating point numbers are not the continuous numbers they emulate and inaccuracies can, on occasions, creep in. To obviate this problem it is sometimes possible to work with integers, but the conversion between floating point and fixed point “integer” format can also

cause an error (an event in the sequence of actions that caused the failure of the Ariane 5 rocket).

Parts 6 and 7 of [IEC 61508] give considerable guidance on which techniques should, and should not, be used in order to achieve each SIL, and a more readable variation can be found in [MISRA 1994].

In fact restrictions of what may, or may not, be used in a programming language is only part of what is necessary when producing safety-related software. All safety-related systems should be developed with a Quality Management Plan [ISO 9000]. A specific plan for software development can be found in [TickIT], and the MISRA Guidelines [MISRA 1994] provides additional guidance on the entire software development lifecycle for safety-related software, in particular for:

- Specification and design
- Languages and compilers
- Configuration management: products
- Configuration management: processes
- Testing
- Verification and validation
- Access for assessment.

It is necessary to maintain a suitable balance between the adequacy of the measures used to achieve a SIL and the cost of doing so, and so the philosophy is based on the building up of confidence in the software. The MISRA Guidelines provide a set of qualitative requirements whose rigour increases with each SIL. Confidence is built up by the developer using two basic techniques:

- **Quality**: by working in accordance with a relevant Quality Plan a developer is assured that all phases of the lifecycle will be performed, and any data that needs to be passed back to an earlier phase (e.g. test results) will be acted upon
- **Knowledge of the System**: Most faults are made because of an inability to manage the actual, as opposed to the perceived, complexity of the system requirements. When it is not possible to mathematically prove the correctness of a system design (the usual condition) it is necessary to go as far down this path as is necessary; the higher the SIL the closer to a proof of correctness under all conditions one has to get. This requires a greater and greater understanding of the system itself.

The practical effect of this approach is that, as the SIL increases, not only must processes be performed, but there must be increasing justification that the actions being undertaken within those processes are the correct ones for that particular system.

Confidence is built up by an assessor in a similar manner. For the lower SILs it is only necessary to confirm that certain tasks have been performed, but as the SIL increases the assessor must gain more and more confidence that the correct lifecycle actions have been undertaken for that particular system.

Appendix I
Electromagnetic compatibility

Although electromagnetic interference (EMI) will occur at random, the same EMI will produce identical effects if the system is in the same state each time it occurs; the same situation that holds for software when it responds to a given stimulus. In addition the normal complexity of electronic circuits, and of software, when combined with the very large number of possible stimuli, means that it will never be possible to fully test the EMC or the software of the system. Testing can therefore only be used to identify faults, not to prove correctness.

The DRIVE II project EMCATT followed the philosophy used by [MISRA 1994] in order to develop a corresponding set of recommendations for achieving SILs for EMC. The main features of this philosophy are:

- EMC should not be added to a system as an afterthought, it must be designed in from the beginning.
- Testing can signal the presence of errors but not their absence, i.e. it cannot guarantee the EMC of a system. Additional forms of verification and validation, performed under a Quality Assurance regime [ISO 9000], are therefore necessary to gain the confidence that the EMC of the system has been developed correctly.
- Quality Assurance techniques are necessary to reduce the possibility of manufacturing faults compromising the EMC of the system.

In order to assess the EMC of a product a number of criteria are identified for each SIL in a "degree of assessment" table. This table shows that as the SIL increases greater knowledge is required of the system and the environment in which it is to operate. This knowledge is used to justify the actions that are undertaken to ensure that the necessary level of confidence is obtained. The degree of assessment table for EMC created in the EMCATT project was defined to correspond to the degree of assessment needed for software as defined in [MISRA 1994]. Although the EMCATT work requires further development, it nevertheless provides a useful starting point for dealing with EMC in "complex" systems.

Appendix J
Control rooms

The recent European HINT project has carried out a multi-modal investigation of the potential human factors problems arising from the introduction of new technologies in transport. One element on this work has been study of how new technologies will affect safety and working conditions in traffic control centres. The same set of issues have emerged, regardless of mode (air, water or road). These issues arise from a change in task for the operators from managing the traffic system directly to one of monitoring a system that is essentially automatic. The implications of these issue for policy are discussed in a set of recommendations by HINT [HINT 1999].

As a result of the change to much more automated systems, important changes will occur in operator tasks and performance. They include:

- **Modification of the situation awareness of the operator.** Situation awareness is the understanding of the current situation and the correct prediction of what will happen next. Awareness of automated system status, system intent, current actions and rationale for those actions are important issues to be taken into account in system design and operation. System feedback is becoming more and more processed and the mode of presentation of this information is decided by the design engineer. Feedback therefore needs to be ***managed***, to ensure comprehension and to prevent sensory overload. Information systems have the potential to increase situation awareness by providing information on aspects of the environment that machines can better perceive than the human senses, but they can also drastically reduce situation awareness by taking the operator out of the loop.

- **Issues of training and re-training.** Training for the future has to take into account the demands of new systems, and information technology in general in all transport modes. Introduction of some new systems may demand re-training of the personnel that operates it. Increased sophistication and innovation in automated devices will also require innovative training methods.

- **Influence of new technologies on the number and type of human errors.** It is unavoidable that new human errors will be generated by the new systems in the new operating environment. It is, therefore, essential that the behavioural response of the users of each new system is carefully studied before the wide scale implementation, and it is ensured that the sum effect of the system is positive so that human errors can be managed and their consequences are not catastrophic.

- **Long term behavioural adaptation** of the operators to the functioning of new systems means that if a change is introduced in a human operated transport system, the operators will adapt their behaviour to the change and this adaptation is not always in line with the intention of the initiators of the change. The main common issue across transport modes is complacency and over-reliance on new, often automatic systems. Delegation of responsibility on a newly implemented system may be another dangerous form of behavioural adaptation.

- **Issues of de-skilling and skill maintenance** of the operator. Automation, which is a central issue in expected new transport technology, even if its degree is different in the different transport modes, will produce a loss in traditional driving and vehicle operation

skills. Situations will occur where those skills are needed and therefore skill maintenance is an important issue. In addition, there will be a need for *re*-skilling. There may be a need for ***more*** skilled people in traffic control rooms, particularly as system complexity increases.

- **System failures** — their occurrence and consequences. It is an important task at the introduction of new systems to ensure that system failures are clearly and immediately reported to the operator, and that the operator be able to take over control over the system. There is a need to have well defined and practised procedures by which the operator can counteract system failures and take over command of the system.

In all of this, training and operational procedures emerge as central. Control room staff need to given adequate training, combined with re-training at regular intervals. Ideally, they should be involved in the design process itself. Moreover, operating procedures need to be unambiguous and take account of how responsibilities are allocated and information is shared among team members and between shifts (they thus need to cover handover from one team to another).

Appendix K
The Safety Case

The Safety Case described in this Appendix is based upon the CENELEC standards for the Railway Industry as described in [Skogstad 1999]. It should be treated as indicative of what will be required, but it will need confirmation for ITS in general and UTMC systems in particular. It should also be noted that it is unlikely that all Safety Cases will contain the same types of information; variations, intelligently applied, will have to be permitted to suit specific situations, especially for novel applications.

The main contents of a Safety Case should be:

1. Definition of the system
2. Quality Management Report
3. Safety Management Report
4. Technical Safety Report
5. Related Safety Cases
6. Conclusion.

K.1 Definition of the system

The purpose of this information is to define the target of evaluation in a unambiguous manner. It should comprise of, where relevant:

- General description of the system
- General overview of the interfaces with other systems
- System hardware structure — a systematic reference to all the hardware units in the entire system
- System software structure — a systematic reference to all the software units in the entire system
- Baseline documentation — this is itself a list of (references to) documents that provide all the configuration data for all requirements, designs, hardware, software, computer chips, drawings etc. A description of any changes since the last baseline should be provided where relevant.

K.2 Quality Management Report

The purpose of this document is to provide the evidence that a sound quality assurance process has been performed. It should comprise of, where relevant:

- Company quality management policies and plans
- Quality assurance certificates
- Register / description of quality assurance models and methods
- Quality audit non-conformances and their current status
- Register of reports from review or inspection work performed
- Register of phase related supplier management reviews

- Type certificates for modules and units, according to the system hardware structure. These certificates should contain information about environmental robustness, including EMC, temperature, shock and vibration
- Equipment test reports
- Installation test report
- Specific site review reports
- Supplier's conclusion — an analysis as to why the activities performed were sufficient.

K.3 Safety Management Report

The purpose of this document is to provide evidence that the activities defined in the safety plan were all carried out. It should comprise of, where relevant:

- The Safety Plan
- Register of competence — all key personnel, including third party assessors
- Register/description of safety models and specific methods
- Register of safety-related internal and external audits
- Register of safety reviews/walkthroughs — on (changed) drawings and software
- Preliminary Safety (Hazard) Analysis
- Detailed Safety (Hazard) Analysis
- Operational Safety (Hazard) Analysis
- Hazard Log — list of all the hazards identified
- Safety / reliability calculations
- Explicit imposed conditions from Hazard Analysis / Log
- Supplier's conclusion — an analysis as to why the activities performed were sufficient.

K.4 Technical Safety Report

The purpose of this document is to explain the technical principles which assure the safety of the design. It should comprise of (references to), where relevant:

- Description of the technical characteristics of the system
- Validation reports† on the requirements
- Validation reports† for hardware modules
- Validation reports† for software units
- Safety certificate for hardware modules and software units — for example a validation report†, a specific Safety Case, or module Approval by some authority
- Validation reports† for all safety-related tools
- Validation reports† for all site specific documentation
- Factory and site acceptance tests reports
- Supplier's conclusion — an analysis as to why the activities performed were sufficient.

† Validation reports in this context should emphasise safety, and include:

- A report from the safety-related review, walkthrough etc.
- An analysis of the safety aspects of the sub-system / module; any potential hazards should be in the Hazard Log
- Specific safety-related testing.

K.5 Related Safety Cases

This document should provide reference to any Safety Cases for other vital systems that contribute to the functional totality of the system.

K.6 Conclusion

This document should form an analysis of why the performed activities, and the system attributes, are sufficient.

Appendix L
Table of Standards

This Appendix contains a list of relevant reference material e.g. standards and guidelines. At the present time it is issued as a separate document (UTMC22/5).