Chapter 14

Safety assessment and human factors

Carl Sandom

14.1 Introduction

This chapter examines the safety assessment of systems that include people. Specifically, the chapter is concerned with the analysis of safety in complex, information systems that characteristically support dynamic processes involving large numbers of hardware, software and human elements interacting in many different ways. The chapter assumes little or no knowledge of either safety assessment or human factors assessment techniques.

Information systems often require complex functionality to assist human operators with intricate tasks such as, for example, the conflict detection and resolution systems that assist air traffic controllers with critical decision-making tasks in modern air traffic management. As well as the complexity of modern technology and organisations, humans are also themselves inherently complex and the human factors relating to the physical and cognitive capabilities and limitations of system operators must also be addressed during the assessment of any complex, interactive system.

Information systems involving extensive human interactions are increasingly being integrated into complicated social and organisational environments where their correct design and operation are essential in order to preserve the safety of the general public and the operators. This chapter focuses on the safety assessment of information systems, typically operating in real time, within safety-related application domains where human error is often cited as a major contributing factor, or even the direct cause, of accidents or incidents.

14.2 Information systems and safety

The safety assessment of modern information systems is a growing concern; for example, command and control (C2) systems are now being developed with the potential for increasingly catastrophic consequences from a single accident. C2 systems that control everyday activities from power generation to air traffic management have the potential to contribute to – if not to cause – deaths on a large scale. Moreover, the contribution of modern Decision Support Systems (DSS), such as in modern battlefield digitisation applications, to hazardous events is often underestimated or worse still ignored.

Information systems typically provide organisational and environmental data to inform decision-making. Depending on its use, this data can lead to erroneous operator actions affecting safety, as was the case when the crew of the USS *Vincennes* incorrectly interpreted the data presented by their C2 system and a decision was taken to shoot down a commercial airliner killing 290 passengers [1]. Despite extreme examples like this, information systems are often not considered to be safety-related.

The view of information systems as not safety-related is often shaped by preliminary hazard analyses concluding that the system in question has no safety integrity requirements when applying guidance from risk-based safety standards such as UK MoD Defence Standard 00-56 [2] or IEC61508 [3]. This perception is often reinforced by anecdotal evidence of information systems that have previously tolerated relatively high *technical* failure rates without incident.

Another prevalent view is often that information systems are 'only advisory' and cannot directly cause an accident – the implication is that the human(s) in the system provide sufficient mitigation between the manifestation of a 'system' hazard and the credible accidents. While this perception may be correct, the assertion is often made without a rigorous analysis of the individual and organisational human factors involved and substantiated arguments being made for the validity of any mitigation claims. Also, this perspective overlooks the fact that credible but erroneous data can be presented by such systems and therefore no mitigation would be provided by operators if the data looks correct.

An approach to the safety assessment of information systems must be taken to identify risks within the system at the different levels, as complex interactions between different system levels can result in hazards caused by a combination of technical and human failures. Also, an analysis of the human factors is essential to understand the significance of the human mitigation that is typically significant within information systems. Without a holistic approach such as this, information systems tend not to be thought of as safety-related.

Before addressing specific issues relating to the assessment of human systems; it is necessary to understand some of the key concepts associated with the general process of system safety assessment. The following section will examine the concepts of safety, risk and hazards before looking at some of the issues relating to the specification of safety requirements for systems involving humans.

14.3 Safety assessment

The term 'safety' has many different connotations and it can be related to many different concepts such as occupational health and safety, road safety or even flight safety. It is important to make the distinction between these concepts and *functional safety* in order to appreciate what it is that safety-related system designers are trying to achieve. Storey [4] maintains that functional safety is often confused with system reliability; however, even the most reliable system may not necessarily be safe to operate. For example, the cause of the Airbus A320 Strasbourg accident was attributed to the fact that the pilot inadvertently selected a descent rate that was too fast – in this example, the aircraft behaved reliably but it crashed into a mountain with fatal consequences. System reliability is necessary but is not sufficient alone to ensure the functional safety of a system.

Functional safety is a difficult concept to define. The current drive towards enhancing system safety in the UK has its origins in the Health and Safety at Work Act 1974 [5] although this act is often incorrectly associated only with occupational safety. There are many different definitions of safety. For example, the Ministry of Defence (MoD) define safety as: ‘The expectation that a system does not, under defined conditions, lead to a state in which human life is endangered’ ([3], p. A-3). Alternatively, the British Standards Institution definition of safety is ‘The freedom from unacceptable risks of personal harm’ ([6], p. 4).

Although these definitions of safety and risk may be intuitively appealing, Ayton and Hardman [7] argue that a major theme emerging from the literature on risk perception is the emphasis on the inherent subjectivity of the concept. The subjectivity associated with risk can be illustrated by the way that an aircraft accident attracts much more media attention than the far greater number of road traffic accidents that occur in the UK each year.

It can be argued that safety should be defined in terms of acceptable loss or tolerability. The UK Health and Safety Executive [5] require risk to be quantified and it can be considered tolerable only if it has been reduced to the lowest practicable level commensurate with the cost of further reduction. This important concept is known as the ALARP (As Low As Reasonably Practicable) principle and it is illustrated in Figure 14.1.

Despite the difficulties in defining safety and risk, a common theme that links many definitions is that risk is a product of the *probability* of an accident occurring and the *severity* of the potential consequences [4, 7, 8, 9]. From the previous discussion, it should be clear that safety and risk are inextricably linked; indeed it may be argued that the task of producing a safety-related system can be seen as a process of risk management.

Lowrance’s definition of safety [9], in terms of risk, has captured this sentiment succinctly and it will be adopted throughout the remainder of this chapter:

> We will define safety as a judgement of the acceptability of risk, and risk, in turn, as a measure of probability and severity of harm to human health. A thing is safe if its attendant risks are judged to be acceptable.
>
> ([9], p. 2)

Information systems developers must understand the issues and develop the skills needed to anticipate and prevent accidents before they occur. Functional safety must be a key component of the system development process and it must be designed into

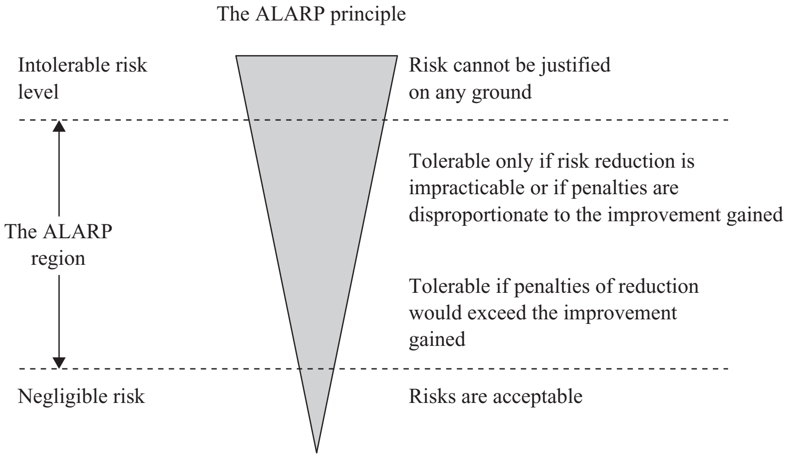
The ALARP principle
Intolerable risk level
Risk cannot be justified on any ground
Tolerable only if risk reduction is impracticable or if penalties are disproportionate to the improvement gained
The ALARP region
Tolerable if penalties of reduction would exceed the improvement gained
Negligible risk
Risks are acceptable

Figure 14.1 The ALARP principle for risk (adapted from [5])

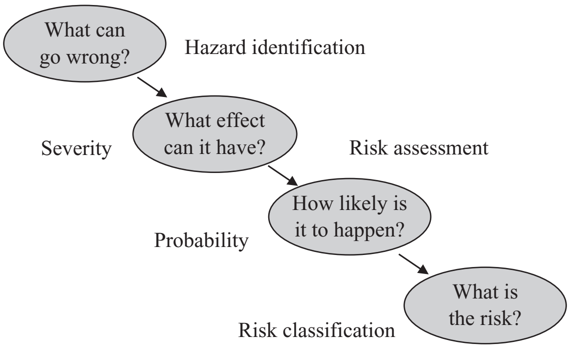

Figure 14.2 Safety assessment process

a system from the onset. System developers need different techniques for quantifying system risks and this must be preceded by the identification and analysis of system hazards. These processes are known collectively as system safety assessment.

Safety-related system designers must undertake safety assessments that integrate the concept of hazards with that of risk. To be comprehensive, a system safety assessment must address: hazard identification (what could go wrong?); hazard severity (how serious could it be?) and hazard probability (what are the chances of it happening?). This process will enable an assessment to be made of the system risk. This basic safety assessment process is depicted in Figure 14.2.

Safety-related systems designers must in some way identify the manner in which a system can cause harm in order to improve the safety of a system by preventing accidents before they occur. In simple terms, systems hazards lead to accidents;

therefore it is important to examine the fundamental question of what constitutes a hazard in a safety-related system.

Hazards have been defined in a number of ways. Defence Standard 00-56 ([2], p. A-2) defines a hazard as a: '*Physical* situation, often following some initiating event, that can lead to an accident'. This definition is unhelpful when considering where the hazards lie within a given system; however, it does imply the important point that a hazard will not always result in an accident. Leveson's definition of a hazard is useful in a systems context:

> A hazard is a state or set of conditions of a system that, together with other conditions of the environment of the system, will lead inevitably to an accident.
>
> ([8], p. 177)

Leveson's definition of a hazard is expressed in terms of both the environment and the boundary of the system. This is an important distinction from other definitions as system hazards can only be fully identified and analysed if a system is considered in the context of its operational environment. Leveson's definition as stated, however, implies that a hazard will inevitably lead to an accident. An alternative view of this hazard cause–effect relationship contends that a hazardous situation will not always lead to an accident and that a properly designed system can be returned to a safe state. From this discussion, a definition of a hazard is proposed which is useful in a *system* context:

> A hazard is a state or set of conditions of a system that, together with other conditions of the environment of the system, may lead to an accident.

Having examined some of the key concepts associated with safety assessment, it is useful to focus on the main reason for assessing any system which, at the start of any project, is to derive requirements and then later to ensure that these requirements have been fulfilled. As this chapter deals with system safety, the issue of safety requirements will now be examined.

14.4 Safety requirements

The terms 'safety requirements' and 'Safety Integrity Levels (SILs)' are often both used synonymously by systems designers. However, although the concept of SILs appears in almost all modern safety standards, there is no consensus about what they actually mean or how they should be used [10]. Nonetheless, the link between development processes and SIL is often used to determine what development activities implementation contractors are required to undertake.

Generally, the higher the SIL the more rigorous the development processes are required to be. However, a problem can arise if the system is deemed to be SIL 0 as this generally implies that the system does not affect safety and therefore no safety requirements are imposed on how it is developed. Information systems in particular are often deemed low or no SIL systems. This can be illustrated with a simple example. For a typical information system, let us assume that the following safety integrity

Table 14.1 SIL claim limits (adapted from [2])

SIL	Failure rate	Quantitative description (occurrences/operational hour)
4	Remote	1.0E-05 to 1.0E-06
3	Occasional	1.0E-04 to 1.0E-05
2	Probable	1.0E-03 to 1.0E-04
1	Frequent	1.0E-02 to 1.0E-03

requirement is specified, based upon an existing system's perceived acceptable failure rate:

The system will have a maximum failure rate of 100 failures/year

Given the typically high tolerable failure rates for information systems, this may not be unusual or unreasonable. If there is only one instance of the system, and it runs continuously, this equates to 8,760 operational hours per year. This gives:

$$\textit{Target system failure rate} = 100/8,760 = 0.01 \text{ failures/op hr}$$

To derive a SIL, reference needs to be made to the appropriate safety standard. If, for example, the SIL claims table of DS 00-56 [2], shown in Table 14.1, is used to determine the resultant SIL, then the system developer may conclude that the requirement is for a non-safety-related system as the target failure rate in this example is less than the SIL1 claim limit.

This simple example illustrates a common approach to determining if a system is safety-related or not based upon the view that safety integrity is *the only* safety requirement for a system. Integrity is not the whole picture, as previously discussed with reference to system reliability and the A320 crash. An alternative view is that it is the specified *functionality* and *performance* of an information system that determines both causes and mitigation of risks within the external environment. Leveson [11] presents compelling evidence, based on her review of major software-related accidents, that software (hence system) reliability has never been the cause of such disasters. Fowler and Tiemeyer [12] offer an excellent and detailed discussion on this perspective and this is extended to address human factors in Sandom and Fowler [13].

Traditional approaches concentrate on failures alone and the impact of the failure to provide the system functionality. However, it is equally important to analyse the protective aspects of the system in operation to identify what system functions mitigate external hazards rather than contribute to them. If the specified information system functionality were insufficient to achieve the necessary risk reduction then, no matter how reliable an information system was, it would not be safe.

Commonly used safety standards, such as DS00-56 [2], IEC61508 [3] and DO178B [14] adopt this failure-based view of safety without emphasising the importance of specifying safe functionality in the first place. Compliance with these standards, whilst giving some assurance of information system *integrity*, does little to ensure the correct functionality and performance of the information system and therefore that they are really safe. This has potentially serious implications for commonly used risk-classification schemes that appear to provide an easy way of converting the assessed severity of a hazard into a tolerable frequency of occurrence and thus into a safety integrity requirement. Setting realistic safety requirements must take into account system functionality, performance *and* integrity.

This has implications when assessing systems and, in particular, when assessing the human contribution to system safety. Any method of assessing the safety of human activities must address human functionality, performance *and* integrity. Before we return to this theme, it is essential to provide a common framework of systems terminology that can be used for the remainder of the chapter.

14.5 Systems and boundaries

It can be argued that if any component of the system directly or indirectly affects safety, then the system should be considered safety-related. However, before pursuing this line of argument, careful consideration must be given to what constitutes a system and where the system boundaries for information systems can typically be drawn.

Figure 14.3 shows a representation of a typical information system and its boundaries. In this representation the core system represents the various subsystems implemented in hardware, software or allocated to human operators. The service level

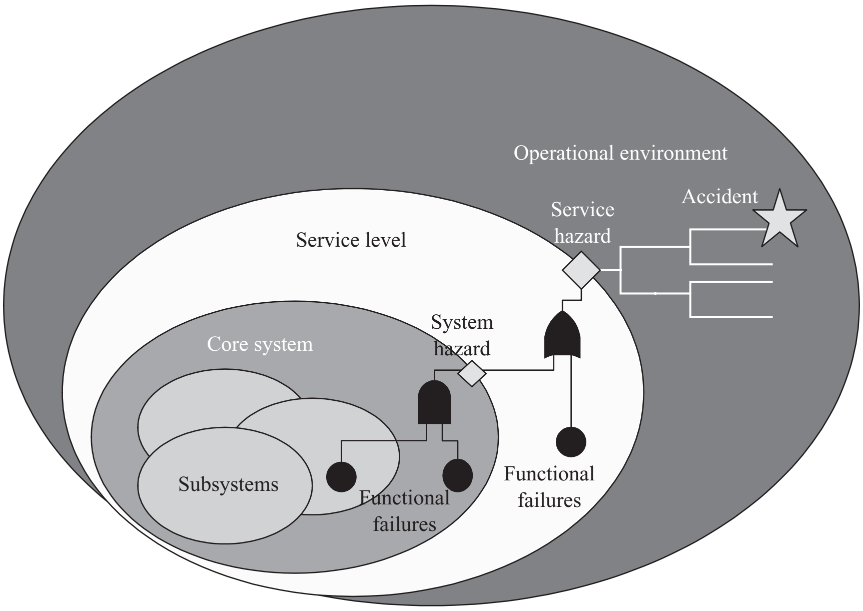

Figure 14.3 A system model

represents the service provided by the information system users or operators, encapsulating the operational procedures and other organisational factors. The service level is usually the responsibility of the operational authority. Finally, the operational environment represents the wider application domain within which the system resides and typically contains people, procedures and equipment issues. For example, an air traffic management system would be a core system used by air traffic control operators providing an ATC service to users in the operational environment that would provide aircraft control.

As discussed in detail in Chapter 1, human factors is a broad discipline concerned with the need to match technology with humans operating within a particular environment; this requires appropriate job and task design, suitable physical environments and workspaces and human–machine interfaces based upon ergonomic principles. Human factors analyses must examine the broad ergonomic, organisational and social aspects of an operational system in use within its operational environment. At the other end of the spectrum, human factors analyses must also examine how human–computer interfaces can foster the safe, efficient and quick transmission of information between the human and machine, in a form suitable for the task demands and human physical and cognitive capabilities.

Analyses of human factors issues in safety-related systems consistently reveal a complex set of problems relating to the people, procedures and equipment (or technology) interacting at each system level of a specific environment. These attributes are normally very tightly coupled and each of these attributes can interact with the other. To undertake a systematic analysis of all aspects of systems safety, the following basic principle should be observed:

> Each system attribute (people, procedures and equipment) must be considered at every system level (core, service, operational) to a depth of analysis commensurate with the human integrity requirements.

To achieve this goal, human integrity requirements must be determined and an argument must then be constructed using this framework to ensure that the whole systems context of use is considered during system safety analyses using appropriate analysis techniques. Generally, system safety assurance requires risk modelling to be undertaken using focused analyses to determine the hazard causes and mitigations.

14.6 Risk modelling

A systematic approach is required to define the interfaces between system components, boundaries and interactions to clearly define the risks and mitigations posed within each system level. This ‘system of systems’ approach to safety case development allows the risks of each separate part of the system to be clearly defined and the relevant stakeholders can provide evidence to underwrite the parts of the system for which they are responsible.

Such an approach is particularly important for information systems that require both technical and operational analyses to define the hazards and their mitigation.

This suggests how important it is to define the boundaries and targets for each of the system levels and use an integrated approach to support the practical development of a realistic safety case.

Figure 14.3 suggests that the scope of human factors analyses must address the whole system, service and operational environment. This vast scope presents a challenge for the systems engineer who needs to consider the safety-related aspects of the system and even then to focus the often limited resources available on the most critical system functions. The processes for determining human or technical safety requirements will necessarily be based upon different analysis techniques when dealing with human rather than technical subsystems.

The safety assurance of information systems must identify risks within a system at the different levels, as complex interactions between different system levels can result in hazards caused by a combination of technical and human failures. Accidents occur in the external environment as depicted in Figure 14.3. However, although a system developer may only be responsible for the safety of the core-system implementation, the effects of core-system hazards in the operational environment must be clearly understood. To undertake the overall process of modelling, risks and mitigation must be understood.

An accident is an unintended event that results in death or serious injury. With reference to Figure 14.3, accidents occur in the operational domain. As discussed, a hazard is a system state that may lead to an accident – whether it does or not, depends on the availability of mitigations to break the sequence of events that would otherwise lead to an accident (this is shown in Figure 14.4). Such mitigations are called consequential (since they relate to the consequences of a hazard, and can be

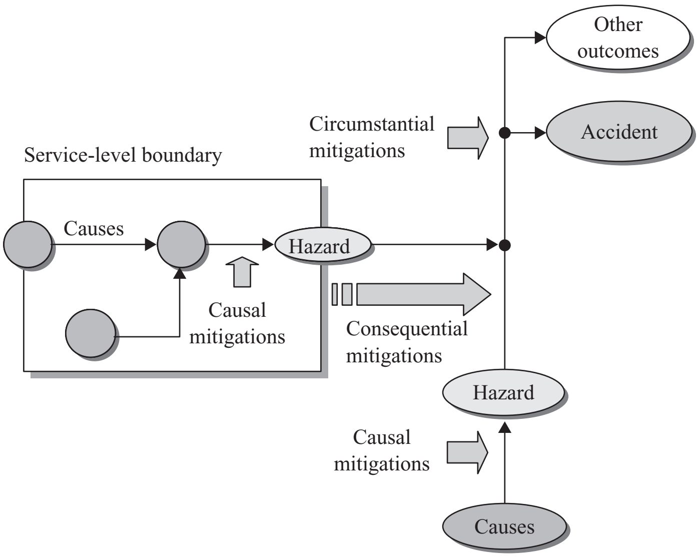

Figure 14.4 Accident sequence

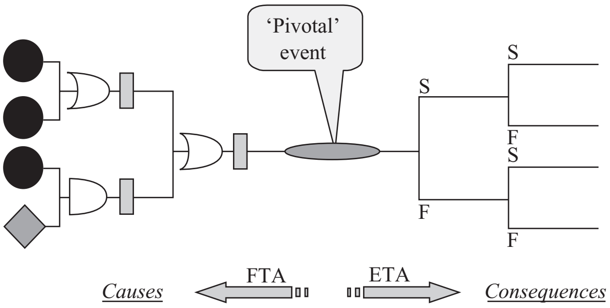

Figure 14.5 Risk model

either deliberately provided or circumstantial (i.e. purely a matter of chance). The likelihood of an accident is also dependent on the likelihood that the hazard would occur in the first place. This in turn is dependent on the frequency of occurrence of the underlying cause(s) of the hazard and on the availability of (causal) mitigations to break the sequence of events between the causes and the hazard itself.

A safety-related system may provide either causal or consequential mitigations. For a typical information system, human operators provide many of these mitigations. System operators often provide sufficient mitigation between the manifestation of a 'system' hazard and the credible accidents. However, as discussed, this is often without a systematic or rigorous analysis of the human factors involved to validate these mitigations and their claimed risk reduction.

A risk model must be constructed by the safety engineer, as illustrated in Figure 14.5. A risk model is a convenient way of modelling risk by linking the *causes* of a hazard, modelled using Fault Tree Analysis (FTA), and the *consequences* of a hazard, modelled using Event Tree Analysis (ETA).

The point in the Fault Tree (FT) hierarchy at which the link to an Event Tree (ET) is established is known as a pivotal event. The pivotal events typically correspond with the main system and or subsystem hazards. One FT/ET pair is constructed for each hazard and values are ascribed both to the probability of occurrence of each casual factor in the FTs and to the probability of success or failure of the outcome mitigations represented by the branches of the ETs. Using the facilities of a mature FTA/ETA tool, the overall probability of an accident from all causes can be determined and compared to the safety target(s).

This process of risk modelling will often be undertaken by systems engineers without fully considering the human hazard causes or, as discussed, the consequential mitigations. A valid risk modelling process must integrate human factors analyses into both the FTA and ETA process to produce defensible and compelling safety arguments. This chapter now considers how realistic human safety assessments of the core and service-level system risks and mitigations can be undertaken and integrated within the systems engineering process to determine human safety requirements for a typical information system.

14.7 Assessing the human contribution to safety

A pragmatic method of assessing the human contribution within the overall safety assessment process is required to focus human factors analysis on the safety-related aspects of the system using suitable human factors techniques. One approach for assessing the human contribution to system safety is outlined here integrating the use of appropriate human factors analysis techniques within the systems engineering lifecycle for the systematic determination and realisation of human factors safety requirements. As discussed previously, the key to safety assurance is to ensure that each causal factor (people, procedures, equipment) must be considered within and between each system level (Figure 14.1) to a depth of analysis commensurate with the integrity required of the human subsystem.

Although the analysis begins with the core system/subsystem level, the approach takes into account the human risks and mitigations at the service and operational levels. Although these techniques are described below in relation to the human subsystems, the method also provides for the analysis of human risks and mitigations at the service and operational levels.

Specific safety-related human factors activities comprise Critical Task Analysis (CTA) and Human Error Analysis (HEA) as depicted in Figure 14.6.

These safety-specific activities should be planned to ensure that there is no overlap with wider, system-level human factors activities while taking maximum advantage of system hazard and risk assessment analyses for the other subsystems. The CTA and HEA activities are tightly coupled and are based upon, and integrated with, the FTA and ETA risk modelling analyses described previously and depicted in Figure 14.5.

Two iterations of each CTA and HEA should be undertaken during the typical systems development lifecycle and, as the analyses become more focused, the results will inform each other as shown in Figure 14.6. These activities are complementary

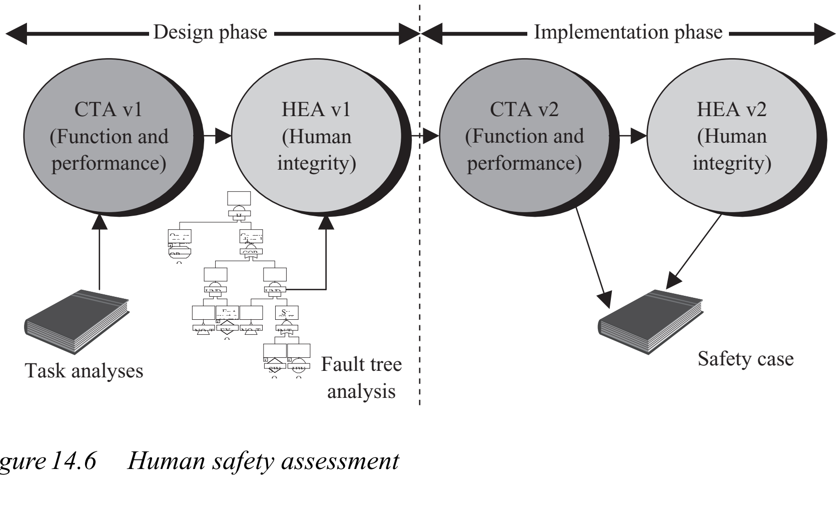

Figure 14.6 Human safety assessment

as CTA and HEA are bottom-up and top-down analysis techniques respectively (from a hazard to human event perspective). This combination of top-down and bottom-up analyses significantly increases the probability of identifying inconsistencies in the individual techniques and thus enhances safety assurance.

As discussed previously, the specification of system safety requirements must address functionality and the associated performance and integrity levels. Integrating human factors analyses into the general safety assessment process facilitates the specification of safety-related human functionality and its associated performance and integrity levels and this process is now described in some detail.

14.7.1 Human safety functions

A CTA can be undertaken to identify and analyse the potential for human performance errors in critical operational tasks. CTA concentrates on the human factors aspects of the Human Machine Interface (HMI). This analysis is a bottom-up technique used broadly to analyse the relationships between system hazards; operational tasks (identified by task analysis; see Chapter 5 for a detailed discussion) and the HMI design. The analysis works in a bottom-up fashion from operational tasks, related to basic error events, to identified service-level hazards.

A CTA can initially focus on the identification and analysis of the relationships between system hazards and safety-related operational tasks. This analysis will enable any hazard and task analyses to be checked for consistency, providing confidence in subsequent safety assurance claims. Any deficiencies – such as hazards with no related operational tasks or operational tasks (deemed as safety-related by subject matter experts) with no relationship to identified hazards – can be highlighted. The CTA will also identify opportunities for hazard mitigation through removal of human error potential and improved information presentation by comparing the task analysis with HMI design guidelines from appropriate sectors (for example Federal Aviation Authority ATM HMI design guidelines [15]). Undertaking a CTA can therefore allow the system developers to identify the human safety functions.

14.7.2 Human integrity targets

For highly interactive systems situated in dynamic environments, the quality of the information acquired through the interface can contribute significantly to system failure, and the design of the human–computer interface can have a profound effect on operator performance and system safety. It is imperative that qualitative and, where appropriate, quantitative safety arguments are made for each critical human failure linked to service-level hazards identified during the system risk modelling. The depth of analysis required to make a compelling safety argument for each critical human event must be determined by these derived human integrity requirements. Analyses should also identify opportunities for hazard mitigation through removal of human error potential and improved information presentation.

The derivation of quantitative human integrity targets for safety-related systems is difficult. Human Reliability Analysis (HRA) techniques have been developed to address this issue (see Chapter 8 for a detailed discussion). However, HRA techniques have mainly been applied successfully within process control environments, such as the nuclear industry for example, where the operating and environmental conditions are relatively more easily quantifiable. HRA techniques are much more difficult, and expensive, to apply meaningfully to human systems with highly dynamic environmental contexts.

A pragmatic method of addressing this issue is to undertake a Human Error Analysis (HEA) focused specifically on the basic human events identified in the system fault trees. HEA analysis is a top-down technique used broadly to model the relationship between service-level hazards and critical human failures, and the mitigating aspects of the system design. For systems which typically have a high degree of operator interaction, many of the FTA basic events will be identified as human interactions. An example fragment of an FTA is shown in Figure 14.7 with the basic human event OP NOT DET.

Once each fault tree is modelled, predictive, quantitative failure data can be input at the bottom from availability and reliability data for all hardware and software based events. By subtracting these values from the associated hazard target, quantitative Human Integrity Targets (HITs) can then be calculated for each critical human event. It should be understood that these basic human events originate from both the system and service levels taking the operational context into account.

The HEA would then focus on developing specific safety arguments for each basic human event to provide evidence that the HITs can be achieved. For critical areas, where the HEA reveals that the HITs are unrealistic, mitigations can be re-assessed and recommendations developed for further action. In this way, no predictions are being made about the human error rates; rather, the HITs are derived from the remaining integrity requirements once the hardware and software failure data is input and a qualitative analysis is undertaken to ascertain if the remaining human integrity requirements are realistic.

14.8 Summary

The technical, social and human complexity involved in the development of modern interactive systems presents a number of problems that are exacerbated when the failure of an interactive system has potentially lethal consequences. Safety-related systems are used in complex social contexts and the integrity of their design and operation is essential in order to ensure the safety of the public and the environment.

The prevalent view is often that information systems are not safety-related even when used within safety-related environments; this perception is often reinforced by anecdotal evidence of information systems that have previously tolerated relatively large *technical* failure rates without incident. The view is often that information systems are ‘only advisory’ and cannot directly result in an accident – the implication is that the human(s) in the system provide sufficient mitigation between the manifestation of a ‘system’ hazard and credible accidents. While this perception may be correct, the assertion is often made without a rigorous analysis of the human factors involved and arguments being made for the validity of the mitigation claim.

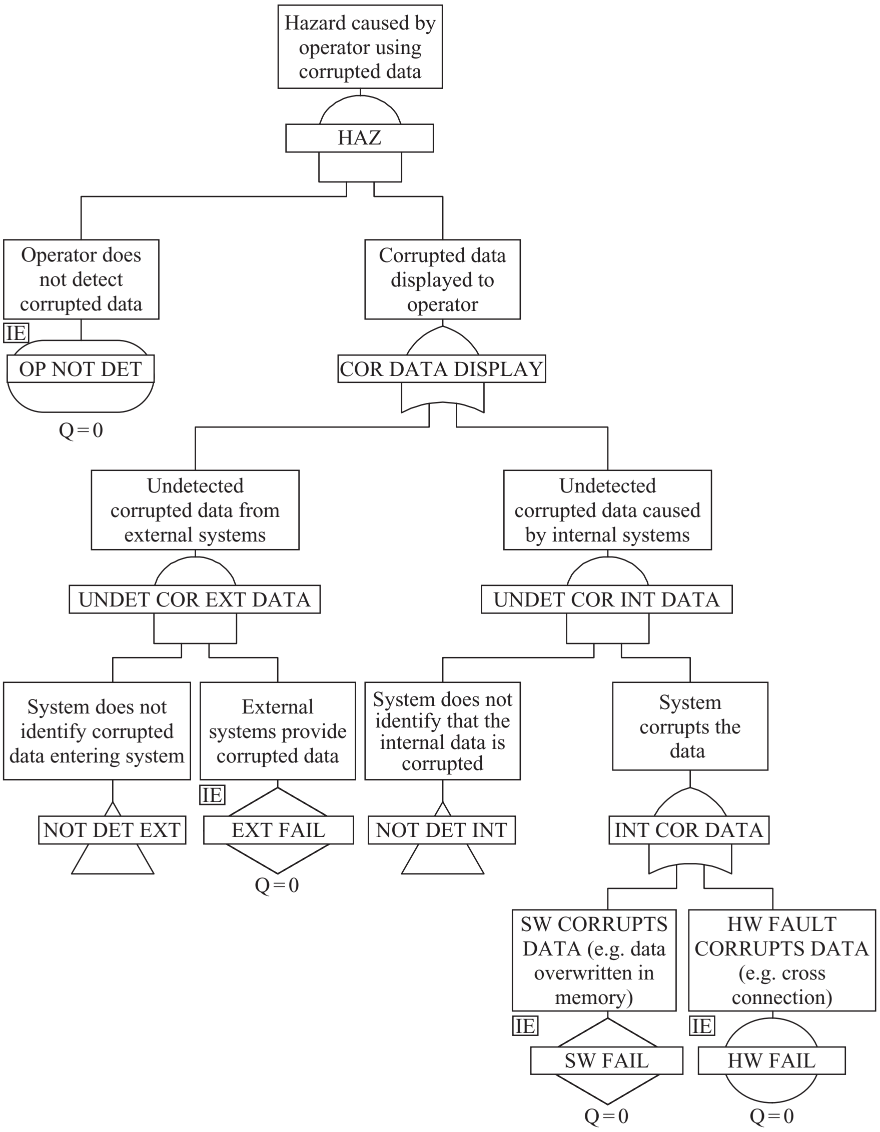
Hazard caused by operator using corrupted data
HAZ
Operator does not detect corrupted data
IE
OP NOT DET
Q = 0
Corrupted data displayed to operator
COR DATA DISPLAY
Undetected corrupted data from external systems
UNDET COR EXT DATA
Undetected corrupted data caused by internal systems
UNDET COR INT DATA
System does not identify corrupted data entering system
NOT DET EXT
External systems provide corrupted data
IE
EXT FAIL
Q = 0
System does not identify that the internal data is corrupted
NOT DET INT
System corrupts the data
INT COR DATA
SW CORRUPTS DATA (e.g. data overwritten in memory)
IE
SW FAIL
Q = 0
HW FAULT CORRUPTS DATA (e.g. cross connection)
IE
HW FAIL
Q = 0

Figure 14.7 Fault tree example

If human factors risks are not considered, a system will not achieve the required level of integrity. If human factors mitigations are not considered, the technical system components may be over-engineered at additional cost to achieve a target level of safety. This chapter has shown how the use of appropriate human factors techniques and methods can be integrated with typical systems engineering techniques for the assessment of human safety requirements in safety-related information systems.

14.9 Further questions

1. Explain how an ‘advisory’ system might be safety-related.
2. Define the term ‘safety’.
3. Explain the ALARP principle.
4. Describe a basic safety assessment process.
5. With reference to Figure 14.3, draw a simple air traffic control system showing its boundaries and where the operators and users are located.
6. Draw a typical accident sequence and describe the different mitigations, particularly those provided by people.
7. Explain how system risk can be modelled and describe how human risks and mitigations relate to this process.
8. Describe a human safety assessment process.
9. Explain the inputs, outputs and process of a critical task analysis.
10. Explain the inputs, outputs and process of a human error analysis.

14.10 References

1 GREATOREX, G. L., and BUCK, B. C.: ‘Human factors and systems design’, *GEC Review*, 1995, **10** (3), pp. 176–185

2 DS 00-56: Safety management requirements for defence systems, Part 1: requirements, UK MOD Defence Standard, December 1996

3 International Electrotechnical Commission, IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems, 65A/254/FDIS, IEC, 1999

4 STOREY, N.: ‘Safety-critical computer systems’ (Addison-Wesley, London, 1996)

5 HSE: The Health and Safety at Work Act 1974, HMSO

6 BS4778: British Standards Institution 4778, 1995

7 AYTON, P., and HARDMAN, D. K.: ‘Understanding and communicating risk: a psychological view’, in REDMILL, F., and ANDERSON, T. (Eds): ‘Safety-critical systems: the convergence of high tech and human factors’. Proc 4th Seventh Safety-Critical Systems Symposium (Leeds, 1996)

8 LEVESON, N. G.: ‘Safeware: system safety and computers’ (Addison-Wesley, London, 1995)

9 LOWRANCE, W. W.: ‘Of acceptable risk: science and the determination of safety’ (William Kaufman Inc., Los Altos, CA, 1976)

10 HAMILTON, V., and REES, C.: ‘Safety integrity levels: an industrial viewpoint’, in REDMILL, F., and ANDERSON, T., (Eds): ‘Towards system safety’, Proceeding of the Seventh Safety-Critical Systems Symposium (Springer, London, 1999)

11 LEVESON, N. G.: ‘The role of software in recent aerospace accidents’. Proceedings of the 19th International System Safety Conference, Huntsville, Alabama, USA, September 2001

12 FOWLER, D., TIEMEYER, B., and EATON, A.: ‘Safety assurance of air traffic management and similarly complex systems’. Proceedings of the 19th International System Safety Conference, Huntsville, USA, 2001

13 SANDOM, C., and FOWLER, D.: ‘Hitting the target: realising safety in human subsystems’. Proceedings of the 21st International Systems Safety Conference, Ottawa, Canada, 2003

14 DO-178B/ED-12B: ‘Software considerations in airborne systems and equipment certification’, 1992

15 FAA: ‘Human factors design guide update (DOT/FAA/CT-96/01): a revision to Chapter 8 – computer human interface guidelines’, National Technical Information Service, Springfield, VA, USA, April 2001

Further Reading

The author is not aware of any texts addressing the detailed integration of human factors techniques into the systems development lifecycle, specifically to address safety and risk management. There are, however, some classic texts on both safety and human factors issues that address the broad principles and a selection of these is given here.

LEVESON, N. G.: ‘Safeware: system safety and computers’ (Addison-Wesley, Boston, MA, 1995)

A classic text on system and software safety that addresses some human factors issues.

PERROW, C.: ‘Normal accidents’ (Harvard University Press, Cambridge, MA, 1984)

An easy and provocative read with an excellent discussion of why complex systems involving humans will inevitably lead to accidents.

REASON, J.: ‘Human error’ (Cambridge University Press, Cambridge, 1990)

The classic text on human error, although the book does not address how to apply the theory to systems engineering.

REASON, J.: ‘Managing the risks of organisational accidents’ (Ashgate, London, 1997)

Seminal coverage of organisational issues relating to safety and the management of organisational safety risk.

STOREY, N.: ‘Safety-critical computer systems’ (Addison-Wesley, Boston, MA, 1996)

Another classic text on safety engineering, although human factors are not addressed as an integral part of the systems engineering process.