Sandom C: *Human Factors Considerations for System Safety*, in Components of System Safety, Redmill F and Anderson T [Eds.], proceedings of 10th Safety Critical Systems Symposium, 5th-7th February 2002 Southampton, Springer-Verlag, UK, February 2002.

Human Factors Considerations for System Safety

Dr. Carl Sandom
Praxis Critical Systems Ltd.
carl.sandom@praxis-cs.co.uk

Abstract

The author has found that in many cases industry produces Safety Case reports that provide only limited safety assurance and, like the proverbial 'head in the sand' ostrich, the dominant system safety risks associated with the human factors are too often ignored. This paper provides a brief outline of the Human Factors discipline and its important relationship with systems safety. The paper then provides a discussion on some of the more commonly experienced human-factors problems relating to systems procurement, human-computer interaction and organisational issues before making some modest proposals for improvements in these areas. The paper concludes that the application of Human Factors techniques promotes engineering solutions that take account of human capabilities and limitations which can address the major risks to systems safety.

1 Introduction

The aim of this paper is to raise awareness of the need to address the safety risks inherent with the Human Factors issues relating to the design, operation and maintenance of safety-critical systems. The paper begins with a brief discussion on the relationship between Human Factors and systems safety and then provides a working definition of Human Factors. In the author's experience, some important, but often neglected, areas of risk relating to Human Factors issues are systems procurement, human-computer interaction and organisational factors. This paper will provide a discussion on some of the prevalent problems encountered in these areas before considering reasons why this situation currently exists and providing some suggestions for improvement. It should be emphasised that this is not a taxonomy for all Human Factors-related risks but merely convenient headings to discuss specific problems encountered in practice. Although many of the views expressed in this paper are particularly relevant to the Defence Sector, it is believed they are also appropriate for other industry sectors.

A distinction needs to be made here between different types of risk which exist in any systems development project. Risks come in many forms and those relevant to this paper are: risks to a procurement programme and safety risks posed by a system. It should be noted that contractual issues often raise programme risks; although they can become risks to safety if safety issues are avoided; the reverse is also true for organisational and interaction risks.

The views expressed in this paper are those of the author and do not necessarily reflect the policies of Thales Defence Information Systems.

2 Human Factors

The development of a safe system relies on the integration of many different engineering skills such as software and hardware engineering for example. The application of Human Factors techniques is often not well understood by those practicing the more traditional engineering disciplines. This section will outline the importance of Human Factors for systems safety and provide a working definition of Human Factors.

2.1 Human Factors and Safety

This paper deals with some of the Human Factors problems associated with the procurement of complex, interactive systems which can be characterised as systems that support dynamic processes involving large numbers of hardware, software and human elements that interact in many different ways [Perrow 1984]. Typical examples of such systems are found in Air Traffic Control, Ambulance Control Rooms and Power Generation Plants. Some complex systems can be safety-critical and these typically rely on people, procedures and equipment to function safely within an operational environment. For systems such as these, it seems obvious to state that the Human Factors associated with the designers, operators and maintainers must be taken into account when making claims about systems safety.

Despite this, safety cases for complex systems containing human operators often consider safety predominantly, or even exclusively, from a technical perspective. Safety cases such as these are typically limited to addressing the hazards arising through technical failures alone despite the fact that human error is repeatedly mentioned as a major contributing factor or even the direct cause of many accidents or incidents. For example, an analysis of causal factors contributing to a situation in which the safety of aircraft was compromised show that approximately 98% of incidents in UK airspace during 1997 were caused by human error (calculated from [CAA 1998a] and [CAA 1998b]). Names such as Herald of Free Enterprise, Clapham Junction and Ladbrook Grove are a grim reminder of disasters which have included human failures in complex systems.

Paradoxically, industry too often concentrates the majority of safety assurance effort upon technical issues often neglecting the human contribution. The human component of safety-critical systems are rarely considered to be safety-critical and are not therefore subject to hazard analysis and risk assessment to the same degree as any other safety-critical system component. The conclusion to be drawn from this is that in many instances, industry produces safety cases that, at best, provide only limited safety assurance as the prevalent errors are related to the Human Factors.

2.2 Human Factors Integration

Human Factors is basically about 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. Systems using computers must demonstrate how their 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. The British Defence Standard 00-25 defines Human Factors as:

" ...an interdisciplinary science concerned with influencing the design of manned systems, equipment and operational environments so as to promote safe, efficient and reliable total system performance." [IDS 00-25/12, p.4, 1989]

Theory is one thing, but practitioners are interested in the pragmatic integration of Human Factors within the systems development life-cycle. Through the application of Human Factors theory and appropriate techniques it is possible to analyse and optimise the human interaction with a system and its environment. A key aim of Human Factors expertise is to minimise safety risks occurring as a result of the system being operated or functioning in a normal or abnormal manner.

Human Factors Integration (HFI) is a phrase used to denote an engineering discipline that applies theory, methods and research findings from ergonomics, psychology, physiology and other disciplines to the design of manned systems. HFI has replaced MANPRINT (MANpower PeRsonnel and INTegration) as the process for managing HFI in defence procurement. It is still structured in broadly the same way, with the six domains of Manpower, Personnel, Training, Human Factors Engineering, System Safety and Health Hazard Assessment as listed in Table 1.

Unlike engineering parameters, Human Factors parameters are not always easily quantifiable. Therefore it is often necessary to use the services of Human Factors practitioners who can use experience to interpret the situation and provide informed predictions when it is not possible to meaningfully measure human performance or relevant criteria.

This brief discussion should give an idea of the type and scope of activities which need to be undertaken by Human Factors professionals and integrated into typical systems development projects. The paper will now look at some of the more common Human Factors-related problems experienced by the author.

HFI DOMAINS	DESCRIPTION
Health Hazard Assessment	Identification and consideration of conditions inherent in the operation or use of a product (e.g. vibration, fumes, radiation, noise, shock, recoil etc) which can cause death, injury, illness, disability or reduce the performance of personnel.
Human Factors Engineering	The comprehensive integration of human characteristics into product design, including all aspects of workstation and workspace design including accommodation / habitability issues.
Manpower	The number of men and women required and available to operate and maintain the product / system.
Personnel	The aptitudes, experience and other human characteristics (including body size & strength) necessary to achieve optimum performance.
System Safety	Application of Human Factors expertise to minimise safety risks occurring as a result of the system being operated or functioning in a normal or abnormal manner. The objective is to minimise to as low a level as reasonably practicable the risk of injury to personnel and damage to equipment.
Training	Specification and evaluation of the optimum combination of instructional systems, education, on job training required to develop the knowledge, skills and attitudes needed by the available personnel to operate and maintain the product to the specified level of effectiveness under the full range of operating conditions.

Table 1: Human Factor Integration Domains

3 System Procurement Issues

The system procurement process is perhaps not usually a topic directly associated with systems safety. However, there is a human factor at work during system procurement and the seeds of failure to adequately address the Human Factors, or even safety, can be sown during the contract negotiations. This section will discuss some of the typical procurement-related problems and risks facing both procurers and potential systems developers.

3.1 Contractual

Generally, a systems procurer, or customer, issues an Invitation to Tender (ITT) for a development contract to a number of competitive contractors. In response to an ITT, the invited contractors must then put together proposals which are both technically and financially persuasive. In today's highly competitive markets, the financial arguments are often more compelling to the potential customer. This inevitably means that all engineering costs within a proposal must be defensible and as such must be perceived to add value to the product.

Customers will inevitably have financial constraints and will, naturally, aim to procure maximum functionality for the minimum cost. Of course the problem here is that the output from Human Factors or safety analyses are generally non-functional requirements which constrain the design of a system rather than add functionality. Consequently, Human Factors or Safety Engineering activities can be perceived to be unnecessary, or unwanted, additions to a contract and the temptation when considering their associated costs is to limit their impact on the contract, or worse still, to ignore them.

From the contractor's perspective, a response to an ITT must contain a proposal which is competitive in every respect in order to win business. With such financial pressure it is difficult, if not impossible, to compete effectively if the cost of Human Factors analyses are added without them having been explicitly requested by a customer. If the contractor believes that there may be a Human Factors-related risk to safety, what could happen is to explicitly exclude such activities from their bid to limit their financial risk, or worse still, to ignore them.

Thus, there can be a situation where both parties are either genuinely unaware of the safety implication of avoiding Human Factors activities or they may individually choose to act like the proverbial ostrich and, metaphorically, stick their heads in the sand and ignore it.

To address these potential seeds of failure, both customers and suppliers need to have a shared appreciation of the value added to a product by Human Factors analyses and the vital link with systems safety. In complex, safety-critical systems there must be a clear customer requirement for safety assurance activities to be underpinned with Human Factors analyses. This would ensure that all contractors cost for the safety-related Human Factors activities from the outset of the project enabling safety to be designed into the product rather than the unsatisfactory alternative of mitigating risk with relatively soft procedures at a later date.

3.2 Operational Environment

An alternative to the picture painted so far is that both parties agree that Human Factors analyses are required from the outset. As with any other system requirement, Human Factors requirements need to be specified in the user and system requirements documents. In practice, this can be difficult as a analysis of Human Factors in safety-critical systems often reveals a complex set of problems relating to the people, procedures and equipment (or technology) interacting within a *specified* environment as depicted in Figure 1.

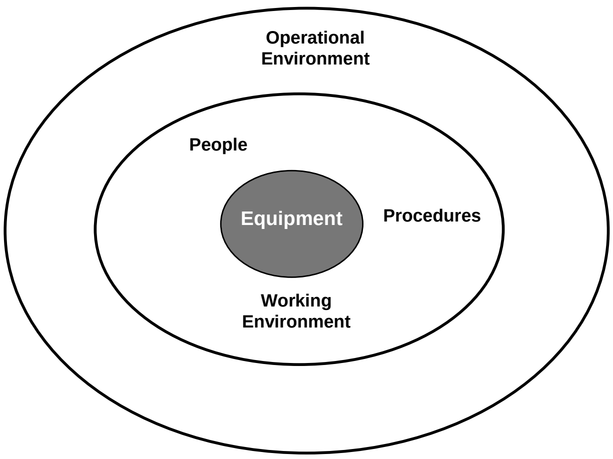

Figure 1: System Boundaries

The environment referred to here consists of both the immediate working environment and the wider operational environment. The working environment raises many physical, ergonomic issues such as lighting, noise or heating levels and the effects upon the human operator in terms of stress, attentiveness etc. Generally, the working environment for a system is easily specified and is not considered further here. However, the operational environment for a system is typically much more difficult to specify, as it requires precise knowledge of how the system will be used and this must be documented in detail. This doesn't just mean specifying the *interfaces* to a system (for example, a communications link protocol at the functional level); this also means specifying the tactical and strategic uses of the system (for example, how calls are prioritised in an emergency services control system).

The specification of the operational environment is important from a Human Factors perspective as this is typically used, along with the people and equipment issues, to develop an *operational concept* and from this, specific operational procedures to ensure that a system is used safely and efficiently. A systems developer would also use the operational concept as the basis for developing the system requirements specification upon which the Human Factors analyses are founded. The system safety analyses, including Human Factors task analyses, must be based upon a comprehensive system requirements specification to ensure that all credible hazards are identified.

In practice, it is difficult, if not impossible, to completely specify the operational concept of a system at the outset and a user may only specify the functionality required from a system without having a complete appreciation of how that functionality will be used in the operational environment. Perhaps this should not be unexpected and there are many explanations of unforeseen environmental changes introduced with the adoption of new technology (for example see [Macredie and Sandom 1999]). The specification of the operational environment can also be a problem when a business sector is dealing with national security and the users are reluctant to make the operational aspects explicit for either new or replacement systems. However, the outcome in both cases can be a system that implements a 'bag of functions' without taking account of the wider operational aspects.

So what can be done about this? Ideally, before an ITT is sent to potential contractors, the system procurer would ensure that the users have decided exactly how the system will be used to permit the specification of the operational environment. This may sound obvious, but in practice it is not unknown for systems to be delivered without the operators fully specifying the intended system use. If the operational concept cannot be fully specified from the outset, for whatever reason, it is necessary to make a number of explicit assumptions concerning the operational issues. It is essential that these assumptions are ratified by all system stakeholders and documented to mitigate the financial risk of rework due to changing operational procedures as the systems development proceeds. Finally, both systems procurers and developers must recognise that any changes to the operational concept or assumptions will impact upon the Human Factors analyses in particular.

4 Human Computer Interaction

Another area where problems are common and misunderstanding is rife concerns system human-computer interactions. To those unfamiliar with the Human Factors discipline, it can be the case that Human Factors are associated entirely with the analysis of the human-computer interface. As discussed previously this is not so, however, the interface is certainly an important aspect. The term Human Computer Interaction (HCI) is used here to mean the *process* of communication between users and a system rather than simply the implementation of the interface (ie. not just human-computer interface).This section will discuss two common problem areas associated with the assessment of human computer interactions in safety-critical systems; namely human reliability and usability.

4.1 Human Reliability

HCI issues are important for safety-critical systems. For complex systems in dynamic environments, an operator must to pay attention to a large volume of information from a variety of sources including sensors and other operators in order to acquire an awareness of the situation in question. In many cases humans are no longer able to appreciate the true situation without the aid of machines, therefore, machines must tell us more of what we need to know and they must do it more effectively and less ambiguously than before [Billings 1995]. The quality of the information acquired through the interface can contribute significantly to human failure and the design of the human-computer interface can have a profound effect on operator situational awareness and system safety. When emergencies arise and system operators must react quickly and accurately, the usability of the system is critical to operator's ability to make decisions, revise plans and to act purposefully to correct the abnormal situation. Analyses of human failures in large control centres have repeatedly shown that operator errors are linked with poor control layout and misleading cues [Booher 1990].

Systems safety assessments are predicated upon calculations of the inherent *dangerous* failure rates which are typically a sub-set of all failures and are therefore not a measure of system reliability. As discussed previously, human failures are typically the most prevalent in a system; yet they are often overlooked by system developers. This may be because hardware reliability techniques are relatively mature and well understood, however, this is not the case when dealing with human reliability. It is very difficult, if not impossible, to predict all the potential mental states of an operator in a complex system. Even if it were possible to identify all the potential mental states, and their effects on human behaviour, the difficulty of estimating the probability of occurrence of each state remains. Human Reliability Analysis (HRA) techniques have attempted to address this issue [see Kirwan 1994].

Arguably however, to a large extent the quantitative aspects of HRA research have been dominated by assumptions that apply to technical systems and often these do not translate to human systems [Woods *et. al.* 1994]. The hazards associated with human failures are very different from the hazards which have historically concerned system designers since they arise directly from the *use* of the system and therefore require some understanding of the cognition and actions of users within the operational environment. This aspect is critical to systems safety assessment yet it often does not fit with 'conventional' views on systems engineering practice.

4.2 Usability

Usability is another popular term used in system specifications - yet there is no accepted definition. Nonetheless, usability is generally taken to mean not only ease of use but the concept also equally involves effectiveness in terms of measures of human performance [Smith 1997]. From this general definition, safety-critical system developers may be tempted to infer that a useable system is, by implication, a safe system. However, usability and safety can be mutually exclusive system properties. It is possible that making an interactive system safe will entail many trade-offs with usability. For example, interface prototyping may reveal a requirement for a complex keying sequence to be replaced with a macro facility allowing a function to be invoked with a single key press. This requirement may enhance system usability, however, it may inadvertently affect the safety of the system if a hazard is associated with the function being invoked. This point may seen obvious, but systems operators and others involved in HCI Working Groups will often support system usability without being aware of all the safety issues and these views often prevail in the design.

While a complex sequence may not be very efficient in terms of usability, it provides a number of opportunities for the operator to become aware that the function being invoked may be hazardous in the current context. It is suggested here that the greatest hazard in a system can be associated with an operator automatically interacting when conscious thought is required. With familiarity, automatic human cognition can become the norm and information is then perceived, interpreted and acted upon with little or no thought. Conscious cognition bears a complex relationship to situational awareness and it seems intuitively unsafe to perform safety-critical tasks while remaining unaware of them even if they are performed well [Hopkin 1995]. The implication is that operator awareness of a situation may not be updated and may therefore be inaccurate. It can be concluded that it is not enough to simply concentrate on the usability of an interactive system to assure functionally safe operation.

4.3 HCI Safety Assessment

Given the difficulties outlined here relating to the assessment and mitigation of Human Factors risks, it may be argued that human error is best examined from a cognitive perspective, as traditional reliability engineering techniques do not appear to fit well with Human Factors concerns. It has been suggested that safety and usability can be mutually exclusive properties, particularly in systems that rely on situational awareness for safe operation. If this is the case, different methods and techniques are required for evaluating safety. It may be more appropriate to quantify safety from a Human Factors perspective in terms of the level of situational awareness acquired through the interface.

A complete discussion on situational awareness is beyond the scope of this paper (see [Sandom 1999] for a detailed discussion). Briefly, however, operator situational awareness can be considered as a mental state acquired through a process of interaction. To assess the impact of situational awareness on systems safety, it is equally important to assess both the mental state and the process. Situation Awareness Global Assessment Technique (SAGAT) is a popular method of assessing the mental state of an operator [Endsley 1995] and Situation Awareness Process Analysis Technique (SAPAT) [Sandom 2001] can be used to assess the acquisition process.

SAPAT in particular aims to identify those potentially hazardous interactions and can help systems developers to make informed trade-offs between usability and safety.

5 Organisational Issues

There are many organisational factors at work during the development of any complex system. This section will discuss some of the typical problems facing systems developers that try to adopt an integrated approach to Human Factors.

5.1 Organisational Failures

Most people would recognise that all systems have a human input, even if it is limited to the fallibilities of the developers who can introduce systematic errors into the design and implementation phases. However, it is perhaps not always appreciated that organisational issues can profoundly affect systems safety.

Consider a simple example of a hypothetical system (adapted from [Woods *et. al.* 1994]). This system has an operator who is required to enter a number when a screen flashes A and enter another number when a screen flashes B. If an operator one day enters the A number when B appears on the screen and the system blows up instead of shutting down, some would conclude that the accident was caused by human error and that would be the end of the investigation. However, that wouldn't help us to understand anything at all about cause and effect. Considering issues such as the system design and understanding how operators solve problems of workload and competitions among goals would provide a more meaningful investigation. Moreover, in the simple example, it could be argued that the failures had been made by the organisation, which is to say people such as designers and managers who created the poor conditions for the operator error.

To address the root cause of the organisational risk to human error it is necessary for the organisation to develop a positive safety culture based upon a sound safety management system. This is often more difficult than it may appear and it cannot be achieved overnight. As for most organisational changes, a safety culture must be adopted from the top-down and senior management may need to be educated to understand that a safety culture cannot be contracted into an organisation via outsourcing agreements. Another common misconception is that an organisation is 'doing' safety if it has an ILS policy in place. Consider how many organisations equate safety with reliability - yet a system may reliably perform a specified function which is unsafe.

5.2 Safety Culture

As a manufacturer and supplier of goods and services, companies have a responsibility and must be fully committed to a policy of compliance with product safety legislation. Product safety should assume prime importance in the design, development, manufacture, assembly, operation, support, maintenance and disposal of company-designed products. Yet it is too easy to focus on the specified *contractual* safety requirements without appreciating that there are legal requirements that must also be addressed. Clearly these obligations will overlap to different degrees, as shown in Figure 2, but an organisation must address both obligations nonetheless.

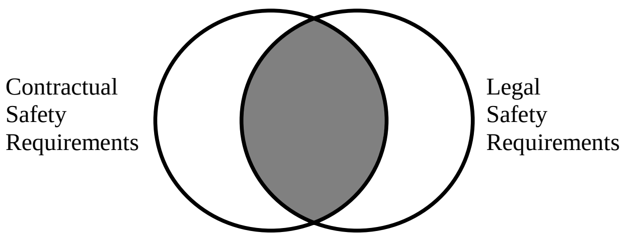

Figure 2: Safety Obligations

A problem can occur for organisations when a contract does not explicitly require Human Factors analyses to be undertaken. Given the previous discussions on the impact of Human Factors issues on safety, it could be argued that the organisation has a legal duty of care to ensure that any related risks are reduced to a level as low as reasonably practicable through Human Factors analyses regardless of contractual obligations. In short, organisations that profess to have a safety culture should also have Human Factors expertise.

5.3 Selling Human Factors

Throughout this paper it has been argued that Human Factors is an important element in the design of effective and safe systems. However, before any profit making organisation can be expected to fund a Human Factors capability, a sound business case must be made to show the potential financial benefits. In practice, this is not easy as the costs and benefits associated with typical Human Factors activities are often difficult to quantify.

A detailed explanation of making a Human Factors business case can be found in [Trenner and Bawa 1998]. However, to summarise, early integration of Human Factors in the design and system life-cycle promotes solutions that take account of human capabilities and limitations. The safety-related benefits include: enhanced usability, reduced error rates, improved in-service performance. Also, early integration of Human Factors into the design process helps reduce the number of design changes and associated costs throughout the whole product life-cycle.

6 Providing Safety Assurance

A crucial question that may have been at the back of the readers mind: What can be done about the concerns discussed here and the apparent lack of safety assurance caused by the neglect of Human Factors? After having looked at some of the common problems what are the solutions? Perhaps disappointingly, this paper does not claim to provide all the answers but merely makes some modest proposals. However, this section will demonstrate how a Human Factors argument could be made for a system safety case.

6.1 Making an HF Argument

A System Safety Case will typically contain arguments and supporting evidence that the system meets or exceeds the required standard of safety. Broadly, the arguments must show that the risks associated with operating or maintaining the system have been reduced to a tolerable level. A main safety objective is to validate all safety requirements and show that they have been successfully implemented. The prevalence of human failures in complex, safety-critical systems has already been discussed. If we accept that Human Factors can contribute significantly to the safety risks in these systems, then a safety argument must explicitly address these issues.

In the construction of safety cases there is a large amount of information to be recorded and managed. Goal Structuring Notation (GSN) is one notation that has been developed to allow hierarchical structuring of such information and is used to express high level arguments with links to supporting evidence. A subset of GSN will be used here to illustrate a Human Factors safety argument.

Briefly, GSN uses a number of concepts including Goals, Strategies and Contextual Information. A Goal can be considered as a statement of a requirement to be met by a system, or some activity to be performed, while a Strategy introduces an element of explanation showing how the safety arguments are constructed. Finally, Contextual information is often necessary to understand a goal or strategy. Figure 3 shows a Human Factors safety argument expressed in GSN.

The safety argument in Figure 3 is based upon the following example, high-level Human Factors requirement:

> System Requirement [HF1]: “*The* design *and implementation of System X shall include consideration of Human Factors Integration issues”*.

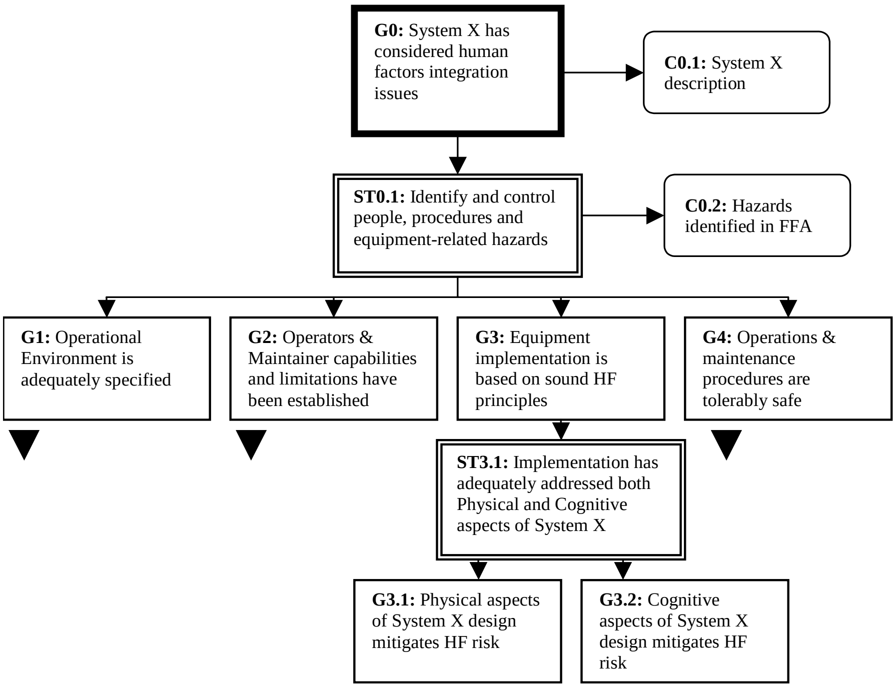

Figure 3: Example Human Factors Safety Argument

Figure 3 shows the top-level goal G0 as a statement of the requirement HF1 to be met by a system developer. In this example, the goal G0 uses the contextual information C0.1 which provides a system description. It has already been stated that safety-critical systems typically rely on people, procedures and equipment to function safely within an operational environment. For systems such as these, it seems logical to use a strategy like ST0.1 in Figure 3 (supported by the contextual information of the safety analyses like the FFA) to structure a Human Factors safety argument in these terms.

Each specific sub-goal in this argument would typically require direct supporting evidence or further decomposition as shown by Goal G3. The type of evidence would be determined by the assurance level required from the system and should ideally include both formative and summative evidence to underpin a

Human Factors argument. This approach would be consistent with Human Factors methods which are broadly categorised as formative, generating evidence during the overall system design process, and summative, generating evidence relating to the evaluation of the final product (Noyes and Baber 1999).

Figure 3 shows only the top-levels of a safety argument and has only decomposed Goal G3 to illustrate the concept. In this example, to follow the strategy of ST3.1, Goals G3.1 and G3.2 would broadly deal with the ergonomic and cognitive aspects of the system respectively. So G3.1 might rely on anthropometric evaluations for example while G3.2 would perhaps use evidence generated by SAPAT analyses or HCI Working Groups.

It is not claimed here that this simplistic and partial example of a Human Factors safety argument is the only way to structure an argument. It is recognised that there are many different ways that an argument can be expressed. However, the example in Figure 3 does illustrate one way in which systems developers could start to address the majority of the risks associated with the operation of complex, safety-critical systems.

7 Conclusions

This paper was intended for an audience of both engineering practitioners and academics to raise awareness of the need to address the safety risks inherent with Human Factors issues relating to safety-critical systems. The important relationship between human factors and systems safety was discussed and it was suggested that human factors issues typically represent the biggest safety risks in complex systems. A working definition of Human Factors was given as influencing the design of manned systems, equipment and operational environments to promote safe, efficient and reliable total system performance. Some important Human Factors considerations relating to systems procurement, Human-Computer Interaction and organisational factors were discussed and some suggestions for improvement were provided. Finally, an example of a Human Factors safety argument was provided to illustrate how systems developers might start to address the majority of the system safety risks and to provide holistic systems safety cases.

From these discussions it can be concluded that Human Factors should be an important consideration in the design of effective and safe systems. Early integration of human factors in the design and system life-cycle promotes solutions that take account of human capabilities and limitations. The safety-related benefits include: enhanced usability, reduced error rates and improved in-service performance. Like safety, human factors is not like a coat of paint that can be applied at the end of a project and addressing some of the issues highlighted in this paper may help industry to produce systems that provide the necessary level of safety assurance.

8 References

[Billings 1995] Billings C. E: Situation Awareness Measurement and Analysis: A Commentary, in Garland D. J. and Endsley M. R., (Eds), Experimental Analysis and Measurement of Situation Awareness, Proc. of an Int Conf, FL:USA, November 1995

[Booher 1990] Booher H R (Ed.): MANPRINT – An Approach to Systems Integration, Van Nostrand Reinhold, 1990

[CAA, 1998a] Civil Aviation Authority: Aircraft Proximity Reports: Airprox (C) - Controller Reported, August 1997 - December 1997, Vol 13, Civil Aviation Authority, London, March 1998

[CAA, 1998b] Civil Aviation Authority: Analysis of Airprox (P) in the UK: Join Airprox Working Group Report No. 3/97, September 1997 - December 1997, Civil Aviation Authority, London, August 1998

[Endsley 1995] Endsley M R: Measurement of Situation Awareness in Dynamic Systems, Human Factors, 37(1), 65-84, March 1995

[Hopkin 1995] Hopkin V D: Human Factors in Air Traffic Control, Taylor and Francis, London, 1995

[IDS 00-25/12 1989] UK Ministry of Defence Interim Defence Standard 00-25 (Part 12)/Issue 1, Human Factors for Designers of Equipment, Part 12: Systems, July 1989

[Kirwan 1994] Kirwan B: A Guide to Practical Human Reliability Assessment, Taylor and Francis, London 1994

Sandom C: *Human Factors Considerations for System Safety*, in Components of System Safety, Redmill F and Anderson T [Eds.], proceedings of 10th Safety Critical Systems Symposium, 5th-7th February 2002 Southampton, Springer-Verlag, UK, February 2002.

[Macredie and Sandom 1999] Macredie R D and Sandom C: IT-enabled Change: Evaluating an Improvisational Perspective. European Journal of Information System, 8:247-259, 1999

[Noyes 1999] Noyes J and Baber C: User-Centred Design of Systems, Springer-Verlag, Berlin, 1999

[Sandom 1999] Sandom C: IEE Proceedings of People in Control - An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres, University of Bath, UK, 21 – 23 June 1999

[Sandom 2001] Sandom C: Situational Awareness, in Noyes J and Bransby M (Eds.), People in Control: Human Factors in Control Room Design, IEE Publishing, November 2001

[Smith 1997] Smith A: Human-Computer Factors: A Study of Users and Information Systems, London, McGraw Hill, 1997

[Trenner and Bawa 1998] Trenner L and Bawa J: The Politics of Usability, Springer-Verlag, Berlin, 1998

[Woods *et. al.* 1994] Woods D D, Johannesen L J, Cook R I and Sarter N B: Behind Human Error: Cognitive Systems, Computers and Hindsight, CSERIAC SOAR 94-01, Ohio State University, December 1994