Do You Get The Picture? Situation Awareness and System Safety

Carl Sandom
iSys Integrity Limited
10 Gainsborough Drive
Sherborne, Dorset, DT9 6DR, England.
carl@iSys-Integrity.com

Abstract

Studies of the dependency between complex, dynamic systems and their human operators often focus on human-computer interactions without considering the emergent properties of human-machine systems in use. As systems become more complex, and typical operating environments more dynamic, the role of the operator has typically changed from providing manual to cognitive control. An understanding of human cognition in context is thus central to the design of human-machine systems and this is particularly pertinent in safety-related systems when the elimination of hazards is a principal concern. This paper will argue that operator situation awareness is an important, safety-related phenomenon and that it can be used to examine human cognition in context in order to add value to system safety. The paper will examine the dominant theoretical perspectives on situation awareness and a model of this critical phenomenon is presented. The paper will show how the proposed model of situation awareness can be used as a framework for the analysis and identification of hazards relating to operator awareness in the context of system use. It is also suggested here that modelling situation awareness is useful in identifying areas of interface design where safety and usability are mutually exclusive. An illustration of the use of this technique is provided to show how the model can inform the design of interactive systems and how it can be used to generate evidence to support system safety claims.

Keywords: cognition, context, hazard analysis, situation awareness, safety, usability.

1 Introduction

Studies of safety-related systems have in the past considered safety predominantly from a technical perspective. Such studies have typically been limited to addressing hazards that could arise through hardware and software failures, yet human factors are becoming increasingly important in the design and evaluation of safety-related systems (Sandom 2007). This change in perspective has revealed a complex set of 'human' problems that are extremely challenging. The hazards associated with human failures are very different from those that have historically been the concern of safety engineers since they arise directly from the *use* of the system and therefore require some understanding of the cognition of users. The identification of interaction hazards arising during system use may help designers to improve the system interface and interactions such that the associated risks are mitigated or even eliminated. However, in order to study these interaction hazards, appropriate research constructs are required to help designers to understand the user's cognition during system use.

The dominant cognitive paradigm in Human Computer Interaction (HCI) research has been based on the human information processor as characterised by the seminal work of Card *et al.* (1983). Although the information processing model has been extremely useful, there is a growing awareness that there are a number of limitations associated with this reductionist paradigm for human cognition (Nardi 1996, Hutchins 1995, Suchman 1987, Winograd and Flores 1986). A key limitation with this model is that it has neglected the importance of how people work when using computer systems situated in the real world (Landauer 1987).

Making the context of the user-system interaction more central in understanding the cognition of the user and the resulting action is a key facet of a perspective referred to as 'situated cognition'. Here, in contrast to the information processing view, it is argued that the cognitive state that leads the user to exhibit 'purposeful, situated action' can only be fully explained in the specific context in which that action takes place. This suggests that an understanding of human cognition requires a holistic approach through careful consideration of the social, organisational and political aspects of HCI in the context of use.

This brief discussion suggests that a comprehensive understanding of situated human cognition is central to the design of interactive systems, and this is particularly pertinent when the elimination of hazards in safety-related contexts is a principal concern. In order to select and develop appropriate research constructs to look at such hazards, it will be useful to briefly consider the nature of the hazards themselves.

2 Human Factors and Systems Safety

Human factors are repeatedly mentioned as a major contributing factor or even the direct cause of accidents or incidents. For instance, an analysis of causal factors contributing to a situation in which the safety of aircraft was compromised show that 97.7% of incidents in UK airspace during 1996 were caused by human error (calculated from CAA 1998a and CAA 1998b). Human errors often occur when there are interaction problems between the user and the system.

By their nature, safety-related systems present unique hazards arising from the interactions between the user and the system and a safety case is usually required to provide a clear and comprehensible argument that a system is safe to operate. A safety case generally consists of claims about a system and evidence which is used as the basis of a safety argument to support those claims (see Figure 1). The safety case provides the assurance that a system is adequately safe for a specific application in a given context. For example, in the UK, National Air Traffic Services are required to produce safety cases for air traffic control systems to satisfy the air traffic control service regulators.

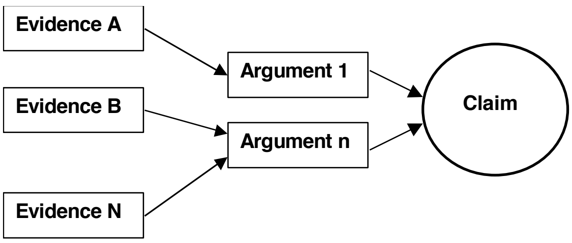

Figure 1 – Safety Claim Structure

Safety arguments, particularly those relating to system hardware components, are often based on evidence taken from reliability data and historical trends. However, it is often much more difficult, if not impossible, to derive accurate reliability evidence to support safety claims relating to many human factors issues such as those associated with the interaction between the system and the operator in a given context (Sandom 2011).

The reliability of the user-system interaction in hazardous situations is extremely important. If the user's interaction is inappropriate, there is the potential for catastrophic consequences. To examine these issues, safety engineers need user-centred ways of evaluating safety-related systems. If designers are to identify interaction hazards associated with the human operator and design mitigating features into the system to reduce the likelihood of the hazards being realised, it is crucial that designers have ways of understanding why users take particular actions in particular circumstances.

The user may act inappropriately because they have problems making sense of what they are doing at a given time. There are several human-centred constructs that may help us to understand these issues, an important one being the idea that people have 'pictures' of what is going on in their interaction with the system. This is often referred to as the user's Situation Awareness (SA). If users make errors in using systems, it may be because their SA is incorrect. A highly usable system may, for example, be so transparent that the users do not correctly develop their 'pictures' of the system interaction as the situation develops. Where users form incorrect or inappropriate 'pictures' of the situation, there is great scope for error, implying that SA has a significant impact upon system safety (Endsley 1995a). Finding ways of assessing and understanding the awareness of the situation held by users will be useful in helping identify areas where users form incorrect awareness and where, as a result, there are hazards. Consequently, situation awareness is an important, safety-related phenomenon that can be used to examine human cognition in context in order to add value to system safety (Sandom and Harvey, 2004).

3 Situation Awareness

In order to develop suitable ways of understanding and assessing SA, it is important to consider the existing research in the area. It is widely accepted that a user must have an appropriate awareness of their situation for the safe operation of any complex, dynamic system (Sarter and Woods 1991). However, SA is a complex concept and it is difficult to find an accepted definition of the term (Charness 1995, Hopkin 1995). Despite this, the widespread interest in SA, particularly within the field of aviation and other similarly complex domains suggests its potential contribution to interface and interaction design (Harris 1997,Garland and Endsley 1995).

In the context of human-machine interaction, current definitions are generally based on opposing views of SA as either a cognitive phenomenon or as an observer construct. The cognitive perspective is the prevalent view, seeing SA as a cognitive phenomenon that occurs ‘in the head’ of the user – though even within this broad perspective there are differing interpretations and emphases. In contrast, if seen as an observer construct, SA becomes an abstract concept located ‘in the interaction’ between user and environment. Despite the differences that exist in theoretical stance, a more detailed discussion will show that there are conceptual similarities between the different perspectives of SA. A detailed study can then be used to help to understand SA in the context of safety-related systems and to make use of it in informing their design.

3.1 Cognitive Perspective

Proponents of a cognitive perspective of SA view it as a phenomenon that occurs ‘in the head’ of an actor in a similar fashion to the dominant cognitive framework of the human as an information processor (Card *et. al.* 1983). Indeed, some even suggest that SA is yet another ‘black box’ component, or (sub-) process, within the human information-processing model (Endsley 1995b). The process-oriented view sees SA as being acquired and maintained by the user undertaking various cognitive activities (Sarter and Woods 1991). Cognitive definitions of SA also generally provide a rich description of key elements of decision making activities in complex systems such as perception, comprehension and projection (Endsley 1995b). There is another view of SA within the cognitive perspective, which sees SA as a product – a state of awareness about the situation with reference to knowledge and information (Endsley 1995a). Some researchers have even integrated the process and product perspectives (Isaac 1997).

Whilst the conflicting views may signify an apparent lack of coherence within the cognitive perspective, Endsley's theoretical model of SA (Endsley 1995b), based on the role of SA in human decision making in dynamic systems, has been widely cited and highly influential in cognitive science research. This model represents a typical cognitive perspective and it proposes three different levels of SA which are relevant to this paper:

Level 1 SA *Perception* of the status, attributes and dynamics of relevant elements in the environment.

Level 2 SA *Comprehension* of the situation based on a synthesis of disjointed Level 1 elements to form a holistic 'picture' of the environment.

Level 3 SA *Projection* of the near-term future of the elements in the environment.

The different levels suggest that SA is based on more than simply perceiving information about the environment, which is often the perceived definition of the phenomenon. Many cognitive accounts of SA suggest that after information concerning relevant elements is perceived, a representation of the situation must be formed before a decision can be made based upon current SA.

This leads to another common notion that is particular to the cognitive perspective with SA often considered synonymously with mental models (Isaac 1997) an area of long time interest for HCI. Seeing the mental model as a subjective awareness of the situation which includes what has happened, what could happen and what a user predicts will happen based on their goals and objectives (Kirwan *et. al*. 1998) suggests that this representation is the 'picture' that the user has (Whitfield and Jackson 1982). Despite making an explicit link with mental models, the models of SA proposed within the cognitive 'school' do not have iterative dimensions to reflect the dynamism of acquiring SA over time. Instead they propose models which capture or explain SA at any given instant in time.

3.2 Developing Perspectives

When seen as an observer construct, SA is explained as an abstraction that exists only in the mind of the researcher. From this perspective, SA is considered as a useful description of a phenomenon that can be observed in humans performing work through interacting with complex and dynamic environments (Billings 1995,Flach 1995a). The description is developed by considering observable behaviour in the environment – what the user does, how the system performs – but is not concerned with directly relating these things with cognitive states of the user. In one sense this might be associated with traditional behavioural psychology. A behavioural stance may simplify the discussion of SA by removing (or at least marginalising) interest in the user's mental state in favour of a reliance on observable action. A behaviourist stance is however much less rich as a research perspective, since no attempt will be made to relate action to intention on the user's part. In moving the SA debate forward, then, and looking for rich models to explain SA, identify hazards and ultimately inform the (re)design of safety-related systems, we would suggest that cognitive views of SA are more useful.

Yet, there are competing views of SA which do not fit neatly into the information-processing stance predominantly taken by the cognitive school, but which might be useful in developing an informed stance on SA. Smith and Hancock (1995), for example, propose a view of SA as adaptive and externally directed consciousness, arguing that there is currently an artificial and contentious division evident within the literature relating to general perspectives of SA as either exclusively knowledge (i.e., cognitive state, or product) or exclusively process. From this view, SA specifies what must be known to solve a class of problems posed when interacting with a dynamic environment. Smith and Hancock (1995) also criticise the lack of dynamism exhibited in the cognitive perspective, contending that SA is a dynamic concept that exists at the interface between a user and their environment. Moreover, they argue that SA is a generative process of knowledge creation and informed action taking as opposed to merely a snapshot of a user's mental model.

There are merits in many of the competing views of SA and the range of views that exist highlight the complexity of SA and the general immaturity of research in the area. The mental state of the user is important in trying to understand the awareness that the user builds up of a situation. Yet researchers often have only observable interaction data on which to draw, tempting them to marginalise mental state as a concern and focus on explaining SA without reference to the user's cognitive processes.

3.3 Situated Cognition Perspective

A helpful, synthetic and pragmatic perspective of SA sees it as a measure of the degree of dynamic coupling between a user and a particular situation (Flach 1995b). This view attaches importance both to the user's cognitive state and to the context or situation in which they are acting, reflecting a move away from traditional information processing models of cognition towards the situated cognition (and situated action) perspective introduced in Section 1 as a developing movement in HCI.

Reflecting this stance, a tangible benefit of SA research is the focus on the inseparability of situations and awareness (Flach 1995b). From this perspective, discussions of SA focus attention on both what is inside the head (awareness from a cognitive perspective) and also what the head is inside (the situation which provides observable data) (Mace 1977). Generally, this stance suggests that the user's current awareness of a situation affects the process of acquiring and interpreting new awareness from the environment in an ongoing cycle.

This view is similar to Neisser's Perception-Action Cycle (1976) which has been used to model SA (Smith and Hancock 1995, Adams *et. al*. 1995) in an attempt to capture the dynamic nature of the phenomenon. Central to this view of SA is the contribution of active perception on the part of the user in making sense of the situation in which they are acting. Such active perception suggests informed, directed behaviour on the part of the user.

As we have seen, one of the problems in making use of SA is the conflicting theoretical perspectives from which SA has been described and researched. Whilst theoretical debate is both healthy and necessary, a pragmatic stance which critically reviews the different perspectives and attempts to synthesise common elements may be a more immediate way of contributing to systems design. A useful outcome of such an approach would be a model that helps designers understand SA and its usefulness in designing interfaces to, and interaction sequences and dialogues within, safety-related systems.

4 Dynamic Situation Awareness Model

As the preceding discussions have highlighted, there are competing and sometimes confusing views on SA and its relation to people and the situation in which they are acting. There is significant on-going research to further these debates and refine the perspectives. Whilst such research is of long-term value in contributing to the maturity of the field and refining explanations of SA, this paper takes a more pragmatic approach, arguing that an attachment to a particular perspective can cause problems. Where there is contention between opposing perspectives, research can tend to become dogmatic which in an immature area may lead to opportunities for furthering our understanding being missed as researchers endeavour to strengthen their particular perspective. This paper is more interested in considering the focus of our research in the area and synthesising constructs from the existing perspectives that may help us make sense of the situations, which we are studying.

This paper will now draw themes, which we see as important to our work in SA, from the theoretical perspectives that we have discussed, and frame them as a dynamic model of SA based upon Neisser's Perception-Action Cycle (1976). We will then use this model to help us analyse and understand SA.

4.1 Awareness

As our discussion of the competing perspectives highlighted, the term SA is often used to describe the experience of comprehending what is happening in a complex, dynamic environment in relation to an overall objective or goal. Regardless of theoretical perspective, it is generally accepted that this experience involves both acquiring and maintaining a state of awareness (Endsley 1995b, Smith and Hancock 1995). This view is shared by Dominguez (1994) who, in an attempt to define SA as both a process and a product, compared 15 definitions and concluded that the perception of expected information in the environment occurs in a continual cycle which is described as 'continuous extraction'. To be useful therefore, a model of SA should reflect the equal importance of both the continuous process of acquiring and maintaining SA and the state of SA itself.

4.2 Situated Action

An area that we see as important, but on which there is much disagreement, is consciousness. Compare, for example, the description of Endsley's (1995b) model of SA with that prescribed by Smith and Hancock (1995). This tension reflects the broader 'cognitive' debate in HCI introduced earlier. Whilst the information-processing view within the cognitive paradigm has contributed substantially to psychology-oriented research, there is a growing view that it is limited and presents a constraint to the advancement of theory in the area. If research in SA is to take a broader perspective than that offered by the information-processing model, it will have to concern itself with issues which reflect deliberate action on the part of those being studied in the specific context in which they are acting. A model informed by this stance, would have to acknowledge the existence of consciousness and its contribution to situated action (Suchman, 1987) (or 'purposeful action'), and reflect that an individual's awareness of a situation consciously effects the process of acquiring and interpreting new information in an continuous, proactive cycle.

4.3 Context

The positions taken in themes I and II reflect the importance of the individual making sense of situations in a particular context, and frame SA in this light. Any model of SA should explicitly reflect this, showing that accurate interpretations of a situation cannot be made without an understanding of the significance of the situation within a particular context. In other words, the context in which an individual is acting has to be understood in order for us to appreciate the importance of particular situations and their likely relation to SA. This coupling of situation to context is suggested as a key issue, and is one which, as we have seen, has emerged as a theme of increasing importance in cognitive science and HCI (Nardi 1996, Hutchins 1995, Suchman 1987, Winograd and Flores 1986).

4.4 Dynamism

When an individual is making sense of the situation in which they are acting, their understanding is informed by them extracting relevant information from their environment. This information is temporal; the same information at different times (and therefore in different situations) may mean different things to an individual. The continuous information extraction process in which the individual is engaged implies that SA requires individuals to diagnose past problems and provide prognosis and prevention of future problems based on an understanding of current information. This suggests that a model of SA must be inherently dynamic, reflecting the development of SA over time, and that it must be responsive to environmental changes, for example in the information available to the individual.

4.5 Dynamic SA Model

The four themes have raised issues which can be used to frame a model of SA (see Figure 2). The model encapsulates the inherent dynamism of proactive extraction (founded on the user's awareness), the significance of context (reflecting the situations in which an individual is acting) and the contribution of both of these themes to 'situated action' in SA.

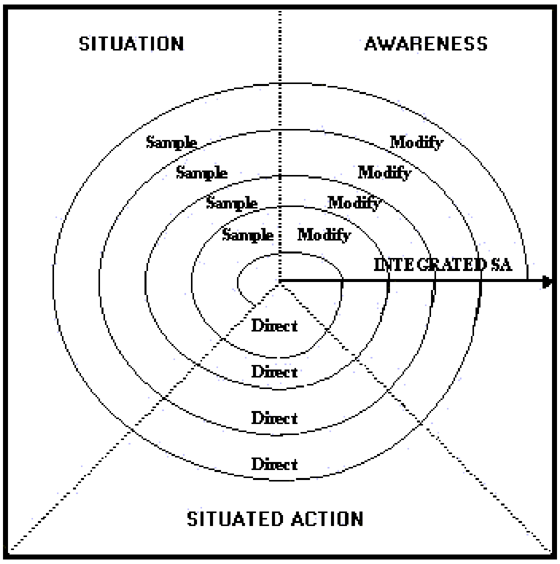

Figure 2 – Dynamic SA Model

The model of SA shown in Figure 2 is adapted from Neisser's Perception-Action Cycle (1976). Neisser's model portrays the adaptive, interactive relationship between an actor and their environment. Pictorially, this model owes much to Boehm's Spiral Model of the software development life-cycle (1988) which is also centrally concerned with issues of iteration and dynamism. It also depicts how awareness information is continuously extracted from a real-world situation and how this is integrated into an individual's awareness to form a mental representation upon which decisions are based and exploratory actions are taken. This model of SA addresses some of the key conflicts between opposing views of SA as either process or product as it encompasses both views. The model shows the inseparability of the SA acquisition process and the resulting (product) state of awareness that recursively direct the selection of relevant situation information in a continuous cycle.

It is worth noting that Norman's well cited action model (1988) appears very similar to Neisser's Perception-Action Model. An important difference, however, is that Neisser maintains that knowledge (or awareness) leads to anticipation of certain information that directs the sampling strategy and increases an individual's receptivity to some elements of the available information. In contrast, Norman's model does not expand on the how information is perceived other than passively and therefore concerns itself only with the process of action.

In Figure 2, the three terms sample, modify and direct are used. In Neisser's model, these terms are related to the environment, knowledge and action respectively. In the adapted model of Figure 2 the terms relate directly to the areas of situation, awareness, and situated action. For the purpose of using Neisser's model in the context of SA, the terms 'situation' and 'awareness' are substituted for 'environment' and 'knowledge' to imply that only a subset of elements of the environment and knowledge relevant to a specific task are considered. This is consistent with the view of SA espoused by Endsley (1995b).

As the individual begins to interact in their environment, they can be considered as moving along the spiral in the model from the central point. An individual may start anywhere in the cycle as, for example, a routine may take over to provoke initial action. Starting arbitrarily, the individual will sample the situation, building a perception of it by extracting and interpreting information content. This may lead the individual to modify their awareness, developing their subjective mental representation of the situation in which they are interacting. Changes in the individual's interpretation of the situation cause them to consciously direct their action (including what/where to sample next), anticipating future states in which they might find themselves and acting accordingly. The 'sample–modify–direct' cycle which the individual can be thought of as having passed through will have developed their awareness in a particular way. As time progresses the individual will cycle through these phases building an integrated awareness that grows with each iteration.

4.6 The Model in Action

In order to illustrate the potential usefulness of the model further, we can consider a specific example. A recent empirical study of a military command and control system revealed that the system displayed many different alerts to the operator. This system required individual alerts to be acknowledged or cancelled using a multiple key switching sequence. However, the vast majority of the alerts were deemed by the operators to be irrelevant and were therefore cancelled using a switching sequence which was consistent for all alert types. It was observed that this alert-cancelling action was carried out so frequently that it had become automatic for the operator. The problem was that the operators also cancelled some alerts containing safety-related information as they carried out the now automatic switching sequence on a screen of multiple alerts – despite the fact that these safety-related alerts were highlighted in a different colour.

We can use the proposed dynamic model of SA to analyse this observed human-computer interaction. In this example, we have based our appraisal of the situation on only observable data; we are talking about SA here as an abstraction that exists only in the mind of the observer.

We could carry out data collection using qualitative methods to probe the users in an attempt to construct a view of their cognitive state, which might enable us to develop a view of the SA of the user, 'defined' in terms of their mental state. In this sense, the type of data to which we have access in a particular instance drives our definition of SA as observer construct of a cognitive phenomenon.

In this example, the sampled situation reveals to the operator that numerous alerts require acknowledgement and this information may have been used to modify the user awareness, but the information contained in the individual alerts is not. The operator action is to cancel multiple alerts as one, chunked, automatic operation. The user is aware only of cancelling multiple alerts and their awareness therefore does not direct them to sample the situation for the cause of the alerts that could be critical in some contexts. The net result is the user has incomplete awareness of a situation despite the fact that the interface displayed the relevant information. Analysing this interaction in terms of the SA model indicates that a breakdown occurs between sampling the situation and modifying the operator awareness.

The model encapsulates a particular view of SA as the fit between a subjective interpretation (awareness) of a situation and the actual situation built through an individual's interaction with their environment (Flach 1996). This perspective of SA suggests that a strong correspondence between the awareness and the situation indicates high SA, while weak correspondence means low SA.

The potential of the model lies in analysing difficulties that affect the user-system coupling, such as interaction breakdowns. The division of the model into areas of activity on the individual's part (sample–modify–direct) provides a structure for researchers to analyse and categorise SA problems. For example, the model could be used to question where the problems in particular situations might have arisen: what information did the individual sample from their environment?; how did this lead them to modify their awareness (what was available through the interface)?; and how, subsequently, did this direct their actions? The structure of the model partitions different areas of interest to allow researchers to concentrate on each as a distinct dimension contributing to awareness that can bring its own set of potential problems. It also allows us to consider the boundaries between these partitions, which is where we believe that many SA difficulties might arise. As individuals integrate sampled information, for example, the modification of their awareness may loosen the coupling between subjective interpretation and the objective situation leading to a reduction in SA.

5 Hazard Analysis

We suggest that the dynamic model of SA proposed in the previous section can be used as a framework for the identification and analysis of hazards relating to operator awareness in the context of system use. Specifically, there are two ways in which the model can contribute to the design of safer systems: identifying interaction breakdowns and identifying automatic interactions, both of which are key to SA. The two areas can be related to research in cognition, specifically the concepts of conscious and automatic cognition, also referred to as reflective and experiential cognition respectively (Norman 1993). Differentiating these two modes of cognition enables us to highlight and compare different aspects of human action which will be of use to our discussion of SA, interaction breakdowns and automatic interaction, and to the improved design of safety-related systems.

Experiential cognition involves the skill of an expert responding automatically to events – without conscious reflection or awareness; in contrast, reflective cognition requires different mental processes based on a higher level of consciousness (Norman 1993). Both modes of cognition are needed and neither is superior to the other – they simply differ in requirements and functions. Rasmussen (1983) also provides a similar view through his 'skill-rule-knowledge' based framework of human behaviour which suggests that human behaviour occurs as a result of different levels of cognition and, implicitly, different levels of consciousness. For example, human behaviour at the skill level, such as an experienced driver changing gears in a car, occurs automatically and without conscious effort (i.e., by experiential cognition).

These issues raises considerations of whether particular interactions undertaken by safety-related system operators should be designed to 'require' automatic or conscious cognition and also how designers might ensure the required cognition through their design. These considerations are important since they have extreme safety implications through their impact on SA.

System interactions should also support the users in achieving their tasks and the design of the interface can have a tremendous affect on the safety of the system (Rajan 1997). Interaction breakdowns can occur when human-computer communication is interrupted - in a safety-related system this could have potentially lethal consequences. Interaction breakdowns occur when a system behaves differently than was anticipated by the user (Winograd and Flores 1986) – when automatic cognition becomes conscious. Interaction breakdowns can trigger an inappropriate action (an act of commission) or it may not trigger any action at all (an act of omission).

An interaction breakdown causes an operator to apply a proportion of their finite cognitive resource to the interaction and not to the system objective. Therefore, interaction breakdowns could be disastrous in a safety-related system such as an aircraft or an air traffic control system if the operator must stop flying or controlling in order to interact with the system. Based on this understanding, it may be argued that the aim of system design should be to eliminate any potential interaction breakdowns, to develop a transparent interface that requires minimal conscious cognition. This sentiment is prevalent within the HCI literature which often equates interface transparency with usability of the system. For example, Norman (1993) argues that interruptions are especially common in the interactions with computer systems and he suggests that to achieve 'optimal flow' (automatic interaction) it is necessary to minimise these interruptions, making the system as usable as possible.

However, it can also be argued that the greatest hazard in a system is associated with the operator 'experiencing' when he should be 'reflecting' – in other words performing automatic processing when conscious thought is required. With experience, automatic human cognition can become the norm; information is perceived, interpreted and acted upon with little or no attention to it. For example, many skilled functions of an air traffic controller possess this characteristic and, for some controllers, it is intrinsic to skill acquisition. Conscious cognition bears a complex relationship to SA, yet it seems inherently unsafe to perform 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. This raises a tension between moves to remove interaction breakdowns by making interactions transparent, and interfaces usable, and the problems caused by the emphasis this places on automatic cognition. There may, we would contend, be times when usability and safety are mutually exclusive since automatic cognition is to be avoided in favour of conscious cognition, with the implication that usability of the system is decreased if the operator is consciously engaged.

The model of SA proposed in this paper may be used as a framework for research studies that aim to identify SA problems associated with interaction breakdowns and automatic cognition by looking for related reductions in integrated SA. These reductions in SA may arise where a mismatch arises between the subjective interpretation and the objective situation. Undertaking research that helps us understand and explain these mismatches should provide input to the interaction and interface design process. They can be used as input to the next generation of the system, which can aim to mitigate against the hazards that they create in current systems.

6 Situation Awareness and Usability

Identifying potential or actual interaction problem areas and addressing them is crucial in safety-related systems and anything that can support this will be a useful addition to the field of safety engineering. Norman (1988) initially suggested that safety-related systems pose a special problem in design and he implied that system safety and usability requirements could be incompatible; although he did not identify when this may be the case.

We have suggested that modelling SA is useful in identifying areas of interface design where safety and usability are mutually exclusive. Specifically, this can occur when the user fails to assimilate critical information resulting from automated interactions as discussed in the previous section. A model of SA could also contribute to the development of system safety cases as safety-related system operators must convince regulatory authorities that their systems are safe to operate and must therefore identify the unique safety requirements relating to their interactive systems (Storey 1996).

It will also help determine the extent to which making the system more usable would actually reduce hazards and increase safety. If it can be shown that making systems more usable in certain situations encourages users to have inappropriate SA, then designers will have to take this into account in designing interfaces and interactions rather than aiming for blanket usability in their systems. This will highlight further complexity in the design of safety-related systems and, through improved understanding of this complexity, help inform interface and interaction design.

There is a general trend to make use of usability in the requirements specification for interactive systems, with usability generally taken to involve not only ease of use but also effectiveness in terms of measures of human performance (Shackel 1991). From this view of usability, safety-related system developers may be tempted to infer that a usable system is, by implication, a safe system. However, as this paper has already suggested, usability and safety can be mutually exclusive properties. So, making use of usability evidence, such as the speed at which tasks may be completed using a given interface, to support claims that aspects of the system are safe may be misleading.

Instead, since safety-related systems are primarily concerned with hazardous failures, safety arguments should focus on these failures and the evidence directly related to them. The model proposed in Figure 2 can be helpful here, in supporting the substantiation of a safety claim as highlighted in the following example:

Hazardous Failure: Controller acts inappropriately due to lack of SA.

Claim: Interface design enables adequate level of SA to be acquired and maintained.

Argument: All safety-significant interactions modify operator awareness.

Evidence A: No automatic safety-significant interactions.

Evidence B: Safety-significant interactions conform to dynamic SA model with no discontinuities, e.g., the sample/modify/direct cycle is followed throughout the user's interaction with the system.

Safety and hazard analysis involve the identification and analysis of risk in order to achieve and maintain a tolerably safe state of system operation. However, as this example shows, it is possible that making an interactive system safe will entail many trade-offs with usability – in this case safety-significant interactions could not be allowed to become automatic or be by-passed in any way. This might be in direct contrast to advice based on usability where, for example, HCI prototyping may reveal a usability requirement for particular complex keying sequences to be replaced with a macro facility allowing a function to be invoked with a single switch action. However, this usability requirement may inadvertently increase the risk of human error if a hazard is associated with the keying sequences. Furthermore, the severity of the hazard associated with the keying sequences may increase during emergency or abnormal situations of a system in use. It seems that it is not enough to simply concentrate on the usability of an interactive system to assure safe operation.

Any design trade-off between usability and safety may also affect the reliability of the cognitive processes involved with acquiring and maintaining SA. If a well-intentioned system developer attempts to eliminate interaction breakdowns in the name of usability, this may have an adverse effect on the SA of the operator; something which is likely to lead to problems in the use of the system. This suggests that SA may be thought of as a critical criterion for safety-related systems and that we should balance the requirements of both SA and usability in the design of interfaces and interaction. In order to advance the field, research needs to concentrate on quantitative measures of SA which may be used to derive safety metrics for evaluating interactive systems. These safety metrics can then, in turn, be used as evidence to support arguments for specific safety claims.

7 Conclusions

This paper has identified operator situation awareness (SA) as an important phenomenon which can be used to examine human cognition in context in order to add value to system safety. The paper reviewed different theoretical views of SA and synthesised key issues from these views into a dynamic model of SA, based upon Neisser's Perception-Action Model (1976). It is suggested that the SA model can be used in suitable studies as a framework for the analysis and identification of hazards relating to operator awareness in the context of system use, and that this might be especially useful in considering safety-related systems. In addition, the results of such studies may be useful in identifying areas of interface design where hazards arise through the development of incomplete SA and where safety and usability are mutually exclusive. Finally, the paper presented a simple example of the use of the SA model to illustrate this position and to show how the SA model can be used in generating evidence to support system safety claims.

The SA model is currently in use in studies of the use of safety-related systems to identify interaction hazards and to make subsequent design recommendations. Only through using the model in complex, real-world settings can an improved appreciation of the model's usefulness be developed as well as the criticality of SA as a phenomenon for the analysis of user-system interaction.

8 References

Adams M J, Tenney Y J and Pew R W (1995), Situation Awareness and the Cognitive Management of Complex Systems, Human Factors, 37(1), 85-104,March 1995.

Billings C E (1995), 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.

Boehm B W (1988), A Spiral Model of Software Development and Enhancement, IEEE Computer, 61-72.

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

CAA (1998b), 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.

Card S K, Moran T P and Newell A (1983), The Psychology of Human Computer Interaction, Lawrence Erlbaum Associates, Hillsdale, NewJersey.

Charness N (1995), Expert Performance and Situation Awareness, 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.

Dominguez C (1994), Can SA be defined?, in Vidulich M, Dominguez C, Vogel E and McMillan G (Eds.), Situation Awareness: Papers and Annotated Bibliography, 5-15, Report AL/CF-TR-1994-0085, Wright-Patterson AFB, Ohio.

Endsley M R (1995a), Theoretical Underpinnings of Situation Awareness: A Critical Review, 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.

Endsley M R (1995b), Towards a Theory of Situation Awareness in Dynamic Systems, Human Factors, 37(1), 32-64, March 1995.

Flach J M (1995a), Situation Awareness: Proceed with Caution, Human Factors, 37(1), 149-157, March 1995.

Flach J M (1995b), Maintaining Situation Awareness when Stalking Cognition in the Wild, 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.

Flach J M (1996), Situation Awareness: In Search of Meaning, CSERIAC Gateway, 6(6), 1-4, 1996.

Garland D J and Endsley M R (Eds.) (1995), Experimental Analysis and Measurement of Situation Awareness, Proc. of an Int Conf, FL:USA, November1995.

Harris D (Ed.) (1997), Engineering Psychology and Cognitive Ergonomics Volume 1: Transportation Systems, Proc. 1st Int. Conf EP&CE, Stratford-upon-Avon, 23-25 October 1996, Ashgate Publishing.

Hopkin V D (1995), Human Factors in Air Traffic Control, Taylor and Francis.

Hutchins E (1995), Cognition in the Wild, Bradford, MIT Press.

Isaac A R (1997), Situation Awareness in Air Traffic Control: Human Cognition and Advanced Technology, in Harris D (Ed.), Engineering Psychology and Cognitive Ergonomics Volume 1: Transportation Systems, Ashgate Publishing.

Kirwan B, Donohoe L, Atkinson T, MacKendrick H, Lamoureux T and Phillips A(1998), Getting the Picture: Investigating the Mental Picture of the Air Traffic Controller, Proc. Conf. Ergonomics Society, 405-408.

Landauer T K (1987), Relations Between Cognitive Psychology and Computer Systems Design, in Carroll J M (Ed.), Interfacing Thought: Cognitive Aspects of Human-Computer Interaction, MIT Press, Cambridge: MA.

Mace W M (1977), Ask Not What's Inside Your Head But What Your Head's Inside Of, in Shaw R E and Brandsford J (Eds.), Perceiving, Acting and Knowing, Hillsdale NJ, Erlbaum.

Nardi B A (Ed.) (1996), Context and Consciousness: Activity Theory and Human-Computer Interaction, London, MIT Press.

Neisser U (1976), Cognition and Reality: Principles and Implications of Cognitive Psychology, San Francisco, W H Freeman.

Norman D A (1988), The Psychology of Everyday Things, New York, Basic Books.

Norman D A (1993), Things that Make us Smart: Defending Human Attributes in the Age of the Machine, Addison-Wesley.

Rajan J (1997), Interface Design for Safety-Critical Systems, in Redmill F and Rajan J (Eds.) (1997), Human Factors in Safety-Critical Systems, Butterworth-Heinemann.

Rasmussen J (1983), Skills, Rules, Knowledge: Signals, Signs and Symbols and other Distinctions in Human Performance Models, IEEE Transactions: Man & Cybernetics, SMC-13,257-267.

Sandom, C., and Harvey, R. S. (2004): *Human Factors for Engineers*, The Institution of Electrical Engineers, UK.

Sandom, C. (2007): Success and Failure: Human as Hero – Human as Hazard. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 57. T. Cant, (Ed.), *12th Australian Conference on Safety Related Programmable Systems*, Adelaide.

Sandom. C. (2011): Safety Assurance: Fact or Fiction? Conferences in Research and Practice in Information Technology (CRPIT), Vol. 133. T. Cant, (Ed.), *Australian System Safety Conference*, Melbourne.

Sarter N B and Woods D D (1991), Situation Awareness: A Critical but Ill-Defined Phenomenon, Int J of Aviation Psychology, 1, 45-57.

Shackel B (1991), Usability - Context, Framework, Definition and Evaluation, in Shackel B and Richardson S (Eds.) (1991), Human Factors in Informatics Usability, Cambridge University Press.

Smith K and Hancock P A (1995), Situation Awareness is Adaptive, Externally Directed Consciousness, Human Factors, 37(1), 137-148, March 1995.

Storey N (1996), Safety-Critical Computer Systems, London, Addison-Wesley.

Suchman L (1987), Plans and Situated Actions, Cambridge, Cambridge University Press.

Whitfield and Jackson (1982), The Air Traffic Controller's Picture as an Example of a Mental Model, in Johannsen G and Rijnsdorp J E (Eds.), Proc. of IFAC Conf. on Analysis, Design and Evaluation of Man-Machine Systems, 45-52, London, Pergamon.

Winograd T and Flores F (1986), Understanding Computers and Cognition: A New Foundation for Design, Norwood, Ablex.