INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN
ICED 05 MELBOURNE, AUGUST 15-18, 2005

A THEORY-BASED ONTOLOGY OF DESIGN INDUCED ERROR

I J Shin, J S Busby, R E Hibberd and C A McMahon

Keywords design induced error, engineering failure, complex systems, ontology development

1 Introduction

At the entrance to the Library of our University there is an electronically controlled gate through which you have to slide a plastic card in order to gain admittance. It is very easy to slide the card through the gate in the incorrect manner. The gate only accepts a particular side of the card and it is easy to forget which side is the correct one to use. Although with experience, you make fewer errors, errors still arise and the queue at the entrance is long because of people who have to try again. This simple example shows the manner in which errors in the use of modern technology arise in everyday life. We propose that the design of systems like the gate to the University Library represent *error inducing systems*. Other examples we have found include ticketing machines of car parks, buses or subways or automatic teller machines at banks, machines that we encounter frequently. In these cases, where the consequences of error are frustration, these consequences tend to be inconsequential. However, in the case of machines and systems used within a manufacturing context or as part of a transportation system, the consequences can be catastrophic. This paper examines how it might be possible to assist designers in identifying potential sources of such *design induced error* (DiE) and to find design solutions that can avoid the recurrence of these.

2 The need for a concept of design-induced error

Errors and failures are an intrinsic part of engineered systems [1]. The history of design is a history of accidents and errors and their avoidance and correction. In some cases, the contribution of design to failure is clear to see: an error in a calculation, an omission or an oversight by a designer leads to failure and the causal relationship is clear. In other cases, by contrast, the failure may arise as a result of the action of the user or operator of the engineered system, and the role of design is less immediately obvious. And yet in many of these cases design is a strong contributory factor because the provisions made by the designer influence the behaviour of the user. The increase in complexity of systems and the extensive use of automation leads to new opportunities for misunderstanding and error and new modes of failure, for example arising from such causes as a mismatch in expectations between designer and operator.

The aim of the work reported here is to draw together theoretical explanations of DiE, and to use these as a basis for the development of an ontology to support the automated or semi-automated processing of accident and failure reports with the aim of providing new insights into DiE. This paper will report on the theoretical development, and will present preliminary results from the construction of the ontology.

To make a system safer, many design philosophies have been introduced including fail-safe design, error-tolerant design, and cognitive ergonomics. These approaches draw on ideas from studies of human error, from previous lessons learned experience of accidents or incidents, and from psychological research. However, there has been less research into the question of how users are led to making errors in their use of systems. For example, the philosophy of error-tolerant design focuses on the construction of systems that do not fail even when users make errors in operating them.

Whilst engineering design has led to the prevention of many accidents, through increasing the reliability of systems, rapidly evolving communication and computing tools developed to deal with the increasingly complex systems that can now be constructed still require human intervention. However, the design of such systems can affect the cognition that users have about both the function and the state of the system. In order to reduce the presence of DiE there is a need to create methodologies that can guide the generation of design concepts.

To illustrate the need for new methodology, consider the rail accident that occurred in 1999 at Ladbroke Grove in London [2]. On 5 October 1999, a three-car train passed a red signal as it was leaving London Paddington, UK, and continued for some 700 metres into the path of a high speed train with which it then collided. As a result of the collision and subsequent fire, 31 people died and 227 were taken to hospital. 296 people were treated for minor injuries on site. This accident, as with all major accidents, was the result of a confluence of a series of factors, one of which was the driver's actions. In this case, the driver inadvertently drove through a signal, signal SN109, which had been showing a stop aspect.

The train, at the time of accident, had an Automatic Warning System (AWS) that consisited of trackside permanent magnets, electro-inductors and inductor suppressors which interface with trainborne AWS equipment. This equipment provides train drivers with an aural and visual indicator of whether an approaching signal shows a clear aspect, a green light, or not. If the signal does not show a clear aspect, it can show a caution aspect, which could be a yellow or a double yellow light, or a stop aspect, which is a red light. The two caution aspects show that although the next track block is clear, subsequent blocks are occupied and therefore the driver should be prepared to stop at the next or next but one signal. If the train travels through a signal showing a stop or caution aspect and the AWS warning is not acknowledged, the brakes on the train are automatically applied.

Prior to the collision, the driver of the three-car train had travelled through three signals: SN43 which had displayed a green light, SN63 which had displayed double yellow lights, and signal SN87, which had displayed a single yellow light. On the approach to signal SN109, the three-car train had been coasting. However, on the approach to signal SN109, the driver increased power, at a point where the signal was not visible, but where other signals on the gantry supporting signal SN109 were. Shortly after accelerating the AWS horn operated to warn the driver that the signal was not showing a clear aspect. Signal SN109 was showing a stop aspect. However, instead of stopping the train, the driver cancelled the AWS warning and began to accelerate at a distance of 107 metres from where the collision occurred.

It was suggested in the report of this incident [2] that the cancellation of the AWS could have been an automatic response. The AWS warning does not distinguish between caution and stop aspects. On the approach to a major station, such as Paddington, the volume of traffic means that many of the signals that drivers encounter would show caution aspects. As a consequence, drivers cancel AWS warnings on a regular basis, which could lead to a potential automation of

their response. In this case, the driver may simply have mistakenly believed that the AWS warning at signal SN109 indicated that it was possible to proceed.

It is conceivable that the driver was not aware that an error had been made. The driver was inexperienced, and so may not have noticed that the train was proceeding onto the wrong section of railway track. Although the driver would be expected to periodically assess the progress in an activity, even following the use of an automated set of skills, this requires that there are cues which indicate that an action has deviated from that planned [3]. Although there had been previous incidents when signal SN109 had been passed at danger, these had been by experienced drivers who had recognised the error when their trains had been directed onto the wrong section of railway track.

In this case, it is difficult to identify any specific failure in the design. The AWS functioned in the manner it should have, and should have drawn the driver's attention to the signal aspect presented. However, whilst the design of the AWS did not lead directly to engineering failure, design of the system has helped induce the human operator to develop a specific behaviour. Use of the system appeared to induce a form of automatic behaviour, which could produce errors that would be undetectable to an inexperienced driver. This case depicts a need for a new approach to investigating the role that design plays in inducing user error, and which can allow designers to gain new insight into how particular designs may function. It is suggested that an examination of the literature on existing forms of human error can support the development of an ontology which provides a basis for the automated or semi-automated processing of accident reports. This processing should enable the identification of DiE cases, and the characteristics of the system that induced user error.

3 Methods

The development of an ontology for the identification of DiE cases involves two strands of research work. The first strand of research involves the development of a metatheory that is used to synthesise the theories of human behaviour that are relevant to understand the manner in which DiE can arise. A metatheory represents a theory about theories [4], and is constructed as a means of identifying the properties of a group of theories that focus on different or similar aspects of a domain. Development of a metatheory provides a means of synthesising theories, their commonalities and discrepancies, in a manner that can allow for the development of a cohesive ontology of these theories and of the sources of DiE.

The second strand of the research is a study of the documentation of accidents and failures to identify evidence of design-induced error and to explore how an ontological approach may assist in the automated or semi-automated processing of the documentation. This paper presents mainly the result of the first strand and outlines the process of the second strand.

4 Towards a metatheory of design-induced error

Underlying the development of a metatheory, an extensive review of errors in the operation of systems has been undertaken. This review illustrated a number of issues in the design of systems, including the manner in which automation is deployed in complex systems [5], the impact of this on operator skill [6], and the degree to which users develop appropriate levels of trust in the systems used [7]. The review also encompasses research that has examined the

differences between users and designers perceptions of the system. This has encompassed work that has examined how users understand the affordances[1] of the system [8]. The review also revealed how problems in the use and evaluation of the system can arise from limitations in the feedback given to the operator by the system [9].

The metatheory that has been developed encompasses three main organising principles based on this review. Firstly, it was noted that error can arise as a result of problems in the transfer of information between the designer and user. Secondly, it was noted that the use of the system may be compromised by inappropriate strategies for temporal decision-making, which may lead to unreasonable time constraints and unacceptable levels of user workload. Thirdly, it was also suggested that the local rationalities of designers and users lead to mismatches between the internal mental representations of the system and its functions, *mental models*, that each hold. These principles have been used as a means of integrating different theories related to the concept of DiE. These principles have also been employed in the processing of a number of example accident report drawn from aviation, marine and general industrial incidents.

4.1 Problems in transferring information about system function

Designers' ideas are embodied in the form and function of the systems they design. Through the design, the designer attempts to provide cues as to the function of the system, although such efforts may be compromised by limitations in the cues that the affordances of the system can provide. The interpretation of the cues provided by the system's affordances are mediated by the experience of the designer or user, which can lead to misinterpretation of the affordances available to the user.

When a user is faced with an unfamiliar artefact or system, the tendency of the user is to try and employ an existing mental model of a system that the presented system may only superficially resemble in order to interact with it [10]. Consequently, the user may interpret cues to the system's affordances in a manner that is contrary to that expected by the designer.

It is also possible to identify examples of how the cues provided by affordances may lead to the generation of hypotheses about the use of systems by users that are contrary to their actual function. For example, when the designers of a missile attempted to improve the stability of a air to air missile through the introduction of rolleron gyroscopes on the edges of the missile's control fins, they would not have anticipated that personnel responsible for the installation of these missiles would assume a different use for the rotating devices. The rotational affordance offered by the rolleron was used to facilitate ease of use during installation, an activity which actually damaged these devices [11].

4.2 Problems in temporal decision-making during complex system use

Increasing use of computer technology has transformed the operator's role in socio-technical systems [6]. One of the most distinguishable points of changes is in *temporal decision-making*, decision making about the progress of an operation, and when intervention in the process should arise [12].

In order to design systems that can be effectively used by operators, it is necessary to know how operators decide when to intervene in the operation of the system and the manner in

[1] Affordances are the properties of something that determine or suggest how it could be used.

which they use their mental models of the system to estimate both their location in a process, and the duration of the process itself. In addition, there is a need to know how operators use cues from the environment to support their decision-making under time pressure.

Systems and artefacts have been evolved into complicated and tightly-coupled forms, and as a result, the speed of systems has increased, leading to quicker completion of actions and faster responses to requests. Operators in the complex system are experiencing conditions that they have not previously met. Problems in temporal decision-making that are encountered in complex systems arise from: increased time pressure, increases in the number of system functions, and the invisibility of system processes.

This means that there is a mismatch between the time required for human operators to develop mental models of the system and the pace with system states change. The problem space required to effectively use the complex system has increased, which means that operators have problems in developing an appropriate mental model of the current state of the system. Their mental models are affected by the high frequency of feedback about decisions they have taken to meet system their goals.

Rasmussen [13] suggested that there were three levels of performance underlying human decision-making, described in Table 1. It would be expected that the performance at the skill-based level of performance is fastest, followed by performance at the rule-based level. In interacting with the system, users may be forced to revert to performance at a rule-based or knowledge-based level when unexpected events arise. However, despite the fact that such performance is time-consuming, the system, due to its inherent complexity, requires rapid responses, leading to a high degree of time-pressure.

Table 1. Description of Rasmussen's (1983) Levels of Human Performance

Type	Description
Skill-Based Level	Actions are the result of sensory-motor performance which are set in motion by a statement of intention, but which are then conducted without conscious control, resulting in smooth, automated and highly integrated patterns of behaviour
Rule-Based Level	The enactment of a series of sub-routines, represented at the skill-based level of performance, might be controlled by a stored rule, which may have been derived from direct or vicarious experience of the system, or from verbal instruction
Knowledge-Based Level	Performance at this level is enacted when no existing procedure is available, and involves the explicit definition of the goal to be attained and the generation and evaluation of alternative plans for reaching that goal

Figure 1 illustrates the manner in which user performance is influenced by the constraints placed by systems during activities that require temporal decision making. In environments of high workload, users have little opportunity to deploy time-consuming knowledge-based process such as identification, decision and planning, but to have to revert to sensory-motor performance controlled at the skill-based and rule-based levels of performance.

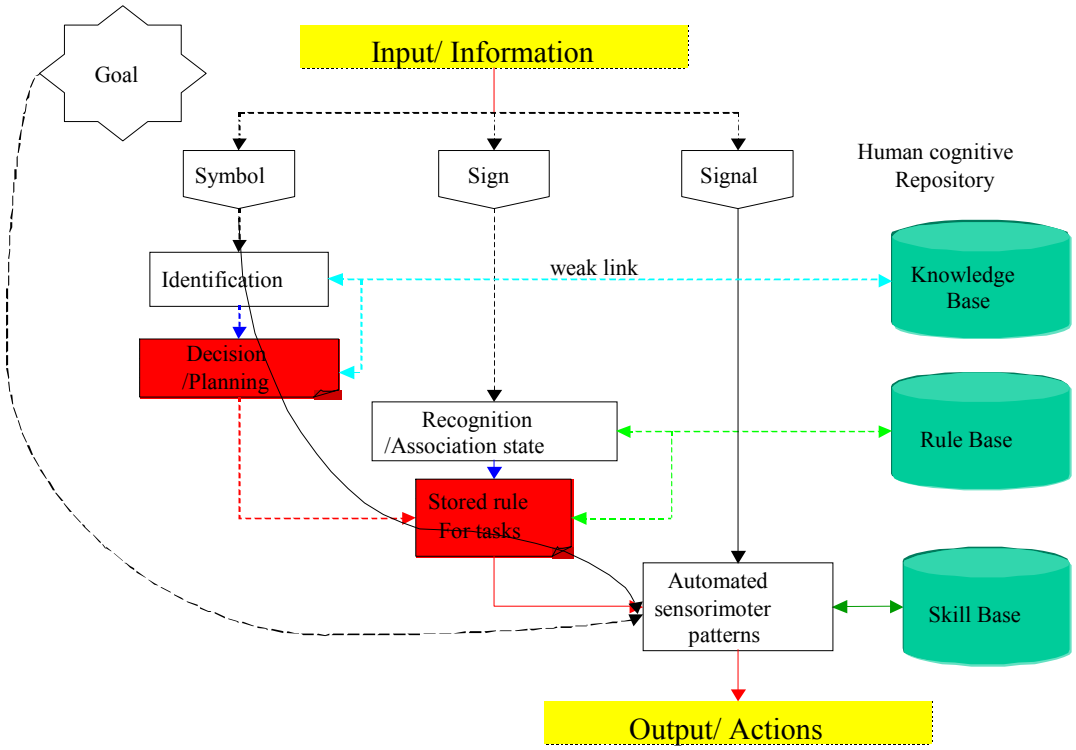

Figure 1. A model of the manner in which operators conduct temporal decision-making
Adapted from Rasmussen (1983)

Temporal decision-making in complex systems has changed the manner in which operators communicate with other users collaborating in the operation of the system. It has been suggested that under time pressure or when facing ambiguous system displays that operators use sensemaking to develop their mental models of the system [14]. Their performance levels are also affected with regard to changes of communication and decision-making patterns from considerable reasoning into such as dynamic reasoning, negotiation with systems and instinct. Therefore, the interaction problems between operators and artefacts in complex systems should be considered as design requirements.

4.3 Problems arising from designer and user local rationalities

User errors can result when the demands the system design places on users exceeds their capabilities. Norman [9] illustrated the manner in which different rationalities of designers and users can lead to conflicting approaches to the operation of the system. This is shown visually in Figure 2. In the construction of a system, the designers generate their own concept of the system (System A) according to their own local rationality (Rationality A). However, the user generates their own perception of the system (System B) according to their own rationality (Rationality B). As Figure 2 illustrates, there may only be a partial overlap between the mental models that designers and users have of the system and the rationality underlying its design. It was suggested that these local rationalities arise because there is no exchange of knowledge between designers and users.

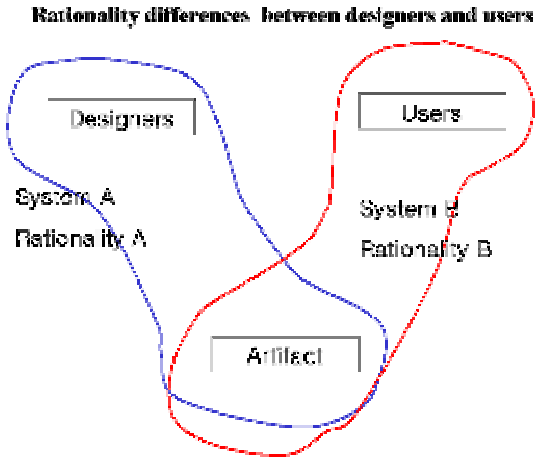

Figure 2. Local rationalities of designers and users [9]

Woods and Cook [15] argued that consideration of the local rationality of operators such as resolving conflicts, anticipating hazards, accommodating variation and change, coping with surprise, working around obstacles, closing gaps between plans and real situations is critical for the development of safer systems. From this perspective, DiE may be defined as the inconsistencies in local rationalities that exist between designers and users. Designers' misunderstandings about operators induce inappropriate design of the artefact and system. For instance, in the Three Mile Island nuclear power plant accident in 1979, operators failed to recognise that the relief valve was stuck open because the indicator on the control panel misled operators. The indicator only showed the state commanded for the valve, but not the actual state of the valve.

The local rationalities held by designers may lead to assumptions made about users and the context in which the system is used which generate DiE. For example, designers' local rationality may not provide an appropriate model of the limitations of users' cognitive perfromance. Similarly, the designers may not reflect on the changes in workload imposed on users generated by change to the system, which may lead to degraded user performance. Finally, the designers' local rationality may not appreciate that the system is not perfect, and so includes inherent deficits that can lead to errors and failures. The assumption of benign system operation may lead designers to ignore the need for the inclusion of devices to allow the user to gain the necessary information to effectively restore the system to a benign state when failure arises.

4.4 Properties of designs that induce user error

In this section, we shall explore how to generate a metatheory of DiE from the myriad theories underlying user error that have been proposed. On the basis of the preceding discussion, we have focussed on the concept of local rationalities as a means of explaining the interaction between design and user error. The distinctive local rationalities of user and designer lead to differing perceptions of the capabilities, functionality, and reliability of the system. In Table 2, a number of theories that describe limitations in human performance, identified from the preceding literature review, are presented, together with an indication of how the local rationalities may lead designers and users to act in a manner that was contrary to the

expectations of designers or to design systems that are incomptible with the capabilities of users.

Table 2. Local rationalities of designers and users from theories of user performance

Theory	Designers' Rationalities	Users' Rationalities
Risk homeostasis	Risk of failure decreased through use of increasingly reliable or defended systems	Increased reliability and defence can be exploited for increased performance
Automation ironies	Introduction of increasingly reliable automation allows exclusion of unreliable user from the system	Systems are able to present information that is opaque and uninterpretable
Trust in automation	Users are able to generate an accurate mental model of the system and when monitoring should arise	Monitoring of the system can be based on own subjective perception of reliability
Automation surprises	Introduction of automation provides protection to the system	Introduction of automation should support reasoning about the state of the system
Plan delegation	Users are planful in their use of artefacts and will deploy in accordance with the goals prescribed by designers' recommended usage	Artefact can be relied upon to support acquisition of desired goals
Design affordances	Affordances of artefact provide access to function	Affordances of artefact indicate the procedure required to complete specific tasks

The first theory, *risk homeostasis*, proposed by Wilde [16] indicates that designers attempts to reduce the risk of catastrophic failure through increased reliability or increasing number of hard defences, such as anti-lock braking systems on automobiles, may be defeated by user behaviour. The users of such systems may assume that the changes to the system allows them to safely increase productivity or performance. In this case, the user and the designer have different goals, the designers have a goal of reducing risk, but the users concentrate on another goal, that of increasing productivity.

The second theory, Bainbridge's [6] theory of *automation ironies*, suggests that designers may believe that the reliability of the system can be improved by excluding the human from the operation of the system. However, as Bainbridge noted it is impractical to remove the user from the system. This still appears a plausible proposition given that the human user possesses the unique ability to perform at the knowledge-based level of performance, required to solve problems that arise in the operation of the system. Automation can gradually erode the ability of operators because they are deprived of experience in using the artefact. As a result, the eroded operator ability may reduce the operator's ability to diagnose faults and plan their use of the system.

The third theory, Muir and Moray's [7] theory of *trust in automation*, noted that that as a result of increasing computerisation of systems, the increasing complexity of systems, and the degraded ability of operators to deal with problems in the system, more and more users tend to

place inappropriate trust in the system, and fail to check all relevant indicators. This may not match the expected degree of monitoring prescribed by the designers of the system.

Sarter and Woods' [5] theory of *automation ironies*, suggests that designers and users have different views of automation. The designer expects that the user constantly monitors the state of the automation and is able to respond to discrepancies in feedback that arise which illustrate that an error, arising from either the actions of the user or from a technical malfunction has occurred. However, the users expect the system to serve them by providing readily-interpretable feedback about the state of the system.

The remainder of the theories illustrate the manner in which the perception of the affordances of artefacts can lead to unanticipated usage. Busby and Hughes' [17] theory of *plan delegation* suggested that designers expect that users are responsible and planful, but users expect that artefacts exist to support the goals they wish to pursue. Similarly, Norman's [9] theory of *affordances* illustrates how the user expects that the properties of the artefact will suggest how to complete a task, whilst the designer assumes that these represent a means of accessing specific functions of the system.

4.5 Meta theory of design induced error

For a theoretical basis of the concept of design induced error, the following propositions are suggested for a metatheory of design induced error from current theories that related to design induced error: (1) human decision making processes need information from artefacts that matches the models that user form about the artefacts (2) if information transferred from designed systems does not match with information that has already been transferred users are apt to make errors, (3) design induced error comes from a mismatch between designers' intentions and users' expectation, (4) temporal decision making that is prevalent in current complex systems needs more comprehensive designs that provide reliable comparative information that matches human cognitive activity, (5) the designer's role to prevent humans from making error is more important than before.

From this perspective a working definition of design induced error is that "design-induced error has both the nature of design error as well as human error that occurs in the form of failures in interactions between the user and the artefact in certain circumstances. It is caused by limitations in the design of artefacts that typically have no effect on operator performance but which, under certain circumstances, can lead to acute or chronic deterioration of operator performance, which can lead to active failure on the part of the operator".

Design induced error is problems of interaction between human and systems. Metatheory of DiE should depict the related phenomena in an interaction model. Each theory in metatheory of design induced error can be shown in different patterns of human-ystem interaction. The interaction patterns between humans and systems related to design induced error may be categorised according to activity degress of human and systems, and information exchange orders of them. The authors suggest an interaction pattern model (Table 3) in terms of relations between performance types (active-inactivity) and interaction orders (initiative-response).

Table 3. Interaction pattern of design induced error

Interaction Pattern (H:Human,	Description	Related theories

S:System) Error type= Initiative – Response		
$E_{A1} = H_{Active} - S_{Active}$ (direct interaction error)	Human requests a system what to do. The system responds but the response does not comply with human expectations.	Design affordance, Gulf of evaluation
$E_{A2} = H_{Active} - S_{Inactive}$ (indirect interaction error)	Human activates something but the system does not respond to the activation.	Gulf of execution, Gulf of evaluation
$E_{B1} = S_{Active} - H_{Active}$ (direct interaction error)	A system demands something for an operator to do. The operator response differs from the system's expectation.	Design affordance
$E_{B2} = S_{Active} - H_{Inactive}$ (indirect interaction error)	The system requests an action but the human does not respond due mainly to the need for too much vigilance work.	Irony of automation, trust in automation
$E_{C1} = H_{Inactive} - S_{Active}$ (indirect interaction error)	There is a task to do, but the human has not kept track of the work. The system addresses the task, but the form of response of the system is not as expected by operators.	Automation surprise, trust in automation
$E_{C2} = H_{Inactive} - S_{Inactive}$ (indirect interaction error)	A procedure is necessary, but the human does not perform the needed procedure due to time pressure, high workload from other procedures etc. the system does not make the operator realise his/her mistake.	Plan delegation
$E_{D1} = S_{Inactive} - H_{Active}$ (indirect interaction error)	There is a hazard, but systems do not convince operators to recognise the hazard, rather let the operator exploit the system capabilities in a potentially harmful manner.	Risk homeostasis, Gulf of evaluation
$E_{D2} = S_{Inactive} - H_{Inactive}$ (indirect interaction error)	An action is demanded before starting a procedure, but the system does not activate the action and neither does the human.	Plan delegation

5 Development of an ontology of design-induced error

Ontologies play a major role in current knowledge management system (KMS) development [18]. In the context of KMS, they are formal descriptions of the concepts and relationships that can exist in a domain, and they are used to allow and support the collection and sharing of knowledge in a domain, in particular so that computational agents can identify legitimate entities and the possible relationships between them when processing the entities. For the development of concept of design induced error, ontological approaches will be used so that the design induced error can be more easily identified in accident reports and engineering documents.

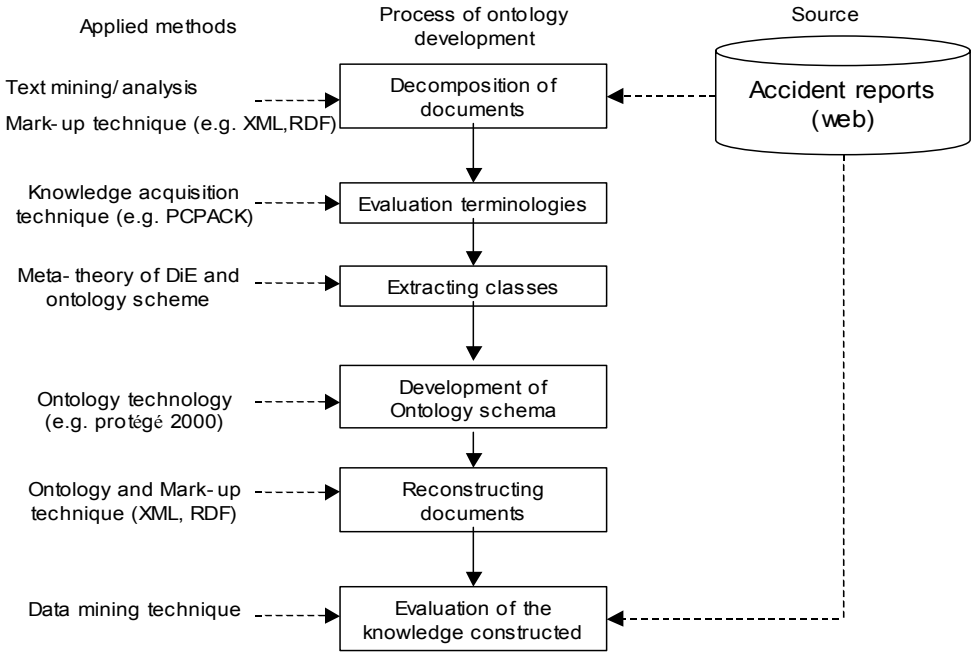

Figure 3. Process of ontology development and application

The process of developing an ontology of design induced error is shown in Figure 3. Initially, the contents of accident reports are being examined in order to identify reports that contain instances of DiE. The characteristic words or phrases that are present indicating DiE are then extracted from the accident reports, clustered and linked to the entities describing the DiE metatheory. The evaluation of the experimental ontology will also be conducted by using accident reports for test purposes, by exploring whether the ontology can be used as a basis for identifying further reports constaining instances of DiE. This research will use a web-based ontology methodology (Protégé 2000) because of considerations of usability of the ontology of DiE.

In order to extract the concept of design induced error from accident reports, we need a map of the ontology process that contains all kind of related events and elements. Figure 4 shows the process map that has been developed to assist in developing the ontology.

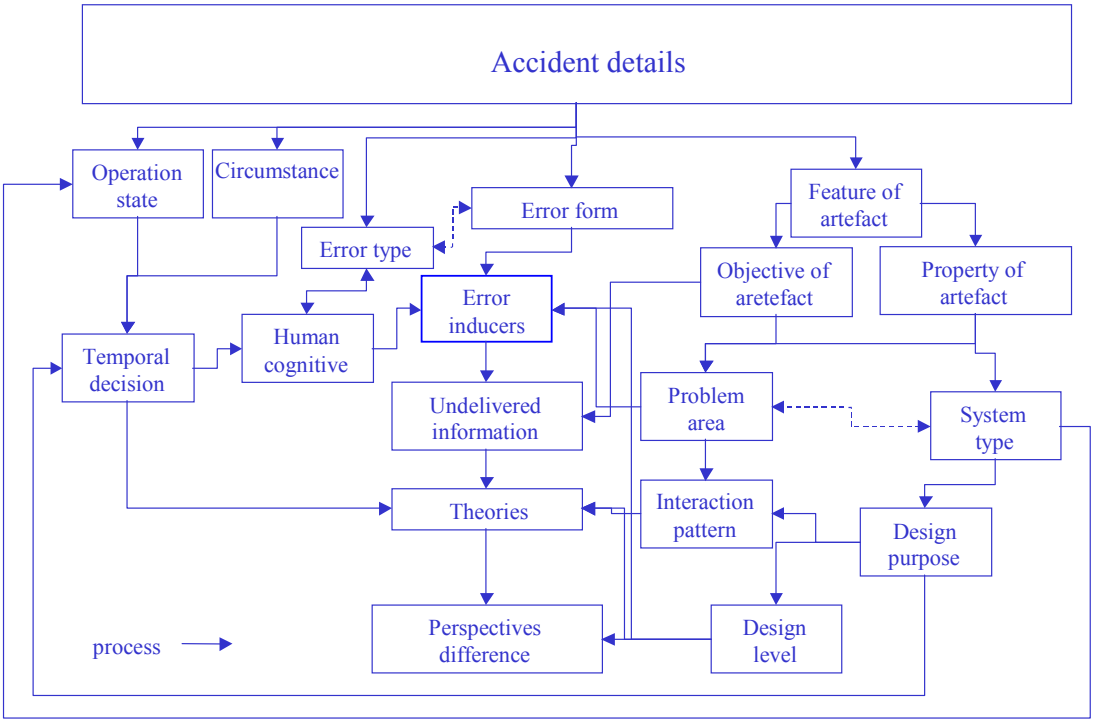

Figure 4. Map of ontology process of design induced error

The completion and verification of the research will apply the developed theory and methodology of DiE in a real design process, especially in safety critical system design e.g. an aviation system or a healthcare system, by using the ontology to assist in the identification and organisation of information concerning possible examples of DiE from available records, and presenting these to designers in a structured form. By applying the ontology in such ways, the theory and methodology of design-induced error can be tested and refined more concretely, with the hope of getting usability and applicability into design worlds (Figure 5).

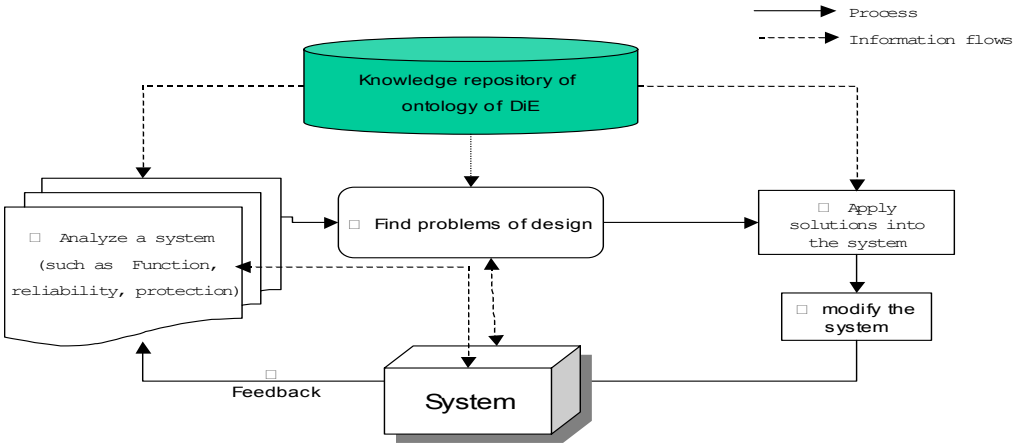

Figure 5. A diagram of an application of the DiE ontology into risk analysis of a system

6 Conclusions

The extensive use of automation, and computers in particular, has led to the development of increasingly complex systems used in areas such as power generation, chemical production, aerospace and marine transportation. The increase in the complexity of such systems has generated new mechanisms for user error, and has led to the requirement for a new understanding of the contribution of design to such errors. This paper provides an overview of different contributory factors in design induced error, and will suggest how new ontological approaches may assist in organising information to assist in that understanding. Existing research has illustrated that there are three main issues to be addressed in the design of systems, including an awareness of how systems communicate their affordances, an awareness of the constraints placed on the user during temporal decision making tasks, and the role that local rationalities play in the design and use of systems.

To overcome the problems posed by these issues, it is essential to combine the insights provided by psychological research into an information technology system that can support designers' reasoning during the development of systems. This paper has provided a summary of the research related to DiE, and suggested a potential means of providing designers to remove the potential antecedents that produce DiE. The ongoing research on knowledge extraction and ontology development is required if the problem of DiE is to be effectively addressed.

References

[1] Petroski, H., "To engineer is human: the role of failure in successful design". St Martins' Press, New York, 1985.

[2] Health and Safety Executive "The train collision at Ladbroke Grove 5 October 1999: A Report of the HSE Investigation." HSE Books, London, 2001.

[3] Reason, J., "Human Error" Cambridge University Press, Cambridge, 1990.

[4] Matthews, P.H. "The Oxford Concise Dictionary of Linguistics." Oxford University Press, Oxford, 1997.

[5] Sarter, N.B and Woods, D.D., "Team play with a powerful and independent agent: Operational experience and automation surprises on the Airbus A-320", Human Factors, 39, 553-569, 1997.

[6] Bainbridge, L., "The ironies of automation". Automatica, 19, 775-780, 1983.

[7] Muir, BM. and Moray, N., "Trust in automation: Part 1 – Theoretical issues on the study of trust and human intervention in automated systems", Ergonomics, 37, 1994, pp1905-1923.

[8] Gibson, J J., "The theory of affordances", in Shaw, R E and Bransford, J (Eds), perceiving, Acting and Knowing, Lawrence Erlbaum Associates, Hillsdale, NJ, 1977.

[9] Norman, D., "The design of everyday things", MIT Press, London, 1998.

[10] Preece, J., Sharp, H., Benyon, D., Holland, S. and Carey, T. "Human-Computer Interaction", Addison-Wesley, Harlow, UK, 1994.

[11] Adamski, A.J. and Westrum, R., "Requisite imagination: The fine art of anticipating what might go wrong", in E. Hollnagel (Ed.) Handbook of Cognitive Task Design. Lawrence Erlbaum Associates: Mahwah, NJ, 2003.

[12] De Keyser, V., "Temporal decision making in complex environments", Philosophical Transactions of the Royal Society, B 327, 569-576, 1990.

[13] Rasmussen, J., "Skills, rules, knowledge: signals, signs and symbols and other distinctions in human performance models". IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, 257-267,1983.

[14] Busby, J.S., Hibberd, R.E., "Artefacts, sensemaking and catastrophic failure in railway systems", IEEE SMC 2004: International Conference on Systems, Man and Cybernetics, The Hague, The Netherlands, 10th. - 13th. October. 2004.

[15] Woods, D. D. and Cook, R. I., "Perspectives on Human Error: Hindsight Bias and Local Rationality", in F. Durso (Eds.), Handbook of Applied Cognitive Psychology, New York, Wiley, 141-171, 1999.

[16] Wilde, G.J.S., "The theory of risk homeostasis: Implications for safety and health, Risk Analysis", 2 (4), 1982.

[17] Busby, J.S, Hughes, E.J., "How plan delegation contributes to systemic failure", Human Systems Management, 22, 13-22, 2003.

[18] Noy, N., McGuinness, D., "Ontology Development 101: A Guide to Creating Your First Ontology", Stanford University, 2003.

I J Shin
Department of Mechanical Engineering
University of Bath
Bath BA2 7AY
United Kingdom
Phone: +44 (0)1225 384049
Fax: +44 (0)1225 386928
Email: enpijs@bath.ac.uk