

Augmenting descriptive scenario analysis for improvements in human reliability design

Shamus P. Smith

Shamus.Smith@cs.york.ac.uk

Michael D. Harrison

Michael.Harrison@cs.york.ac.uk

The Dependability Interdisciplinary Research Collaboration
Department of Computer Science
The University of York
York YO10 5DD, United Kingdom

ABSTRACT

It is typical for cycles of iteration to be used to refine the current state of the design of a system so that it more closely meets its requirements. Such refinements are in terms of the original requirements specification and any new requirements that have been identified during this process. However, not all defined requirements are equally essential, particularly in high consequence systems where there are issues of dependability. Although descriptive methods for scenario analysis can be used to highlight new requirements, it can be difficult to evaluate the impact of these new requirements.

In this paper, we exemplify this problem and investigate how numeric methods can be used to highlight the impact of consequences identified by descriptive scenario analysis. An example from the context of human reliability analysis is presented and dependability issues for system design are considered.

Keywords

Descriptive and numeric analysis, scenario based design, human reliability design, THEA, HEART

1. INTRODUCTION

Iterative methods are common in the development of computer systems. Within software system life-cycles, such methods are used to refine the current state of the design of a system so that it more closely meets its requirements. This is particularly evident in the design and prototyping phases of a system's development.

In this paper we are concerned with the design phase and with the step preceding a new iteration being applied to a design. By design iteration we mean the process of applying newly identified, or refined, requirements to an existing design. In the literature there are many candidate methods

for design analysis (for examples see [8]). These techniques provide a mechanism for analysing designs to identify the requirements for alternative and/or new designs. This process needs to provide two components: the new requirements and the rationale for the application of the new requirements.

Typically, design analysis techniques evaluate the current design and look for problems (for example usability issues [5]). The identified problems are used to construct recommendations to solve design problems. However, before these recommendations can be considered and applied as new requirements, it is necessary for some rationale to be provided. Therefore after the application of a design analysis technique, there are three issues that need to be addressed:

1. Does the analysis technique provide a structure, for the identified problems, to allow the designer to successfully argue/defend the recommendations for redesign? This is particularly important when the argument concerns the dependability or safety of the design.
2. Which of these recommendations are *most* important, i.e. preferred requirements, for the new design?
3. Is it possible to optimise the work effort for the redesign by using the two issues above to focus on the critical new requirements?

These three issues are at the core of the work that is discussed in this paper. We are particularly interested in the arguments that can be developed through this process to support the identification of new requirements and to focus the redesign process. The format for the remainder of this paper is as follows. Section 2 introduces the work described in this paper in the context of system design for dependable systems. Next we define the example context, human reliability analysis (HRA), and the design analysis technique we have applied (Technique for Human Error Assessment - THEA [7]), including a small example. This will be followed, in Section 4, by a discussion of the descriptive arguments that can be developed from the THEA analysis. A treatment of statement belief, expert judgement and requirement impact will then be presented. Section 5 will introduce a numeric approach (Human Error Assessment and Reduction Technique - HEART [9]) and demonstrate its application to the issues raised by the THEA analysis. The

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SAC 2002, Madrid, Spain
Copyright 2002 ACM 1-58113-445-2/02/03 ...\$5.00.

paper concludes with a summary of conclusions and scope for future work.

2. DEPENDABILITY AND DESIGN REQUIREMENTS

When developing systems that require some level of dependability it is critical that faults are found in systems before they result in undesirable consequences. As with most software systems, it is beneficial to identify and correct faults early in the software life-cycle [8]. In this paper we are interested in the use of scenario based design where cycles of scenario descriptions can be used to refine the current state of a system design so that it more closely meets its requirements and potential faults are eliminated in this context.

At this stage of the design process, problems, leading to faults with their system consequences, will have been identified. These may be viewed as new requirements for a redesign. However, not all requirements are equal and whether these requirements must be addressed is a matter for expert judgement. Some requirements may be more critical to the dependability of the system, and considered essential to any redesign, and others may have only minor consequences for the development.

In this paper we explore how quantification of the dependability of new design requirements may be used to reinforce descriptive scenario analysis and will discuss its limitations. In order to have a demonstrable example, we have scoped our work to one area of interest for system dependability: human reliability analysis (HRA).

3. HUMAN RELIABILITY ANALYSIS

Kirwan [4] observes that one of the primary goals of human reliability analysis is to provide a means of properly assessing the risks attributable to human error and for identifying ways of reducing system vulnerability to human error impact. He notes that this is achieved by three principal functions; (i) identifying *what* errors can occur (Human Error Identification), (ii) deciding *how likely* the errors are to occur (Human Error Quantification) and (iii) enhancing human reliability by *reducing* this error likelihood (Human Error Reduction).

We have investigated how descriptive methods for human error identification can be augmented by techniques that generate numeric values for human error quantification. The aim of this process is to enhance human reliability through the reduction of human errors that these processes facilitate. In Section 5 we investigate a technique for human error quantification but before this can happen, the process of human error identification is required. For this we are using a scenario based technique developed at The University of York called THEA.

3.1 THEA

THEA (Technique for Human Error Assessment) [2, 7] is a technique developed to help designers in interactive systems to anticipate interaction failures or human errors that may be problematic once their designs become operational. The technique is intended for use early in the development life-cycle, as design concepts and requirements concerned with

safety and usability, as well as functionality, are emerging [2]. Fields, Harrison and Wright [2] note that errors in human reliability can be regarded as failures in cognitive processing. They present an outline of a variant of Norman's [6] execution-evaluation model of human information processing (see Figure 1).



Figure 1: Cyclic model of human information processing

Five components from Norman's cyclic model are used as the basis for identifying ways in which human information can potentially fail. THEA consists of a checklist of questions about the performance of each of the cognitive components. Using a scenario based approach, the questions aim to identify where cognitive failures might occur which lead to behavioural errors.

Due to space constraint, full coverage of THEA is not possible and the reader is directed to [2, 7]. A THEA example for this paper will be presented in Section 3.3 but before we can apply this technique, we must specify the domain, and more specifically the scenario where this analysis is focused. Although the example we present is based in the physical world, the principles of the treatment apply over a broad range to environments including software systems.

3.2 The domain and scenario

The problem domain involves safety dependency issues onboard an oil tanker. In the scenario we are considering, the vessel has entered into some stormy conditions and the crew are preparing a lifeboat in case there is a need to abandon the vessel. Although the lifeboat can be launched from the ship's bridge, it must be manually primed beforehand. This involves a crew-member going on deck with a key to unlock the storage constraints/handles on the lifeboat. The key used in this task is also the key that is used to initiate the lifeboat launch from the ship's bridge.

3.3 Fragment of the THEA analysis

A fragment of the THEA analysis from the scenario described in Section 3.2 can be seen in Figure 2 where the analysis is split into eight components. Four sets of rows associated with the four cognitive failure areas discussed in Section 3.1 and four columns that make up the structure of THEA. These consist of the checklist questions, the causal issues, the consequences and any design issues.

The questions column is the same for every THEA analysis and the other spaces are completed by the domain expert doing the analysis. For our example, we have only included a selection of questions taken from each of the four failure

areas. In a full analysis, there are four *goals* questions, four *plans* questions, four *actions* questions and eight *perception, interpretation and evaluation* questions.

4. QUALIFYING THE ISSUES

For each answered question, THEA produces a triple structure from design analysis comprising of the causal issues, associated consequences and suggested design issues. These triples can be presented as binary statements (either present or absent). THEA provides subjective declarations of possible design needs with an associated rationale that may be subject to external scrutiny.

This can be problematic as the statements are constructed by experts which are subjective in nature and are summary statements and as a result bias can be introduced into the description. Also the level of detail that is described and the number of alternative solutions proposed is determined on a case by case basis at the expert's discretion.

Analysis of THEA, as a descriptive approach, raises two main issues. Firstly, what level of belief can be associated with the expert judgement and the structure provided by the technique and secondly, how can we decide which recommendations are most important in the context of a redesign, i.e. what is the *impact* on the redesign process.

4.1 Belief, expert judgement and structure

There is evidence of the questionable value of expert judgement [1] and the associated belief in those judgements. Hollnagel [3] notes that expert judgements are an uncertain and imprecise source of information.

What THEA does provide is a structure for documenting the issues that have been elicited via the analysis. On an individual THEA question basis, the triples in the structure could be used to build an argument for the identified issue. However, THEA does not provide a mechanism to show the dependence of individual statements of triples. Therefore, if the statements are changed at a local level in the THEA structure, any global consequences are not necessarily evident. The filtering of any associated changes in the other THEA entries is completely at the whim of the expert and their knowledge of these consequences. Inconsistencies in the *issue, consequence* and *design issue* statements could easily be introduced that would then cast doubt on the validity of any associated design based arguments.

Also there is no weighting on any of the statements in such arguments. Therefore all statements may be considered to be of equal importance. This is clearly not the case for most sets of requirements.

4.2 Design issue impact

When there is a large set of requirements the challenge of determining the most appropriate requirements for a redesign is difficult. If a technique like THEA is used, its output is a set of design recommendations/issues. As noted by Pocock et al. [7] the design issues identified by THEA are "intended to assist designers reason about errors at the early stages of a design before it becomes impractical or prohibitively expensive to effect a longer term design change or implement shorter term procedural 'fixes' or limitations."

Unfortunately, there is typically no indication of the impact of the design issues to any redesign. This impact must be determined by the reader of the recommendations. This can easily lead to an ad hoc approach to redesign and the selection of new requirements for a redesign. Ideally, it would benefit the redesign process to be able to get an objective view of the design recommendations. Hopefully, this would allow informed decisions to be made in terms of the scope of the design and the consequences for the system. The use of a numeric approach to this problem will be considered in the next section.

5. QUANTIFYING ISSUE IMPORTANCE

Our aim in this section is to investigate the addition of numerical precision to reinforce or highlight a notion of impact for the new requirements. This involves ranking the descriptive design recommendations provided by THEA using a candidate approach for HRA probability generation called HEART (Human Error Assessment and Reduction Technique) [4, 9].

5.1 HEART overview

HEART [9] is a quick technique for the quantification of human reliability. It is based on a review, by its author, of both literature on human factors and of experimental evidence showing the effects of various parameters on human performance. The technique defines a set of generic human error probabilities (HEPs) for different types of tasks. These are used as the starting point for HEART quantification. After a task has been classified, an analyst then determines whether any error-producing conditions (EPCs) are evident in the scenario under consideration. For each error-producing condition, the generic human error probabilities are multiplied by the error-producing condition which increases the human error probability.

An example of HEART will be described in Section 5.2. The reader is directed to [4] for an overview of HEART and other techniques for human reliability analysis. They will not be discussed in detail here as our motivation for using HEART in our example is threefold. Firstly, HEART is based in human reliability analysis. This considerably eases the task of combining the data from the approaches and simplifies the job of our domain expert. Secondly, both techniques have been developed using the same rationale, that is, to be quickly applied methods to identify the "big" problems in a target domain. Thirdly, in the human reliability analysis community, HEART is readily understandable by all interested parties and is a way of supporting dialogue about human reliability estimates [7].

5.2 HEART application to THEA

The descriptive approach, as discussed in Section 3.3, is suggestive of problems in our design. When applying human reliability analysis to high consequence systems, such problems are of particular concern. For the example in this paper, we have applied a HEART analysis to the THEA material presented in Figure 2 to refine any justifications for the redesign recommendations. In the scenario analysis four design issues were identified by the descriptive method, namely:

Questions	Causal Issues	Consequences	Design Issues
GOALS, TRIGGERING & INITIATION			
G1: <i>(Is the task triggered by stimuli in the interface, the environment or the task?)</i>	No, on command of the Captain.	The Captain may fail to trigger the crew-member to remove the handles.	Some form of interlock to prevent launch if handles are not removed.
G4a: <i>(Can a goal be achieved without all its 'subgoals' being correctly achieved?)</i>	No, crew-member must return key to the Captain before the lifeboat can be launched.	If the crew-member is disabled deck-side, the lifeboat can not be initialised.	Alternative method of initialisation.
G4b: <i>(Can a goal be achieved without all its 'subgoals' being correctly achieved?)</i>	No, crew-member must return key to the bridge.	Crew-member may lose the key.	Secure key to crew-member.
PLANS			
P2: <i>(Are there well practised and pre-determined plans?)</i>	Yes, crew training.	-	-
ACTIONS			
A3: <i>(Is the correct action dependent on the current mode?)</i>	Yes, crew-member must ensure they have the key while on deck.	Potential danger from: 1) Bad weather and 2) Premature lifeboat launch.	Crew-member must remove key from bridge before going on deck.
PERCEPTION, INTERPRETATION & EVALUATION			
II: <i>(Are changes to the system resulting from user action clearly perceivable?)</i>	Yes, crew-member can see the removed handles from the lifeboat.	-	-

Figure 2: THEA Fragment

1. Interlock to prevent the launch of the lifeboat if the handles are not removed (G1 from Figure 2)
2. Alternative method of initialisation (G4a from Figure 2)
3. Secure key to crew-member (G4b from Figure 2)
4. Crew-member must remove key from bridge before going on deck (A3 from Figure 2)

Error Producing Condition	HEART effect	Assessed significance
Little or no independent checking or testing of output	X 3	0.12
No obvious way to keep track of process during an activity	X 1.4	0.25
Hostile environment	X 1.15	0.12

Figure 3: HEART EPCs and significance effects

As a starting point for HEART analysis, the expert has identified that this task is one that is a routine, highly practised, rapid task involving relatively low levels of skill. This description is matched to generic categories [9] in a HEART analysis to provide a starting value of human unreliability.

The next stage of a HEART analysis is the identification of error-producing conditions (EPCs) that are evident in the scenario and would have a negative influence on human performance. The domain expert examined the causal and consequence issues defined in the THEA analysis and identified three HEART EPCs that range over the design issues; (1) Little or no independent checking or testing of output, (2) no obvious way to keep track of process during an activity, and (3) hostile environment.

Each EPC has an associated value (from [9]) that indicates the predicted effect and the extent to which unreliability will change due to the EPC. However, there are different levels of significance for any EPC. As the EPC values are general, an assessed proportion of effect significance is used to customise the specific relevance to the unreliability calculation. In this example, the domain expert has determined that the crew are highly trained and this includes training for bad weather. Hence, low significance values have been associated with the

EPC effects. A summary of these values can be seen in Figure 3.

The nominal likelihood of failure for a scenario based task is calculated by the product of the initial starting value of human unreliability and the assessed effects of the relevant¹ error producing conditions. The application of the HEART analysis to all the design issues provides us with a ranking for the problems identified by the descriptive method. The ranked design issues can be seen in Figure 4.

5.3 Numeric impact

The priority listing can be used as part of the justification process for arguing about implementing redesign options in terms of maximising the reduction of negative consequences in a scenario. Hence, the ranking can be seen as a numeric measure for consequence impact.

From our scenario, having the crew-member remove the key from the bridge before going on deck is a critical action in

¹Not all EPCs, and their associated assessed effects, are necessarily applicable for all design issues.

Design issue	Likelihood of failure (%)
A3: Crew-member must remove key from bridge before going on deck	2.78
G1: Interlock to prevent lifeboat launch if the handles are not removed	2.52
G4a: Alternative method of initialisation	2.24
G4b: Secure key to crew-member	2.04

Figure 4: Design issue rankings based on the HEART analysis

terms of the task we have examined. A number of dangerous consequences can result if this is not carried out, for example the lifeboat may be launched while the handles are still in place. This would have a number of dangerous results including damage to the ship, the lifeboat and possibly a crew-member who was on deck. Therefore, the numeric method has refined the design issue recommendation process to allow the designers to make better, informed, decisions in the context of the redesign of the system.

6. DISCUSSION

In this paper, we have demonstrated how a descriptive analysis can be augmented by the use of a numeric technique to refine a measure of impact for identified problems in a design. In an example, numeric probabilities of human reliability are used to determine the significance of the descriptive recommendations. While we have been using THEA and HEART as examples of descriptive and numeric methods, to a certain degree, the use of these methods is arbitrary. There are a host of alternative methods that could be substituted in the current examples. What is of more importance is the process that is involved and the role that probabilities play. In our examples we have investigated the development/evaluation of new requirements for a design. This has involved two levels of refinement of the issues identified from example scenarios.

The first refinement is after the initial application of the descriptive method. Initially, the descriptive method identifies areas of concern, and/or issues that require attention, in the current design. The severity of these issues can be identified by impact analysis on the consequence of such issues. Although, as noted in Section 4.1, issues are commonly defined as *being of concern* without differentiation, in practice, expert judgement would be used to rate the severity of the issues, at least informally, based on the consequences of the issues. This informality, and therefore lack of credibility, is what we wish to reduce by the application of a numeric technique.

The second level of impact refinement is in the use of a numeric method to indicate probabilities that can be used to highlight the severity of a design deficiency. In our example we have been using HEART to identify the likelihood of failure due to human unreliability. As we are interested in dependable systems, the level of reliability can be used as an assessment criterion, e.g. if some component is very unreliable then this could be seen as having a higher justification for redesign.

7. CONCLUSIONS AND FUTURE WORK

In this paper we have examined the use of descriptive methods to build initial recommendations for new design requirements and have investigated the use of numeric methods to enrich the justification for these requirements. This blending of the descriptive and numeric approaches is a step towards satisfying dependability considerations for system developments. Although we have applied two particular techniques (THEA and HEART) in a single domain (human reliability analysis), we feel that this type of analysis process is applicable over other techniques and domains. The approach supports the redesign process and provides a mechanism to increase developer confidence that the work is progressing in a cost, e.g. time or effort, effective way.

However, the work presented in this paper is only an initial step. The numbers that are generated, and the associated descriptive statements, are all subjective measures and are influenced by expert judgement bias. Also any arguments that are developed from this process have only a limited notion of structure and are presented in a non-rigorous form. With dependability requirements come industrial standards and levels of certification. If an approach is to become useful in industry then a more formal structure and defined blending of the descriptive to the numeric will be required. These are issues that the authors are currently investigating.

8. ACKNOWLEDGMENTS

This work was supported in part by the UK EPSRC DIRC project, Grant GR/N13999.

9. REFERENCES

- [1] P. Ayton. How bad is human judgement? In G. Wright and P. Goodwin, editors, *Forecasting with Judgement*. Wiley, Chichester, England, 1998.
- [2] B. Fields, M. Harrison, and P. Wright. THEA: Human error analysis for requirements definition. Technical Report YCS-97-294, The University of York, Department of Computer Science, 1997. UK.
- [3] E. Hollnagel. *Human Reliability Analysis: Context and Control*. Computers and People Series. Academic Press, London, 1993.
- [4] B. Kirwan. *A Guide to Practical Human Reliability Assessment*. Taylor and Francis, London, 1994.
- [5] W. M. Newman and M. G. Lamming. *Interactive System Design*. Addison-Wesley, Harlow, UK, 1995.
- [6] D. A. Norman. *The Psychology of Everyday Things*. Basic Books, 1988.
- [7] S. Pocock, M. Harrison, P. Wright, and P. Johnson. THEA - a technique for human error assessment early in design. In M. Hirose, editor, *Human-Computer Interaction: INTERACT'01*, pages 247–254. IOS Press, 2001.
- [8] I. Sommerville. *Software Engineering*. Addison-Wesley, Harlow, England, fifth edition, 1995.
- [9] J. C. Williams. HEART - a proposed method for assessing and reducing human error. In *9th Advances in Reliability Technology Symposium*. University of Bradford, 1986.