Published in the *Safety-Critical Systems Club*'s Newsletter, May issue, 2004 (pp. 6-9)

# Designing dependable systems needs interdisciplinarity

Denis Besnard & Cliff Jones

Centre for Software Reliability
School of Computing Science
University of Newcastle upon Tyne
Newcastle upon Tyne, NE1 7RU

denis.besnard@ncl.ac.uk
cliff.jones@ncl.ac.uk

## 1. Introduction

Modern computer-based systems pose a huge challenge to designers if they are to achieve dependability of the delivered service. These challenges are recognised for safety-critical systems such as medical devices, industrial process supervision workstations or autopilots. But even for systems where life is in not at stake, the need for properties like reliability, security, maintainability is becoming ever more pressing. Historically, a combination of methods derived from the purely technical fields of computing science, mathematics and statistics were used to provide some form of guarantee that the overall system will behave as prescribed. Human considerations were not totally overlooked from such approaches, but the increasingly intimate connection between the purely technical system and the humans surrounding it requires a more explicit consideration of psychological and social dimensions. Such questions as "Can users revert to manual mode?"; "Are the security features usable?"; "Does the system match established practices?" become crucial to the success of the overall *computer-based system*.

We outline an overview of the relevance of these questions in the workplace and emphasize the interest of an interdisciplinary approach to computer-based systems. We will draw on the wisdom acquired in a major interdisciplinary project to shed some light on the need for non-IT disciplines and their contribution to the understanding of dependability.

## 2. The DIRC project and the dependability challenge

DIRC[1] is a multidisciplinary research project addressing the dependability of large computer-based systems. It gathers five British Universities into a 6-year consortium funded by EPSRC. The objective is to produce knowledge, methods and tools targeted at informing designers of computer-based systems about the risks, challenges and skills required to build and assess such systems.

DIRC brings a strong commitment to interdisciplinary approaches. Until the mid 1980's, there was an implicit design assumption that operators had to adapt to the tool with which they interact. Later, the ubiquity of computers made it evident that making computers usable required considerations going beyond computer science. IT designers need to understand the human component in socio-technical systems and therefore to communicate with other disciplines. It is this dialogue that DIRC advocates, by arguing that dependability of modern computer-based systems can no longer be achieved without interdisciplinarity.
Making automated agents cooperate with human operators is a real challenge and the question of making them cooperate reliably is still not entirely resolved. In order to better understand the

[1] Dependability: an Interdisciplinary Research Collaboration. Visit DIRC at www.dirc.org.uk

challenges raised by this cooperation, three examples on which DIRC has produced publications are discussed. These highlight three different cases where dependability can be sub-optimal, namely the overriding of computer control by operators, trade-offs in security, and workarounds in assembly lines. Comments on these examples will follow in Section 3 in which potential improvements and ways forward will be considered.

### 2.1. Operators reverting to manual mode

Clarke *et al.* (2003) show how humans adapt their work to local contingencies. An ethnographic study was conducted of a steelworks factory producing steel slabs. The study focused on the use of a computer-driven rolling mill. Slabs are produced to a required size by rolling large metallic rolls in a series of passes. Because there is a variety of steel quality and slab dimensions, operators have developed various control strategies. For instance, operators sometimes bypass the computer and shift to manual mode for the final passes on slabs of a particular thickness. In doing so, they reduce the number of passes in order to avoid slabs taking a U-shape or turning up, which are occurrences that not always avoidable under computer mode. As quoted from Clarke *et al.* (2003): "…*because the computer, at less than 45, pisses about…does 4-5 passes…that's what's causing turn-up.*"

The work reported highlights how operators develop strategies that compensate for flaws in the automation. The latter may be fit-to-purpose under nominal work settings but adaptations are required for any other case. In this example, the adaptations performed by the operators prevent the occurrence of undesired outcomes. If such adaptations did not take place, the production would be (at best) much longer due to the necessary remaking of malformed slabs.

### 2.2. Usability trade-offs in IT security

Passwords are a widespread IT security mechanism. But their vulnerability normally hides beyond purely technical considerations: when one looks at how passwords are used in the workplace, human cognitive limitations become obvious. Users cannot remember long or randomly generated passwords and resort to external aids such as sticky notes on monitors. Generally speaking, the use of passwords raises several usability problems. Ultimately, security faces a paradox where by increasing the complexity and number of passwords, the level of protection can actually decrease (Weirich & Sasse, 2002).

Users who write down passwords act on the basis of an equation where risks, costs and benefits are core factors. Given their perception of risk, users trade-off the cost of memorising passwords against the benefits of seeking ease-of-work (Besnard & Arief, 2004). Similar trade-offs apply to file sharing, patching software or updating anti-virus software. The picture seems to be that risk-unaware users seek immediate benefits at the potential cost of expensive failures. Their behaviour can be seen as driven by a rule of least effort where a security measure standing in the way of accomplishing the main task is unlikely to be followed.

### 2.3. Workarounds in assembly lines

Voß *et al.* (2002) carried a field study of a company assembling diesel engines and relying on a computer-based tool to track orders, deadlines, special customisations for particular customers, etc. The tool is used to control the production process, from the management of the stocks all the way down to delivery dates. The software is designed in such a way that all the parts needed for an engine have to be in-stock before the assembly can begin. This is sometimes an unworkable constraint for the operators who can work on areas of an engine for which parts are available. However, because the software system does not allow this sort of ad-hoc adaptations to contingencies, operators were forced to make up items "in stock" for the parts that were missing in order to continue the assembly (Later, when the missing parts get delivered, they are mounted on the engine and the stock is set back to zero).

Procedures do not rule human behaviour (Fujita, 2000). Humans do not obey rules if the latter are perceived to obstruct the accomplishment of a task. Here, the cost of waiting is avoided by a deviation from the procedure. When this happens, it is usually a symptom that the tools and procedures in use do not match the operators' needs or intentions. This mismatch, which often involves managerial

decisions (Reason, 1995), has already caused very serious accidents in other areas of the industry (see the Tokaimura incident report by Furuta *et al.*, 2000).

## 3. The future of dependable systems

From the viewpoint of computer system design policy, dependability does not rely solely on technological inventions but also in further improvements in the way the *range* of human particularities is reflected in the technology. This requires taking into account the inputs from a number of disciplines. The three examples described above are now reviewed and possible ways forward suggested.

### 3.1. Reverting to manual in process control

The steelworks factory study shows how an acceptable level of dependability is achieved in the service through an ad-hoc collaboration between human operators and an imperfect piece of technology. Dependability of service (producing correctly shaped metallic slabs, in this instance) is not a property of a technical artefact but the outcome of a collaboration between human agents and imperfect machines. In this respect, dependability is just an ideal - yet valuable - objective. The reality is that the service, via human compensations for incorrectness, is made less undependable.

### 3.2. Improving the human side of security

Security must be user-centred (Zurko & Simon, 1996). Generally speaking, the design of security products and policies should rely more on the rules of human-computer interaction. Passwords must be, at least, easy to remember and reduced in number as much as possible. As far as end-users are concerned, the ideal number of passwords is zero, so any measure getting closer to an *effortless* security is a step forward to better security in general. As a design principle, end-users should not be expected to contribute to security. The latter should be transparent for whom it is not the primary task.

### 3.3. Workarounds as symptoms of system's flaws

Workarounds are unsupported configurations. They are violations revealing a lack of flexibility and a need for configurability. One way of avoiding violations and dangerous workarounds is to design around human practices. If this is not a design decision, it will be enforced in an ad-hoc manner by users, out of any control. Integration of practices into design is not a novel idea but Voß *et al.* (2002) experienced and extended the concept to that of a long-term *immersion* of the designer into the work context.

## 4. Conclusion

This paper has presented three cases where DIRC investigated the dialogue between humans and some form of automation. Therefore, the technical aspects of the failures described herein only account, if at all, for a portion of the picture. Within the scope of this paper, a range of human factors are needed in order to capture the complexity of designing dependable computer-based systems. This article is hoped to convince one that:

- Dependability of service is not a solely technical notion;
- Simple usability issues impair security;
- Workarounds happen whenever tools do not match work practices.

For the sake of clarity, the examples presented above are discrete ones. However, they usually appear jointly in large systems, at different organisational layers, and at various degrees of visibility. Identifying them and reconciling them are the challenges and this is why interdisciplinarity is needed. DIRC is advocating for more and more effort to be allocated to acknowledging the non-IT factors involved in the lifecycle of large computer-based systems. The hope is that the future dependability of technical socio-technical systems will overcome one of its current weakest links: the integration of human-related issues to the design of complex computer-based systems.

## 5. References


Besnard, D. & Arief, B. (2004). Computer security impaired by legal users. To appear in *Journal of Computers & Security*.

Clarke, K., Hughes, J., Martin, D., Rouncefield, M., Sommerville, I., Gurr, C., Hartswood, M., Procter, R., Slack, R. & Voss, A. (2003). Dependable red hot action. In Kuutti, K., Karsten, E. H., Fitzpatrick, G., Dourish, P. & Schmidt, K. (Eds.) Proceedings of the *European Conference on Computer Supported Cooperative Work*, Helsinki. Dordrecht. Kluwer (pp. 61-80).

Fujita, Y. (2000). Actualities need to be captured. *Cognition, Technology & Work*, 2, 212-214.

Furuta, K., Sasou, K., Kubota, R., Ujita, H., Shuto, Y. & Yagi, E. (2000). Analysis report. *Cognition, Technology & Work*, 2, 182-203.

Reason, J. (1995). A systems approach to organized error. *Ergonomics*, 38, 1708-1721.

Voß, A., Slack, R., Procter, R., Williams, R., Hartswood, M. & Rouncefield, M. (2002). Dependability as ordinary action. Proceedings of *SafeComp2002*, Catania, Italy (pp. 32-43).

Weirich, D. & Sasse M. A. (2002). Pretty good persuasion: A First Step Towards Effective Password Security in the Real World. Proceedings of *New Security Paradigms Workshop*, Cloudcroft, NM (pp. 137-144).

Zurko, M. E. & Simon R. T. (1996). User-Centred Security. Proceedings of *Workshop on New Security Paradigms*, Lake Arrowhead, CA (pp. 27-33).