

Research in-progress

Error-proofing the design process to prevent design-induced errors in safety-critical situations

Ron Day, Yvonne Toft and Ryan Kift

Centre for Railway Engineering, Central Queensland University, Australia

Abstract

Background: Design-induced errors all too often result in accidents and disasters in safety critical systems. Examples of design-induced error will be taken from company investigations and government enquiries reporting the part design process errors play in the events, many of which have caused death and/or injury. **Aims:** The study investigates the link between design-induced error and design process error. Current thinking on strategies to reduce the incidence of design-process errors including participative design will be considered. **Methods:** The concern with design process error and its link to design-induced error is being studied in a three-part research program incorporating online surveys, interviews and data mining. The surveys and interviews involve two groups. The first group includes network controllers, control room support staff and professional helpers, such as change agents, trainers and human factors practitioners. The second group includes designers, developers, testers and others involved in the design process of new technologies. **Results and Conclusions:** Preliminary results from controllers indicate a concern with the lack of participation in the design process. Designers reflect that this as one of the causes of design process error. In addition, they point to inadequate design specifications and issues with testing as other major causes of error. The end result of this study will be the production of an analytical tool that can be applied to guide the design and development of new technologies, so that design-induced and human response errors are minimised when new technologies are introduced into safety-critical situations.

©Day et al: Licensee HFESA Inc.

Background

The railway line from Sydney to Perth crosses the Nullarbor Desert and is a single line with occasional passing loops [1]. A train moves into one of these loops by operating a set of line points from the train with a radio operated device. On the 18th August 1999, a freight train was waiting at the Zanthus loop for the Indian Pacific passenger train to pass [2]. The second driver on the freight train was waiting by the points control box. The box was unlocked and he had his finger poised to push the button to change the points, so that the freight train could resume its journey as soon as the Indian Pacific had passed. Unfortunately, he pressed the button before the Indian Pacific had passed. As a result, the Indian Pacific was diverted into the loop where it collided with the freight train. Thirty-one passengers and four railway staff sustained immediate injury. Twenty-one of those were conveyed by the Royal Flying Doctor Service to the Kalgoorlie Hospital. Another 12 railway staff members reported injury some time after the accident. Repairs to the trains were estimated in this report to cost more than \$6 million [2]. The subsequent cost was much higher. The accident was caused by human error viz. the second driver pushed the button before the Indian Pacific had passed the loop. However, that human error was a result of a design-induced error in that, the technology had no mechanical or electrical interlocking system to prevent the movement of the points, before the passenger train had passed [2].

A design-induced error can be defined as an error carried out by a human where the primary reason for the inappropriate human behaviour can be shown to be a fault or faults in a piece of electronic or mechanical equipment. A simple example would be where the effect of someone moving a switch is opposite to the labelled instruction, or worse still, where the switch had no labelling to indicate the effect of moving it one way or another. The design-induced error in the Zanthus case can be seen to be a result of a design process error, where a technological device was released without thorough testing. A design process error describes a fault or faults in a device that have not been identified and corrected before the device is implemented.

This study is directed at the rail industry, but has wider implications for other transport systems including air and road, and for a range of safety-critical industries, including mining and power generation and distribution, and support agencies, such as police, ambulance, fire and State Emergency Services (SES). Each of these industries and systems relies on communications and control technologies, and these technologies are being updated and replaced at an increasing pace [3].

Many researchers have concentrated their efforts on end-user human error as the prime cause of accidents and disasters [4] [5] [6], but as the Zanthus rail collision example demonstrates, in at least some cases, end-user human error can be traced to

design process error [4]. This raises some questions that are being looked at in this study:

- Is it possible to determine whether design-induced errors are caused by design process errors?
- Can it be shown that design process errors are caused by human error?
- Is it possible to identify design process errors and their causes so that corrective action can be taken to reduce the incidence of design-induced error for end-users?

Design-induced Error

We can find an element of human error in most accidents and disasters that occur in safety-critical systems. Within the reports documenting these events, it is possible to identify at least some human error that is design-induced, as the Zanthus rail collision example demonstrates. Many of the errors shown in Table 1 can be described as design-induced [7] [8]. There is agreement that systems design and systems operation can both contribute to design-induced errors.

Table 1. Systems Design and Operational external error types

Indicator	Description
Operational errors [7] [8]	<ul style="list-style-type: none"> • Use of wrong switch, lever, or control • Misinterpretation of instrument indication • Inability to reach or see control • Inability to see or interpret instrument or indicator • Failure to respond to warning • Selection or use of incorrect system-operating mode (mode confusion) • Overreliance on automated system (automation complacency).
Operational conditions that contribute to design-induced errors [7] [8]	<ul style="list-style-type: none"> • Inadequate primary equipment control or display arrangement • Inadequate primary display data or data format • Inadequate hazard advisory or warning display • Inadequate system instructions or documentation • Inadequate system support or facilities • Inappropriate type or level of automation, or excessive mode complexity.

Although errors, such as using a wrong switch, misinterpreting an instrument reading or failing to respond to a warning can be explained as cognitive errors [9], they can also be seen as design issues. The switch, instrument or warning signal could possibly be found to be wrongly labelled, in the wrong position or operating in a manner not consistent with normal operation [10] [11] [12].

A 1996 study of the pilot-aircraft interface on modern flight decks, commissioned by the United States (US) Federal Aviation Commission (FAA), found there were many design deficiencies and shortcomings in the design process [10]. Interface problems included confusing and unclear display symbology and nomenclature, a lack of consistency in flight

management systems interfaces and conventions, and poor compatibility between flight deck systems.

Of particular relevance to this study are those errors that result from design issues. Many operator errors can be attributed to a poorly designed human-computer interface (HCI) [13], but interface design is only a part of the concern with design-induced error. A frightening case of a cancer radiation therapy machine, where no basic error-checking routines had been included in the code to prevent incorrect keyboard entry, demonstrates a different design process error [11]. A patient received lethal doses of radiation because the user made a wrong key press on a keyboard. The user was not aware that the wrong key press had not been cancelled by the machine, because a misleading message on the screen suggested the machine had not worked. This was a clear case of a design-induced error by the operator that could be traced back to the design process, where a series of coding errors and misleading error messages were not detected by the designers. Stringent quality assurance procedures during the design process should have identified these problems, before the system was installed.

Design Process

The design process is often described as a series of steps or stages forming a Systems Development Life Cycle model (SDLC). There are many variations between SDLCs, but they all assume that a system needs to be conceptualised before being designed, and once it has been designed it must be engineered, tested and implemented. Some writers see maintenance as part of the life cycle and a few add retirement as the final stage. The original SDLC model, *Waterfall*, was introduced into design theory around 1967 [14]. This model allows no participation of end-users in the design or development stages. Employing a top-down management strategy, a perceived need leads to the formation of a concept for change. This concept is developed into a design from which specifications are drawn to guide the engineering and testing of the new system. Once approved, the new technology is implemented.

The implementation stage is often the first time end-users have contact with, or in some cases knowledge of, the new technology. Where the design does not meet end-user needs, work practices or task requirements, expensive delays and retro-fitting are required. This has been seen recently with the Queensland Health Commission payroll disaster, where some health workers were not being paid correctly more than a year after a new payroll system was introduced. An independent report stated the designers did not take the steps necessary to ensure the design concept reflected workplace requirements, nor did they carry out a planned testing of the system, before it was implemented [15].

Problems similar to the payroll example, that caused time delays and budget blowouts, led to the proposal of later SDLC models, allowing a degree of input from end-users, sometimes in testing the system before implementation, sometimes during concept discussions, or occasionally in team assessments at various stages of the systems development. New SDLC models have been proposed where strategies are

varied to include user testing at several stages of the SDLC, or to break the project into manageable chunks, where users are able to trial the system, one step at a time. Table 2 lists the major SDLC models and the degree of participation by end-users in the design and development stages [16].

Table 2. End-user participation in the SDLC

SDLC models	Participation by end-users
Waterfall	None in earlier examples. Some involvement in final testing later [14]
V-model	Assisting with testing at the conclusion of each development stage. Identified problems raised during next development stage [17]
Incremental	System developed incrementally with each section being released and tested 'on-the-job' before next section is added [18]
Evolutionary Development (EVO)	A progression of small 'Waterfalls' where each section can be completed in a short time. Users get access at the end of each cycle and can offer feedback [19]
Spiral	Combines features of the Prototyping and Waterfall models including the advantages of breaking the project into chunks and allowing end-users access to some SDLC stages for validation [20]
Prototyping (Iterative)	End point not known at beginning of project, so incomplete versions are trialled by end-users until final form evolves [21]
Adaptive - Agile	Real time communication (preferably face-to-face) involving iteration and incomplete end point [22]
Joint Application Design (JAD)	End-users involved in the design and development stages through a series of collaborative workshops [23]
Rapid Application Development (RAD)	End-users actively participate in prototyping, writing test cases and performing unit testing [24]

The second to fourth items in Table 2, *V-model*, *Incremental*, *Evolutionary Development* and *Spiral* SDLC models, follow the lead of the *Waterfall* model, where the end point has been clearly identified and all steps in the SDLC move in a regulated manner to that conclusion. Once the problems with the original *Waterfall* were accepted, later models attempted to address the participation of end-users in the development stages, most often by engaging end-users in some form of testing of the system, before it was released. The iterative *Prototyping* model and the *Adaptive* models that followed introduced a paradigm shift. In these models, the end point is not clear. This change in emphasis allows end-users to participate more widely in the SDLC stages and contribute more substantially to the overall design of any new technology being introduced into their control rooms. These models describe a progression from no involvement of end-users in the design, development or testing of new technologies to an increasing degree of user participation in the process. This change was driven by the high cost of retrofitting and time delays when it was discovered that technologies developed in isolation did not meet the task requirements of the end-users. The reworking became necessary when unacceptable errors were being made by the end-users of the new system.

Designers need to discover the true nature of the tasks for which they will design systems. *The design of information systems*

should be based on explicit analysis of work rather than assumptions about work' [25]. The greater the degree of user participation in the design process, the greater the chances are of achieving a fault-free system that closely fits requirements, on time and on budget. In addition, the end-users are more likely to be familiar with the system, know that it will help them in their work, and make fewer errors while using it [26] [27].

Method

The concern with design process error and its link to design-induced error is being studied in a three-part research program. This study uses a mixed methods approach [29], incorporating online surveys, interviews, and data mining. The surveys and interviews involve two groups, control room staff and others involved with the use of new technologies in control room settings, and the designers and developers and others working on the design and development of those technologies.

The list of end-users, researchers and human factors (HF) professionals who are being contacted include:

- Network controllers, control room support staff and managers from safety-critical industries, including air and rail transport, and power generation and distribution.
- Hardware and software support staff.
- Professional helpers, such as change agents, trainers and HF practitioners.
- Control room and control system professionals.

The list of designers, developers and User Experience (UX) professionals who are being contacted include:

- In-house designers in large rail, power, air and government organisations and other safety-critical systems.
- Developers, testers, UX consultants and others involved in the design process of new technologies.
- External design companies developing mechanical and technological control systems.
- Design and development professionals.

The design-induced error survey includes questions about design-induced errors experienced at the workplace with control technologies and participative design activities, including involvement in design concept formation and system testing. The design process error survey investigates the thinking processes and other strategies used in design concept formation and the degree of involvement in the design process by stakeholders, including end-users. Questions are asked about the stages in the design process where errors can occur and whether effort is put into ensuring that implemented control systems have been error-proofed [28] before delivery. These surveys were developed following a review of the literature and were reviewed by experts in the field, before being implemented. Each survey was preceded by a pilot study, where a number of issues were identified and corrected. The surveys will be uploaded to the Zoomerang website, a site that offers researchers a platform for mounting questionnaires quickly and easily. This website also offers an introductory analysis of the responses and the ability to export the data in a form that can be read by other systems.

Both end users and designers will be interviewed and asked questions that attempt to draw out further information concerning the themes investigated by means of the surveys. Interviews will be supported by observation of these workers as they carry out their normal duties. Data mining of appropriate databases will be conducted for corroborating evidence to provide a triangulation effect for the central themes. The databases to be examined include Contributing Factors Framework (CFF), a national collection of data relating to rail accidents; Australian Transport Safety Bureau (ATSB); Bureau of Infrastructure, Transport and Regional Economics (BITRE) and Australian Emergency Management Library (AEML). The CFF database will be examined for instances of rail accidents, where it can be shown that controller human error and/or errors in the technology have contributed to an adverse event. The three other databases will be examined for instances where controller human error and/or errors in the technology have contributed to accidents in a wider spectrum of safety-critical situations, including road and air accidents, power generation and distribution, mining and emergency services activities as well as rail events.

Quantitative data from the surveys will be analysed using SPSS and qualitative data from the interviews will be processed through NVivo. Corroboration for the results from the two data sets will be sought from official records in the databases.

Results

A preliminary pilot survey was circulated as an online questionnaire in an attempt to identify the major issues among network controllers, control room managers and support staff, researchers and HF practitioners. From 68 completed responses, there is a resounding call (96%) for end-users to be involved in the design and development of new technologies they will use. Only 40% of participants reported they had experienced any involvement in design. Many respondents believe end-users understand the work needs and their participation in the design stages is crucial to ensure the technology matches the task requirements and is likely to help reduce design-induced error.

The results showed that the preliminary survey did not clearly identify the kinds of design-induced errors that occur and the impact those errors have on safety-critical situations. Neither did the survey attempt to address the issues surrounding design process errors. The decision was taken to modify the original survey to directly address design-induced and design process errors.

Discussion and conclusion

The move to automatic (driverless) operation of trains and the introduction of other over-the-horizon innovations means a far greater role for technology. For instance, automatic operation requires control technologies that are capable of starting and stopping the movement of the trains accurately, controlling the speed and distance between trains on the same line and providing control over the opening and closing of doors, scanning of tracks with video, infra-red rays and laser beam technology, so that a person or object falling on

the track can be detected immediately and action taken by the system [30].

The need for design processes to be as error free as possible becomes crucial. Traditional software development methods cannot cope effectively. The question we have to face when considering over-the-horizon technologies is, what will be the impacts of new systems being guided by more complex technologies, if design process errors have not been removed? Current practices leave us with little confidence that newer and more complex systems will not present even greater risks, because of design-induced errors stemming from design process errors.

Although this is currently a work in progress, it is confidently expected that a significant relationship will be shown to exist between design process errors and design-induced errors. It is also expected that it will be possible to clearly identify the nature and causes of design process errors and that these identifiers can be fashioned into a battery of tests that can assist project managers and other key stakeholders in the design process to take preventive action that will reduce and perhaps remove the incidence of design-induced error from new technologies for rail network control. Although the study has particular reference to railway network control systems, because of the similarity of the issues, the results of this study and any analytical tools that may result could potentially have application to other safety-critical systems.

References

- [1.] McDonald, W, 'Restoring the Nullarbor: The application of vital telemetry to self restoring points across the Nullarbor', *IRSE*, July 2000.
- [2.] Independent Investigation Report: Collision Indian Pacific Passenger Train 3AP88 and Freight Train 3PW4N. In: *Transport Do*, editor. Perth: Department of Transport; 1999.
- [3.] Robertson, TS & Gatignon, H, 'Technology Development Mode: A transaction cost conceptualisation', *Strategic Management Journal*, vol. 19, pp. 515-531, 1998.
- [4.] Harris, D, Stanton, NA, Marshall, A, Young, MS, Demagalski, J & Salmon, P, 'Using SHERPA to predict design-induced error on the flight deck', *Aerospace Science and Technology*, vol. 9, no. 6, pp. 525-532, 2005.
- [5.] Casey, S, *The Atomic Chef and other true tales of design, technology, and human error*, Aegean, Santa Barbara, California, USA, 2006.
- [6.] Green, M, *Human Err vs Design Error*, viewed Mar 2 2011, <http://www.visualexpert.com>, 2009.
- [7.] Endsley, MR, 'Situation Awareness and Human Error: Designing to support human performance', *High Consequence Systems Surety Conference*, Albuquerque, NM, 1999.
- [8.] Whitlock, C & Wolf, JT, 'Accident Investigation Guide', in Appendix 7 - *Human Factors Accident and Incident Analysis Checklist Summary*, United States Department of Agriculture (USDA), Washington DC, USA, 2005.

- [9.] Rasmussen, J, 'Human error and the problem of causality in analysis of accidents', *Philosophical Transactions of the Royal Society of London*, vol. B 327, pp. 449-462, 1990.
- [10.] Harris, D, Stanton, NA, Marshall, A, Young, MS, Demagalski, J & Salmon, P, 'Using SHERPA to predict design-induced error on the flight deck', *Aerospace Science and Technology*, vol. 9, no. 6, pp. 525-532, 2005.
- [11.] Casey, S, *The Atomic Chef and other true tales of design, technology, and human error*, Aegean, Santa Barbara, California, USA, 2006.
- [12.] Green, M, *Human Err vs Design Error*, viewed Mar 2 2011, <http://www.visualexpert.com>, 2009.
- [13.] Shelton, CP, *Human Interface/Human Error*, viewed Nov 27 2010, http://www.ece.cmu.edu/~koopman/des_s99/human/, 1999.
- [14.] Fitzgerald, B, 'Systems development methodologies: the problem of tenses', *Information Technology and People*, vol. 13, no. 3, pp. 174-185, 2000.
- [15.] AAP, *Queensland Health payroll problems far from over*, viewed Mar 4 2011, http://www.arnnet.com.au/378221/queensland_health_payroll..., 2011.
- [16.] Day, R, 'Minimising Railway Control Room Errors Resulting from the Interplay of Design Process Errors and Design-induced Human Errors', paper presented at *ICREAPRC2011*, Hong Kong, 2011.
- [17.] Boggs, R, 'The SDLC and SIX SIGMA - an essay on which is which and why?', *Issues in Information Systems*, vol. V, no. 1, 2004.
- [18.] Kanjilal, J, *Understanding Agile Software Development*, viewed June 21 2010, <http://www.dotnetjohn.com/articles.aspx?articleid=268>, 2008.
- [19.] May, EL & Zimmer, BA, 'The Evolutionary Development Model for Software', *Hewlett-Packard Journal*, no. 4 August, pp. 1-8, 1996.
- [20.] Boehm, B, 'A Spiral Model of Software Development and Enhancement', *Computer*, IEEE Computer Society Press, vol. 21, no. 5, pp. 61-72, 1986.
- [21.] Floyd, C, 'A Systematic Look at Prototyping', in R Budde (ed.), *Approaches to Prototyping*, Springer-Verlag, New York, 1984.
- [22.] Ambler, SW, *The Agile System Development Life cycle (SDLC)*, Ambysoft, viewed May 24 2010, <http://www.ambyssoft.com/essays/agileLifecycle.html>, 2005.
- [23.] Haag, S, Cummings, M, McCubbrey, DJ, Pinsonneult & Donovan, *Phase 2: Analysis: Information Management Systems for the Information Age*, McGraw-Hill Ryerson, 2006.
- [24.] Whitten, JL, Bentley, LD & Dittman, KC, *Systems analysis and design methods*, 6th edn, Irwin/McGraw-Hill, 2004.
- [25.] Vicente, KJ, *Cognitive Work Analysis*, Lawrence Erlbaum Associates Publishers, London, 1999.
- [26.] Norman, DA, *The Design of Everyday Things*, Basic Books, New York, 2002.
- [27.] Lidwell W, Holden, K, Butler, J, *Universal Principles of Design*, Rockport, Beverly, Mass., 2010.
- [28.] Chao, LP & Ishii, K, 'Design process error-proofing: Strategies for reducing quality loss in product development', paper presented to the *IMECE2005*, 2005.
- [29.] Johnson RB, Onwuegbuzie AJ. 'Mixed Methods Research: A Research Paradigm Whose Time Has Come', *Educational Researcher*. 2004; 33(7):14-26.
- [30.] IRSE-ITC, 'Semi-automatic, driverless and unattended operation of trains', *Institution of Railway Signal Engineers (IRSE)*, 17 June, 2010.