This paper appeared in the proceedings of *Safecomp 96 - E Schoitsch (ed) The 15th International Conference on Computer Safety, Reliability and Security, Vienna , Springer Verlag 1996.*

PERE: Evaluation and Improvement of Dependable Processes

Authors
Robin Bloomfield†, John Bowers‡, Luke Emmet†, Stephen Viller*

†Adelard,	‡Department of Psychology	*Computing Department
London, UK	Manchester University, UK	Lancaster University, UK
+44-(0)181-983-1708	+44-(0)161-275-2599	+44-(0)1524-593793
{reb | loe}@adelard.co.uk	bowers@hera.psy.man.ac.uk	viller@comp.lancs.ac.uk

Abstract
In the development of systems that have to be dependable, weaknesses in the requirements engineering (RE) process are highly undesirable. Such weaknesses may either introduce undetected system weaknesses, or otherwise significant costs may arise in their correction later in the development process. Typically, the RE process contains a number of individual and group activities and thus is particularly subject to weaknesses arising from human factors. Our work has concerned the development of PERE (Process Evaluation in Requirements Engineering), which is a structured method for analysing processes for weaknesses and proposing process improvements against them. PERE combines two complementary viewpoints within its process evaluation approach. Firstly, a classical engineering analysis is used for process modelling and generic process weakness identification. This initial analysis is fed into the second analysis phase, in which those process components that are primarily composed of human activity, their interconnections and organisational context are subject to a systematic human factors analysis. In this paper we briefly describe PERE and provide examples of the application experience to date.

1 Introduction

Requirements engineering (RE) is the process within the earlier phases of the system lifecycle that concerns the discovery, analysis, negotiation and definition of system requirements, resulting in a specification of what the system must do in order to satisfy user needs, integrate with other installed systems, satisfy commercial demands, meet safety regulations and so on. The importance of the RE process is generally recognised and it is acknowledged that problems originating in the RE process are hard to detect and expensive to put right later on in the system's development. Furthermore, in the context of dependable systems, getting the requirements wrong may have disastrous consequences.

Within the REAIMS[1] project, we have been developing a number of improvement strategies to address problems in RE, particularly focusing on the

[1] Requirements Engineering Adaptation and IMprovement for Safety and dependability

development of dependable systems. In this paper we report on one aspect of the REAIMS work that has considered the safety and reliability of the RE process itself. PERE (Process Evaluation in Requirements Engineering) is a method for assessing requirements processes, examining them for weaknesses and proposing protections against those weaknesses. Although PERE has been specifically developed for the evaluation of requirements processes, the analysis and process improvement techniques employed are applicable to problems within the broader process improvement domain. Process evaluation and improvement may be necessary in any domain where the process is required to be dependable.

In this paper we briefly present an overview of the PERE method and its background, and give examples of its application. Further details on PERE can be found in [1].

1.1 Dependable systems

Dependable systems are conventionally those in which failure of one or more RAMSS (Reliability, Availability, Maintainability, Security and Safety) attributes would have critical consequences. Within Safety Engineering, numerous techniques have evolved to aid engineers in safety analysis and risk reduction for safety critical systems. Such techniques include Fault Tree Analysis, Event Tree Analysis, Failure Modes and Effect Analysis, and Hazops [2]. Recent effort has considered the application of such techniques to computer-based systems [3, 4], although there is little work in the application of such techniques to the development process itself. Furthermore, existing quality improvement frameworks such as SEI CMM [5], Bootstrap [6], and those associated with ISO 9000 [7], do not focus on the particular problems of the *development* of dependable systems.

1.2 Process weaknesses due to human factors

Classical hazard and safety analyses of processes focus on the mechanistic aspects of that process. However, it is increasingly recognised that RE processes need to be understood in social as well as technical terms [8, 9, 10, 11], and thus may be subject to process weaknesses arising from human factors. A comprehensive process analysis must therefore give consideration to the human factors of the process by taking a more human centred view of the process than is traditional.

The human factors literature is diverse and impacts on RE activities from multiple angles. Due to current space restrictions we shall only touch on the wealth of relevant literature; more comprehensive reviews can be found in [1, 12, 13].

1.2.1 Errors and violations in individual work

A large amount of research into “human error” [13] has emerged from cognitive approaches to the understanding and modelling of individual failures. This work has generated important distinctions such as that between skill-based, rule-based and knowledge-based “levels” of cognitive activity [14]. Skill-based errors—otherwise known as *slips* and *lapses*—occur in the execution of routine skilled work, typically characterised by “strong but wrong” error behaviour [13]. Rule-based behaviour, where previously generated “if…then” rules are applied, can be

subject to rule-based mistakes if those rules are “bad” or “misapplied”. Knowledge-based mistakes arise when an individual is working in a novel situation and is not able to reuse a pre-packaged solution, or previously generated rule. *Hindsight biases*, *confirmation biases* and *availability biases* are examples of how solutions to current problems can be distorted through the misapplication of prepackaged solutions.

Furthermore, hazards may also be caused by procedural *violations* if the procedures are overly prescriptive, poorly defined or do not support the processes actually followed.

1.2.2 Group process losses

Social psychological research has concentrated on the effects of working in social and group settings. This wide and diverse body of research includes work on phenomena such as *social facilitation* [15], *group performance* [16], *group leadership* [17], *conformity and consensus* [18], the effects of *minority opinion* [19], *group polarisation* [20] and *groupthink* [21].

Such phenomena have been studied in a vast variety of settings, from political decision making to industrial shopfloor work, in both naturalistic and laboratory-based studies. While RE processes have not been an explicit topic of extensive study for social psychologists, these group weaknesses associated with how teams perform together and coordinate their work can confidently be assumed to be potential sources of process losses for socio-technical development processes such as RE.

1.2.3 Organisational context

It is increasingly recognised that the organisational context and safety-culture surrounding a process is a further determinant of the safety of that process. For example, *latent organisational failures* [13] may lie dormant until some active trigger event coupled with insufficient defences precipitates an accident. Debates between the *Normal Accident* [22, 23] and *High Reliability* [24] theorists, on the scope for optimism concerning safety for organisations operating in hazardous conditions, have resulted in recommendations aimed at improving organisational reliability. These include strong “safety culture”, high levels of technological and personnel redundancy, decentralised authority, organisational learning, and so on.

2 Method description

PERE is an integrated process improvement method that combines two complementary viewpoints onto the process under analysis:

1. *Mechanistic viewpoint*—an analysis of the process in mechanistic terms, as a number of interconnected process components. This analysis uses techniques adopted from classical safety analysis, adapted for a consideration of the RE process.
2. *Human factors viewpoint*—an analysis based on the application of human factors and social scientific principles to assess weaknesses and protections at

an individual, group and organisational level using the results of the mechanistic viewpoint to scope the analysis.

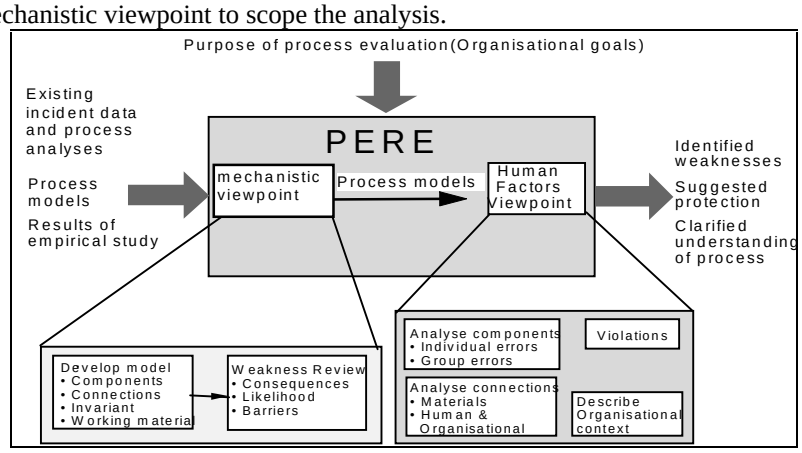

Figure 1: Overview of PERE[2]

An overview of the method can be seen in Figure 1. This dual viewpoint approach has been adopted since it has the following advantages:

- *Structured, usable approach*—PERE enables human factors considerations to be presented in a usable manner, through the application of a structured grounded checklist. This checklist is *grounded* in that each item contains references to human factors review documents and *structured* since the user is guided through the checklist by means of navigational questions. This navigation is guided and scoped by the results of the mechanistic viewpoint analysis. As a result, a manageable subset of the checklist is used, preventing the combinatorial explosion of having to consider each checklist item for each component.
- *Sensitive to actual RE process improvement needs*—since RE processes in practice combine human and automated processes, it is appropriate to combine two complementary viewpoints within the method, each concentrating on different aspects of the process. PERE exists within the process improvement paradigm and combines both “hard” and “soft” process improvement approaches.
- *Knowledge dissemination*—PERE integrates classical engineering analysis and human factors analysis. This structured, usable, yet technically defensible approach means that engineers in the process and safety domains will have access to the relevant social scientific research and broader human aspects that determine process dependability and which would not typically be within their domain.

[2] Other REAIMS modules such as PREview-PV and MERE can be used to supply process data or complement any existing process documentation.

- *Enhanced coverage*—since each viewpoint comes from a different research tradition, there is a certain amount of redundancy in the PERE process, resulting in increased coverage of the process under analysis as process weaknesses are trapped under different guises. This redundancy further improves the dependability of the PERE process itself.

2.1 Mechanistic viewpoint

PERE's mechanistic viewpoint (see Figure 2) has its origins in the classical safety analysis technique, Hazops [2], and Object-Oriented inspired analysis.

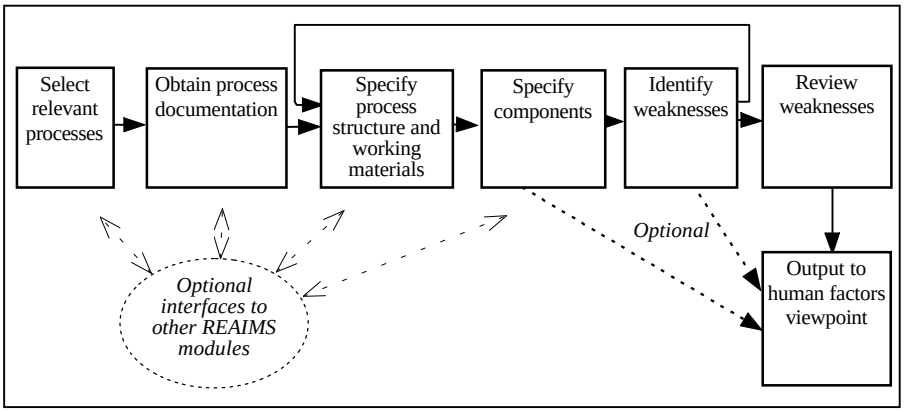

Figure 2: PERE's mechanistic viewpoint

For this viewpoint it is assumed that both human and machine activity in the process are analysable into components. The model we describe is based on the principles of using modularity and abstraction to describe systems, considering generic component classes (process, transduce, channel, store and control) as subject to generic component weaknesses, and explicitly considering the "working material".

Once the process structure and working material is described, the PERE analyst completes a PERE component table (a row of which is shown in Figure 3) to describe the process model. This process model is then reviewed for weaknesses by considering the generic weaknesses associated with each component and also the specific weaknesses associated with the components attributes.

Component name	Component Class	Interfaces and working material	(Optional) State	Invariant	(Optional) preconditions and resources	(Optional) external control

Figure 3: PERE Component Table (PCT)

In documenting this analysis a PERE Weakness Table (see Figure 4) is completed. The weaknesses identification and review steps are iterated until no more weaknesses are identified. The results of the mechanistic analysis are then

passed on to the human factors viewpoint, although provisional results may be fed forward if, say, one component is considered to be particularly vulnerable to human error.

Actual Weakness	Weakness Class	Likelihood	Consequence	Possible protections	Possible secondary weaknesses

Figure 4: PERE Weakness Table (PWT)

2.2 Human factors viewpoint

For the human factors viewpoint (see Figure 5) the top level analysis shares the perception of the mechanistic viewpoint of processes in terms of interconnected components. As a result, the human factors viewpoint builds on the mechanistic analysis.

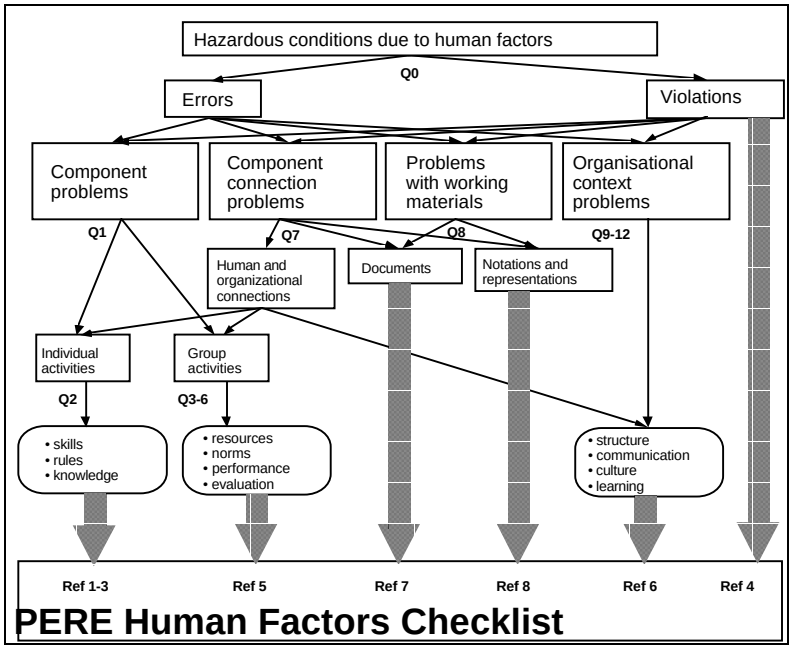

Figure 5: PERE's human factors viewpoint

In this phase we consider those components that are composed primarily of human activity, their interconnections and working material, and organisational context. The analysis proceeds by means of a series of structured questions (see Figure 6), which enables the analyst to search for only those human factor weaknesses that are relevant for the particular process under consideration (e.g. it is not generally necessary to consider knowledge-based component weaknesses for a skill-based component such as typing).

The application of the human factors viewpoint concludes with a completed PERE human factors table (see Figure 7), which includes suggested protections against the identified weaknesses. Of course whether they should be actually implemented for a particular application depends on factors such as the *reason* for investigation, an assessment of the *risk* associated with the weakness, and considerations of *prioritisation* and financial *cost* of the protections.

Q0 Is it suspected that this process component, its connections or its working materials can be vulnerable to error and/or violation?
Q1 Is the component principally characterised by individual or group activity?
Q2 Is the component principally characterised by skill-based, rule-based or knowledge-based activity?
Q3 (resources) What are the available human resources for the group to fulfil its function?
Q4 (norms) How is the function of the group presented to group members and what are the norms (specifications of what the group and its members should do) that govern the activity of the group in executing this function?
Q5 (performance) How are the contributions of group members produced and coordinated?
Q6 (evaluation) How are the contributions of the group members and the overall products of the group (decisions, jointly authored documents or whatever) evaluated?

Figure 6: Selection of navigational questions in the human factors viewpoint

PERE also recognises that some process improvements may have *secondary weaknesses* associated with them. For example, introducing increased monitoring and redundancy into a process may reduce the chance of error propagation, but decrease the manageability of the process at a higher level. If such process improvements are more risky than the existing weakness, process redesign may be more preferable than evolutionary incremental improvement. Another indication that process redesign is necessary is if the existing process encourages or requires extensive procedural violation.

	Name	HF weakness analysis	Likelihood	Consequence	Possible protections	Possible secondary weaknesses
Component problems						
Interconnections and working material problems						
Organisational context problems						

Figure 7: PERE human factors table (PHT)

3 Applications and future work

PERE has been applied in different contexts by different users (see also [25]). These have included applications to RE processes in the aerospace and railway industries. In this section we give an overview of how PERE has been applied to the development of a system for enhancing corporate memory (MERE), to a software engineering process, and to a typical standards making process.

3.1 Corporate memory process

MERE (Managing Experience in Requirements Engineering) is another module in the REAIMS family that concerns the capture and reuse of experience within an organisation, such that previous incidents and good practice—often dubbed "corporate memory"—can generate requirements for other similar projects and products. The MERE process defines the lifecycle of these generated requirements from the collection of incident data, through elaboration and validation, to application and verification for a new product.

The application comprised an initial site visit and process observation from a human factors viewpoint, followed by the development of a process model and a full application of PERE. The PERE analysis aided the ongoing development of MERE by providing some insights and suggestions for how the MERE process might be improved through simplification and redesign.

3.2 Software engineering process

PERE can also be applied in a single pass "fast-track" approach. One such application on a REAIMS partner's formal specification process was conducted over two days and involved a number of meetings between PERE analysts and process stakeholders. The analysis was primarily aimed at evaluating a process guide that had been written, by means of constructing and analysing a process model built from stakeholder interviews and the process guide. Although it would be normal for a PERE analysis to involve more in-depth process capture and analysis, there was some payback even for this "fast track" application, in terms of different types of weaknesses identified in the process as described by the process guide.

3.3 A standards making process

A standards making process can be considered to be an RE process in which the user requirements of the industrial standardisation participants are captured, negotiated and developed into a standards document. Typically, the process is primarily constructed from complex human centred activities, such as document production, group meetings and document review activities.

PERE was applied to the standards process [26] in order to gain increased understanding and identify possible options for process improvement. This increased understanding is needed, since the current standards process may be long and protracted (possibly up to 10 years per document), and standards making as a result may seriously lag behind technological and market developments within the industrial sector that the standard was designed to support.

The initial standards process model was built from official and supporting standards documentation, resulting in a standards model that was considered to be typical of many of the processes by which standards emerge in national and international standards organisations. This initial modelling was augmented with field work, which involved interviewing and observing standards makers. The aim of this field work was to improve the process model that had been constructed and

to elicit information on what standards makers considered to be the *actual* problems they faced. The results of this application have included:

- *increased process understanding*—in the form of process models and identified weaknesses of the actual, rather than idealised, standards process. For example, it was seen that although the *document production* aspects of standards production are typically well supported by the current process, other more human centred aspects, such as *consensus building*, may only be implicitly supported.
- *process improvement suggestions*—in terms of possible process protections and process redesign options to safeguard against the identified weaknesses;
- *preliminary validation of PERE*—PERE was able to pick up many of the actual weaknesses identified by standards makers.

3.4 Future work

PERE is being exploited by REAIMS partners in the course of their everyday work, and is under continuous development. We are investigating tool support for PERE, and a "shareware" version of PERE is available on the world wide web[3].

4 Acknowledgements

The authors would like to thank project members and reviewers for helpful comments throughout the development of PERE. This research has been conducted as part of the CEC ESPRIT project number 8649, REAIMS. The project partners are GEC Alsthom, Adelard, Aerospatiale, Lancaster University, Manchester University, RWTÜV, Apsys, Digilog. The order of authors is alphabetical.

5 References

1. Viller, S., Emmet, L., Bowers, J., Bloomfield, R. (1996) PERE: A Method for Requirements Process Dependability, Submitted to IEEE Symposium on Requirements Engineering-RE'97, 5-8th January 1997, Annapolis MD (also available as technical report CSEG/4/96, from Cooperative Systems Engineering Group, Computing Department, Lancaster University).
2. Kletz, T.A., Hazop and Hazan—Identifying and Assessing Process Industry Hazards. Institution of Chemical Engineers, Rugby, UK, 1992.
3. Kletz, T., Chung, P., Broomfield, E. and Shen-Orr, C., Computer Control and Human Error. Institution of Chemical Engineers, Rugby, 1995.
4. McDermid, J.A. and Pumfrey, D.J., A development of hazard analysis to aid software design. In: Proceedings of COMPASS'94 (Gaithersburg, MD, 1994) IEEE Computer Society Press.
5. Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V., Capability maturity model, version 1.1. IEEE Software 10, 4 (1993) pp. 18-27.
6. Bootstrap Project Team, Bootstrap: Europe's assessment method. IEEE Software 10, 2 (1993) pp. 93-95.

[3] http://www.comp.lancs.ac.uk/computing/research/cseg/projects/reaims/

7. Huyink, D. and Westover, C., ISO 9000. Irwin Professional Publishing, New York, 1994.
8. Bowers, J. and Pycock, J., Talking through design: requirements and resistance in cooperative prototyping. In: Proceedings of CHI'94 (Boston, MA, 1994) ACM Press, pp. 299-305.
9. Goguen, J.A., Social issues in requirements engineering. In: Proceedings of RE'93 (San Diego, CA, 1993) IEEE, pp. 194-195.
10. Quintas, P., Ed., Social Dimensions of System Engineering: People, Processes, Policies and Software Development. Ellis Horwood, London, 1993.
11. Westrum, R., Technologies and Society: The Shaping of People and Things. Wadsworth Publishing Company, Belmont, CA, 1991.
12. Bowers, J., Viller, S. and Rodden, T., Human Factors in Requirements Engineering, REAIMS Deliverable D1.2, REAIMS/WP1.2/LU004, Lancaster University, 29th August 1994.
13. Reason, J., Human Error. Cambridge University Press, Cambridge, UK, 1990.
14. 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, 3
15. Manstead, A.S.R. and Semin, G.R., Social facilitation effects: mere enhancement of dominant responses? British Journal of Social and Clinical Psychology 19, (1980) pp. 119-136.
16. Steiner, I.D., Task-performing groups. In: Contemporary Topics in Social Psychology Thibaut, J.W., Spence, J.T. and Carson, R.C., Ed., General Learning Press, Morristown, NJ, 1976.
17. Hemphill, J.K., Why people attempt to lead. In: Leadership and Interpersonal Behaviour Petrullo, L. and Bass, B.M., Ed., Holt, Rinehart & Winston, New York, 1961.
18. Van Avermaet, E., Social influence in small groups. In: Introduction to Social Psychology Hewstone, M., Stroebe, W., Codol, J.-P. and Stephenson, G.M., Ed., Basil Blackwell, Oxford, 1988, pp. 350-380.
19. Maass, A. and Clark, R.D., Hidden impact of minorities—15 years of minority influence research. Psychological Bulletin 95, 3 (1984) pp. 428-450.
20. Isenberg, D.J., Group polarization: a critical review and meta-analysis. Journal of Personality and Social Psychology 50, (1986) pp. 1141-1151.
21. Janis, I.L., Victims of Groupthink. Houghton Mifflin, Boston, MA, 1972.
22. Perrow, C., Normal Accidents. Basic Books, New York, 1984.
23. Sagan, S.D., The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton University Press, Princeton, NJ, 1993.
24. La Porte, T.R. and Consolini, P.M., Working in practice but not in theory: theoretical challenges of 'high reliability organizations'. Journal of Public Administration Research and Theory 1, 1 (1991) pp. 19-47.
25. Märtins, F., Schippers, H., Viller, S., Bowers, J. PERE: Process Evaluation in Requirements Engineering with special consideration of human factors, In: Design for Protecting the User, 13th Annual CSR Workshop, 11–13th September, Bürgenstock, Switzerland 1996
26. Emmet, L. and Bloomfield, R. Application of PERE to the standards process; REAIMS Deliverable D5.2a, REAIMS/WP5/AD/W/103; Adelard; 1996