REAIMS: Requirements Engineering Adaptation and Improvement strategies for Safety and Dependability

This article reports on the REAIMS project, a 2 year Esprit project (project number EP8649) focusing on the development and assessment of requirements engineering processes for dependable systems.

INTRODUCTION

Failings in requirements engineering activities place all subsequent life-cycle phases at risk and may lead to cost over-runs, quality deficiencies and customer dissatisfaction. This is especially true if these failings result in errors which remain undiscovered until the software product is in service. If the product is safety-related then their discovery may take the form of a serious accident. REAIMS starts from the position that in a safety critical system, the activities of requirements engineering and safety and hazard analysis are closely related. Hence, a dependable requirements engineering process in which concern for safety is properly integrated is a prerequisite for the development of safe systems. REAIMS' key aim is the improvement of requirements engineering processes for safety-critical and dependable systems.

REAIMS is addressing this aim at a number of different levels from requirements engineering process assessment techniques to specific process improvement methods to guides to good practice. All these technologies emerging from REAIMS work are being validated by their application to real safety-related projects undertaken by REAIMS' two large industrial partners. The common factor to these technologies is that they each address a particular problem with the requirements engineering process for safety-critical systems development. In particular, the four areas concentrated on in REAIMS are: poorly *structured* information about requirements relative to the critical concerns of users; human factors problems in the process of *co-operative work*; the lack of *memorisation* of new experience emanating from similar systems development projects; and incorrect *reasoning,* at the abstract level, about the requirements specification.

The main results to emerge from REAIMS are described below. Each key technique is being packaged as one of the REAIMS family of modules designed to be applicable to a wide range of organisations and requirements engineering processes.

Viewpoints for requirements engineering

REAIMS module: **PET-RE** (Process Engineering Technology—Requirements Engineering)

A process based around *System Viewpoints* to guide the discovery, analysis and management of software requirements is proposed as a means to improve the dependability of these activities. In contrast to other methods, including those with a notion of viewpoints, where an available human source of every requirement is assumed, this work recognises that domain knowledge may be too diverse to guarantee that all requirements can be elicited and that many requirements, including safety-related ones, may be implicit in the domain itself. Techniques are provided to focus the analysis on the domain from the perspective of interactors, stakeholders or domain phenomena, to draw out these requirements, to identify conflicting requirements where they occur, and to help make informed decisions to resolve these conflicts.

An important feature of this work is that it makes explicit what is often implicit in good requirements engineering practice. Adoption of the method does not therefore imply wholesale replacement of an organisation's existing practices. However, adoption of the central concepts should result in a dependable requirements engineering process which is geared to making best use of available domain knowledge, using overriding concerns such as safety to drive the process.

Viewpoints for process improvement

REAIMS module: **PET-PI** (Process Engineering Technology—Process Improvement)

In the same way that viewpoints may serve as a structuring mechanism for software requirements, they can also be used to structure the requirements for a *process* as an input to an overall process improvement activity. Hence, the participants and other interested parties in a requirements engineering process are used as the foci of an analysis of the process to discover its strengths, weaknesses and proposed improvements. Process viewpoints complement the PERE approach to process evaluation (below) and can be used to support different improvement and measurement strategies such as Bootstrap, SEI, ISO9000, and ami.

Process evaluation in requirements engineering

REAIMS module: **PERE** (Process Evaluation in Requirements Engineering)

The requirements engineering process for any non-trivial system, and consequently for any safety-related system, will inevitably involve the cooperation of several people along the way from early requirements elicitation through to the final specification. The importance of attending to the human aspects of the design of the systems being developed is widely recognised. For example, ergonomic, human-computer interaction and cooperative work studies routinely inform the design of many products from video equipment to air traffic control systems. However, until recently there has been little recognition that human factors also influence design quality, and therefore safety, indirectly through the processes, activities and tasks employed by the designers.

There is the potential for substantial benefits if lessons learned from human factors work could be applied to organisations' requirements engineering processes in a practical and an economic manner. REAIMS is developing a method based on a fusion of techniques from conventional hazard analysis and human factors research. This method can be used on its own, or as part of a wider process improvement strategy. Existing processes need not be fully documented, although any existing documentation is used as a starting point. The result of the analysis is a documented requirements engineering process, a list of components of the process which are vulnerable to error due to individual, social/group, or organisational factors, and recommendations for possible improvements to defend against these vulnerabilities.

Memorisation of experience

REAIMS module: **MERE** (Memorisation of Experience for Requirements Elaboration)

When considering the requirements engineering process for complex systems, an inherent problem is the potential loss of individuals' experience gained from their involvement in a series of projects. If these people move within the organisation, leave, or retire, this experience is either lost or transferred to long, opaque documents that are easy to ignore and often forgotten about. This problem is particularly acute for safety-critical systems development where the complexity of the systems, and the processes by which they are developed, is even greater.

The MERE process aims to address this problem by putting in place a means for systematically elaborating Rules/Recommendations (R/Rs) for application in new designs, based upon experience as it is encapsulated in incident reports, feedback from maintenance and operations, and so on. All experience facts are recorded in a database, and then used to derive R/Rs which are subsequently validated for accuracy and means of application. This results in a database of R/Rs for the organisation's whole product range, from which extractions can be made at the inception of a new project to generate requirements for application in the design of the product.

Formal reasoning in requirements engineering

REAIMS module: **FRERE** (Formal Reasoning in Requirements Engineering)

Formal methods are now recognised as being an essential part of specifying requirements for safety-critical systems, and their use is recommended or mandated in many application areas. There are problems, however, in making the transition from 'informal' requirements, informed by domain knowledge and expertise, to specifications which can be formally reasoned about.

This area of REAIMS work addresses these problems in two ways. Firstly, safety-critical systems development requires a defined process, and formal methods should be clearly situated within this. We are developing such a process which is tailored to the use of formal methods, and allows for the transition between informal requirements and formal specifications. Secondly, much of the domain-related information contained in more informal requirements is lost when a formal specification is created. The process developed here aims to provide an error-free transition to formal specification, whilst maintaining traceability to the original requirements to improve confidence that this process preserves their original meaning.

CONTACT DETAILS

Further details about the REAIMS project and it's various modules can be obtained from:

Robin Bloomfield

Adelard
3 Coborn Road
London
E3 2DA
UK

+44 (0)181 983 0217

Herbert Schippers

RWTÜV
Institute for Information Technology
Im Teelbruch 122
D-45219 Essen
GERMANY

+49 (0)201 825 5120

REAIMS partners

GEC Alsthom, France (Coordinating partner); Adelard, UK; Aerospatiale, France; RW TUV, Germany; Lancaster and Manchester Universities, UK; Apsys, France (sub-contractor); Digilog, France (sub-contractor)