Knowledge Management in Safety-Critical Systems Analysis

Guy Boy
EURISCO International, France

Yvonne Barnard
EURISCO International, France

INTRODUCTION

Knowledge management in the design of safety-critical systems addresses the question of how designers can share, capitalize, and reuse knowledge in an effective and reliable way. Knowledge management is situated in groups, organizations, and communities, playing different roles in the design process. Design of safety-critical systems has specific properties, such as dealing with complexity, traceability, maturity of knowledge, interaction between experts, awareness of the status of information, and trust in knowledge. Documentation is of crucial importance in design processes, ensuring that these properties are taken care of in a proper and reliable way. However, writing is not an easy task for engineers, and support is needed. Several knowledge management solutions, both tools and organizational setups, are available to support design work, such as active notification of changes, personal and team workspaces, active design documents and knowledge portal solutions.

SITUATING KNOWLEDGE MANAGEMENT

Knowledge management (KM) has become an important research topic, as well as a crucial issue in industry today. People have always tried to organize themselves in order to capitalize, reuse, and transfer knowledge and skills among each other within groups. Poltrock and Grudin (2001) propose the triple distinction team-organization-community for groups. KM tools and organizational setups usually emerge from the requirements of one of these kinds of groups. Note that we do not dissociate a KM tool from the group that is likely to use it.

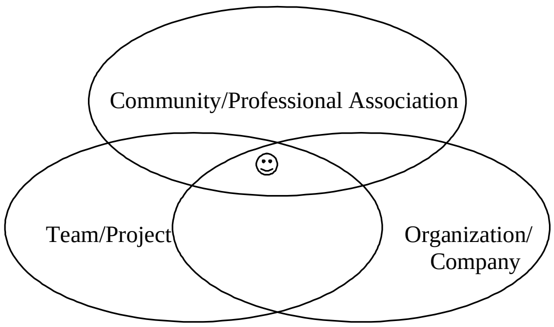
A team is a small group of persons that work closely with each other, but not necessarily in the same location. A leader often coordinates its work. Team participants typically fulfill different roles. They strongly need to communicate. The following groups are examples of teams: software development teams, proposal writing teams, conference program committees, and small operational groups such as customer support or research project teams. Support technologies include: buddy lists, instant messaging, chat, Groove (a peer-to-peer team collaboration environment), Quickplace (provides an instant virtual team room where information is managed), BSCW (both a product and a free service for managing information for self-organizing groups, Bentley, Horstmann, & Trevor, 1997), video conferencing, data conferencing, and eRoom (team workspaces with shared workspaces, calendars, and discussions through a Web browser).

The structure of an organization is typically hierarchical. Modern organizations are usually geographically distributed. They strongly need to be coordinated. The following groups are examples of organizations: companies, governments or government agencies, and non-profit organizations. Support technologies include: e-mail, calendars, workflow, Lotus Notes (an integrated collaboration environment), intranet applications and webs, document management systems, and broadcast video.

Communities share a common interest but no structure. They are usually geographically distributed and provide services to people (e.g., the European KM Forum, Amazon.com). The following groups are examples of communities: citizens of a city or neighborhood, special-purpose chat groups, virtual world citizens, auction participants, stamp collectors, and retired people. Support technologies include: Web sites, chat rooms, and virtual worlds.

In the field of safety-critical systems, teams, organizations, and communities inter-relate in order to insure quality on both products and processes. They are highly constrained. Usually teams are made to carry out projects and programs; they may be multi-national for example. Organizations are made to manage people within a consistent space, such as a national company that is more appropriate to handle social laws and customs of the country where it is chartered. Communities are made to help people who share the same kind of work practice to refer among each other, such as a community of electrical engineers. We summarize these distinctions in Figure 1.

Figure 1. An individual may belong to a project team, a company, and a professional association at the same time.



A project team exists only during the time of the related project. A company may have several projects or programs that themselves may involve people from others companies. A company may become obsolete when the type of products it produces is no longer appropriate with the current market. Professional communities survive the obsolescence of both projects and companies. They actually may also become obsolete when either technology and/or the social world change.

In this article, we will present specific issues brought by the design of safety-critical systems, and human factors related to documentation generated and used in design processes. We will also focus on related current design issues. The specificity of safety-critical design knowledge will be presented. Several KM management solutions will be discussed. The article concludes with a discussion on the difficulties and challenges of KM in engineering.

The article is coming from several knowledge management projects performed in cooperation with groups of engineers in large aerospace and telecommunication companies. In particular, most recent findings come from the European Research and Development project WISE (IST-2000-29280; www.ist-wise.org). In WISE (Web-Enabled Information Services for Engineering), we study workpractices of engineers in large manufacturing companies, and we design practical methods to easily share and access essential knowledge and information for their tasks. These methods are supported by the development of an engineering knowledge portal application. The industrial partners involved in this project are Nokia and Airbus. Other partners are Cyberstream Interface SI, PACE, EURISCO International, Norwegian Computing Centre Helsinki University of Technology, and Technical University of Berlin.

Designing Safety-Critical Systems

Safety-critical systems have specific properties that directly affect the way knowledge management is carried out. Examples of safety-critical systems are aircraft, power plants, medical equipment, and telecommunication systems. They are basically complex, as complete as possible, and described by mature knowledge. Safety is not only a matter of end-user emotion, attention, and cognition; it is also a matter of organization and people involved in the whole lifecycle of related products. They involve experts that need to cooperate. For that matter, traceability of decisions is crucial.

Safety-Critical Systems Communities as Families

People working on safety-critical systems, in domains such as aerospace, nuclear power plants, and medicine, form strongly connected communities of practice that could be seen as families. They have their own meetings, workshops and conferences, even journals, where they can exchange experience, foster research, and improve knowledge on safety-critical systems in general. These communities work across organizations and teams. They tend to become references and initiate standards in the related field. They are recognized bodies for knowledge validation, providing principles for assessing knowledge maturity.

Dealing with Complexity

Even if the designers of safety-critical systems should always have in mind to design for simplicity, what they have to do is inherently complex. Systems are complex, and processes to design and develop these systems are complex. In the design process, designers rely on knowledge that is available in the form of handbooks, lessons learned, and best practices. Designers have to take into account the experiences with older systems, on which the new system is usually building, making sure that incidents and accidents that have happened are no longer possible in the new design. Designs are verified and validated in extensive, well-defined processes. In the end of the design process, certification by different authorities and certification bodies can also play a large role. In order to get a system certified, one has to be able to justify the choices that were made, to prove, as far as possible, that all knowledge about problems with similar systems has been taken care of, and that the system will function safely in all kinds of difficult and even disastrous scenarios.

Related Content

The Outcome of Knowledge Process for Customer of Jordanian Companies on the Achievement of Customer Knowledge Retention

Amine Nehari-Talet, Samer Alhawariand Haroun Alryalat (2010). *International Journal of Knowledge Management (pp. 44-61).*

www.irma-international.org/article/outcome-knowledge-process-customer-jordanian/39090

Introduction to the Special Issue: An Australian Perspective on Organisational Issues in Knowledge Management

Frada Bursteinand Henry Linger (2006). *International Journal of Knowledge Management (pp. 1-5).*

www.irma-international.org/article/introduction-special-issue/2673

Enhancing E-Business on the Semantic Web through Automatic Multimedia Representation

Manjeet Rege, Ming Dongand Farshad Fotouhi (2009). *Semantic Knowledge Management: An Ontology-Based Framework (pp. 329-340).*

www.irma-international.org/chapter/enhancing-business-semantic-web-through/28824

Managing Indigenous Knowledge in Tanzania: A Business Perspective

John Jackson Iwataand Ruth G. M. Hoskins (2017). *Managing Knowledge Resources and Records in Modern Organizations (pp. 198-214).*

www.irma-international.org/chapter/managing-indigenous-knowledge-in-tanzania/173805

Design of Knowledge Based Analytical Model for Organizational Excellence

Sonal Pathakand Rashmi Agrawal (2019). *International Journal of Knowledge-Based Organizations (pp. 12-25).*

www.irma-international.org/article/design-of-knowledge-based-analytical-model-for-organizational-excellence/216837