NordDesign 2004 – Product Design in Changing Environment
18-20 August 2004, Tampere, Finland

A CONCEPT FOR SAFETY AND DEPENDABILITY INFORMATION EXPLOITATION IN MAINTENANCE PLANNING AND PRODUCT DEVELOPMENT

Juhani Viitaniemi

Production Engineering
VTT Industrial Systems
Tekniikankatu 1
P.O. Box 1307
FIN-33101 Tampere
FINLAND
E-mail:
Juhani.Viitaniemi@vtt.fi

Arto Säämänen

Production Engineering
VTT Industrial Systems
Tekniikankatu 1
P.O. Box 1307
FIN-33101 Tampere
FINLAND
E-mail:
Arto.Saamanen@vtt.fi

Markku Reunanen

Reliability and Risk Management
VTT Industrial Systems
Tekniikankatu 1
P.O. Box 1306
FIN-33101 Tampere
FINLAND
E-mail:
Markku.Reunanen@vtt.fi

Knowledge management, decision-making, data collection, data analysis, transponder, safety, dependability

Abstract

Maintenance services are becoming increasingly important in the current business environment. Emphasis on the availability and maintainability over the entire life cycle of modern, complex technical systems calls for relevant product-specific information. This information begins to grow already when the product development starts and accumulates throughout the operational phase of the product. Continuous availability of information on the safety and dependability characteristics and the system condition is required for the fluent operation of the system, e.g. for maintenance planning or decision-making purposes. In acute situations, such as in disturbances, the information must be readily accessible, e.g. instructions on how to ensure that a system is in a safe state for the intended repair action. In this paper a concept for the safety and dependability background information system has been proposed. It includes the identification of basic structural elements of the background information system, and procedural steps for creation and exploitation of the information contained in the system. Also problematic aspects and implications of the concept have been discussed.

1 Introduction

Machines are becoming more complex and they will be increasingly customer configured from baseline machines (e.g. passenger cars) or even tailored for customer needs (e.g. storage automation systems). Configuring or tailoring continues through the entire service life. Therefore, machines will be unique also in terms of their safety and reliability characteristics, and there will be information that should be easily available. It has been recognised that Information technology and computers will play an important role in managing this huge

amount of safety information, and will contribute to its systematic and widespread implementation [Mattila.96]. Easy information availability is valued even though skilful workers are used to operate and maintain the machine. In this paper the terms product, system and machine are used interchangeably to characterise an artefact.

Product lifecycle related data has been studied for various reasons [Anon.02]. Processes within the product lifecycle, ranging from target setting to operation and decommissioning, will generate and use plenty of product-specific information. Typically, this information is used to promote production, logistics and business. On the other hand, this product-specific information could also be valuable for the operator, especially during the operation and maintenance. At the moment there is a problem of how these two information demands can be fulfilled simultaneously.

The term "safety and dependability information" is difficult to define precisely. Currently, safety and dependability information is produced at different points in time, and in different organisations over the life cycle of the product. Moreover, the essential safety and dependability data is typically contained in different information systems and in different formats within companies. Almost all information concerning a product is somehow related to its safety and dependability performance. At least the scope, context and purpose of the product, together with its environment, are examples of such information. Obviously, information requested by, e.g. the standards ISO 18000, IEC 60300, EN 50126, EN 292, EN ISO 12100, and EN 1050 can serve as a basis for defining safety and dependability information.

Among other things, safety and dependability information should improve the comprehension of the product. Therefore the structure of this information has to be reasoned taking into account the operational environment and human activity (Figure 1).

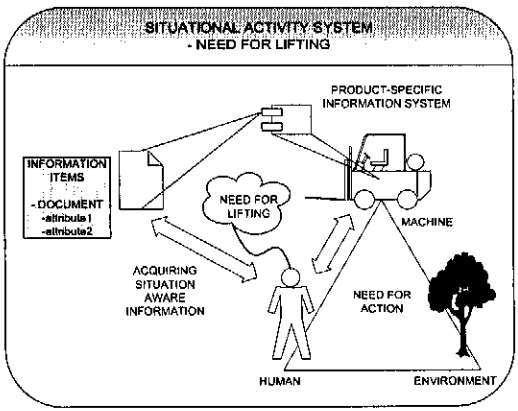

Figure 1. The situational activity system as the context of need for safety and dependability information.

Context awareness is based on the products, systems and machines that form the operational environment and interacting with the human [Norros et al.03]. The viewpoint therefore must be the whole operational system while the machine usually represents just only one

component of the operational environment. This means that product design approach should be system-oriented; aiming to facilitate the design of complex systems by providing flexibility and adaptation to meet unpredictable demands of their future usage [Rasmussen.86; Vicente.99]. Standard EN 50126 proposes a process model to fulfil the system-oriented demands of product design from the safety and dependability point of view. The standard places a strong focus on the co-operation between the vendor and the customer.

One example of safety and dependability information systems has been proposed by Reunanen [Anon.04; Reunanen et al.04]. It aims for better availability and utilisation of product-specific acute safety and dependability information. The technological parts used in the concept include: 1) A system for locating/storing product-specific information (TAG), 2) A mobile system for the utilisation and updating of safety and dependability knowledge in daily operations and acute situations (EXP), and 3) A background information system with data analysis, synthesis and management capabilities for processing information (TOP). In the concept the technology of transponders that can be attached to a work machine or a product, is adopted. Transponders (e.g. RFIDs) can act as smart embedded information subsystems that are capable of buffering and storing the transferred data close to the product or system, and are also easily available. Transponders can also transfer data wirelessly to users, while e.g. users are engaged in service or repair work, in order to be able to identify and avoid the hazards involved in the activities.

This paper aims to conceptualise part of the above mentioned background information system (TOP). The focus is on using the system in the context of everyday operation and maintenance situations. The paper presents how the user of the system may directly use and influence the content of the background information system and also influence the future product development by providing feedback. The paper presents how other information management systems existing in the company could be used to create knowledge items relevant to the safety and dependability concept.

2 Need for safety and dependability information exploitation

Traditionally, information on safety and dependability is transferred from the vendor to the user as a documentation including, e.g. operation and maintenance instructions and other product data. The documentation is normally delivered in printed format, which hampers the usability of the information in daily operations, especially while handling acute situations. To improve the usability, the documentation is increasingly delivered in electronic format. This does not, however, necessarily allow contextual information inquiries to be carried out in acute situations because the linkage between the information and the product structures is typically too weak. For contextual use, the information content should be structured in a different way.

New ways to exploit safety and dependability information are a business opportunity. Benefits may include, e.g. lower costs, less incidents, longer uptimes, and higher quality. At the design stage, important baseline information on safety and dependability is produced. In order to be successful, collaboration between the vendor and the customer - especially regarding information exchange - are needed. A comprehensive view on collaboration and the required information management practises is given in EN 50126. Even though this standard describes RAMS (Reliability, Availability, Maintainability and Safety) processes to be used in railway applications, the same principles can be applied to other fields of applications.

As Figure 2 shows, the RAMS programme has an important role in the information exchange during the lifecycle of a product. Both vendor and customer should have their own RAMS processes to manage important RAMS information and these two processes will coincide in the application-specific RAMS programme.

Useful information for the application-specific RAMS programme is contained in various information systems (Figure 2). The system manufacturer manages product-specific information using, e.g. PDM (Product Data Management) information systems. On the other hand, the system operator manages product specific safety and dependability information, e.g. with safety management systems and CMMS (Computerised Maintenance Management System). The information exchanged in the application specific RAMS programme should take advantage of the information existing in current information systems.

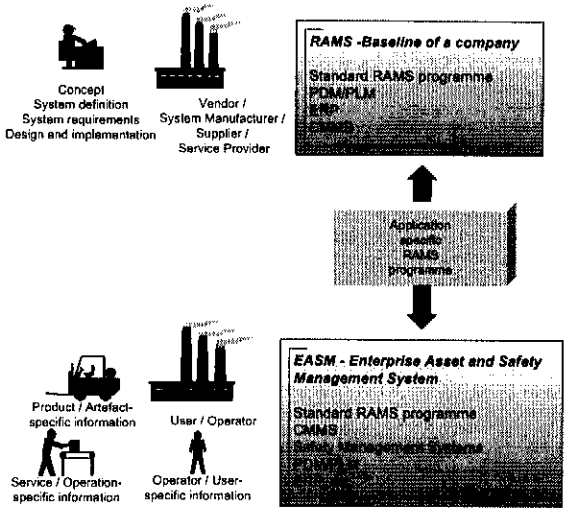

Figure 2. Safety and dependability information generation and information transfer via RAMS programme.

3 Current information systems as safety and dependability information sources

Modern technology offers a variety of sources that are either adopted widely or could be easily adopted for information sources. Examples include PDM systems or PLM (Product Lifecycle Management) systems, CMMS and safety information management systems. Typically, PDM/PLM systems include a huge amount of product-related information. In addition to the basic/standard product descriptions and documents, PDM/PLM systems include information relevant to each individual product configuration. For information on maintenance events, the CMMS contains, e.g. a plant-level technical equipment register and functionalities that allow the planning of maintenance tasks, and the management and acquisition of spare parts. Safety management systems typically contain information on risks, injuries, incidents, hazardous chemicals and other documents concerning occupational safety issues at a plant.

As PDM has a focus on data and configuration management it is fundamental to PLM [Amann.04]. PDM provides the infrastructure required to deliver the two fundamental characteristics of PLM: a) Providing universal, managed access to product and plant definition information, and b) Maintaining product and plant information definition integrity through product structure management, configuration management, and workflow-enabled change management. Therefore, PDM will be the primary starting point of PLM implementations. PLM emphasises that product-associated capital and information have become a strategic business initiative [Anon.02, Horne.04]. PLM allows a company to manage product-related information and processes throughout the lifecycle of the product, and in the extended enterprise it is used to create and utilise the information [Anon.01]. It may also include workflow and processes across the product lifecycle thereby integrating people, processes, business systems, and information.

The most important element of PDM is the item. Item types are [Martio.02, Peltonen et al.02]: a) Physical items such as systems, assemblies, parts, components, accessories, b) Document items, c) Product models and software, d) Service items such as operation and maintenance manuals. Practical implementations of PDM/PLM system features vary, but the basic principles are quite similar. A useful feature of a product PDM data item is the use of the attribute to manage, e.g. different types of customer-specific definitions and for categorising item properties. This categorising feature could be a useful approach for managing some safety and dependability information.

The useful features of PDM for safety and dependability information management include: a) Information can be saved in a structured format with useful links for retrieval purposes (e.g. linkages to material, functions, manufacturing, maintenance, services), b) Exact product configurations are available and traceable including all related data and data files, c) Easy and secure data modelling capabilities for creating and changing data models, d) Scalability also for small installations, e) Data check-in and check-out services for user applications, f) Integration of data to allow information exchange with other systems [cf. Peltonen et al.02].

CMMS help maintenance organisations manage, e.g. work orders, material and resource control, and purchasing. The following lists modules found in many CMMS applications:
- Technical equipment register (tag number system),
- Work order system,
- Preventative maintenance,
- Spare parts management and acquisition,
- Maintenance history,
- Resource planning system,
- Budget system,
- Legal requirements,
- Condition monitoring and control,
- Drawings and document system,
- Safety,
- Analysis module.

The history and analysis modules are usually developed least. In order to be able to support plant dependability assessment, the module should contain information on, for example:
- Failures,
- Maintenance work carried out,
- When failure occurred, and when maintenance was carried out,

- Cause of failure,
- Time usage and cost,
- Downtime and use of spare parts.

4 Concept to facilitate exploitation of safety and dependability information

Successful management of safety and reliability of machines requires the continuous availability of safety and reliability information during the entire life cycle of machines. At the moment, this information is not easily accessible because it stems from various and diverse origins along the machine lifecycle. This information may also have dubious conformity and integrity of content. Figure 3 outlines a concept that seeks to solve these problems and challenges with respect to safety and dependability information exploitation. The concept aims for better availability and utilisation of safety and reliability information within and between organisations. Thereby, it will enhance the transfer of safety and reliability information and thus, supports the decision making in daily operations in companies.

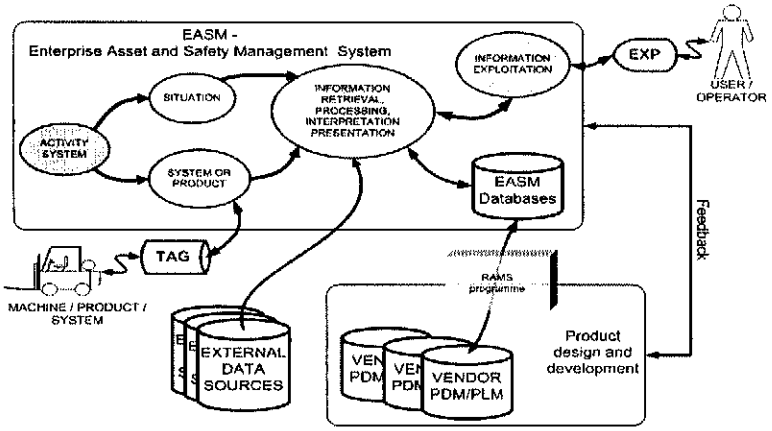

Figure 3. An outline of the concept to facilitate the exploitation of the safety and dependability information.

The following important features of the concept are covered in this article:

- Activity system and contextual information
- RAMS programme and vendor PDM/PLM
- EASM database

4.1 Activity system and contextual information

Figure 4 outlines the elements of the activity system. The activity system approach is important because it will link the safety and dependability information to the activity of a human-machine-environment system (Figure 1). Firstly, the activity system needs to be identified. Basically, the activity system will present (at an appropriate level of detail) who is doing what with which product item in which environment. Based on the activity system, situational activities and related functions of both the human and machine must be defined in such way that the missions and purposes of the system will be achieved. These will form the

basis for identifying and designing the safety and dependability structures of the background information system. It is important that the relation between the situation and corresponding product items is created already in the product design. This approach defines the way the information is proposed to be structured in the EASM database.

When the information is needed, e.g. in an acute maintenance situation, the situational activity system is determined together with the specific product item and the situation. This can be done by, e.g. using TAG and EXP devices [Reunanen et al.04]. The situational activity system relates the operator's working context to the information found in the EASM database.

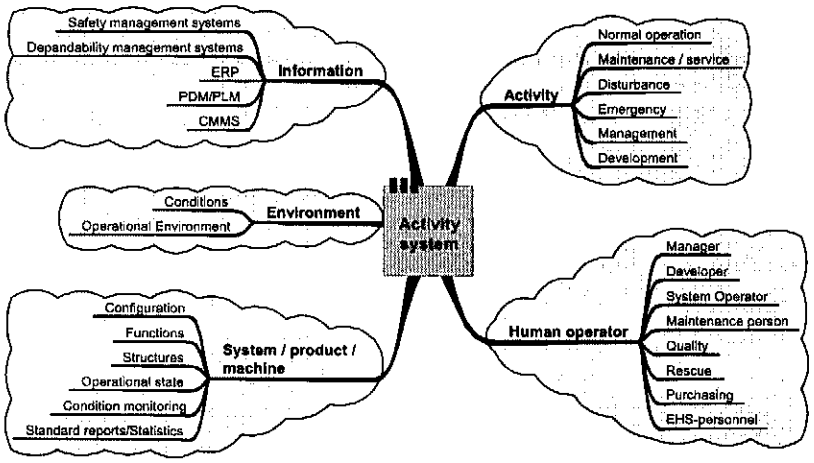

Figure 4. Outline of the main level elements essential to describe contextual information via an activity system.

Information related to the activity system may be found from sources such as safety management systems, dependability management systems, and PDM/PLM or CMMS.

4.2 RAMS programme and vendor PDM/PLM

Currently, formal procedures to set RAMS requirements and to run formal RAMS programmes between vendor and customer are not a common practise. Therefore, practises for exchanging RAMS information during the product development phase are typically poor or non-existing. In this paper, the model of a comprehensive RAMS process described in EN 50126 is used.

The content of the application specific RAMS programme will be agreed between vendor and customer. This programme will define what safety and dependability information is made available to be stored in the EASM database. As a result, the RAMS programme will configure the corresponding EASM database model. During the design phase of the product, the vendor will produce the baseline of the safety and dependability information. This information would also be beneficial to store in the vendor's PDM/PLM together with other product related data. However, product data structures for safety and dependability information should be created.

Safety and dependability information is mainly exploited during the operation and maintenance phase of the product lifecycle. However, additional RAMS information is also produced continuously along the lifecycle. This information is mainly used and produced in the user's or service provider's organisation, and may also be beneficial to store this information using a similar product data structure as is used in PDM/PLM systems. This would facilitate a continuous information exchange and feedback between user and vendor even after the product delivery.

4.3 EASM database

The EASM database uses safety and dependability domain models for storage and retrieval of information. It also contains information on product structures and configuration, similar to PDM/PLM and CMMS (Figure 5).

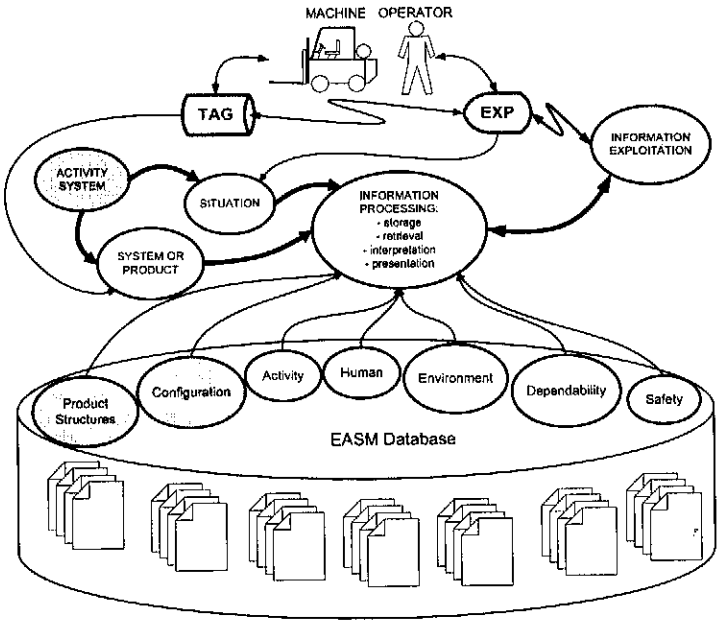

Figure 5. EASM database concept for safety and dependability background information system.

Activity, human and environment information represents, e.g. activities possible in the system, different roles of operators as well as environmental conditions or other components of operational environment. This kind of information is contained also in CMMS and safety management systems. In order to create contextual information exploitable for the user, the information processing utilises the EASM database, product-specific information from TAG, and available external databases. The information is presented to the operator via an EXP device. The EXP and TAG devices together inform the EASM, e.g. about the situation and target (product, item) of the activity.

5 Discussion

Based on a quick literature search, it can be claimed that the PDM/PLM systems' capabilities and usefulness in the area of safety and dependability information exploitation are poorly recognised. Although especially PLM systems do emphasize "*a strategic business approach that applies a consistent set of business solutions in support of the collaborative creation, management, dissemination, and use of product definition information across the extended enterprise from concept to end of life-integrating people, processes, business systems, and information*" [Anon.02], the method of applications implemented is one-directional and oriented on how a vendor could provide a user with a relevant data package concerning the product changes, which may even concern safety, health or dependability matters. The typical users of these systems are design-oriented. This study provides a contribution to motivate vendor and customer to use the same information content.

Compared to the common PLM approach, the novelty in the contribution of this study is the provision of a methodology for bi-directional information flow arrangement and sophisticated communication tools concerning particularly safety and dependability issues. The main benefit in this contribution is also the use of similar information systems and especially similar but enhanced information structures at vendor and user sites to promote conformity in the availability of safety and dependability information. A challenge is to get the EASM implementation to efficiently meet the areas of safety and dependability business relevancies of a vendor and a user concurrently and also maintain information integrity in multipoint access systems. Methods to integrate safety and reliability design tasks into the design process of the machine exist [Reunanen.93, Østerås.98, Kivistö-Rahnasto.00] and the contribution of this study is an implementation concept to apply those. Also, there are demands on the use of this information in safety management, e.g. in risk assessment at work or in continuous improvement of safety communication, safety culture, or behavioural safety issues [Kuusisto.00], with which this implementation concept coincides.

Safety and dependability information should freely flow between the companies involved. Much of the product-related information is created at the product design and manufacturing phases by the product vendor. This information is also essential for the user to facilitate safe and efficient operation and maintenance of the product. The RAMS programme provides a means to improve the quality of the safety and dependability information to be delivered to the user. It also facilitates the information flow between the vendor and the user.

Product development would in turn benefit from the feedback concerning the operation and maintenance phase. Organisational boundaries may, however, effectively hamper the information flow between organisations. Threats against information confidentiality and security may even completely block the information flow. On the other hand, new business concepts, such as partnerships, may facilitate the bi-directional information flow between partners. This will enhance the utilisation of new business models to achieve new levels of safety and reliability in complex systems [Warrington&Jones.03].

Production facilities typically consist of several independently purchased machines delivered by various vendors. Also, the maintenance of the production facilities may be outsourced to an external maintenance service provider. Therefore, the customer should be able to create links to several different external information systems or be able to create their own safety and dependability information database (such as EASM). In the first case, real-time links would be critical from the point of view of daily operations. Hence, it is recommended that the EASM database is mainly a local database system.

The most relevant situational activity systems should be identified in design or product development, thus making the design more systematic. But the more complex the product, the more meaningful the systematic process in acquiring the safety and dependability information becomes. RAMS may facilitate the involved companies to analyse the situations and relate relevant safety and dependability information into the product structure. Thus, this process should continue actively along the product's lifecycle.

Evidently, it is not easy to recognise all safety and dependability related situations for many reasons. Various reasons include: poor coverage of analysis, learning of work skills is not ideal, modifications are done, or assembly errors occur. Therefore a continuous process for acquiring complementary and corrective information is useful.

The information systems used for managing RAMS documentation may differ drastically in customer's and vendor's organisations. Therefore, a common ontology for RAMS information should be defined in order to facilitate configuration and transfer of both the situational information and the safety and dependability information.

References

Amann, K., "PDM to PLM: Evolving to the Future", COE Newsnet, February 2004 [cited 16 April 2004] http://www.coe.org/newsnet/feb04/

Anon.01, "collaborative Product Definition management (cPDm): An Overview", A CIMdata Report, 2001, 46 p.

Anon.02, "Product Lifecycle Management", A CIMdata Report, 2002, 12 p.

Anon.04, "FI-TOOL - Management of safety and reliability knowledge during the lifetime of working machine" [on-line], VTT Technical Research Centre of Finland, Tampere, 2004 [cited 16 April 2004] http://www.vtt.fi/safety/topic1/fitool/indexe.htm

EN 50126, "Railway applications. The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)".

Horne, M.E., "Dassault Systems V5 - Not Just a CAD System", COE Newsnet, February 2004 [cited 16 April 2004] http://www.coe.org/newsnet/feb04/

Kivistö-Rahnasto, J., "Machine safety design. An approach fulfilling European safety requirements", VTT Publications 411, Espoo, 2000, 99 p.

Kuusisto, A., "Safety management systems. Audit tools and reliability of auditing", VTT Publications 428, Espoo, 2000, 174 p + app. 48 p.

Martio, A., "Web configured products and services", SoberIT, Helsinki University of Technology, 38 p. [cited 16 April 2004] http://www.soberit.hut.fi/ICTEC/lectures/20021015_Martio.pdf

Mattila, M., "Computer-aided ergonomics and safety - A challenge for integrated ergonomics", International Journal of Industrial Ergonomics, Vol.17, No.4, 1996, pp. 309-314

Norros, L., Kaasinen, E, Plomp, J. and Rämä, P., "Human-Technology Interaction Research and Design. VTT Roadmap", VTT Tiedotteita – Research Notes 2220, Espoo, 2003, 118 p. + app. 11 p.

Peltonen, H., Martio, A. and Sulonen, R., "PDM Product Data Management" [in Finnish], Edita Publishing Oy, 2002, 169 p.

Rasmussen, J., "Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering", North-Holland, Amsterdam, 1986, 215 p.

Reunanen, M., "Systematic safety considerations in product design", VTT Publications 145, Espoo, 1993, 124 p.

Reunanen, M., Scholliers, J., Säämänen, A., Viitaniemi, J. and Välisalo, T., "Improving Safety and Dependability by Enhancing the Availability of Product Specific Information", PSAM 7 – Proceedings of The 7th International Conference on Probabilistic Safety Assessment and Management, Cornelia Spitzer and Ulrich Schmocker, Springer-Verlag London Ltd. London, 2004. In press.

Vicente, K.J., "Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work", Mahwah, NJ, Lawrence Eribaum Associates, 1999, 392 p.

Warrington, L. & Jones,J.A., "A Business Model fo Reliability".Proceedings of Annual Reliability and Maintainability Symposium, 2003, pp.459-463.

Østerås, T., "Design for Reliability, Maintainability and Safety: Procedures and Methods for Conceptual Design" NTNU-rapport 1998:23, Trondheim , 216 p.