A Framework for Dependability Evaluation of Mechatronic Units

Hans-Dieter Kochs, Jörg Petersen

Institute of Information Technology
Faculty of Engineering
University of Duisburg-Essen, Germany

Abstract: Mechatronic units are characterized by a complex interaction of functions from mechanics, electronics, communication and computer systems. These different fields of technology as well as influences from the operating environment must be reflected in the dependability consideration, for which so far no comprehensive framework exists. In this contribution, a framework for consideration of dependability of mechatronic units starting from a definition of the term "dependability of mechatronic units" is proposed. Special attention is put on to the influence factors including human-machine interfaces, and real-world constraints, which thoroughly have to be identified and considered. Following questions have to be regarded: What is understood by the term dependability of mechatronic units? Which influencing factors have to be considered? How the dependability is assessed? This contribution also wants to initiate a scientific discussion outside the fault tolerance community.

1 Introduction

Asking experts from industry and universities, what they do understand by the term “dependability of mechatronic units” different and not comprehensive answers are given. This is not a surprise, since presently neither a uniform and consistent vocabulary nor appropriate methods and procedures for the consideration of dependability of mechatronic units exist. Responsible persons expressly stress the fact that a high dependability both in the design and in the operating phase is essential. Serious accidents in recent time underline the necessity for systematic and integrative considerations of dependability of mechatronic units.

In the past, cooperating individual units of the respective fields of technology were independently designed. Today, complex systems strongly integrate components of different fields of technology such as mechanics, electronics, sensors, actuators, embedded computer systems as well as distributed networking. In the opinion of the authors, separately regarded technologically different subsystems, which are up till now considered independently, must be analysed, designed, united, and optimised also at system level. So far, no uniform, integrating, and suitable framework for an extensive consideration of reliability and safety exists, which fairly meets real-world requirements.

In Germany there are numbers of standards and regulations for the reliability and safety of individual application domains, which reflect the domain specific state of the art. Also extensive literature as well as numerous conferences are concerned with new technological developments (see bibliography). These are usually concerned with special reliability and safety aspects within the individual areas or parts of systems (e.g. computer, software, hardware, communication networks), considered isolated within a larger application.

The term dependability was established by the fault tolerance community for computer systems with high reliability and safety requirements. Since this term describes reliability and safety related questions more comprehensively than the single terms reliability and safety do, the idea is to extend this term dependability to mechatronic components and systems.

2 A Definition of Dependability of Mechatronic Units

Definitions of the term dependability for computer systems with high reliability and safety requirements for example can be found in (Laprie 1991, Laprie 1995, Misra 1993, Pradhan 1995, Avizienis 2001). Definitions for reliability are also contained in technical rules and regulations (DIN 40041, DIN EN ISO 9000) and for safety in (DIN EN 292, DIN EN 1050, DIN EN 61508, DIN IEC 65A, DIN VDE 31000, VDI/VDE 2180, VDI/VDE 3542).

All these reliability and safety related definitions were usually introduced for individual fields of technology, for example real time computer systems, train systems, airplanes, power stations, crane systems, medicine-technical products, or machine tools. The definitions often date back to the years 1980 to 1990, in which new areas like the mechatronics and new technologies like the Internet and mobile telephones were still to a large extent unknown. With regard to the design, the operation, and maintenance of mechatronic units, the term dependability is defined as following based on and extending the well-known definitions:

> **Definition of dependability of mechatronic units**
>
> **Dependability of mechatronic units is defined as the qualitative and quantitative assessment of degree of performance of reliability and safety related predefinitions taking into consideration all relevant influencing factors (attributes).**

Through this definition, it will be expressed to what extent humans can rely on the considered unit. This will state how far the unit will behave in a demanded way taking into consideration all relevant influencing factors. Thus, all determining characteristics of the different technological fields of mechatronic units and the environment have to be considered and explicitly regarded.

3 A Framework of Dependability Consideration of Mechatronic Units

Fig. 1 shows the suggested framework. Based on the intention of the above definition, the activities (framed), their effect directions (arrows), and the results at the interfaces (dashed lines) are represented.

The thinly dashed drawn frame contains all substantial steps necessary for the definition of dependability. The result of dependability evaluation is given by the definition as "... the qualitative and quantitative assessment of degree of performance of reliability and safety related predefinitions taking into consideration all relevant influencing factors ...". The result manifests itself in the interface (c) in fig. 1. In each case, the dependability depends on the predefinitions[1] on the left side. The assessment[10] at the "output" (interface (c) in the fig. 1) always refers to the predefinition at the "input".

In the following, the points and aspects of 1 - 11 (upper indices in fig. 1) are described. Starting point for the consideration of dependability is a detailed technological and functional analysis and specification (also called system analysis) for the unit to be examined (interface (a)), which is the source and the initial point for the predefinitions and the determination of the relevant influencing factors.

The dependability of a unit must be assessed with reference to the reliability and safety related **predefinitions**[1]. These are described in the following points.

A consideration **unit**[2] should be understood as an abstraction unit with fixed boundaries e.g. a concrete construction unit, a device, a component, a plant or some part of it. In the unit, all influencing factors[7] (and thereby fields of technology) must be considered. The terms component and system are to be replaced by the general term unit. Depending upon the dependability task, a component as well as a system can be regarded as a unit.

The dependability evaluation always refers to a fixed **time period**[3]. This can range from some hours (transient dependability) up to the entire life time (stationary dependability).

The **reliability and safety related requirements**[4] are specified from the task, the problem to be solved, the analysis, and specification (interface (a)). They cover e.g. the functions of normal operation, required behaviour in the event of a failure, fail-silent-, fail-reliable-, or fail-safe-behaviour.

The qualitative and quantitative **criteria**[5] (for assessment of degree of performance of reliability and safety related requirements[4]) contain the characteristics and description forms, e.g. texts, visual representations, measurements, or metrics.

The (optional) **acceptance**[6] values contain e.g. to be kept limit values for dependability.

Also contractual definitions can have influence on the dependability e.g. guarantee, liability requirements, and contractual penalties since they can affect the draft of fault tolerance structures to a large extent.

The predefinitions 2 to 6 are usually necessary for the analysis of the influencing factors[7]. An analysis of these factors may result in a refinement of the predefinitions (fig.1) and can cause an iterative or recursive analysis process. This is indicated by the transition from 7 to 1 in fig. 1. The predefinitions are also necessary for modelling[8] (e.g. for the design of reliability block diagrams or fault trees), calculation[9], and assessment[10]. For this reason, the arrows arising from the predefinitions cannot be assigned directly to the inner blocks.

The **influencing factors**[7] summarize all the values, which have influence on the dependability of the unit. Reliability and safety related analysis of all relevant influencing factors - including their identification - is the most difficult task of a dependability evaluation.

The importance of the influencing factors is to be particularly referred in this contribution, since they reflect the influences of the technologies and the "real-world constraints" on the dependability, see section 4. The influencing factors can be evaluated qualitatively e.g. by text description, and quantitative e.g. by quantities, measurements, or metrics. The result of the analysis of the influencing factors is a reliability and safety related specification (interface (b) in the fig. 1), which forms a basis of the evaluation.

An essential task in dependability evaluation is **modelling**[8]. Models can be e.g. reliability block diagrams, fault trees, Markoff models, and Petri-Nets, or combination of these. The consideration of the influencing factors in appropriate models is a very difficult research task. Already modelling can reveal weak points (without calculation).

Several methods exist for **calculation**[9] e.g. the Boolean procedure, the minimal cut procedure, or the Markoff process. To what extent these methods are suitable for complex mechatronic systems requires further research work, too.

The **assessment**[10] has to rate the calculation results of the models according to the definition of dependability ("… degree of performance …"). The results must be documented properly.

During the steps modelling, calculation, and assessment, refinements of the steps prior may be necessary.

The framework does not make any statement, which instance (outside of the interface (c)) judges the decision (yes/no) of the fulfilment of the requirements.

The steps 8 - 10 document the "... the qualitative and quantitative assessment of degree of performance of reliability and safety related predefinitions taking into consideration all relevant influencing factors ..." according to the definitions.

Dependability-referred design[11] is the removal of weak points e.g. by use of other technologies, or the design of fault tolerance structures concerning reliability or safety. The consideration of dependability can supply both identification of the weak points and a statement about the dependability gain of the fault tolerance procedure.

The framework does not describe a strong waterfall like concept, which will straightly go "top down", but contains flexibility being necessary for an iterative or recursive refinement process.

4 Influencing Factors (Attributes)

Because of the impact of the influencing factors on the dependability of mechatronic units, some more details on these are given in this section. A unit is not dependable if at least one important influencing factor is neglected (e.g. Kochs 2001). For mechatronic units a sample of influencing factors is listed in the figs. 2 and 3. The detection of important influencing factors is a difficult task that require a comprehensive knowledge of the unit and its environment (real-world constraints). Depending upon application domain and taking into account new technology developments, in particular the influencing factors in the figs. 2 and 3 must be modifiable and extensible in the sense of a construction kit.

For example, a high dependability of a X-by-wire-system can only be attained by comprehensive dependability analyses which consider mechanics, hydraulics, sensors, actuators, and information and communication technology in an integrative approach.

The dependability analyses should be reproducible and transparent at any time. This will be especially important for the acceptance of such new systems. To what extent the existing methods and procedures can be used, extended, and combined, or new ones have to be developed, is regarded relevant for research.

Particularly, the internal and external influencing factors, e.g. dependencies in the fault and failure chain or environmental influences, usually have crucial influence on the reliability (including availability) and safety of a system. Humans in the operating chain can prevent faults (e.g. by prudent and experience-based ways of acting) and unintentionally produce faults. Human mistakes are in many cases jointly responsible for failures, accidents, and disasters. For example, the airplane and train disasters in recent years are always attributed to an "unfortunate chain of events" - according to the official reports. This is - in plain text - a chain of dependent failures (possibly from different fields of technology), including mistakes and actions produced by humans. These influencing factors are often considered rudimentarily or are even neglected.

A comprehensive viewpoint of dependability includes the necessity that a system should be submitted to a theoretical and practical dependability check in certain time intervals (e.g. for airplanes like Concorde, cable cars, high-speed trains, nuclear power plants), in order to detect safety risks.

For all aspects of dependability, so far a high attention has been dedicated to the development of mathematical procedures (calculation[9], in fig. 1). There seems to be a less lack of calculation procedures but a need for considering relevant influencing factors in modelling[8]. More precise, the man-machine interaction, and the internal as well as the external influencing factors considerably determine the dependability. Pure theoretically determined results can lead to absurd results if e.g. common-mode failures (dependent failures), mistakes by humans, or incorrect maintenance are ignored. Unfortunately, the analysis of accidents and damages certifies this again and again. Therefore, a substantially higher priority has to be dedicated to these aspects.

Because system sizes, complexities, and costs will increase, a trend can be observed to increase dependability during practical operation and maintenance phases (this today is usually the way regarding mass software). Examples for this trend in mechatronic units are the accumulating recall actions of the automobile industry or the ICE3 (FAZ 2003, a, b).

A future approach for complex mechatronic systems could therefore be to equip units with a kind of basis dependability (fix part) and to extend dependability (variable part) during operation or maintenance phases, assumed the system concept would permit this. To this topic, no general applicable research work is known yet.

5 Example

The proposed definition of dependability, which led to the development of the suggested framework for dependability of mechatronic units, originate to a large extent from an investigated example system (heavy load manipulator) of the DFG SFB 291 as well as from the experience with the computation of the reliability of large control systems. The dependability consideration of the heavy load manipulator is described in (Kochs 2002).

Under all aspects of the dependability of mechatronic units, high attention must be dedicated to the cooperating different technologies. Usually, this results in complex dependability networks, in which the (logical) states from units of different technological fields (sub-units) are "meshed", thus, they cannot be considered separately according to the fields of technology. An example of this is the dependability block diagram of the investigated unit "arm segment system of a heavy load manipulator", a concept study of a 5-link mechatronic subsystem represented in fig 4. Without going into detail, the block diagram impressively shows the meshing of the three fields of technology (mechanics, electronics and information and communication technology including computers). Particularly this is outlined by the example of the minimal cut thickly framed (failure of electronics E_4 and the mechanics M_3).

An advanced modelling and computation of all significant minimal cuts, including the consideration of faulty operations by humans, the operational and special influencing factors are described in (Kochs 2002).

As state of the art, no methods are known admitting the dissolving of these meshed networks in order to separately model and computate the individual technological areas.

6 Conclusion

The dependability of a mechatronic unit always is referred to the predefinitions taking into consideration all relevant influencing factors (attributes). They have to be analysed carefully and as completely as possible, since dependability mainly depends on these attributes. The proposed definition of dependability of mechatronic units leads to extensive consequences according to modelling, calculation, and assessment. The different technological areas e.g. mechanics, hydraulics, electronics, sensors, actors, information, communication, and computer technology, and last but not least the human-machine interaction are ”meshed“ in a complex manner resulting from their functional cooperation.

An integrated evaluation is proposed, whereby the decomposition of complexity will not be performed on the technological level, but on the level of dependability methodology. A decomposition of complexity at technological levels with separate dependability analysis in principle is questionable.

The procedure of dependability evaluation should be systematic, transparent, reproducible, extensible, and computer-aided for the wide area of different fields of technology. Extensive research and development activities are necessary with respect to different kinds of application domains. The results should be incorporated into regulations, rules, and guidelines. At the address of the industry, dependability assessments are not ”add-ons“, and not free of charge!

As a consequence of shorter and shorter development time, decreasing technological cycles, and always stronger competition, it should be thought about the possibility, to provide complex products with a special kind of basis dependability (fix part of dependability) and an extension of dependability during maintenance and operation phases (variable part of dependability), for which the unit has to be designed and prepared at early stages of the development process.

Bibliography

A selection of references is given characterizing the evolution from the terms reliability and safety towards the dependability of units. In the area of mechatronic dependability only relatively few publications, and particularly application examples exist.

Selection of regulations and standard guidelines in Germany

BA 1988. *Sicherheitsklassen - Vergleich von Sicherheitsanforderungen in Mechanik, Hydraulik, Pneumatik, Elektrotechnik und Elektronik.* Bundesanstalt für Arbeitsschutz Dortmund, Berlin, Forschungsbericht Fb 543. ISBN 3-88 314-782-6.

BAUA 2000. *Betriebsbewährung von Hard- und Software beim Einsatz von Rechnern und ähnlichen Systemen für Sicherheitsaufgaben.* Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dortmund, Berlin. Forschungsbericht Fb 888. ISBN 3-89701-542-0.

DIN 6789 1990-9. *Dokumentationssystematik:*
Teil 1: *Aufbau Technischer Produktdokumentationen.*
Teil 2: *Dokumentationssätze Technischer Produktdokumentationen.*
Teil 3: *Änderungen von Dokumenten und Gegenständen, Allgemeine Anforderungen.* Beuth-Verlag, Berlin.

DIN 25424, Teil 2, 1990-4. *Fehlerbaumanalyse: Handrechenverfahren zur Auswertung eines Fehlerbaumes.* Beuth-Verlag, Berlin.

DIN 25448 1990. **(IEC 60812)**. *Ausfalleffektanalyse (Fehler-Möglichkeits- und Einfluss-Analyse*). Beuth-Verlag, Berlin.

DIN 31051 1985. *Instandhaltung; Begriffe und Maßnahmen.* Beuth-Verlag, Berlin.

DIN 31052 1981-6. *Instandhaltung: Inhalt und Aufbau von Instandhaltungsanleitungen.* Beuth-Verlag, Berlin.

DIN 40041 1990-12. *Zuverlässigkeit - Begriffe*. Beuth-Verlag, Berlin.

DIN EN 292-2 2000. (Entwurf). *Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze* (identisch mit ISO/DIS 12100-2). Überarbeitung von EN 292-2: 1991 und EN 292-2: 1991/A1: 1995. Beuth-Verlag, Berlin.

DIN EN 1050 1996. *Sicherheit von Maschinen - Leitsätze zur Risikobeurteilung, DIN EN 1050.* (Ausgabe 1997-01) Beuth-Verlag, Berlin.

DIN EN 61078 1996. **(IEC 61078)**. *Techniken für die Analyse der Zuverlässigkeit - Verfahren mit Zuverlässigkeitsblockdiagramm.* Beuth-Verlag, Berlin.

DIN EN 61508 (Veröffentlichung durch die DKE in Vorbereitung). *Funktionale Sicherheit - Sicherheitssysteme (E/E/PES)*. Diese Norm ersetzt die nationalen Normen DIN V VDE 0801 (VDE 0801), DIN V 19250 und DIN V 19251. Die DKE beabsichtigt, diese Normen zurückzuziehen.

DIN EN ISO 9000 - 4 2000. *Normen zum Qualitätsmanagement und zur Darlegung von Qualitätsmanagementsystemen. Leitfaden zum Management von Zuverlässigkeitsprogrammen.* Beuth-Verlag, Berlin.

DIN IEC 65A 1996. *Funktionale Sicherheit, Sicherheitssysteme, DIN IEC 65A/183, 184/CDV (VDE 0801 T5, T6)*. Beuth-Verlag, Berlin.

DIN IEC 706, Teil 1, 1986-12. *Leitfaden zur Instandhaltbarkeit von Geräten.* Beuth-Verlag, Berlin.

DIN IEC 61025 1993. **(IEC 61025)**. *Störungsbaumanalyse.* Beuth-Verlag, Berlin.

DIN IEC 61070 1992. **(IEC 61070)**. *Prüfverfahren zum Nachweis einer stationären Verfügbarkeit.* Beuth-Verlag, Berlin.

DIN VDE 31000, Teil 2, 1987-12. *Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse - Begriffe der Sicherheitstechnik - Grundbegriffe.* Beuth-Verlag, Berlin.

VDI/VDE 2180, Blatt 1, 1998. *Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) - Einführung, Begriffe, Erklärungen.* Beuth-Verlag, Berlin.

VDI/VDE 2180, Blatt 4, 1998. *Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) - Berechnungsmethoden für Zuverlässigkeitskenngrößen von PLT-Schutzeinrichtungen.* Beuth-Verlag, Berlin.

VDI/VDE 3542, Blätter 1 - 4, 2000. *Sicherheitstechnische Begriffe für Automatisierungssysteme.* Beuth-Verlag, Berlin.

VDI 4001, Blatt 2, 1986. *Begriffsbestimmungen zum Gebrauch des VDI-Handbuches Technische Zuverlässigkeit.* Beuth-Verlag, Berlin.

VDI 4002, Blatt 1, 1986. *Systemtechnische Grundlagen; Erläuterungen zum Problem der Zuverlässigkeit technischer Erzeugnisse und/oder Systeme.* Beuth-Verlag, Berlin.

VDI 4003, Blätter 1 - 5, 1983 - 1986. Die Blätter beinhalten die Anwendung zuverlässigkeitsbezogener Programme und allgemeine Forderungen an ein Sicherungsprogramm, Klasse A. Beuth-Verlag, Berlin.

VDI 4004, Blätter 1 - 4, 1986. Die Blätter beinhalten Zuverlässigkeits-, Überlebens-, Instandhaltungs- und Verfügbarkeitskenngrößen. Beuth-Verlag, Berlin.

VDI 4005, Blätter 1 - 5, 1981 - 1983. Die Blätter beinhalten Einflüsse von Umweltbedingungen (mechanische, thermisch-klimatische, chemisch-biologische und elektromagnetische) auf die Zuverlässigkeit technischer Erzeugnisse. Beuth-Verlag, Berlin.

VDI 4006, Blätter 1 und 2, 1999 - 2002. Die Blätter beinhalten menschliche Zuverlässigkeit (Ergonomie und quantitative Bewertung). Beuth-Verlag, Berlin.

VDI 4008, Blätter 1 - 8, 1984 - 1999. Die Blätter 1 bis 9 enthalten Voraussetzungen und Verfahren für Zuverlässigkeitsanalysen. Beuth-Verlag, Berlin.

Selection of publications and reports concerning reliability and safety

Avizienis, A., Laprie, J. C., Randell, B. 2001. *Fundamental Concepts of Dependability.* UCLA CSD Report no. 010028.

Billinton, R., Allan, R. N. 1992. *Reliability Evaluation of Engineering Systems: Concepts and Techniques.* Plenum Press, London, New York.

Birolini, A. 1994. *Quality and Reliability of Technical Systems.* Springer-Verlag, Berlin.

Bubb, H. 1992.*Menschliche:* Zuverlässigkeit, Definitionen, Zusammenhänge, Bewertung. ecomed, Landsberg/Lech.

Dhillon, B. S. 1991. *Robot Reliability and Safety.* Springer-Verlag, Berlin.

Echtle. K. 1990. *Fehlertoleranzverfahren.* Springer-Verlag, Berlin.

Frankfurter Allgemeine Zeitung (FAZ). 2003 a. *Weißer Zug, grüne Banane und Schwarzer Peter - Die Pannenserie des ICE3 zeigt: Das Zusammenspiel von Bahn und Industrie ist verbesserungsfähig.* 04.03.2003, S. T1.

Frankfurter Allgemeine Zeitung (FAZ). 2003 b. *Elektronik macht Autos anfälliger.* Ausgabe 06.05.2003, Seite T3.

Görke, **W.** 1990. *Zuverlässigkeitsprobleme elektronischer Geräte.* BI-Hochschulskripte. Bibliographisches Institut, Mannheim (1969, überarbeitete Version 1990).

Kochs, H.-D. 1984. *Zuverlässigkeit elektrotechnischer Anlagen.* Springer-Verlag, Berlin.

Kochs, H.-D., Hilmer, H., Nisbach, T. 1999. *Efficient Approximate Reliability Evaluation using the Markovian Minimal Cut Approach.* Journal of Universal Computer Science. 10/1999, Springer-Verlag, Berlin, (http://www.jucs.org/), pp. 644-667.

Kochs, H.-D. 2001. *Schwachstellenanalyse am Beispiel der Concorde.* Automatisierungstechnische Praxis atp, 10/2001, S. 38 - 43.

Laprie, J. C. 1995. *Dependability - Its Attributes, Impairments and Means in Predictability Dependable Computing Systems.* B. Randell, J. C. Laprie, H. Kopetz and B. Littlewood Ed., Springer-Verlag, Berlin.

Laprie, J. C. (Ed.) 1991. *Dependability: Basic Concepts and Associated Terminology.* Springer-Verlag, Berlin.

Littlewood, B., Strigini, L. 2000. *Software Reliability and Dependability: a Roadmap.* 22nd International Conference on Software Engineering (ICSE).

Messerschmidt-Bölkow-Blohm (Ed.) 1986. *Technische Zuverlässigkeit.* Springer-Verlag, Berlin.

MIL-HDBK-217F 1990. *Reliability Prediction of Electronic Equipment.* Department of Defense, Washington. D. C.

Misra, K.B. 1993. *New Trends in System Reliability Evaluation.* Elsevier, Amsterdam.

NPRD95 1995. *Nonelectronic Parts Reliability Data Book.* IIT Research Institute / Reliability Analysis Center, 201 Mill Street, Rome, New York 13440-6916.

Pham, H. (Ed.) 2003. *Handbook of Reliability Engineering.* Springer-Verlag, London.

Peters, O. H., Meyna, A. 1985. *Handbuch der Sicherheitstechnik.* Band 1 und 2. Carl Hanser Verlag, München.

Pradhan, Dhiraj K. 1995. *Fault-tolerant Computer System Design.* Prentice Hall PTR, New Jersey.

Schneeweiss, W. 1999. *The Fault Tree Method.* LiLoLe-Verlag GmbH, Hagen.

Schneeweiss, W. 2001. *Reliability Modeling.* LiLoLe-Verlag GmbH, Hagen.

Swain, A.D., Guttman H. E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* NUREG/CR-1278, Sandia Laboratories, Albuquereque.

Zhang, T., Horigome, M. 2001. *Availability and Reliability of System with Dependent Components and Time-Varying Failure and Repair Rates.* IEEE Transactions on Reliability, pp. 1151-158.

Selection of publications and reports concernig dependability of mechatronic systems

DFG-Sonderforschungsbereich (SFB) 291 2001. *Elastische Handhabungssysteme für schwere Lasten in komplexen Operationsbereichen.* SFB-Abschlussbericht, Duisburg.

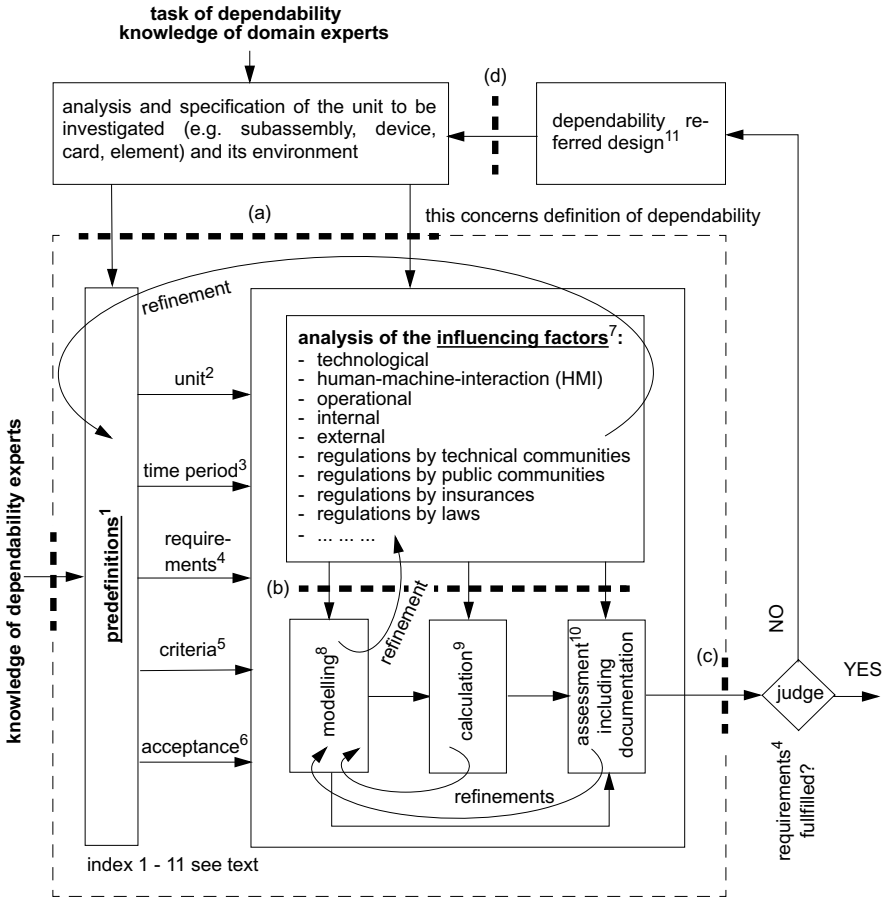
Kochs, H.-D. 1998. *Mechatronic System Dependability - New Discipline or Old Fashion?* FTCS-28: 28th Annual International Symposium on Fault-Tolerant Computing, München. pp. 298.

Kochs, H.-D. 2002. *Mechatronic System Dependability Analysis - An Application Example. International Conference on Architecture of Computing Systems ARCS 2002.* Workshop Proceedings. Karlsruhe. pp. 55-65.

McLaughlin Harpel, B., Bechta Dugan, J., Walker, I. D., Cavallaro, J. R. 1997. *Analysis of Robots for Hazardous Environments.* IEEE Annual Reliability and Maintainability Symposium, pp. 111-116.

Tähemaa, T., Reedik, V. 2000. *On Reliability Dimension in Product Development of Mechatronic systems.* Third International Symposium on Tools and Methods of Competitive Engineering (TMCE 2000), pp. 197-202.

Yang, W. 2003. *Mechatronic Reliability.* Springer-Verlag, Berlin - Tokyo.



interface results:

(a) technological specification (concerning the influencing factors (attributes) and predefinitions)
(b) reliability and safety related specification (considering the predefinitions[1] and influencing factors[7])
(c) assessment of the dependability evaluation (results)[9]
(d) design of fault-tolerance structures

Figure 1: Framework of dependability evaluation of mechatronic units.

- **mechanics (inclusive e.g. hydraulics, pneumatics)**
  - subsystem structure[12]
  - time response and system behaviour
  - breaking strength, tightness (e.g. hydraulics)
  - kinematic redundancy (e.g. for manipulators, robots)
  - safety/protection areas
  - wearout, deterioration
  - ...

- **electronics**
  - subsystem structure[12]
  - time response and system behaviour
  - electromagnetic compatibility (EMC)
  - mechanical and climatic influence
  - wearout, deterioration (e.g. of integrated circuits)
  - ...

- **informatics/computer science**
  - software and hardware architecture[12]
  - time response and system behaviour
  - performance
  - data integrity
  - ...

- **communication**
  - network architecture[12]
  - time response and system behaviour
  - data confidentiality, authenticity, security, commitment
  - ...

Figure 2: Technological influencing factors (attributes) of figure 1 - Part 1.

The structure/architecture of the specific technological areas, indicated by 12, may include local fault-tolerance structures (e.g. fail-operational and fail-safe structures). Global fault-tolerance structures cover several technological areas and are considered as structural features of the unit itself.

- **human-machine-interaction (HMI)**
  - operability/serviceability[12]
  - failure of handling, wrong decision, fast/poor reaction
  - ...

- **operational**
  - supervision and control
  - failure management, e.g. failure detection, diagnoses, and avoidance
  - maintenance, e.g. inspection, repair, updates
  - logistics, e.g. spare, and wear parts
  - documentation, education, training
  - ...

- **internal (intra-unit factors - inherent influencing factors)**
  - failure (e.g. fault, outage, error) of parts of the unit
  - dependent failure between parts inside the unit, e.g. common mode failure, consecutive failure
  - shut-down of parts of the unit (e.g. for protection areas)
  - ...

- **external (from outside the unit - real-world-influencing factors)**
  - climatic influence, e.g. temperature, humidity, water
  - phys. influence, e.g. vibration, overload, contamination
  - chemical influence, e.g. corrosion
  - „intelligent attacks", destruction
  - ...

- **regulations by technical communities - technical rules and regulations**
  - e.g. EN, IEEE, ISO, DIN, VDI, VDE, see bibliography
  - ...

- **regulations by public communities**
  - which specific limiting risks do the community accept, e.g. accidents and failures of nuclear power, public traffic, mobile telecommunication?
  - ...

- **regulations by insurances**
  - covered risk by insurance
  - product liability
  - ...

- **regulations by laws**
  - e.g. in public traffic, e.g. automatic controlled vehicles
  - ...

Figure 3: Influencing factors (attributes) of figure 1 - Part 2.

All these regulations may influence essentially the dependability design of a unit, e.g. fault-tolerance structure [11]

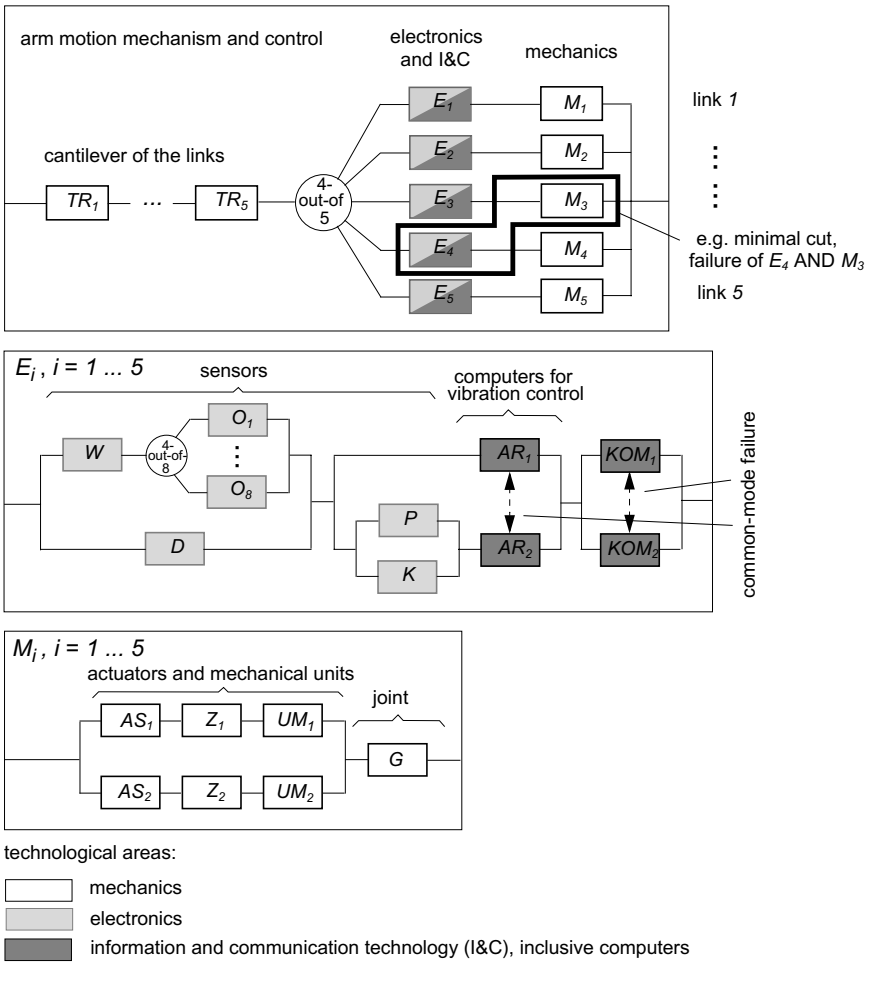


Figure 4: Dependability block diagram of the 5-link system and their subsystems as an example of a mechatronic unit (Kochs, H.-D. 2002).