Söffker, D.; Krajcin, I.; Wolters, K.: Fault tolerant design and improved availability of active composite elastic structures. Proc. 12th SPIE Symposium on Smart Structures and Materials, March 6-10, 2005, San Diego, CA, USA.

Fault Tolerant Design and Improved Availability of Active Composite Elastic Structures

Söffker, D., Krajcin, I. and Wolters, K.

University Duisburg-Essen, Chair of Dynamics and Control, Lotharstr. 1, 47057 Duisburg, Germany;

ABSTRACT

New functionalities, higher comfort and increasing performance requirements are often be solved by adding new technologies to existing (passive) solutions. Monitoring and control approaches uses additional sensors and actuators, new materials, microprocessors and new devices realizing new and improved functionalities. Two effects are becoming more and more interesting:

i) the lifetime of new actuators/materials strongly depends on the usage-history,

ii) the functionality of the new composed systems depends on the functionality of all elements.

In the consequence, the availability of such new systems is decreased by the number of elements and depends strongly on the use. These effects are known and act against new developments improving performance behavior also in mechanical engineering, automotive systems etc. This will be also the case for multifunctional composite or compound systems and is actually within the focus of the Structural-Health-Monitoring (SHM)-community.

Concepts of reliability engineering are known and applied successfully to safety critical systems. Within this contribution a concept will be given to understand system performance as a combination of systems structural design, useful application of modern control and diagnosis approaches and the control of the operating parameters affecting the failure rate of operating systems. The innovation is

a) the combination of structural design (how to locate sensors/actuators; how to get safe sensor informations; how to ensure acting forces (by which actor)),

b) methods of analytical redundancy increasing systems availability for online-use,

c) an approach to monitor systems failure rate and affecting the control and/or operating systems to ensure stability and integral functionality of the whole system.

Briefly explained, the subject of the contribution is that the complex adaptronic system (plate, sensor, actuator, internal or external control realization) should be understood as a dynamical, fault tolerant, and variable-structure which realizes functionality, performance, availability and works safe. The contribution will illustrate the concept in general and uses the practical example given in the parallel contribution.[1] Core of the health monitoring concept is that changes by altering and also wear and usage are understood as effects leading to failure. The monitoring concept will use diagnostic approaches and a dynamical model of system changes realizing a complete diagnosis and supervision concept based on the model-based fault diagnosis illustrated in[1] and probability models about assumed life-time distributions of piezoelectric materials.

Based on a similar approach in,[2] here, the concept is illustrated for the experimental system and first results with this experimental system will be given.

Keywords: Flexible structures, model-based fault detection, structural-health-monitoring, reliability engineering

Further author information: (Send correspondence to Söffker, D.)
Söffker, D.: E-mail: soeffker@uni-dusiburg.de, Telephone: +49 (0)203 379 3429
Krajcin, I.: E-mail: krajcin@uni-duisburg.de, Telephone: +49 (0)203 379 3023
Wolters, K.: E-mail: wolters@uni-duisburg.de, Telephone: +49 (0)203 379 3422

1. INTRODUCTION

New functionalities, higher comfort and increasing performance requirements are often be solved by adding new technologies to existing (passive) solutions. Monitoring and control approaches uses additional sensors and actuators, new materials, microprocessors and new devices realizing new and improved functionalities. Two effects are becoming more and more interesting:

i) the lifetime of new actuators/materials strongly depends on the usage-history,

ii) the functionality of the new composed systems depends on the functionality of all elements.

In the consequence, the availability of such new systems is decreased by the number of elements and depends strongly on the use. These effects are known and act against new developments improving performance behavior also in mechanical engineering, automotive systems etc. This will be also the case for multifunctional composite or compound systems such as piezomaterials, magnetostrictive alloys or shot memory alloys and is actually within the focus of the Structural-Health-Monitoring (SHM)-community. This contribution explains a new and systematically structured methodological approach to avoid and eliminate failures in mechatronical systems in an integrated intelligent way and to achieve a desirable or required amount of utilization in compliance with a defined failure rate. The result is an enhancement of the dependability of such a system.

2. SYSTEM DESIGN APPROACHES

2.1. The Common Way

The common way illustrated in Figure 1 consists of a structural reliability analysis of the function design of a planned system. This analysis is accomplished with tools like the FMECA or the fault tree analysis. The result of these analysis may lead in a redesign of the system which is also analyzed in view of its dependability. At the end of this closed-loop process, an optimal reliable system appears. If faults still may occur, with which the cause can not be eliminated by a redesign, a module for fault diagnosis and isolation (FDI) is added to the system. The FDI module enables the detection of unwanted system behavior or system states and the classification of these detected characteristics to special faults. The FDI uses signal or modelbased methods to detect a fault. A modelbased approach, the PI-Observer is used in[1] to detect and localize a crack in a bean or plate structure. The displacement is simultaneously been measured by strain gauges and a laser sensor. Here the PI-Observer can be used once to detect if the signal of the strain gauge or the laser is faulty. By the use of probabilistic or geometric classification the faults are assigned to special categories of faults. Even modern methods from the field of Artificial Intelligence like Fuzzy-Logic or Neural Networks are used. If the possible fault is effecting the safety of the system or the users health (or effecting the usage, the comfort or other important properties of the system or other goods) a Limp-home-mode LHM module is added to the system. Its function is to supply a minimum functionality of the system in the case of faults and subsystem failures. Usually this is achieved by a kind of structural or functional redundancy. Also a reconfiguration of parts of the system is possible. At the end of these development process there is a system with the add-ons FDI and LHM. In the worst case, the add-ons are badly integrated in the structure and in the functionality context of the system. Even the dependability of the system including the add-ons is unknown and maybe worse than without the add-ons. The latter is comprehensible because every additional component in a system is a new source for faults and failures and may have new fault activating effects on its linked or adjacent components. And every additional component in a serial linked system reduces the system dependability.

2.2. The New Design

In Figure 2 the proposed new design strategy is illustrated and combines methods and procedures of structural reliability analysis, FDI and LHM techniques to achieve a system with optimal functional and spatial integrated components for FDI and LHM with high system dependability. The methods and procedures of FDI and LHM are integrated in the reliability analysis and the design review of the system. At the end a high integrated system with a small probability of failure can be achieved. Please note that this approach allows a dynamical change of the inner structure of the system including the equally important modules FDI and LHM. The system also

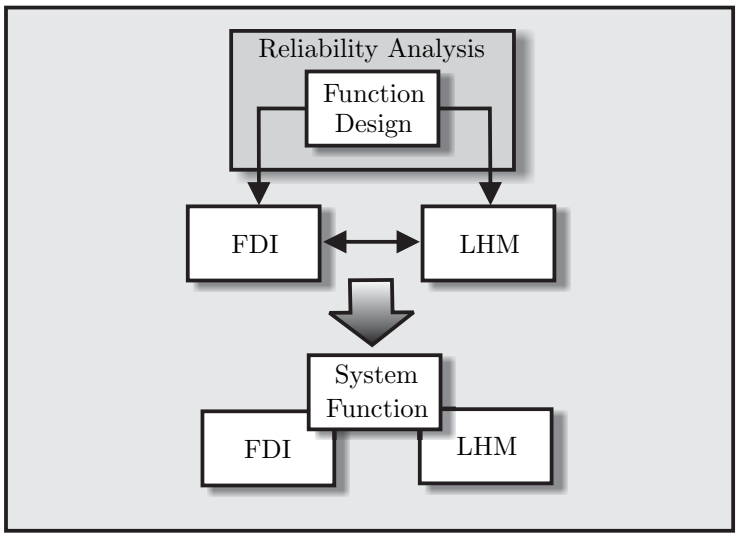

Figure 1. The common way to design systems

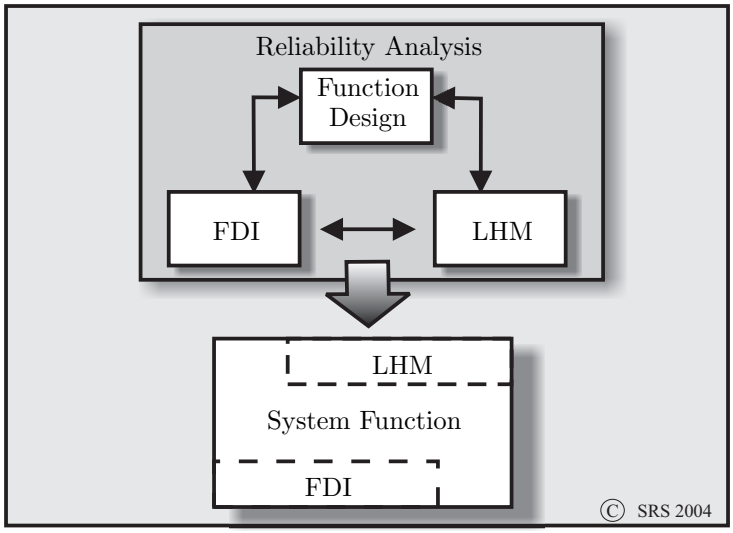

Figure 2. The new approach that includes the FDI and LHM ind the System Reliability Analysis

possesses restructuring abilities. Some criterions distinguishing the new approach from the classical one are given with Table 1. A minus indicates that the given criterion is not considered in the design method while a plus indicates that it is considered. It can be seen, that the new approach results to an optimal integrated system, in which the additional functionalities of the FDI and LHM modules are incorporated with minimum effect on the failure behavior of the whole system.

2.3. The Advanced New Design

The advanced new design includes the reliable integrated FDI and LHM to detect faults and to maintain a minimum of functionality for safety operations. Besides faults like faulty signals which can lead to a failure, system can fail by the consequences of its usages. Every usage is associated with a damage of the system. In this case, damage means any parameters that may lead to a failure if they are cumulated. This damage may result out of mechanical, thermal or electrical loads to the system. Usually the probability of failure increases

Table 1. Criterions to distinguish between the potential of the two given methods to design fault tolerant, reliable systems

Criteria	Common way	New approach
Fault tolerance	+	+
Fuctional integration of all modules	-	+
Spatial integration of all modules	-	+
Relaibility analysis of the system incl. all modules	-	+
Optimal Integration of FDI and LHM concerning system reliability	-	+

with proceeding usages, depending on the individual load history and the actual load of the system. The failure of the system occurs by fatigue or corrosion and it is a stochastic event. So the methods of FDI are not suitable to detect a failure due to usage conditions. The Safety and Reliability Concept (SRCE), already intorduced and explained in[3] deals with the calculation of a reliability characteristic depending on the actual load and the load history of a individual system. Furthermore a concept to prevent the system from stochastic failure is presented.

2.3.1. The SRCE-Concept

The Safety and Reliability Control Engineering Concept (SRCE), links the level of fault diagnosis to the operation management level to allow a controllable intervention. The concept enables a used, stressed technical system to run up to a specific life-time in compliance with a defined failure probability by controlling the increase of the failure probability. If the system is a safety-related system, it is indispensable and at the same time impossible to fully determine every failure mode or to test all possible behavior. The objective is to design and operate the system in such a way as to prevent dangerous failures. If dangerous failures may arise from random hardware failures that occur from different loads applied to the system, the SRCE-concept can also be used to calculate and to minimize the probability of these failures.

The concept can be divided into two main tasks:

1. The first task is to get relevant signals or parameters out of the components. This can be realized with methods of fault detection and isolation like virtual sensors (parameter estimation, observers) or sensing devices (signal-based methods).

2. The second task is to transform these into stress-oriented characteristics which are then to be used to obtain reliability characteristics. This can be done with empirical relationships, like mentioned in[4] which provide life models of the correlation between the load (in terms of voltage, temperature, moisture, stress etc.) and the maximum utilization.

Thus the resulting probability of failure is depending on the actual use of a component and the applied load history, in the case of piezomaterials the voltage. This probability of failure is therefore a quantity of the further possibility of a used component's utilization (Söffker 2000). The real system - illustrated in Figure 3 - is running under known operating parameters and has a defined, unknown real failure behavior. The SRCE-concept uses information about operating parameters and/or some measured or observed signals which indicate the applied load. The reliability characteristics are calculated and can directly be used in terms of monitoring, maintenance or supervision, or in a following step, in terms of control. This means, that the operating parameters (like the maximum voltage) are changed/modified to achieve a desired, minimized increase of the reliability characteristic. The result is that the utilization can be expanded beyond the maximum utilization of the system possibly with changed operating parameters. This can be achieved in compliance with a defined failure probability but with loss of performance.[2] The fault or damage diagnosis has to deliver information about a stress which is a unique physical consequence of the applied loads. An example of this diagnosis is described in.[5]

In Figure 5 the possible effect and the potential of the SRCE-control ist illustrated. Here the reliability characteristic is plotted over the accumulated utilization U. The reliability characteristic represents characteristics like the failure rate or the probability of failure, which should be as small as possible. The value RC_U describes a value at which an expected amount of utilization has to be achieved. It may be appropriate to have more than

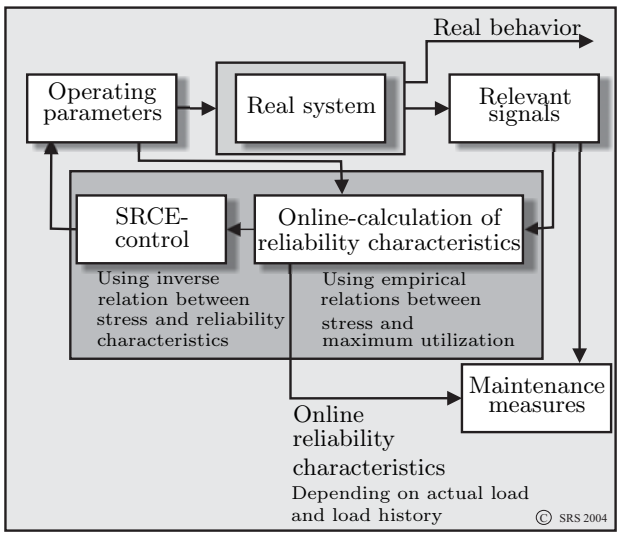

Figure 3. Structure of the SRCE-consept

one RC_U like $RC_{U_1} < RC_{U_2} < ... < RC_C$. The higher value RC_C represents a critical value of reliability characteristic at which a shutdown of the system has to be arranged. The dotted line represents the progression of the reliability characteristic as expected for the system. The solid line represents the actual reliability characteristic of the system depending on its stress history and its actual stress. At a certain reliability characteristic = RC_T the actual accumulated amount of utilization U_1 is compared with the expected amount U_2. If $U_1 < U_2$ with a certain level of tolerance, the operation parameters have to be changed to decrease the applied loads. Without any change and the assumption of a further development of the stress related to the past load development, the critical reliability characteristic = RC_C will be achieved with an amount of utilization U_{max_1}. This is indicated by the dash-dot line. The result would be that the expected operational end, defined by U_{max_2}, will not be achieved. If the effect of limited operating parameters and its resulting stresses to the reliability characteristic is known, then the change results in the development indicated by the solid line from U_1 to U_{max_2}, which has a smaller gradient than the dash-dot line. Hence the level of the maximum performance and load is limited by the value of the maximum reliability characteristic expressed by the solid line.

It is also possible to control the reliability characteristic. In Figure $RD_{T_1}, ..., RD_{T_4}$ indicate values of reliability characteristic which exceed a given threshold. At these points of utilization the load has to be changed in order to prevent an unacceptable growth of the reliability characteristic, indicated by the dash-dot lines. The threshold may be given by a trajectory of the reliability characteristic with a defined tolerance. The potential of this approach is the possibility to extend the maximum amount of utilization of the individual system and to control its probabilistic failure behavior by changing the operating parameters or mode.

From a more idealistic point of view, the advanced integrated approach leads to a system which shows reduced failure tendency, due to the fact that the SRCE-module is able to detect the failure (from a stochastic point of view) in advance, so the system theoretically is not able to fail (due to the emergency shut-down or reduced performance set by LHM module). In detail this means that system faults will be detected by the FDI and at least minimum operation will be guaranteed by the LHM while stochastic failures and failure due to deterioration will be avoided by monitoring the actual failure rate of the system and the system will stop operation before a critical point.

The Table 2 mentions some criterions to compare the three different approaches according to systemfailure and systemreliability.

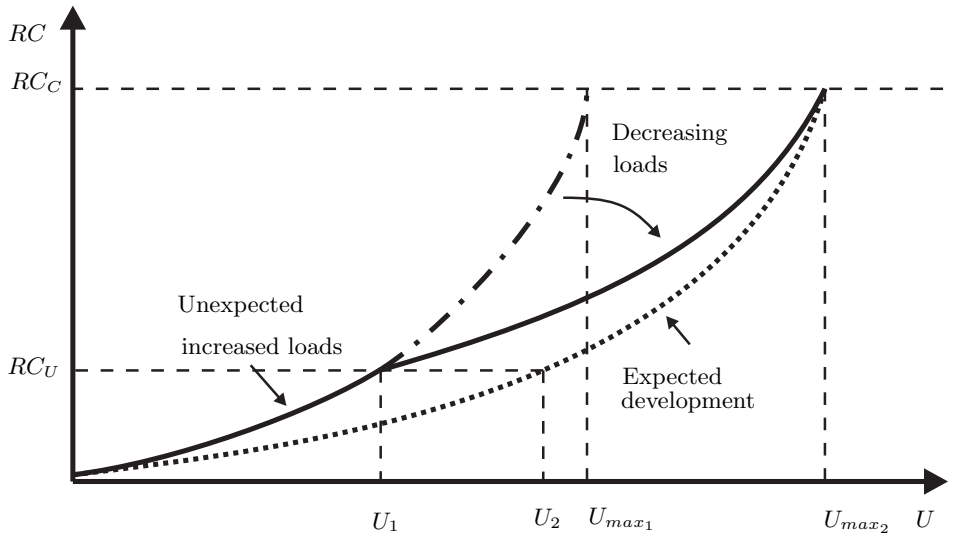

Figure 4. Illustration of the proposed approach

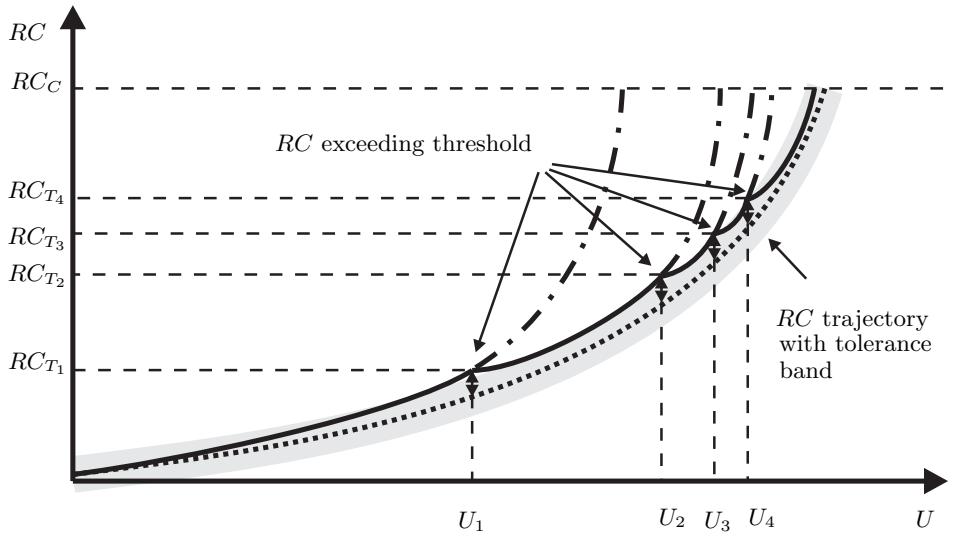

Figure 5. Illustration of the proposed approach

Table 2. Criterions to distinguish between the potential of the three given methods

Criteria	Common way	New approach	Advanced new approach
Fault tolerance	+	+	+
Functional integration of FDI and LHM	-	+	+
Spatial integration of FDI and LHM	-	+	+
Optimal Integration of FDI and LHM concerning system reliability	-	+	+
Prediction of probability of failure	-	-	+
Anticipate maximum utilization	-	-	+
Consideration of stachastic failures	-	-	+

2.4. CONCLUSION

The introduced new concepts present new ideas for designing complex systems in which FDI and LHM can be integrated in order to get high operational reliability. Modern technical systems depend more and more on FDI and LHM since the complexity of these systems increase the fault occurrence probability which require the monitoring of more system states to achieve the necessary system behavior. The implementation of these modules to the system may strongly reduce the appearance of failures but at the same time result in a decreasing dependability of the whole system. So both modules have to be integrated in the framework of system reliability analysis also during the lifetime of the system. Using virtual sensors yield to reconstruct nonmeasurable system states and in this way help to realize inside views into systems inner dynamics. These measurements can be used for FDI, to ensure redundancy for the sensors and contribute to realize reliability oriented approaches like the SRCE-concept. The SRCE-concept provides a probabilistic statement about the individual probability of system failure depending on the load history and actual usage of this system. This probability changes with changing operation parameters and thereby with changing loads. By monitoring this probability it is possible to anticipate the end of a systems durability and to stop operating before the system fails. So it is consequent to continue the new approach with SRCE-concept to achieve new quality of safe systems. This advanced new approach which is presented for the first time, may lead to a new design approach to design and run, to speak optimistically, failure free systems. In these systems faults will occur and even damaging processes will happen, but with the implementation of an intelligent faulttolerant FDI, combined with a LHM and the implementation of the SRCE-Concept no failure will stop the operation.

REFERENCES

1. I. Krajcin and D. Söffker, "Diagnosis and control of 3d elastic mechanical structures," (San Diegeo, California), 6- 10 March 2005. soon to be released.
2. K. Wolters and D. Söffker, "Improving systems availability by combining reliability and control engineering techniques," in *Structural Health Monitoring 2004*, C. Boller and W. J. Staszewski, eds., *Proceedings of the Second European Workshop*, pp. 711–720, 2004.
3. D. Söffker, "Online-determination of reliability characteristics as a modul of the SRCE-concept," *at* **48**(8), pp. 383–391, 2000.
4. L. Simoni, "A general phenomenological life model for insulating material under combined stresses," *IEEE Trans. on DEI* **6**, pp. 250–258, April 1999.
5. D. Söffker, "Robust fault detection of large vibrating structures by the means of control theory," in *Proc. 12th ASME Conference on Reliability, Stress Analysis and Failure Prevention*, H. Pusey, ed., pp. 751–762, (Virginia Beach), April 1997.