ACTA IMEKO
ISSN: 2221-870X
December 2022, Volume 11, Number 4, 1 - 6

How to stretch system reliability exploiting mission constraints: A practical roadmap for industries

Marco Mugnaini[1], Ada Fort[1]

[1] *University of Siena DIISM Department, Via Roma 56, Siena, Italy*

ABSTRACT
Reliability analysis can be committed to companies by customers willing to verify whether their products comply with the major international standards or simply to verify the design prior of market deployment. Nevertheless, these analyses may be required at the very preliminary stages of design or when the design is already in progress due to low organizational capabilities or simple delay in the project implementation process. The results sometime maybe be far from the market or customer target with a subsequent need to redesign the whole asset. Of course, not all the cases fall in the worst scenario and maybe with some additional consideration on mission definition it is possible to comply with the proposed reliability targets. In this paper the author will provide an overview on the approach which could be followed to achieve the reliability target even when the project is still on-going providing a practical case study.

Section: RESEARCH PAPER

Keywords: Reliability design; mission; reliability assessment; reliability enhancement

Citation: Marco Mugnaini, Ada Fort, How to stretch system reliability exploiting mission constraints: A practical roadmap for industries, Acta IMEKO, vol. 11, no. 4, article 17, December 2022, identifier: IMEKO-ACTA-11 (2022)-04-17

Section Editor: Francesco Lamonaca, University of Calabria, Italy

Received August 14, 2022; **In final form** November 19, 2022; **Published** December 2022

Corresponding author: Marco Mugnaini, e-mail: marco.mugnaini@unisi.it

1. INTRODUCTION

In the literature it is possible to find many examples discussing on advance re-search on reliability assessment and analysis. Most of these papers discuss on advanced methods for reliability allocation and improvement. Nevertheless, such methods are often lacking practical implementation and may result for actual implementation tricky or require a set of information not always available in practical cases. For example, in [1] the authors provide an approach based on Baysan analysis for parameter estimation presenting an interesting approach for process parameter evaluation which embeds a priori information to solve lack of data. In [2] the authors present a paper addressing reliability prediction modelling based on Kalman filtering applied to Ion batteries while in [3] AI approaches are used to solve reliability problems on Oil&Gas contexts. Other papers such as [4]-[5] describe general method for reliability assessment based on the most commonly used database such as MIL-HDBK-217F, OREDA or others, as function of temperature and environment. In some other papers, instead, there are fine analysis on predefined structures as in [6] where the advantages of different hardware solutions are compared with the aim to show how small changes on the practical implementation may lead to different results. Usually, such achievements are obtained by means of different architectures without comprising the implications of mission changes [6]-[12].

On practical basis, moreover, the systematic lack of confidence bounds in presenting results and the impossibility for companies to provide additional analytic description in addition to synthetic results like the over-used mean time to first failure or mean time between failures (MTTF, MTBF) to their evaluation make the transmission of information very difficult to direct customers or other realities [13]-[20].

The correct reliability design can be successfully approached by means of theoretical analysis if the design is followed since the very beginning phases of product development [20]-[21]. Unfortunately, especially in small companies where resources are very limited, the designers usually underestimate the reliability allocation problem demanding such analysis to a subsequent phase. In general, it is not easy to find in the literature a practical guide for companies which is able to embed both the theoretical and the actual application implications in a suitable way [22]. Some applications on the contrary, address the thrust of measurements without taking into consideration hardware and software reliability even in industrial contexts [23]-[25].

In this paper the authors would like to show on a practical way how implications on mission definition can be exploited for

reliability evaluations. In section I there's an introduction describing the critical aspects of reliability assessment and design com-pared to the present literature. In section II there's a description of the formal approach used in describing borderline conditions where predictions maybe far from desired results. In section III a case study about a general electronic board design is treated where it is possible to see how reliability targets which seems far from original design maybe matched just introducing considerations on mission profile. Finally in section IV the conclusions are discussed.

2. MODELS AND METHODS

Reliability design is always following well established rules from an academic standpoint. Starting from a problem definition and a mission description a design flow diagram and subsequent reliability block diagram can be approached and built. Nevertheless, the most complicated part of the reliability evaluation and function description is the choice of the proper failure rate or probability density function for the components describing the item to be designed. An easy and reasonable approach for companies is to rely on their a priori knowledge and build Bayesian based models. As an alternative companies may exploit internal or external database with the risk of selecting components with similar failure models but used in very different context resulting therefore in too conservative evaluations or completely wrong forecast. Another issue is the overall absence of confidence bounds in companies forecast which makes the result outcome useless.

Mission profile definition if one of the most critical things among the ones previously cited which make reliability forecast subject to interpretation. As it can be easily understood the same item used in a different environment or with a different time apportionment or duty cycle may have, as a final result, very different reliability prediction. On the other hand, mission definition is very often neglected as a powerful tool to stretch system, subsystem or item reliability tailoring the application to a more realistic scenario.

In Figure 1 there's the flow diagram of a commonly used approach in industry design concerning reliability aspects. This simplified version of the design is often considered in a generalized way which may lead to underestimates of specific important details.

Two important aspects should be underlined concerning the fact that not always field data are available on similar project mission profiles and databases maybe used in an unproper manner obtaining too conservative results or too optimistic forecasts.

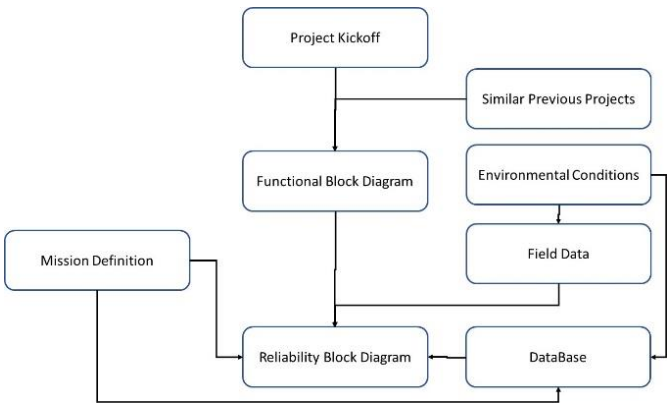

Figure 1. General flow diagram used in companied when designing a project to fulfil reliability requirements.

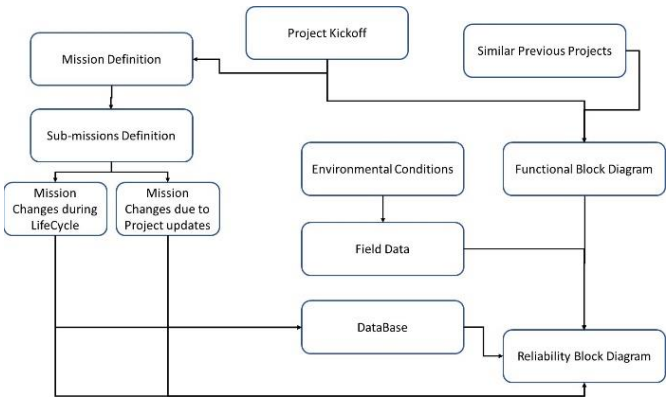

Figure 2. Project reliability definition embedding operative conditions and mission definition.

Mission definition is another aspect which is often not investigated properly with the limitation to provide a general mission description avoiding subdividing it in a set of several submission according to the whole lifecycle of the item which is to be designed. Figure 2 represent a more detailed view of this approach which should be taken into consideration by companies in the general development phase whenever reliability (and more in general reliability availability safety and maintainability RAMS) aspects are involved.

3. ABOUT ILLUSTRATIONS AND TABLES

Let's consider a system designed to drive some signaling infrastructure in the railway context. Such example nicely fits the scope of this paper from the moment that the safety and reliability requirements are so tight that not considering the mission profile could lead to several system further redesign.

In Figure 3 the general architecture composed by a power sartup system, a vital power source, a set of configuration memories a couple of microprocessors implementing the 2oo2 architecture an optional third CPU for managing external communication, a set of auxiliary electronics, a drive output system and a set of actuators is represented. Sample equations for specific components are available on reliability standards for discrete and semiconductors and they are in the general form as equation (1):

$$\lambda_c = \lambda_b \cdot \prod_{i=1}^{n} \Pi_i \,, \tag{1}$$

where λ_c is the overall failure rate, λ_b is the basic failure rate without any correction factor but the ones due to temperature, stress and inner model and Π_i are the corrective factors depending on the specific model characteristics, environment and quality.

The generalized form of the mission for this kind of general architecture *2oo2* for a signalling system can be summarized with the following sentence: "Being able to function safely for at least 40000 hours". Companies general approach is to try to design an architecture complying the safety integrity level (SIL) 4 safety standard (which is a must in such context) and the MTBF requirements as described above with a blind approach. Additional requirements may include the use of a specific

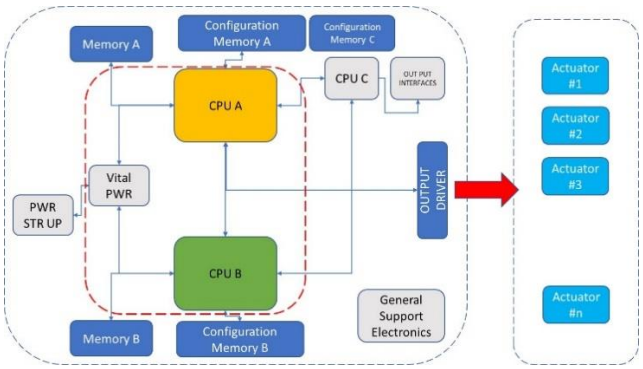

Figure 3. Sample rough electro-mechanical project of a system for railway applications with reliability and safety requirements to be interfaced with signaling system.

database for components failure rate which can be the MIL-HDBK-217F with the part stress approach.

Such new information lower our first estimation to the following MTBF (we are now neglecting the confidence bounds just to deliver the information on how such figure can be transformed changing slightly the scenario).

An additional consideration could be added embedding in the analysis the environment and the enclosure temperature which for such application in middle Europe can be standardized as 40 °C and Ground Fixed (according to the selected database).

If now the designers would like to move far from the preliminary design results of MTBF several options come into the field. Component with improved quality could be considered even if such information as a matter of fact is not described anywhere in any component datasheet. At least the Military Handbook classification cannot be easily found and therefore such approach requires an effort which is not selected from designers practically. As an alternative it is possible to evaluate for standard discrete components (especially capacitors or resistors) the derating factors which reduce most of time to just voltage ratio or pawer ratio. Again, this approach may result in a generalized one due to lack or resources and time considering the number of such components present in a huge electronic project like a signalling system for railway applications. A more effective option, which is often neglected by most designers, is the possibility to allocate to each subsystem composing the system a different mission profile or a different duty cycle. These two concepts are intrinsically embedded in the preliminary design phase as well as in the detailed one. Nevertheless, the possibility to match a better design exploiting such features is barely

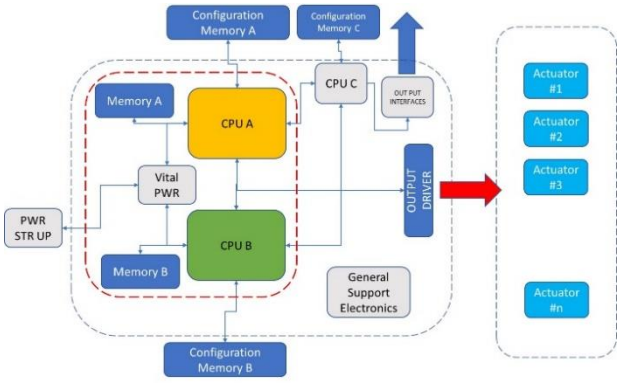

Figure 4. Reviewed functional block of the interfacing system for railway applications where mission contribution is included.

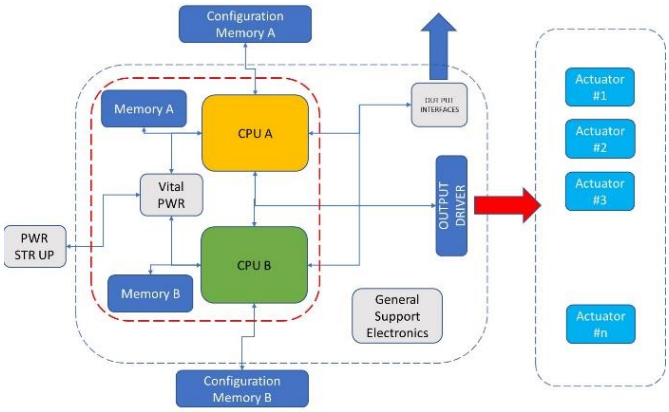

Figure 5. Reduced system design to minimize the impact of low duty cycle component on the original design improving the system reliability and not affecting the system architecture.

underestimated during assessment phase. Considering Figure 4, it is possible to see that the three configuration memories and the start up power unit have for sure a different mission with respect to the overall design and additionally for sure that may have a different duty cycle.

Once such considerations have been taken to the design if the target MTBF is still not achieved further improvement may pass through component reduction or alternative redundant configurations. If the first approach could be followed it would be preferred because these applications usually imply safety considerations as well. In Figure 5 an additional improvement due to a resizing of the CPU capabilities is shown. In such diagram the additional CPU C has been embedded in the others removing in this way the additional configuration memory and correspondent circuitry.

It is therefore possible to represent such units out of the original schematics and to modify the reliability block diagram (RBD) accordingly as shown in Figure 6.

Simulation results can be accomplished exploiting some commercial software. In this case Relyence part calculator has been exploited to compare different configurations outcomes. In Table 1 the system not comprising any mission impact on subsystem and exploiting MIL HDBK 217F database is considered and results shown. In Table 2 a mission consideration as well as power and voltage derating have been comprised in the evaluation. The configuration Memories as well as CPU C and some ancillary electronics have been used with 1 % duty cycle

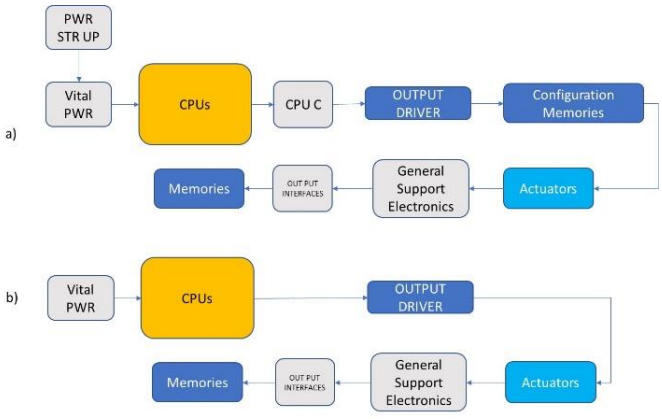

Figure 6. Comparison of the rough RBD of the original signalling interfacing system a) and the reduced one b) embedding consideration on the mission definition.

Table 1. Results of simulation not embedding mission impact on subsystem and exploiting MIL HDBK 217F database.

Name	Failure rate in f / (10^6 h)	MTBF in h	Failure rate in %
Main Board	18.708	53453.07	100.00
Configuration Memories	6.03	165837.5	32.23
CPU2oo2	2.204	453720.5	11.78
Clocks	0.574	1742160	3.07
ETH1	0.203	4926108	1.09
ETH2	0.203	4926108	1.09
Start Power Up	0.506	1976285	2.70
Gen Vit 2oo2	0.715	1398601	3.82
General Electronics	1.147	871839.6	6.13
CPU C	2.237	447027.3	11.96
Vital Power	1.884	530785.6	10.07
PWR Start Up	0.841	1189061	4.50
Actuator	2.164	462107.2	11.57

Table 2. Results of simulation embedding mission profile and duty cycle on subsystem and exploiting MIL HDBK 217F database.

Name	Failure rate in f / (10^6 h)	MTBF in h	Failure rate in %
Main Board	8.052	124192.75	100.00
Configuration Memories	0		0
CPU2oo2	0.575	1739130.4	7.15
Clocks	2.204	453720.51	27.37
ETH1	0.203	4926108.4	2.52
ETH2	0.203	4926108.4	2.52
Start Power Up	0		0
Gen Vit 2oo2	0.715	1398601.4	8.88
General Electronics	1.147	871839.58	14.24
CPU C	0		0
Vital Power	0	0	0
PWR Start Up	0.841	1189060.6	10.44
Actuator	2.164	462107.21	26.88

Table 3. Results of simulation embedding mission profile and duty cycle on subsystem and exploiting ANSI Vita database.

Name	Failure rate in f / (10^6 h)	MTBF in h	Failure rate in %
Main Board	4.816	207641.196	100.00
Configuration Memories	0	0	0
CPU2oo2	2.263	441891.295	46.99
Clocks	2.127	470145.745	44.17
ETH1	0.024	41666666.7	0.50
ETH2	0.024	41666666.7	0.50
Start Power Up	0		0
Gen Vit 2oo2	0.67	1492537.31	13.91
General Electronics	0.995	1005025.13	20.66
CPU C	0	0	0
Vital Power	0	0	0
PWR Start Up	0.099	10101010.1	2.06
Actuator	0.614	1628664.5	12.75

reflecting the actual use on a 24 h real timescale. These new considerations have brought to results shown in Table 2 where significant improvement on the overall MTBF have been achieved.

Table 4. Comparison of the MTBF and Failure Rates of the three improvements proposed in the analysis. Confidence bounds are 95 %.

Name	Failure rate in f / (10^6 h)	MTBF in h
Main Board ANSI VITA	4.815 748	207 652.05
Main Board MHDBK 217	8.052 190	124 189.81
Main Board MHDBK 217 NM	18.708 161	53 452.61

If the result is still not acceptable according to the design another approach could be to negotiate a new reference database. One of the most accepted one is the ANSI Vita one. In such database the components coming from the MIL HDBK 217F Have been actualized considering the advancement of the technology. For example, microcontroller which were not present in the previous version can be now considered as subset of microprocessors. The drawback is that this database is not an independent one and has been derived with the contribution of several companies. Results of this significant improvement are shown in Table 3.

Finally in Table 4 it is possible to compare the three different kind of results which can be obtained just applying these different deviations from a standard approach.

A final overview on the different kind of implementation depending on the environmental variation can be shown in Figure 7 and Figure 8. Three different environments ground benign, ground fixed and ground mobile (GB, GF and GM) are compared in such figures showing the different contributions in terms of failures per million hours (FPMH) depending on the environment selected and on the used database.

In Figure 7 the MIL HDBK 217F database has been exploited while in Figure 8 the ANSI Vita one has been used. It is important to highlight how differences in results are kept even in

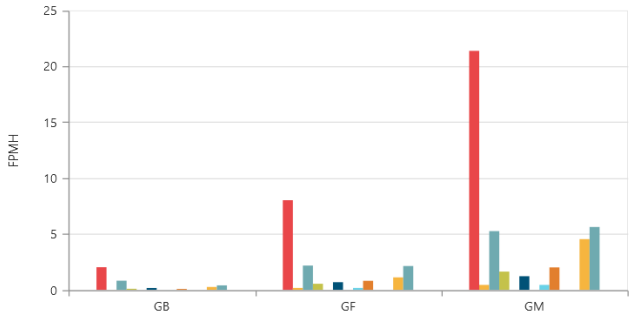

Figure 7. System behaviour under three different environment Ground Benign (GB), Ground Fixed (GF), Ground Mobile (GM) according to MIL HDBK 217F.

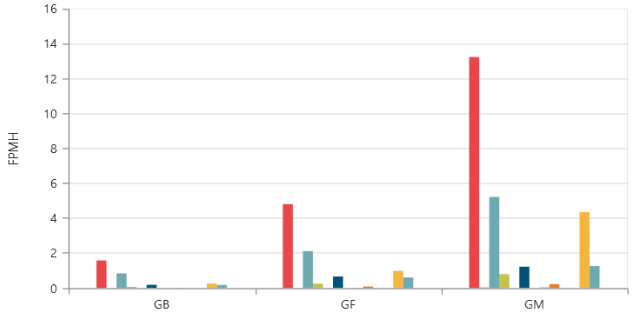

Figure 8. System behaviour under three different environment Ground Benign (GB), Ground Fixed (GF), Ground Mobile (GM) according to ANSI Vita.

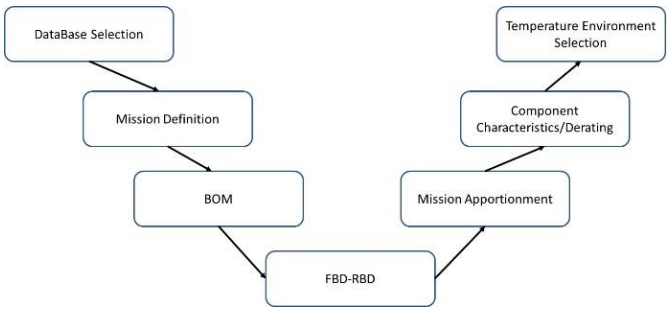

Figure 9. CAP General designers' roadmap to simplify reliability requirements achievements TION.

the changes of environment making this latter database more attractive for non-fully conservative and more modern approaches.

The process which should be followed in assessing reliability requirements after preliminary design should be the one described in Figure 9.

The first step consists in negotiating with the final customer the exploitable database from the moment that results are really affected by such choice. Then after the bill of materials (BOM) has been defined and the mission correctly described, it is crucial to identify which subsystem are subject to duty cycle modification. Components quality level even if important is not crucial especially if referred to MIL HDBK 217F from the moment that such information is difficult to be gathered from any commercial supplier. Temperature information instead is vital as well as operative environment due to the fact that great part of final analysis outcome depends on the. Once this step has been accomplished.

4. CONCLUSIONS

In this paper the author tried to analyze a recurring problem during design phases. Usually, the producers of electro-mechanical reliability assembly are more focused on general performance than on reliability verification. This approach inevitably implies a huge effort in final redesign and long negotiations with final customers due to the lack in the procedural design. The authors tied to highlight that sometimes no redesign is needed but a more precise and detailed description of the system mission may allow a redefinition of the reliability evaluation criteria. As a general concept these aspects should fall in the optimized and best practices of item design but as a matter of fact it may happen that due to the high volume or project complexity such aspects may be neglected. It has been shown on an actual example how by following some basic steps, as suggested in the manuscript, it is possible to minimize the impact of redesign and achieve satisfying results. This paper tries to fill a gap which is not described often in the literature because it has to deal with some peculiar aspect of the specific design but whose general rules can be applied almost in any engineering project. The analysis shows moreover the possibility to exploit different database which are not selected in common projects usually to the lack of information on their exploitability even when there are changes in the operating environment.

ACKNOWLEDGEMENT

This study has been conducted exploiting a research licence of Part analysis provided by Relyence Software.

REFERENCES

[1] M. Mugnaini, M. Catelani, G. Ceschini, A. Masi, F. Nocentini, Pseudo Time-Variant parameters in centrifugal compressor availability studies by means of Markov models, Microelectronics Reliability, vol. 42, 2002, pp. 1373-1376.
DOI: 10.1016/s0026-2714(02)00152-x

[2] Van-Trinh Hoang, N. Julien, P. Berruet, Design under constraints of availability and energy for sensor node in wireless sensor network, Conference on Design and Architectures for Signal and Image Processing (DASIP), Karlsruhe, Germany, 23-25 October 2012, pp. 1-8.

[3] S. B. Guedria, J.-F. Frigon, B. Sanso, An intelligent high availability AMC design, IEEE Radio and Wireless Symposium, Santa Clara, CA, USA, 15-18 January 2012, pp. 159-162.
DOI: 10.1109/RWS.2012.6175334

[4] Q. Weiwei, J. Jingshan, J. Yazhou, Research on the numerical control system reliability model using censored data, 16th Int. Conference on Industrial Engineering and Engineering Management (IE&EM '09), Beijing, China, 21-23 October 2009, pp. 1204 – 1207.
DOI: 10.1109/ICIEEM.2009.5344468

[5] K. Zhao, D. Steffey, Analysis of field performance using interval-censored incident data, Annual Reliability and Maintainability Symposium (RAMS), Fort Worth, TX, USA, 26-29 January 2009, pp. 43-46.
DOI: 10.1109/RAMS.2009.4914647

[6] T. Addabbo, A. Fort, M. Mugnaini, V.Vignoli, E. Simoni, M. Mancini, Availability and reliability modeling of multicore controlled UPS for datacenter applications, Reliability Engineering and System Safety 149, May 2016, pp. 56-62
DOI: 10.1016/j.ress.2015.12.010

[7] S. J. Briggs, M. Bartos, R. Arno, Reliability and availability assessment of electrical and mechanical systems, Thirtieth IAS Annual Meeting Industry Applications Conference IAS '95, Conference Record of the 1995 IEEE, vol. 3, pp. 2273 – 2281.
DOI: 10.1109/IAS.1995.530592

[8] G. Ceschini, M. Mugnaini, A. Masi, A reliability study for a submarine compression application, Microelectronics Reliability, vol. 42, September–November 2002, pp. 1377-1380.
DOI: 10.1016/s0026-2714(02)00153-1

[9] M. Catelani, M. Mugnaini, R. Singuaroli, Effects of test sequences on the degradation analysis in high speed connectors, Microelectronics Reliability, vol. 40, August–October 2000, p. 1461-1465.
DOI: 10.1016/S0026-2714(00)00150-5

[10] Chun Su, Jinyun Shen, A Novel Multi-hidden Semi-Markov Model for Degradation State Identification and Remaining Useful Life Estimation, Quality and Reliability Engineering International Journal, vol. 29, issue 8, 8 October 2012 pp. 1181-1192.
DOI: 10.1002/qre.1469

[11] D. Zamalieva, A. Yilmaz, T. Aldemir, Online scenario labeling using a hidden Markov model for assessment of nuclear plant state, Reliability Engineering and System Safety, vol. 110, February 2013, pp. 1-13.
DOI: 10.1016/j.ress.2012.09.002

[12] Diego Alejandro Tobon-Mejia, Kamal Medjaher, Noureddine Zerhouni, G. Tripot, A Data-Driven Failure Prognostics Method Based on Mixture of Gaussians Hidden Markov Models, IEEE Transaction on Reliability, vol. 61, issue 2, pp. 491-503.
DOI: 10.1109/TR.2012.2194177

[13] L. E. Baum, T. Petrie, Statistical inference for probabilistic functions of finite state Markov chains, Ann. Math. Stat., vol. 37, no. 6, December 1966, pp. 1554-1563.

[14] L. E. Baum, G. R. Sell, Growth functions for transformations on manifolds, Pacific J. Math., vol. 27, no. 2, 1968, pp. 211- 227.

[15] L. Rabiner, A Tutorial a tutorial on hidden Markov models and selected applications in speech recognition, Proc. of the IEEE, vol. 77, no. 2, February 1989
DOI: 10.1109/5.18626

[16] M. Bicego, C. Acosta-Munoz, M. Orozco-Alzate, Classification of Seismic Volcanic Signals Using Hidden-Markov-Model-Based, Generative Embeddings, IEEE transactions on geoscience and remote sensing, vol. 51, issue 6, June 2013, pp. 3400-3409. DOI: 10.1109/TGRS.2012.2220370

[17] A. Ben Salem, A. Muller, P. Weber, Dynamic Bayesian Networks in system reliability analysis, IFAC Proceedings Volumes, vol. 39, issue 13, 2006, pp. 444-449. DOI: 10.3182/20060829-4-CN-2909.00073

[18] P. Vrignat, M. Avila, F. Duculty, S. Aupetit, M. Slimane, F. Kratz, Maintenance policy: degradation laws versus Hidden Markov Model availability indicator, Proc. of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 226, issue 2, 2012, pp. 137-155. DOI: 10.1177/1748006X11406335

[19] Y. F. Li, R. Peng, Availability modeling and optimization of dynamic multi-state series-parallel systems with random reconfiguration, Reliability Engineering and System Safety, vol. 127, July 2014, pp. 47-57. DOI: 10.1016/j.ress.2014.03.005

[20] S. S. Rao, Reliability engineering Design, McGraw Hill.

[21] A. Birolini, Reliability Engineering: Theory and Practice, Springer 6th Edition 2010.

[22] A. Fort, F. Bertocci, M. Mugnaini, V. Vignoli V. Gaggii, A. Galasso, M. Pieralli, Availability Modeling of A Safe Communication System for Rolling Stock Applications, Proc. of the IEEE I2MTC2013 Conference, Minneapolis, MN, US, 06-09 May 2013, pp. 427-430. DOI: 10.1109/I2MTC.2013.6555453

[23] T. Addabbo, A. Fort, R. Biondi, S. Cioncolini, M. Mugnaini, S. Rocchi, V. Vignoli, Measurement of angular vibrations in rotating shafts: Effects of the measurement setup nonidealities, IEEE Transactions on Instrumentation and Measurement, 2013, 62(3), pp. 532–543. DOI: 10.1109/TIM.2012.2218691

[24] A. Lay-Ekuakille, S. Ikezawa, M. Mugnaini, R. Morello, C. De Capua, Detection of specific macro and micropollutants in air monitoring: Review of methods and techniques, Measurement, vol. 98, February 2017, pp. 49–59. DOI: 10.1016/j.measurement.2016.10.055

[25] T. Addabbo, A. Fort, M. Mugnaini, L. Parri, S. Parrino, A. Pozzebon, V. Vignoli, An IoT Framework for the Pervasive Monitoring of Chemical Emissions in Industrial Plants, Proc. of the Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy, 16-18 April 2018, pp. 269–273. DOI: 10.1109/METROI4.2018.8428325