SYSTEMATIC FAILURES IN FUNCTIONAL SAFETY AND THE PROBABILITY MEASURE

Hendrik Schäbe
•
dr.hendrik.schaebe@gmail.com

Abstract

In this paper the probability measure is discussed. The point of interest is, whether probabilistic models are stable under different conditions and if they can be used further on, when conditions change. Systematic failures, as described in many standards of functional safety, play a role regarding this problem. Reducing systematic failures also means, to keep probabilistic calculus working. However, systematic failures have not been studied systematically regarding the question to keep the probability measure. An outline is given on the connection between systematic failures and the possibility to use probability calculus in technical problems in exploitation situations, where data from e.g. lab experiments are extrapolated to use conditions.

Keywords: systematic failures, probability measure, standardization

I. Introduction

There are two main sources of knowledge for RAM (Reliability, availability and Maintainability) engineers. On the one hand side, there are textbooks on probability and statistics. There is a lot of them and here only a classic one authored by Mann, Schafer and Singpurwalla [1] shall be mentioned. Reading these books the impression is the following: Reliability and safety are in fact described by a sufficient low failure probability or probability of occurrence of a dangerous event, the latter in many cases being a failure of a safety system. All the probabilities can be derived for a system, using probabilities for subsystems, components and events.

On the other hand side, there exist standards on reliability and safety. Focusing on safety we see, that these standards [2-6] require, that there should be also measures against so called systematic failures. Then, the natural question arises, why these measures are necessary, if probability describes the behavior of a system sufficiently completely? When speaking about a system, one might address hardware and software separately as well.

In this paper, however, only hardware failures shall be considered, so the paper is dedicated to a discussion of the problem of systematic hardware failures and its connection to the use of probabilistic arguments.

In section two the use of probability in reliability and safety is described. The third section is dedicated to probability as such. A definition is provided and discussed. Some regularity conditions are derived and it is shown, that certain influences just can invalidate the application of probability calculus. In the following, fourth, section the concept of systematic failures is described and it is shown, which systematic failures need to be reduced, which might invalidate probability calculus. In the fifth section two examples are given: early failures and aging, which could violate the assumptions of an important probabilistic model, the exponential distribution.

A main instrument against systematic failures is hazard analysis, derivation of risk reducing measures and specification, including these measures. This is considered in section six. The last section provides conclusions.

II. Use of Probabilistic Methods in Reliability and Safety

A good overview of the use of probabilistic methods can be found in the book of Birolini [7]. The reliability is introduced as the "probability of an item to perform its required function under given conditions for a stated time interval." The definition provides a link to probability and a link to conditions, that this probability can be used. These are the "given conditions", which are not yet further specified. Then, a distribution function and a failure rate function are introduced, which depend on time. The failure rate function of a system is usually bathtub shaped.

Why is probability used in the context of reliability and safety? There are so many influences on a failure or a dangerous event, that cannot be described completely and this insecurity is then modeled by a probability, see e.g. the book of Härtler [8].

Almost all models in reliability and safety are probabilistic ones. Always, a probability of failure or a probability of occurrence of a dangerous event is computed using probability algebra. On the one hand side there exist sophisticated models in theory, alas engineers restrict themselves to much simpler models.

A very simple model is the use of the exponential distribution for times until failure or a dangerous event. For dangerous events, such a choice is logical, since dangerous events occur seldom and one might assume a Poisson process for them, resulting in exponentially distributed times until the occurrence of the event.

In reliability, the failure rate of a lifetime distribution is known to be bathtub shaped, starting with an early failures phase, followed by a phase of constant failure rate and finally, aging and wear cause leading to an increasing failure rate. Using the exponential distribution is a simplification assuming the absence of early failures and neglecting aging and wear – or assuming that this phase has not yet started. For details see e.g. Mann Schafer Singpurwalle [1] and Jensen [9]. A much better model is the Weibull distribution or even other, more complicated models. They are more flexible and can model also tendencies as early failures or wear and aging. However, either there exist insufficient data or the analyst simply did not think about those models.

So, most analysts are stuck with the exponential distribution and its parameter, the failure rate or event rate. The source for the parameter of the exponential distribution are either tables as the NPRD [10], standards with tables as EN 61709 [11], or the book of Proske [12] (to name some examples) or own statistics collected from life time experiments or observations.

These data have then to be adapted to other use cases, where it is assumed that the original conditions still hold. The latter is frequently done by simple engineering judgment. This is the point, where it becomes interesting: can one really assume that the probability distribution function of the time to failure or dangerous events is the same when using it also under another, new situation than the original one, i.e. the situation where statistics have been collected or the data from which the failure rate in the handbook has been computed?

III. Basics of Probability

Until now, probability has been only mentioned in a rather intuitive way. In this section it shall be explained, what probability is. In this paper, the axiomatic definition is used, that originates from Kolmogorov [14]. A good explanation can be found in Pollard [15]. For further reading, we refer to Braband and Schäbe [13].

Probability is a non-negative measure defined on a set, which becomes one for the entire set and which is additive for all disjunct subsets of the original set. It is also required to define a so-called sigma algebra, which defines how elements of the set have to be combined, so that finally, the sigma algebra contains all elements of the original set and combinations of them and combinations of elements of the sigma algebra.

So far, the probability has not yet any practical meaning. It is then interpreted as a limit of frequencies of events that are represented by elements of the sigma- algebra [15].

In case of symmetry, the probability can even be determined theoretically. Assume a dice with six sides, then caused by the symmetry we have

$$P(E_1) = P(E_2) = P(E_3) = P(E_4) = P(E_5) = P(E_6),$$

$$P(E_1) + P(E_2) + P(E_3) + P(E_4) + P(E_5) + P(E_6) = 1.$$

Here E_k denotes the event that the dice shows number k on its top when being thrown. Obviously, we have

$$P(E_k) = 1/6, \text{ for all } k = 1,\ldots, 6.$$

Another example for determination of a probability comes from thermodynamics, see Landau and Lifschitz [16]. If a thermodynamic system with many degrees of freedom is considered, then in the phase space, all points being on a hyper-sphere defined by conservation laws (energy and momentum) are considered equally probable. If the situation is not completely symmetric, then the distribution will change from a simple uniform distribution on the sigma algebra to another distribution function.

If, however, there are singularities, probabilistic laws will seize to be applicable. An example is a hacker attacking a system, see Braband and Schäbe [13]. Here, the concept of probability will fail in cybersecurity applications.

Another example would be the influence of high voltage from a railroad traction system. If a system is not able to withstand such an influence or it is not consequentially separated from high voltage, it would simply instantaneously fail and any probabilistic considerations derived from nice lab experiments will become obsolete. Here, again a simple strong influence factor will violate the symmetries that are necessary for the existence of a probabilistic law.

Another example is load. If the load on a mechanical system is different in a use case compared with lab conditions, the probability law will still exist, but this law will change. See for instance Schäbe and Viertl [17].

So, we have two principal problems when using probabilistic models. This holds especially, when we have gotten a result under one condition and we want to transfer it to another condition, which we would judge to be equivalent:

(A) One needs to make sure, that the concept of probability can be used. The conditions for the existence could be violated, since there would exist a singular influence leading to reactions that cannot be measured with a probability. Even if under certain conditions, under which failure rates have been obtained, a probability law existed, under some new conditions such a singular influence might occur and probability would fail to exist.

(B) One also needs to consider influences that will not violate the assumptions for a probability to exist, but that might change the probability measure itself. An example are loads.

These two goals (A) and (B) are important to achieve, if the same probability model shall further be used.

IV. Systematic Failures

When having a first glance at reliability and safety, one might get the impression that everything is described by probability and if once we have determined the parameters, we can use them in all situations. However, there occur also systematic failures. These are failures caused mainly by humans or by faulty processes, which are also set up and run by humans.

Consequently, the impression that simple probability calculations using data from the bookshelf would be sufficient, is misleading.

IEC 61508 [5] part 4 defines random and systematic failures as follows:

3.6.5: “a random hardware failure is a failure that occurs at a random point in time that is the result of one or more possible hardware degradation mechanisms”;

3.6.6: “a systematic failure is a failure deterministically associated with a certain cause that can only be eliminated by modifying the design or the process, operations, documentation, or other factors".

In this section and the following, only measures against systematic failures in safety are considered. This is caused by the fact, that for reliability there has not been systematic research on systematic failures and measures against them. Usually, systematic failures are simply neglected. We refer to Shubinski and Schäbe [18] for similarities between functional reliability and functional safety, explaining that measures against systematic failures in safety can be equivalently used in reliability.

According to Shubinski and Schäbe [19] , failures are distinguished according to the mechanism, which has caused them. The random hardware failure is related to aging and degradation processes. On the contrary, the systematic failure is related to errors in design processes etc. However, also these failures manifest themselves in a stochastic manner, when the failure mechanism is triggered, so they are only deterministic in the sense that one certain well—defined cause can be indicated [20]. This cause occurs in a random manner, so the time of occurrence is random. This randomness is caused by the environment which causes a random influence.

To be precise, here one should distinguish two sub-cases:

a) The system contains an error, e.g. a software error. Another example can be a system that is not able to withstand certain high or low temperatures, although those are specified. There is no aging. As soon as an influence activates this error, the system fails at a random time. Randomness is caused by the randomness of the exterior influence.

b) Due to erroneous processes the system has a weak point. This weak point is e.g. decreased robustness w.r.t loads, environmental influences etc. An example are under-dimensioned mechanical parts that fail caused by fatigue. In fact an additional random failure mechanism is activated by a design error that would have been excluded otherwise. Without occurrence of the design error, the component would have been dimensioned strong enough.

In both cases a probabilistic model might still be valid, however a systematic failure might also completely destroy probabilistic laws, caused by an error leading to instantaneous failure of the system, as in the high-voltage example in the previous subsection.

Measures against systematic failures were introduced, so that systematic failures could be neglected in comparison with stochastic ones.

Systematic failures have never been described using probabilistic models, since no one knows how to do this. And this is apparently difficult to do, since for some systematic failures probabilistic models simply do not work.

Methods against systematic failures have been derived by groups of experts, that have compiled sets of these measures based on their experience. Sometimes, standards from other areas have been used. Since the experts in the standardization groups collected to their best knowledge methods to reduce systematic failures in order to keep the random failure model being the dominant one, they also derived many methods that are also suitable to preserve probabilistic models. But this was not their main intention.

The standards on functional safety [2-6] provide measures against systematic failures that can be classified roughly in the following groups:

- Quality management
- Safety management
- Principles for safety architecture
- Principles of safe design
- Safety analyses
- Verification and Validation methods
- Testing
- etc.

These groups of measures can be found in many safety standards with different detail. Partially, standards are carrying over experience from other areas and therefore also from the standards of these areas, the mother standard IEC 61508 [4] serves as a source for many others. The tables of measures against systematic failures are a compilation of experience of the engineers.

So, there is no direct relation between the long list of measures against systematic failures and the two goals (A) and (B) as defined above in section 3.

V. Examples

I. Burn-in

As an example, let us consider burn in [9]. Burn-in is used to cope with early failures. In fact these are specific procedures of quality management and testing used to avoid early failures. Burn-in is one measure, to keep the lifetime distribution an exponential one – if aging is neglected as of now. Here it must be noted, that the specific measures to carry out burn-in tests are not specified in most of the standards. Burn-in is not mentioned in EN 50126 [21] / EN 50129 [2] and RTCA/DO-254 [6]. ISO 26262-4 [22] mentions a burn-in test in 9.4.1.2.a) as a requirement for ASIL C and higher. IEC 61508-2 [4] requires a burn-in test for SIL 3 and SIL 4 in table F.1 line 40.

This clearly shows, how different standards treat an important measure to cope with early failures in different extent. Most of them do not mention burn-in, only two standards [4,22] mentions burn-in.

II. Prevent aging

Another aspect to maintain the model of the exponential distribution is to ensure that the failure rate is constant, i.e. aging must be neglected, too. This means that components need to be replaced early enough before aging occurs. Sometimes, entire systems are replaced, before aging starts.

Aging is not treated in RTCA/DO 254 [6], EN 50129 [2], EN 50126 [21], ISO 26262-4 [22], so all standards are ignorant towards aging and just quietly support that components are not used too long, somehow.

Another example for the importance of measures against systematic failures is that the activation of additional failures modes must be prevented, when turning from lab conditions or other use conditions under which the failure rate has been obtained using statistical methods to another operating condition. So, it is totally important to obey standards on environmental conditions and electromagnetic compatibility, as mentioned in the standards on functional safety. If not, there could be two consequences:

- additional failure modes would be activated caused by unforeseen and not clearly defined environmental conditions or
- a deterministic failure could even occur, since the system would be out of specification.

VI. Specification and hazard analysis

In addition, a system needs a really good and complete specification. The fact that the specification must have a certain quality is dealt with by different standards. This is discussed in the following subsections for different areas.

I. Automotive

ISO 26262-4 [22] dedicates chapter 6 to this question. In clause 6.4.5. of ISO 26262-8 [23], clause 6 is cited for requirements to the specification. There, general criteria are specified as

- unambiguity,
- comprehensibility,
- atomicity,
- internal consistency,
- feasibility and achievability,
- verifiability,
- necessity,
- free from implementation,

- completeness,
- conformity.

These requirements come mainly from system engineering and help to build up a good specification. However, completeness can only be guaranteed as far as in the hazard and risk analysis all possible hazards and risks have been identified and relevant requirements have been derived to sufficiently reduce the risks.

It is worthwhile noting, that ISO 26262-3 [24] chapter 6 gives only general requirements to the hazard and risk analysis. In annex B some explanation on the risk classification is given. Examples are focused on driving situations. Part 10 of ISO 26262 [25] gives some further guidance on the hazard and risk analysis. There is no good guidance to look for hazards, that are introduced by possible components of new technology into the vehicle. This becomes evident, when battery electric vehicles, vehicles with a fuel cell and pressurized hydrogen etc. are analyzed.

II. Industrial technology

IEC 61508-1 [26] requires in 7.10.2.4 how to write a specification:

a) clarity, preciseness, unambiguity, verifiability ,testability, maintainability, feasibility,

b) comprehensibility,

c) it is expressed in natural or formal language and/or logic, sequence or cause and effect diagrams that define the necessary safety functions with each safety function being individually defined.

and further in 7.10.2.6.

a) a description of all the safety functions,

b) response time performance,

c) safety-related system and operator interfaces,

d) all information relevant to functional safety that may have an influence on the safety-related system design,

e) all interfaces, necessary for functional safety,

f) all relevant modes of operation of the EUC (equipment under control, i.e. the system, that is regarded),

g) all required modes of behavior of the safety-related systems shall be specified.

For industrial technology, IEC 61508 [4,5,24] does not give guidance on other hazards besides pure electrical ones. One needs to look at ISO 13849-1 [27] and DIN EN ISO 12100 [28] that give a really good guidance on hazard analysis and assists with lists of hazards to cover almost all possible hazards.

III. Railroad

For a specification, the following requirements need to be fulfilled [18]:

a) completeness, precision, unambiguity, verifiability testability and maintainability,

b) aid comprehension by those who are likely to utilize the information at any stage of the system life cycle,

c) expressed in natural or formal language and/or logic, sequence or cause and effect diagrams,

d) the defined set of requirements is suitable to define a system that is fit for the intended purpose.

The standard EN 50126-1 [18] provides a list of sources for hazards in 7.4.2.1:

a) system normal operation,

b) system fault conditions,

c) system emergency operation,

d) foreseeable system misuse, excluding deliberate misuse,

e) system interfaces,

f) system functionality,
g) system configuration parameters,
h) system operation, maintenance and support issues,
I) system disposal considerations,
j) human factors,
k) occupational health issues,
l) mechanical environment,
m) electrical environment,
n) natural environment to cover such matters as snow, floods, storms, rain, landslides etc.

Although general, it shows, which aspects need to be covered. For a good hazard analysis more detailed checklists are necessary, using other standards, as e.g. [27,28].

IV. Aerospace

RTCA-DO 254 [6] provides in 10.3.1. a set of subjects that should be covered by the requirements:

1. The system design and safety requirements allocated to the hardware,
2. Identification of applicable standards for the hardware,
3. Hardware functional and performance requirements, including derived requirements and stress limits for normal use,
4. Hardware reliability and quality requirements, including requirements related to failure rates, exposure times and design constraints,
5. Hardware maintenance and repair requirements throughout the hardware item service life,
6. Hardware manufacturability and assembly requirements,
7. Hardware testability requirements,
8. Hardware storage and handling requirements,
9. Installation requirements.

General requirements on the requirements specification, as provided by other standards, are missing.

Chapter 2 of [6] describes the hazard analysis process, leasing to five different system development assurance levels A-E. Detailed guidance on hazard analysis as in the other standards mentioned in this section is missing.

V. Analysis

We see that the requirements for a specification have many common points. However, for carrying out a hazard analysis the procedures are very different and they do not have the same coverage of new and unknown hazards in all the different areas. The coverage of unknown hazards is not only important for preventing of aging, but hazards need to be detected to avoid many systematic failures that could later lead to a violation of the assumption on the existence of the probability measure. The latter can either be distorted, or perhaps probability concepts are not applicable due to deterministic influences.

VII. Conclusion

The analysis has shown that there are a lot of measures against systematic failures in the standards. Also Birolini presents in chapter 3 of his book [7] a set of qualification tests for electronic components, which is a partial set of requirements. However, the measures presented in standards and textbook cannot yet be systematically related to effects, where the probability concept becomes void or where it is just changed. The measures against systematic failures are heuristic ones and they are compiled by engineering judgment, partially using experience from other areas. Sometimes there are points missing, as e.g. burn-in. For some cases, such measures can be indicated in some standards only, as for burn-in [9] or for electronic components [7]. This relation, however, has not yet been systematized and has not be incorporated into the standards.

Requirements for specifications are mostly uniform, requirements for hazard analyses are really different with different depth. The hazard analysis is the main instrument to systematically identify influences that can violate the probabilistic model. As a consequences, one should look for a deep and comprehensive hazard analysis method to find as many hazards as possible. The functional safety standard of the coinciding area might give here only insufficient guidance, so the additional use of other standards is encouraged.

No explicit proof exists that the measures against systematic failures are sufficient to prevent an influence on the probabilities that are given as a result, with the intention to show that the system is safe or sufficiently reliable. Especially, the different measures against systematic failures for different SILs or design assurance levels cannot be proven to be sufficient in a strict sense. No quantification is given for a possible change of the computed probability caused by systematic failures. This seems to be impossible.

A lot of research is still needed to clarify,

a) what probability really means in the engineering context and

b) which methods need to be applied during the entire design process to ensure that the probabilistic models stay valid, when results obtained in a lab or by observation under certain real life conditions are used under exploitation conditions.

In the meanwhile, using consequently the measures against systematic failures as proposed in [2-6] is a good approach. Nevertheless, a few thoughts about the probabilistic models used, their appropriateness in the specific situation and some thoughts about the extrapolation from the data at hand to the current use case are in place. A third aspect is a good and comprehensive hazard analysis.

References

[1] Mann, N.R. and Schafer, R.E. and Singpurwalla, N.D., Methods for Statistical Analysis of Reliability and Life Data, J. Wiley and Sons, New Yok, Chichester, Brisbane, Toronto, 1974

[2] EN 50129, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling, 2018

[3] ISO 26262-5 Road vehicles — Functional safety — Part 5: Product development at the hardware level, 2018

[4] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic
safety-related systems, 2010

[5] IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations, 2010

[6] RTCA DO 254 / EUROCAE ED-80, Design Assurance Guidance, For Airborne Electronic Hardware, 2000

[7] Birolini; A., Reliability Ebgineering, Theory and Practice, Springer, 8th edition, 2017

[8] Härtler, G., Statistisch gesichert und trotzdem falsch? (Statistically ensured but nevertheless wrong) Springer, 2014.

[9] Jensen, F., and. Petersen, N.E., Burn in, J. Wiley & Sons, Chichester, New York, Brisbane, Toronto, Singapure, 1982

[10] Nonelectronic Parts Reliability Data Handbook, RIAC Automated Databook 2011

[11] EN 61709 Electric components - Reliability - Reference conditions for failure rates and stress models for conversion, 2017

[12] Proske, D. Catalogue of Risks, Springer, 2008

[13] Braband, J., and H. Schäbe, H. (2016), Probability and security – pitfalls and chances, Safety and reliability, 36:1, 3-12

[14] Kolomogoroff, A.N. Foundations of the theory of probability, New York: Chelsea Pub. Co., 1950

[15] Pollard, W. E., Bayesian Statistics for Evaluation Research, Sage Publications, Beverly Hills, London, New Delhi, 1986

[16] Landau, L.D., and Lifschitz, E.M., Statistical Physics, Volume 5 in Course of Theoretical Physics Third Edition, Pergamon Press, 1980

[17] Schäbe, H. and Viertl, R. (1995) An Axiomatic Approach to Models of Accelerated Life Testing, Eng. Fract. Mechanics, 50, No.2, 203-217.

[18] Shubinsky, I.B. and H. Schäbe, H. (2012) On the Definition of Functional Reliability, Reliability: Theory & Applications Vol.7 No. 4, 8-18.

[19] Shubinsky, I.B. and Schäbe, H. (2021), Errors, Fault and Failures, Dependability, vol. 21, no.2, p. 24-27.

[20] Braband, J., H. Gall, and Schäbe, H, Proven in Use for Software: Assigning an SIL Based on Statistics in: Handbook of RAMS in Railway systems – Theory and Practice, Qamar Mahboob, Enrico Zio (Eds.), 2018, Boca Raton, Taylor and Francis, Chapter 19, p.337-350

[21] EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, 2017

[22] ISO 26262-4 Road vehicles — Functional safety — Part 4: Product development at the system, 2018

[23] ISO 26262-8 Road vehicles — Functional safety — Part 8: Supporting processes, 2018

[24] ISO 26262-3 Road vehicles — Functional safety — Part 3: Concept phase, 2018

[25] ISO 26262-10 Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262, 2018

[26] IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements, 2010

[27] ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 2015

[28] DIN EN ISO 12100 Safety of machinery –General principles for design – Risk assessment and risk reduction, 2011

Acknowledgement

The author wishes to thank A. Bochkov for his valuable comments on the paper.