CONTRIBUTION TO RELIABILITY ANALYSIS OF HIGHLY RELIABLE ITEMS

D. Valis, Z. Vintr

•

University of Defence, Brno, Czech Republic

e-mail: david.valis@unob.cz, zdenek.vintr@unob.cz

M. Koucky

•

Technical University of Liberec, Liberec, Czech Republic

e-mail: miroslav.koucky@tul.cz

ABSTRACT

In recent years the intensive efforts in developing and producing electronic devices have more and more critical inference in many areas of human activity. Engineering is one of the areas which have been also importantly affected. The paper deals with dependability namely reliability analysis procedure of a highly reliable item. The data on manufacturing and operating of a few hundred thousands pieces of electronic item are available and they are statistically a very important collection/set. However, concerning some items the manufacturing procedure was not checked and controlled accurately. The procedure described in the paper is based on the thorough data analysis aiming at the operating and manufacturing of these electronic elements. The results indicate some behaviour differences between correctly and incorrectly made elements. It was proved by the analysis that dependability and safety of these elements was affected to a certain degree. Although there is a quite big set of data the issue regarding the statistical comparability is very important.

1   INTRODUCTION

The application of electronic elements introduces a number of advantages as well as disadvantages. Let us start with operating process itself – the operating is more ecological, smoother and cheaper. Also the area of safety, both passive and active, is optimised. On the other hand the complexity of a system is getting higher as well as its sensitivity to previously not perceived factors. The electronic elements are also applied into so called service and comfort systems. However new the technology would be, all the elements are subject to certain factors set by a design, manufacturing, operating and environment in which they are used. Besides performance and utility properties we are supposed to follow dependability as well. Regarding electronic elements they are highly reliable and in terms of dependability measures they are at the highest level. If the elements are well manufactured and their construction and software equipment meets the required dependability level, we are usually satisfied and there is no reason to act otherwise. If occasional fluctuations in the dependability level do not limit the function or safety of a system or its operating, the problem of unreliability of electronic elements in systems is not so serious. The real problem is not meeting the requirements and errors.

In the paper we are going to address reliability assessment of a highly reliable electronic item. In this paper the evaluated application is perceived as an item produced for systems´ specific use/utilization. Item is implemented in a system in order to control one of the step functions of the system. The manufacturer has had long term experience of item manufacturing. This item is also widely introduced into the market where it successfully meets the parameters within technical applications. The introduced item has been applied in the systems´ environment many times and no major problems have been detected regarding its function.

As we know from previous publications the item is initialised by start power. Unfortunately non-intentional causes resulted in non-compliance with the manufacturing process during development and manufacturing a new item. While manufacturing the item a relatively minor shortening of program protocol took place, thereby shortening the initialisation time. This situation resulted in the production of many tens of thousands of incorrectly manufactured items where the initialisation time was shortened by the program. The non-compliance with the manufacturing process was detected only by accident and that was after some time. However, most of the items manufactured this way have been mounted in systems and they have been in operation.

The non-compliance with the manufacturing process itself, thereby shortening the programming time might not be a serious problem. More related circumstances might be the real problem. The first one is the fact that the items have been mounted in systems and they have been in operation. Another quite serious problem is the fact that a item function failure can result in failure occurrence on the device which is supposed to perform a system's step function. If a system step function is just being used, its interruption-failure might lead to a critical accident with serious consequences. In case this type failure occurs, it affects significantly system's dependability. Moreover, it breaks the confidence in the step function which leads to the lack of confidence in a system as a whole.

Resulting from the arguments mentioned above the producer decided to solve the problem immediately. The producer wanted to find out if the errors occurring when manufacturing items have a possible effect upon operational dependability – reliability. Basically a few solutions could have been taken into account at that moment. Finally two of the solutions were chosen to be accomplished.

One of the options is to carry out a one-side interval calculation of a item reliability measure at a required confidence level. This intention is easy to be fulfilled since the data on the item operation were carefully and systematically collected. The aim of the paper is to describe an estimation procedure of a reliability measure and assess the validation of the statistical hypothesis testing based on the available data.

Suggesting and carrying out an accelerated reliability test of item is another option. However, this method is not included in this paper and represents a separate methodology. All terms mentioned here are in accordance with the (IEC 60050/191).

2   FIELD DATA ASSESSMENT PROCEDURE

The procedure follows widely known and basic approaches and terminology (IEC 60050/191). The producer provided data on the item operation over a complete period. Regarding the nature of the analysis the following facts were agreed on:

1) The aim of the analysis was to calculate the one-side item reliability interval. The item "programmed incorrectly" was assessed first, and the item "programmed correctly" was assessed as the second. The calculation of a reliability one-side interval determined for each set separately was the outcome of the analysis.

2) The next step was to compare both items sets and decide whether the „incorrect programming" can/cannot affect the item's reliability. A one-side interval was determined at a required confidence level and it specifies a minimal reliability level of a item set obtained by a calculation.

3) The operation time of the item started the moment a production range was produced plus two weeks (the assumption that it will be delivered to the customer, mounting into the system, and physical start of the operation).

4) The real operation time equivalent was determined by recommending the standards and is based on a calendar time (GS 95003-1, GS 95003, GS 95003-4). The real operation time is believed to start at the moment as stated in point 3). The transforming coefficient value following the sources/standards mentioned above is: dormant time versus operation time ≈ 24,836 : 1.

5) The standard IEC 60605-4 "Equipment reliability testing - Part 4: Statistical procedures for exponential distribution - Point estimates, confidence intervals, prediction intervals and tolerance intervals" has been used for calculating the reliability measure one-side interval at a required confidence level.

6) The reliability confidence interval was set according to common roles. One of the very accurate levels which were decided to be used is 95%. This level was used for following calculations.

7) End of observation, censoring by time is given by the date of 31st December 2008. This was negotiated with the item producer.

8) The hour [h] is a reliability measure unit.

Since the standard IEC 60605-4 deals with a few possible types of the assessed sets, it is necessary to determine what type it is referred to. The operation profile and the agreement that the analysis assessment will be finished on a certain day indicate that this is a case of a specific field test finished by time without replacing the item. This assumption resulted in the following solution taking into account the standard mentioned above (IEC 60605-4).

Following the standard (IEC 60605-4) recommendation a lower limit of mean time to failure at the required confidence level was calculated. In order to estimate one-side interval of a lower level of mean time to failure we used the following equation (see also Holub 1992, Lipson & Sheth 1973, Neson 1982, Kapur & Lambertson 1977):

$$m_{l\,F/C} = \frac{2.T^{*F/C}}{\chi^2_{\alpha,\nu}} \tag{1}$$

where $m_{l\,F/C}$ - is a lower limit of mean time to failure of either „F" – „incorrectly" programmed sets or „C" – „correctly" programmed sets; $T^{*F/C}$ - is accumulated operation time of all items sets (either „F" – „incorrectly" programmed or „C" – „correctly" programmed) observed in the operation during an evaluation period. It is calculated using the equation $T^{*F/C} = \sum_{t=i}^{n} t_i^{F/C}$ („t_i" = accumulated real operation time of all items of i-th production range of either „F" – „incorrectly" programmed sets or „C" – „correctly" programmed sets, where the n is number of the production ranges. The interval is the period in which they are put into operation which lasts up to the day when the temporary observation is finished; $\chi^2_{\alpha,\nu}$ -chi square for a given number of degrees of freedom ν; „α" – confidence level agreed on 95%.

Since it is a one side censored set (it is censored by the agreed date when the observation is to be finished; this date is the last possible day when the operation record is to be made), the number of degrees of freedom ν to determine chi square is going to be calculated using the standard recommendation**Ошибка! Источник ссылки не найден.** following the formula:

$$\nu = 2r^{F/C} + 1 \tag{2}$$

where: r is a number of events (failures) in a given group of sets.

Based on the assumptions and the calculation which have been made before, the reliability measure values for correctly and incorrectly programmed items were found. These values were calculated at the required confidence level. By comparing these values we were able to determine whether the error affects the item reliability during a manufacturing process.

However, concerning the field data we face a theoretical problem. The data set is apparently different concerning a digit place in terms of the operation time of the item sets. It means that correctly manufactured items obviously operate for a shorter time than the ones manufactured

incorrectly. This situation can affect a calculation procedure as well as a comparison of the results. Taking into account this situation it is necessary to test the field data using the statistical test which is supposed to prove their comparability. The procedures proving the statistical equivalence of the evaluated sets is part of another contribution. The objective of the statistical analyses is to compare two sets of data both of which have non-similar size.

2.1 Example of the application of above mentioned procedure

Here will be presented restricted part of the above mentioned procedure. The procedure given in this example is the same as used in the whole analysis. The difference is that no information about portion of data or other relevant indicators will be provided.
Data were provided in following form:

Number of production range:	1.
Number of items produced in this range:	4 200
Date of production:	16.1. 2006
Number of failed items in this range:	1
Date of failure:	12.10. 2006

Ad section 2, point 3), 4), 7), 8)

Number of days in operation:	43 days
Number of hours in operation for 4 199 items:	1030 h
For 1 item:	238 h
Total hours in operation for all items from this range:	4 325 710 h

Following the calculation (1) and (2) it is:
$$\nu = 2r^{F/C} + 1 = 2.1 + 1 = 3$$
and

$$m_l = \frac{2.T^*}{\chi^2_{\alpha,\nu}} = \frac{2 . 4\,325\,710}{7,8} \cong 1\,109\,156 \cong 1.10^6\,h$$

It means that lover limit of one side confidence interval for MTTF of the item is approximately $1.10^6\,h$.

The assessment of the other sets which represent the electronic items made (both correctly and incorrectly manufactured) is carried out in the same way. Finally the decision about the failure rate comparability is performed. From the reason of keeping the industrial confidence of the data and their assessment we can not present full range of the calculations made. We can only present that the difference between correctly and incorrectly manufactured items is noticeable.

3 RISK ANALYSIS RESULTING FROM THE FAILURE OCCURRENCE

In this phase of observing the object we are talking about partially predictive risk assessment. We could choose fully theoretical way of assessment usually made during design. However we do have the field data are available so we may also use the process approach. Following one of the approaches we would focus on individual risk contributors which would be thoroughly examined. The classic probability methods might be used for determining the event occurrence probability. The expert assessment based on the defined scales would be used for analysing the consequences. Next issue which might be used is recommendation of the standards dealing with such kind of items. One very suitable method is mentioned in the standard SAE J 1739:2002.

Usually we do not count on other factors when dealing with theoretical risk analysis. However, some special characteristics still exist and that is the reason why one of the possible approaches where another factor occurs is described below. However, further verification and validation of the obtained result will pose a problem while assessing the risk theoretically. In our case, when undesired event occurrence probability might be recorded when observing the field data, the result will be more realistic and consequent verification of the result will be also possible. Such event occurrence information is not a prediction then, but it is estimation based on the real information. Consequence decisions resulting from the occurred event might be regarded as a prediction in this case. Consequences description options are stated below.

Using either fully standardised approach, namely industrial standards or software support can be another option when analysing the risk. An event occurrence rate or its criticality may be obtained using well known dependability analysis methods, e.g. FMECA, PHA or OSHA. The total risk is usually based on these two contributors we often work with in industry practice. Concerning software support when analysing the risk it is possible to use widely available tools, e.g. Risk Spectrum based on the FTA method supported by the ETA method, or the tools by Relia Soft or Item Software – Item QRAS which uses both methods individually but basically leads to the same result.

Using so called soft methods when analysing the risk and dependability is another possibility. It is namely about non-stochastic methods which are based mostly on the deterministic approach and iteration principles. Also the probability plays an important role but most approaches of these methods are based just on empiricism and practice. The methods would be used namely for analysing the event consequences and also the event occurrence but on a limited scale. The determination is not often unambiguous and also it is not easy to decide what defined scale the consequences belong to. We would highly recommend fuzzy logic which allows us to work very well with qualitative characteristics of some events, and which is able to quantify them. If we were to define individual process states in system operation and they would represent the periods in which the system is run, we would be able to determine to what extent the event belongs to a defined state while an event occurs. That is how we would cover the failure criticality level regarding the defined states set and the time vector in which a system might occur during its operation/technical life. Unfortunately, in this paper there is no space for presentation and development of this approach.

Generally speaking we can use standardized criteria by which every failure is evaluated following the previously defined scales. Using the point estimations the Risk Priority Number is added to each failure mode. The RPN is then used for downward arrangement of the assessed failures. The failures with a risk number going above the defined scale undergo the corrective actions which are supposed to reduce the risk number sufficiently.

3.1   Evaluated factors

The existing model described in standards (e.g. IEC 60812:2006 and SAE J 1739) considers two evaluated factors, Probability – P and Severity – S, or three evaluated factors, Probability, Detection and Failure Consequences. These factors result from a fully quantitative assessment where the risk is expressed by a conjunction of probability and consequences

$$R = P * S \tag{3}$$

The Detection Factor – D in a full quantitative assessment would decrease the probability that a failure will not be detected during design/manufacturing process (see e.g. 0), thus

$$R = P * D * S \tag{4}$$

whereas its value would belong to the interval <0;1> (or <0;100%>).

As we deal with an electronic item which might be installed inside systems, the SAE standard is very suitable to be applied.

3.2 Scales for assessment

In the standards (e.g. IEC 60812:2006 or SAE J 1739) for example there are scales for assessment for all three criteria which are used in industry. The scales are put in the form of tables with verbal explanation of every level at the scale. These are severity, occurrence probability and detection scales. Sometimes a consequence scale in relation either to the customer or manufacturing process or operation is completed. These scales are going to be used in the next procedure. Other existing and used scales are for example those which are applied in a part of software, Item Toolkit or Reliasoft XFMEA.

3.3 Risk Priority Number *RPN*

The Risk Priority Number is a crucial criterion for detecting weak points in a system, and corrective actions which decrease the risk resulting from the device failure are convenient to be applied to these weak points. The magnitude of the Risk Priority Number *RPN* is given by conjunction of point estimations of probability, detection and consequences. Since the Risk Priority Number is given by conjunction of point estimations, it is a case of a dimensionless quantity as in equation (4). $RPN = P*D*S$

The values interval depends on the selection of assessment scales. Concerning the scales put in the (see IEC 60605-4 or MIL-STD-1629a) the range of the Risk Priority Number is 1 up to 1000 (=10^3) (EN 60812:2006, MIL-STD-1629a, SAE J 1739). The application of corrective actions involves all the events of the Risk Priority Number value exceeding 125. In our case we can talk namely about:

The effort to minimize an event occurrence - this was achieved especially by detecting the manufacturing disagreement and correcting it. This act should provide reliable item operation at a higher level;

The effort to minimize consequences severity of a failure which might occur – this is provided by using standard security measures which are not expected to modify;

The effort to improve detection of a possible failure – this is provided by a sufficient quality manufacturing.

The consequence of an event occurrence is in the range "9" to "10" according to the standard. The frequency according to the same standard is "low" and detection is "moderate" at maximum using the same source. Therefore we need to carry out some design change to improve the item´s *RPN*. From this point of view is the service of such item very dangerous and may cause inadvertent situation with very sad consequences.

Example of the assessment:

Using the approaches above and the recommendations in the standards we may get following values for the *RPN* calculation.

The occurrence might be "2" at minimum according to the rating.

The severity might be "9" at minimum according to the rating.

The detection ability might be "5" at minimum according to the rating.

Therefore, the calculation of the *RPN* is:

$RPN = P*D*S = 2*9*5 = 90$

This is the lowest level of the *RPN* which might be got.

As said before, as we see that one of the values is "9", we have to apply countermeasures.

3.4   Criticality matrix

In some applications where no detection is assessed apart from failure probability and its consequences it is possible to use a so-called criticality matrix (sometimes it is designated as a risk matrix). The measures used in the matrix correspond with those ones which have been discussed above.

Contrary to an exact value calculation as it takes place when assessing by the *RPN*, an event positioning in the matrix is a crucial one. The example of criticality matrix which could be used for risk assessment is taken from the standard (EN 60812:2006) and is put in Table 1.

To place a failure mode into a certain matrix field, the scales categories for consequence assessment are to be defined (in Table it is put as Severity Levels and Occurrence Frequency of Failure Effect). The weak point of such scales is the fact that they can be different considering more application fields, and they are defined mostly by an analyst/decision maker. The following scale used for assessing the probability put in the standard serves as an example.

Criticality number 1 or E, Improbable, probability of occurrence: $0 \leq P_i < 0,001$;
Criticality number 2 or D, Remote, probability of occurrence: $0,001 \leq P_i < 0,01$;
Criticality number 3 or C, Occasional, probability of occurrence: $0,01 \leq P_i < 0,1$;
Criticality number 4 or B, Probable, probability of occurrence: $0,1 \leq P_i < 0,2$;
Criticality number 5 or A, Frequent, probability of occurrence: $P_i \geq 0,2$.

Regarding the criteria described above we can talk about the following intervals distribution of *RPN* components:

The Severity Component could range over the values 5 – 10;
The Probability Occurrence Component could range over the values 1 – 2;
The Detection Component could range over the values 1 – 3.

Adequate corrective measures for decreasing all the values of the obtained *RPN* components were taken.

Table 1. The example of a risk criticality matrix

Frequency of occurrence of failure effect	Severity levels			
	1 Insignificant	2 Marginal	3 Critical	4 Catastrophic
5. Frequent	Undesirable	Intolerable	Intolerable	Intolerable
4. Probable	Tolerable	Undesirable	Intolerable	Intolerable
3. Occasional	Tolerable	Undesirable	Undesirable	Intolerable
2. Remote	Negligible	Tolerable	Undesirable	Undesirable
1. Improbable	Negligible	Negligible	Tolerable	Tolerable

4   CONCLUCION

The procedure as described above was used to calculate reliability of the single sets which served as correctly and incorrectly programmed items. Following the obtained results a possible effect of a manufacturing error upon the items reliability was estimated. Following the results it is obvious that manufacturing error could affect items reliability in some way. Both sets are from the statistical point of view slightly different, which is an essential piece of information. This fact should be referred to when carrying out statistical data evaluation using the introduced tools.

5   ACKNOWLEDGEMENTS

REFERENCES

BMW Group Standard; GS 95003-1 *Electrical/Electronic Assemblies in Motor Vehicles – General Information*.

BMW Group Standard GS 95003 *(Supplement 1) Electrical/Electronic Assemblies in Motor Vehicles – Tests*.

BMW Group Standard GS 95003-4 *Electrical/Electronic Assemblies in Motor Vehicles - Climatic Requirements*.

IEC 600 50 (191) (IEV) 1990. *Dependability and quality of services*.

IEC 60605-4 2004. *Equipment reliability testing - Part 4: Statistical procedures for exponential distribution - Point estimates, confidence intervals, prediction intervals and tolerance intervals*.

EN 60812 2006. *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*.

MIL-STD-1629a 1998. *Procedures for performing a failure mode, effects and criticality analysis*.

SAE J 1739 2006. *Potential Failure Mode and Effects Analysis in Design, Manufacturing and Assembly and for Machinery (Design FMEA, Process FMEA and Machinery FMEA)*.

Holub, R. 1992. *Dependability tests (stochastic methods)*. Brno: Military Academy, 1992.

Lipson, CH., SHETH, N.J. 1973. *Statistical Design and Analysis of Engineering Experiments*; New York: Mc Graw Hill.

Neson, V. 1982. *Applied Life Date Analysis*, New York: John Wiley and Sons.

Kapur, K.C.; Lamberson, L.R. 1977. *Reliability in Engineering Design*; New York: John Wiley & Sons.