Novel Model of Proof Test Coverage Factor

György Baradits*, János Madár*, János Abonyi**

*SIL4S, Baláca u. 54, H-8200 Veszprém, bgs@sil4s.com, janos@sil4s.com

** Department of Process Engineering, Pannon University, Egyetem u 1, H-8200 Veszprém, Hungary, abonyij@fmt.uni-pannon.hu

Abstract: The Safety Instrumented Functions (SIF) play main role in the safety industry. For every SIF there is safety integrity requirement which is described by the Safety Integrity Level. The SIL value of a SIF mainly determined by the failure rates of the components of a SIF and the proof testing. This paper briefly describes the proof testing, and discusses the problems of classical implementation of proof testing. The goal of this article is to propose a new model for dangerous undetected faulires and investigate how this model influences the proof testing strategy.

Keywords: safety instrumented function, maintenance, proof test, dangerous undetected failure, SIL, Markov analysis

1 Introduction

In the 1990s, companies and industry groups developed standards to design, build, and maintain, that time called, ESD system focusing only the PLC part of the system. The PLC, in safety application", was classified according the German Standards [1] – [7]. The first general safety standard, the IEC 61508 [8], was issued in 1998, which in this topic dramatically changed the safety thinking both in general and industrial segment specific. This standard firstly introduced the principle of Safety Instrumented Systems (SIS) and Safety Instrumented Function (SIF). In 2004 the IEC 61511 was published as a process industry sector safety standard [9], which is valid for Chemical, Petrochemical, Oil and Gas Industry.

The main concept of the safety standards are the protection layares which can precent agains accidents. A process is a safe state only if hazardous event cannot occur. However in a typical industrial processes, a hazardous event can happen at any time,.hence several type of protection layers are in place: e.g. basic process control system, safety instrumented systems, passive and active mechanical devices (relief valve, dike).

Safety systems have, compared to the control systems, additional requirements concerning safety related aspects, e.g. the safety integrity. The safety integrity is especially important for the Safety Instrumented Function (SIF) which is the only sclable protection layer. SIF is an automated function of safety system that prevents against and/or reduces the unwanted consequences. To maintain high safety integrity there is a need to preriodically do a proof test. That means one have to design not only safety system, but the maintenance activity of the safety system as well.

This paper briefly describes the proof testing, and discusses the problems of classical implementation of proof testing. The goal of this article is to propose a new model for dangerous undetected faulires and investigate how this model influences the proof testing strategy.

2 Safety Integrity Level and Proof Testing

The IEC 61508 defines the safety intergrity level (SIL) of a SIF as the higher the safety integrity level, the lower the probability that the given SIF is incapable of performing its safety function. To determine the safety integrity level one must take into consideration all failure cases which can lead to unsafe state. For every SIF the minimal SIL is determined. It means that the SIL is avery important quantity: if the a SIF's SIL value is not enough high, the SIF is not enoug good and the risk is too high.

The SIL is calculated from the avarage Probability of Failure on Demand (PFD) value:

$$SIL = floor\left(-\log\left(PFD_{avg}\right)\right) \tag{1}$$

The PFD is the probability that a given SIF cannot perform its safety function when there is a need (demand) for it. To calculate the PFD one must make a failure analysis. According the standard the failure rates are grouped as follows during the failure analysis:

- Safe detected – λ_{SD}
- Dangerous detected - λ_{DD}
- Safe undetected - λ_{SU}
- Dangerous undetected - λ_{DU}

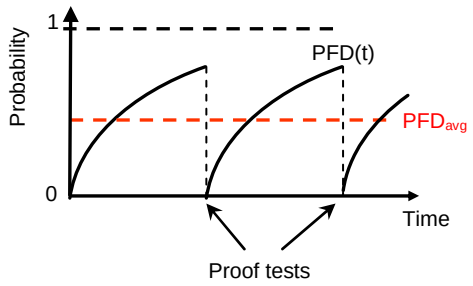
A failure is safe when the failure drives the system into safe state (called spurious trip), while the dangerous failure is when the system is unable to take action on demand (this is the dangerous state). The failure is detected if an automated

diagnostic system can detect the failure *in-situ*. Assuming that the failure rates are constants the PFD can be calculated as:

$$PFD(t) = e^{-\lambda_{DU} \cdot t} + e^{-\lambda_{DD} \cdot MTTR} \quad (2)$$

where the MTTR is the mean time to repeair. Becasue the MTTR is practically a low value, the dangerous undetected failures are really critical.

The (2) equation implies that the PFD(t) will be near 1 sooner or later because it always increase with time and converges to the 1. In this case the PFD_{avg} also would be near 1, and the SIL value would be 0. Luckily it is possible to reveal the dangerous undetected failures too by a manual testing of the SIF. This called "proof test" in the safety standard. So proof tests serves to reveal dangerous failures which otherwise remain undetected. Proof test should be executed periodically to detect the DU failure in time. The following figure shows the effect of the proof test on the PFD value:



One can see that the SIL value of a SIF determined by the failure rates of the components of a SIF and by the proof testing. If the SIF exits and failure rates are given and proof testing is the only method to increase the safety integrity

3 Proof Test Coverage Factor

3.1 Imperfect Proof Testing

The IEC 61508 defines the proof test as a "*periodic test performed to detect failures in a safety related systems so that the system can be restored to an "as new" condition or close as practical to this condition.*" Practically it means that the proof test is always perfect or near perfect. The Figure 1 illustrates that model concept.

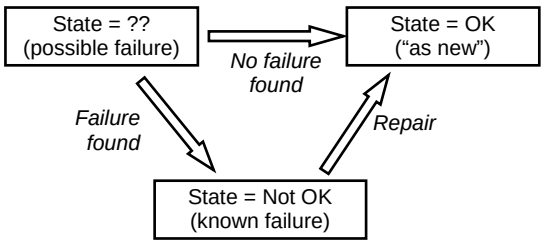


Figure 1
IEC 61511 safety instrumented systems life cycle model

A SIF always constints of three parts: sensor(s), logic solver and final element(s). The standard was developed for E/ES/EPS systems for which that model concept is acceptable. But that concept is doubtful for filed devices, especially for valves. Even if the valve works well during the test - i.e. no failure found by the proof test - it does not mean that the valve can be considered as “new” due to the corrosion, erosion, and other environmental stress. Tiezema [10] also claims that “*IEC 61508 standard considers proof tested equipment as “new” after the test ... Maybe this is valid for electronic system ... but it is surely not acceptable for most sensors and final elements*”.

In this article we will focus on actuators because usually they contribute the most to the probability of failure on demand of a safety loop. In order to demonstrate it let us investigate a simple SIF: e.g. there is a SIF which consists of a generic pressure transmitter (sensor), a generic SIL 2 certified PLC (logic solver) and a generic ball way with a 3-way solenoid valve (actuator). Table 1 shows the failure data (achieved from Exida database) and calculated PFD_{avg} values of this SIF. One can see that the actuator part determines more than 70% of the total PFD_{avg}.

Table 1
Example SIF (pressure trip)

SIF part	**Failure data (from Exida database)**	**PFD_{avg} (1 year)**	**PFD_{avg} %**
Generic pressure transmitter	$\lambda_{DD} = 7.0 \cdot 10^{-7}$ 1/h $\lambda_{DU} = 6.0 \cdot 10^{-7}$ 1/h	$2.63 \cdot 10^{-3}$	17.7%
Generic SIL 2 certified PLC	$\lambda_{DD} = 4.3 \cdot 10^{-6}$ 1/h $\lambda_{DU} = 2.6 \cdot 10^{-7}$ 1/h	$1.14 \cdot 10^{-3}$	7.7%
Generic air actuated ball valve + generic 3-way solenoid valve	$\lambda_{DD} = 0$ $\lambda_{DU} = 2.5 \cdot 10^{-6}$ 1/h	$1.08 \cdot 10^{-2}$	72.8%

The authors has prepared about one hundred safety study in the Refinery Industry, and found that the actuator part determines more than half of the PFD value in most cases (especially if the actuator is a valve). The [11 12] also indicates that valves contribute the most of PFD_{avg} of a safety loop.

3.2 Covarage Factor Approach

Because proof testing has significant influence on the final PFD_{avg} value, the imperfectness of proof testing is not negligible. But how the imperfectness of a proof test can be quantified? The classical approach is introducing the so-called proof test coverage factor similarly to the diagnostic coverage factor. The proof test coverage factor (PTC) gives the fraction of undetected failures which can be detected by proof testing. Namely the undetected failure rate is separated into two parts:

$$\lambda_{DU}^{PT} = PTC \cdot \lambda_{DU} \tag{3}$$

$$\lambda_{DU}^{NPT} = (1 - PTC) \cdot \lambda_{DU} \tag{4}$$

where λ_{DU}^{PT} is the rate of dangerous undetected failures that can be revealed, and λ_{DU}^{NPT} is the rate of dangerous undetected failures that cannot be revealed by proof testing.

The application of this approach is very easy: when the PFD is calculated one has to calculate two PFD curve with the two failure rates and summarizes them. The following figure illustrates it:

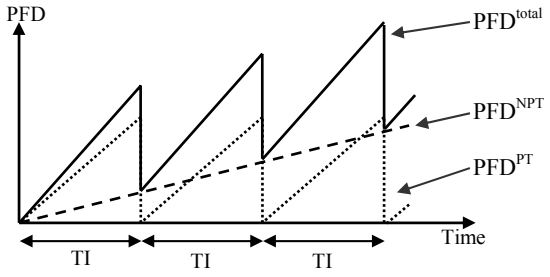


Figure 2
IEC 61511 PFD with proof test coverage factor

3.3 Problems with Coverage Factor Approach

The application of proof test coverage factor is easy and widely accepted in the functional safety practice. SIL calculation programs, e.g. exSILentia, also can take into consideration the proof test coverage factor. It is obvious that this factor cannot be neglected. Table 2 shows how the PFD_{avg} depends on the PTC factor for a generic ball valve actuator (actuator from Table 1).

Table 2
Influence of PTC on PFD_{avg} for a generic air actuated ball valve with 3-way SOV

PTC %	PFD_{avg} for 10 years (PTI = 1 year)
100%	$1.08 \cdot 10^{-2}$
90%	$2.04 \cdot 10^{-2}$
80%	$2.99 \cdot 10^{-2}$
70%	$3.93 \cdot 10^{-2}$
60%	$4.86 \cdot 10^{-2}$

Table 2 illustrates that the PTC factor has very big influence on the SIL calculation. Hence a question arises: How many the proof test coverage factor should be in a particular case?

Unfortunately, as far as we know, there is no any guideline about the scale of PTC factor! The IEC 61508 and 61511 standard do not mention the proof test coverage factor, and most articles which deals with proof testing just assume (explicitly or implicitly) that testing and repair are perfect. Tiezema [10] claims that "*high proof test coverage factors can hardly be demonstrated for sensors and final elements*" but do not give specific example or proof.

It seems to be that virtually nobody has ever asked what really means the PTC factor and everybody uses it without thinking over it. So first let us think over what the PTC factor means. It means that there are some random hardware failures which cause that the system will not able to perform its function on demand and these failures are not detectable by proof-test. E.g. in a case of valves, there are random failures that cause that the valve cannot close properly and it is not possible to detect these failures by proof test.

But a proof test usually consists of a real simulation of the safety function. So if the proof test is comprehensive enough, the chance of not found a dangerous failure is near zero (i.e. the PTC will be near 100%). It means that a low PTC value should mean that something is wrong with the proof test procedure. But a proof test must be comprehensive because the standard demands it. Additionally, to do a comprehensive proof test of a safety valve is also possible in practice: it is enough to do a full stroke test and a leakage test at process conditions.

Here we get into a contradiction: on one hand we claim that the proof test coverage factor cannot be high for final elements (valves) but on the other hand we concluded that it must be near 100%. The next section will show why we got this contradiction and what the right solution is.

4 New Model of Undetected Dangerous Failures

4.1 Why a New Failure Model is Needed

The above conducted contradiction comes from that the proof test coverage factor is a bad concept for modeling the problems of field elements. The quantity of PTC factor depends on the proof test procedure itself and there is no any direct connection between the PTC factor and the subsystem as e.g [10] inspires it. The proof test is imperfect due to that the proof tested equipment cannot be considered as "new" even after the successful test and not because the proof test procedure is wrong. Certainly it is possible that the proof test procedure is wrong but this case is not the topic of this article.

In order to understand the above statements a few aspects of failure model have to be considered. In the IEC 61508, the hardware failure model is very simple: every subsystem has only two states (from viewpoint of dangerous failures):

- Good state: the subsystem can perform its function.
- Bad state: the system cannot perform its function.

The following figure shows that concept (focusing on the dangerous undetected – DU – failures and proof test):

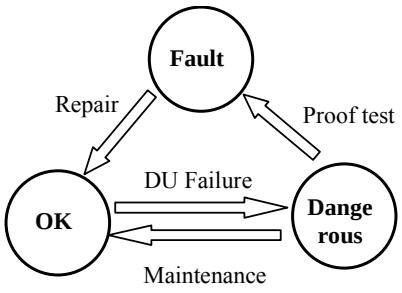


Figure 3
Classical model of DU failures (based on IEC 61511)

One can see that this failure model has a big deficiency: the system will be always restored to a perfect ("as new") condition after a well performed proof test just because there is no other state in the model. In order to understand why the classical failure model is too simple, we shall consider the types of failures. There are two main types of hardware failures:

- Sudden failure
- Degraded failure

The sudden failure is typically a random hardware failure that may happen at any time. The sudden failure does not have "memory", so the rate of sudden failure is typically constant over time.

A typical degraded failure is a failure which comes from corrosion, erosion, deposition, high temperature and other effects from the process. These effects accumulate slowly with the time hence the degraded failure has "memory". It means that the rate of degraded failure changes over time.

The IEC-61508 standard always calculates with constant failure rate, so it cannot take into account the dangerous failures from the degradation. It is acceptable for E/ES/PES systems, where the degraded failure is not important, but not acceptable for mechanical systems (especially for valves) where the failures from degradation are very important. E.g. depositions on seat, corrosion or erosion of moving parts are typical problems of a safety valve that may lead to dangerous failure. So there is a need for a model that takes into account the degraded failures too.

4.2 Degraded Failure Model Concept

The most important difference between degradation failure and sudden failure is that the sudden failure resembles a binary variable while the degradation failure resembles a continuous variable. The sudden failure will happen or will not happen at a given time period with the same probabilites. There are not other possibilities. While thee degradation is usually a slow process; the system changes slowly but it can perform its function for a long time.

Even if the system can perform its function after some degradation, it does not mean that the system is in perfect condition because a degraded system can fail more easily than an "as new" system. It means that to describe the degradation we must introduce a new state which models the degradation of the system.

Hence the main concept is to incorporate a new intermediate state into the failure model that represents the degradation. Figure 4 shows the suggested model concept (focusing on the DU failures) which we call "degraded failure model".

In this model there are three possible states of a component:

- "As new" state: the system is in perfect state.
- Intermediate state: the system is not perfect due to the degradation but it can perform its safety function.
- Dangerous state: the system cannot perform its safety function.

Please note that the intermediate degraded state is defined as the system can perform its safety function when it is in this state. It means that a proof test cannot distinguish between perfect state ("as new" state) and intermediate degraded state.

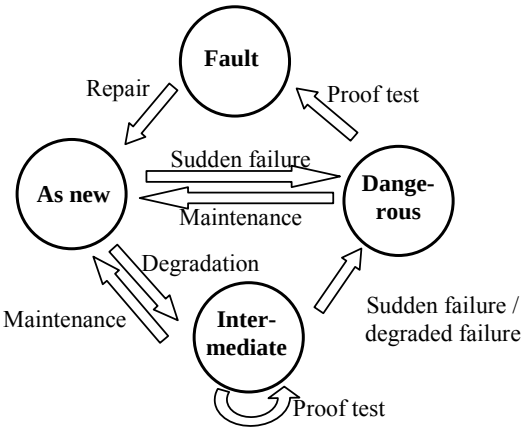


Figure 4
New DU failure model ("degraded failure model")

Theoretically it is possible to define more complex models, e.g. in which there are several intermediate states which represent the different stage of degradation. But in this work we will not use more complex models because this model is enough complex to examine the effects of the degradation failure on the proof testing strategy.

4.3 Markov Model

The following figure shows the Markov model of the degraded failure model:

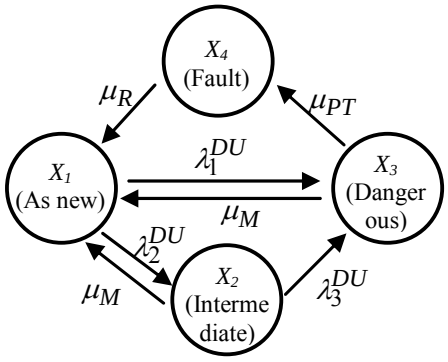


Figure 5
Markov model of the "degraded failure model"

The model has three failure-type state transition rates:

λ_1^{DU}: DU failure rate from "as new" state to "fault" state,

λ_2^{DU}: DU failure rate from "as new" state to "intermediate" state,

λ_3^{DU}: DU failure rate from "intermediate" state to "fault" state.

The model also has three repair-type state transition rates:

μ_M: rate of maintenance,

μ_{PT}: rate of maintenance,

μ_R: rate of repair.

The above rates can be calculated as

$$\mu_M = 1/T_M,\ \mu_{PT} = 1/T_{PT} \text{ and } \mu_R = 1/MTTR \tag{5}$$

where T_M is the periodic interval of maintenance, T_{PT} is the periodic interval of the proof-test and $MTTR$ is the mean time to repair.

The following equitation describes transition matrix for the Markov model:

$$P = \begin{bmatrix} -\left(\lambda_1^{DU} + \lambda_2^{DU}\right) & \lambda_2^{DU} & \lambda_1^{DU} & 0 \\ \mu_M & -\left(\mu_M + \lambda_3^{DU}\right) & \lambda_3^{DU} & 0 \\ \mu_M & 0 & -\left(\mu_M + \mu_{PT}\right) & \mu_{PT} \\ \mu_R & 0 & 0 & -\mu_R \end{bmatrix} \tag{6}$$

So the differential equation for the state probabilites:

$$\frac{dX}{dt} = P \cdot X \tag{7}$$

where the X is a column vector of the state probabilites: $(X_1, X_2, X_3, X_4)^T$ as defined in Figure 5.

4.4 Simulation Results

To investigate the effect of degradation we chose three cases:

1. In the first case, there is no degradation failure, but only sudden failure. I.e. $\lambda_1^{DU} = 2.5\ 10^{-}6$ 1/h, $\lambda_2^{DU} = \lambda_3^{DU} = 0$ 1/h.

2. The second case, there is sudden failure and sudden failure too assuming that the rate of sudden and degradation failure is the same. I.e. $\lambda_1^{DU} = 1.25 \cdot 10^{-6}$ 1/h, $\lambda_2^{DU} = 1.25\ 10^{-6}$ 1/h, $\lambda_3^{DU} = 1.25 \cdot 10^{-6}$ 1/h

3. The third, there is no sudden failure but only degraded failure. I.e. $\lambda_1^{DU} = 1.25 \cdot 10^{-6}$ 1/h, $\lambda_2^{DU} = 1.25\ 10^{-6}$ 1/h, $\lambda_3^{DU} = 1.25 \cdot 10^{-6}$ 1/h.

The three different cases illustrates the effect of degradation on the proof test. As the degradation becomes more and more important the proof test will have less less effect on the PFD even if the covarage factor of the proof test is 100%, and on the other side, the maintaince become more and more imporant.

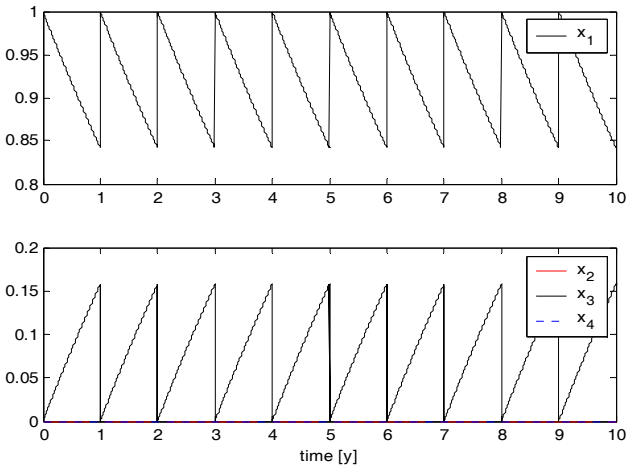


Figure 6
Simulation results: 1. case

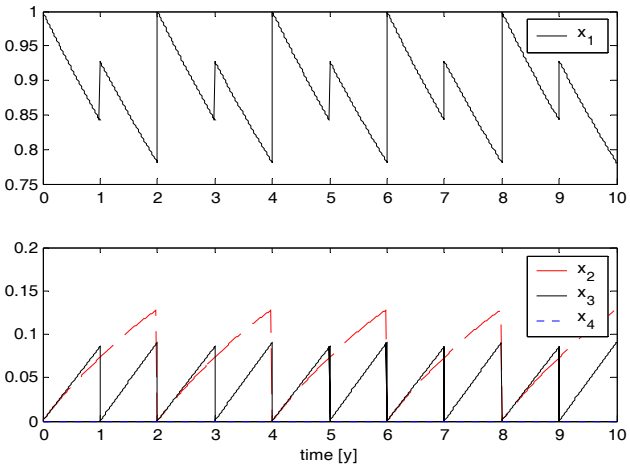


Figure 7
Simulation results: 2. case

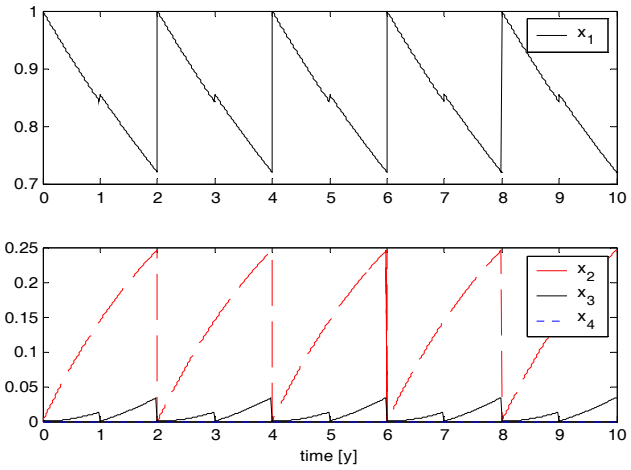


Figure 8
Simulation results: 3. case

Conclusions

The E/EP/EPS safety systems play the very important role in the functional safety engineering. These systems realize the so-called Safety Instrumented Functions (SIFs) which are widely used everywhere in the process industry. The goal of SIFs is to prevent the accidents but - because nothing is perfect - even a SIF may fail when there is a demand to perform its function. The main measure to avoid that is the proof testing, i.e. testing the SIFs if they have undetected failure or not.

The proof testing of E/EP/EPS safety systems are defined in the safety standards (IEC 61508 and 61511) but the interpretation of it is problematical. The model offered by the standard is too simple and generates problems introducing the proof test coverage factor into the functional safety practice without any interpretation and examples of it. We illustrated that there it is not unambiguous how to choose that factor and there is a conflict between the different practical considerations when one ask about its meaning.

We showed that there is a need to focus on the feature of dangerous undetected type failure and to find a good model which can solve the above problem. We introduced a new model for dangerous undetected failures that can incorporate the degradation type failures. The simulation results of the model shows that as the degradation failure become more and more important the efficiency of the proof testing is decreasing and the maintenance become more and more important.

Acknowledgement

Authors would like to acknowledge the support of the Cooperative Research Centre (VIKKK) (project III/2) and Hungarian Research Found (OTKA T049534). János Abonyi is grateful for the support of the Bolyai Research Fellowship of the Hungarian Academy of Sciences and the Öveges Fellowship.

References

[1] TÜV Book, Microcomputer in Safety Application, Safety Classes 1…5 level

[2] DIN 3100 – General Requirement, AK 1…8

[3] DIN V VDE 081 Microprocessors in Safety Application

[4] DIN V 19250 Basic Safety Evaluation for Measurement & Control

[5] DIN V 19250 Requirements & Measures, Qualitative Consideration

[6] VDE 0116 Electrical Equipment for Burner Application

[7] DIN EN 954 Safety for Machinery

[8] IEC 61508 1 – 7: Functional safety of electrical / electronic/programmable electronic safety - related systems.

[9] IEC 61511 1 – 3: Functional Safety: Safety Instrumented Systems for the Process Industry Sector

[10] R. J. Tiezema, Risk Reduction in the Process Industry - Proof testing, 2003

[11] M. J. M. Houtermans, J. L. Rouvroye, D. Karydas, Risk Reduction Through Partial Stroke Testing, 2004

[12] W. M. Goble and J. V. Bukowski, "Development of a Mechanical Component Failure Database," 2007 Proceedings of the Annual Reliability and Maintainabiltiy Symposium, NY: NY, IEEE, 2007