Advantages of Detecting Failed Individual Components of Redundant Safety Systems in the High/Continuous Demand Rate Mode

Luiz Fernando Oliveira and Siegfried Eisinger
DNV GL

ABSTRACT

The IEC 61508 standard on functional safety has become one of the most influential international standards related to safety and reliability in various industrial sectors. In the standard, two different ways to quantitatively evaluate the safety integrity level (SIL) of safety systems are proposed which depend on the demand rate regime that the SIS is subject to. The focus of this paper lies in the intermediate and high demand modes. We start from the concept of system hazard rate as the frequency of a hazardous event that leads to an accident in a process plant. For simplification, the process plant is assumed to be protected by a safety instrumented system (SIS) and, in this case, for the low demand rate the system hazard rate is a function of the frequency of an initiating event (also named the SIS demand rate) and the probability of failure on demand (PFD) of the SIS. The novelty of the current paper is that we investigate the effect of the demand rate on the hazard rate of redundant systems when the demand can detect the failed states of individual components which can then be repaired before the occurrence of the failure of the redundant safety system. The results of this paper show that, under this condition, the system hazard rate exhibits an unexpected behavior in the intermediate to high demand region. It is shown that under such conditions, the plant accident rate can be less than the values of the PFH calculated with the equations given in IEC 61508 by orders of magnitudes depending on the value of the SIS repair rate.

1. INTRODUCTION

Since the publication of its first edition, the IEC 61508 [1] standard on functional safety has become one of the most influential international standards related to safety and reliability in various industrial sectors. In the standard, two different ways to quantitatively evaluate the safety integrity level (SIL) of safety systems are proposed which depend on the demand rate regime that the SIS is subject to. A set of equations are proposed for the evaluation of the Probability of Failure on Demand (PFD) of SIS subject to low demand rates and a different set is proposed for the evaluation of the Probability of Failure per Hour (PFH) for SIS subject to high demand rates. It is thus necessary to establish in which of the two demand modes the SIS is operating before its SIL value is evaluated. For that, a discrimination rule is given in the Standard. Since the rule is offered without any accompanying sound explanation and it seems to be somewhat arbitrary, this subject has raised the interest of several analyst working in this field.

The influence of the demand rate on the safety integrity levels of safety systems was already recognized as an important factor much before the publication of the first edition of IEC 61508 [1]. Already in 1982, the issue was addressed in a paper by Lees [2] where he also listed some equations proposed as early as 1975 by Lawley and Kletz [3] to be used for high demand situations. In 1987, one of the authors (L.F.O.) co-authored two papers [4, 5] with the first (as far as we know) formal models for the evaluation of the hazard rate which explicitly included the demand rate in addition to the failure and repair rates of the system components. Markov models were used in both papers. A review of those models together with references to earlier work can be found in the book by Lees [6]. Still before the publication of IEC 61508, Frutuoso e Melo [7] developed a semi-Markov model to treat the problem to circumvent some of the known limitations of the Markov method which included considerations on the fixed periodic test periods and non-exponential repair times.

Since the publication of IEC 61508 [1] in 1998, some authors have addressed the issue of the effect of the demand rate and the different methods to evaluate the SIS reliability in the low and high demand regimes. A paper that appeared almost concomitantly with IEC 61508 [1] is that by Misumi and Sato [8] where the authors extensively investigate the relationships among demands, demand-states and proof-tests using fault trees. New ideas are proposed such as a demand-state, spurious demand-state, and mean time between detections. The explicit incorporation of the process demand in the reliability modelling of safety

systems also appeared in a Markov model proposed by Bukowsky [9] where it is concluded that the explicit incorporation of process demand is necessary to assess SIS safety performance appropriately, and that a simple arbitrary division between low demand and high demand is insufficient.

In his PhD Thesis, Innal [10] criticizes the ambiguity of the definitions of low and high demand modes given in the first editions of both IEC 61508 [1] and IEC 61511 [11].

Jin et al [12] extensively discussed several important aspects of the modelling for SIS reliability performance quantification, and used a Markov model to demonstrate their implementation. Among many others, they discussed the issue of the demand as a functional test of the safety system, and even touched on one of the central points of the current paper, which is the question of the demand being able or not to detect failed states of individual components of redundant systems. But they did not pursue it further because they restricted their application to a single channel system.

To close this brief review, it is important to say that the present paper was motivated by the research conducted by K. Tveit for her MS Thesis [13] at University of Oslo, of which some results were presented at ESREL 2015 Conference [14].

2. OBJECTIVES OF THIS WORK

The models developed in this work can be used throughout the whole spectrum of the demand mode, but the focus of this paper lies in the intermediate and high demand modes. We start from the concept of system hazard rate as the frequency of a hazardous event that leads to an accident in a process plant. For simplification, the process plant is assumed to be protected by a safety instrumented system (SIS). In this case, for the low demand mode, the system hazard rate is a function of the frequency of an initiating event and the probability of failure on demand (PFD) of the SIS. The initiating event is typically a plant-driven event which demands an action of the SIS to prevent the occurrence of a plant accident. Therefore, the frequency of the initiating event is also named the SIS demand rate.

As shown in Section 1, the general effect of the demand rate on the system hazard has already been studied by some authors [2-10]. The novelty of the current paper is that we investigate the effect of the demand on the hazard rate of redundant systems when the demand can detect the failed states of individual components which can then be repaired before the occurrence of the failure of the redundant safety system. The results of this paper show that, under this condition, the system hazard rate exhibits an unexpected behavior in the intermediate to high demand region.

The system hazard rate in the high demand region has been (incorrectly) named Probability of Failure per Hour (PFH) in IEC 61508. It is indicated by our results that depending on the SIS repair scheme, the use of Probability of Failure per Hour (PFH) based on the equations for a continuous demand as proposed in IEC 61508 leads to very conservative results in the high and continuous demand regions. This is very important for the industries that rely on safety systems that operate subject to high demands such as the railway industry.

3. DESCRIPTION OF THE WORK

3.1 General Considerations and Assumptions

The main considerations and assumptions made in the models used in this paper are listed below.

1. The only type of failure of the components of the safety systems which are taken into account is the dangerous undetected failures; this means we are neglecting the dangerous detected and the safe failures.
2. Component failure rates and repair rates are exponentially distributed.
3. Component failures are considered to be independent, therefore common-cause effects are not considered here.
4. Components of redundant safety systems are equal, that is, they have the same failure and repair rates.
5. Tests of components of redundant safety systems are periodically and simultaneously performed.
6. Tests and repairs are perfect. Test duration is neglected and the mean repair time is considered to be much less than the time between tests (but not negligible).
7. Multiple repair teams are available when needed.
8. The demand rate generated by disturbances in the process plant protected by the safety system is constant in time, that is, the number of demands in a given time interval is Poisson distributed with constant intensity.
9. Whenever the process plant is online, the generation of demands is independent of the status of

the safety system.

10. The demand is assumed to be instantaneous, that is, demand duration is not taken into account.
11. In the Markov model, calculations are done for the period between two consecutive proof tests which are assumed to be repeated throughout the life of the process plant; average values are obtained for the cited interval.

Some assumptions, such as 1, 3, 6, and 10, are adopted because they help highlight the features of the models that we want to convey in this paper. The consideration of exponentiality of the failure and repair rates assumptions is made because it is inherent to the Markov model and is also used in all references. Other assumptions, such as 4, 5, 7, and 9, are adopted here because they approximate very well the usual practice in the process industry. The consideration of assumption 8 is made for the sake of simplicity and because it is a very reasonable one with respect to what happens in the process industry. Assumption 11 would not be necessary if a multiphase Markov method were used but under assumption 6 (typical of industry practice), the differences in results are very small. All the adopted assumptions can be relaxed with the simulation method. The Markov model can also conceptually treat several of them but in some cases, the complexity increases so much that the model may become practically untreatable.

Both Markov and simulation methods were used in this paper. Separate calculations were run to make sure that the results are correctly obtained. The two methods give very similar quantitative results that fit the same descriptions throughout the whole demand space from low to continuous demands.

3.2 - Modelling

Two models are analyzed in this work and they are differentiated among them by the capability of a demand to reveal failed states of individual components of redundant systems.

When the SIS is in a failed state, the demand always detects this condition, simply because the SIS safety function will not be accomplished and an accident will happen. On the other hand, when the SIS is in a working state, the demand will always indicate this condition but it may or may not reveal the failed states of individual components of redundant systems. That depends on how the safety system is configured. For instance, in the case of a 1oo2 blocking system, if one of the components is up and the other is down, the SIS safety function will be accomplished by the up component. When this happens, the operators may or may not learn that one of the components is down, depending on whether the SIS is or is not configured to indicate such condition.

Therefore, with respect to this factor, the two models considered in this paper are:

- **Model A**: the demand is not capable of detecting failed states of individual components when the SIS is in a working state, and
- **Model B**: the demand is capable of detecting failed states of individual components when the SIS is in a working state.

In IEC 61508 [1] it is not considered that a demand can reveal the failed state of a channel when the system is in a working state. But it does consider that a test can detect the failed state of a single component (when the system is in a working state) and that its repair is conducted with the plant online. Nevertheless, the latter condition is only important in the low demand region.

3.3 – Markov Models

Markov models have been developed for 1oo1, 1oo2, 1oo3, and 2oo3 safety system configurations, but only the Markov model for the latter configuration are presented here. The Markov model diagrams for the 2oo3 system are given in **Figure 1** for Model A and in **Figure 2** for Model B. In both figures the triplet in parentheses (X,Y,Z) indicate the number of working channels (X), number of failed undetected channels (Y) and number of failed detected channels (Z) in the state (definition of the states).

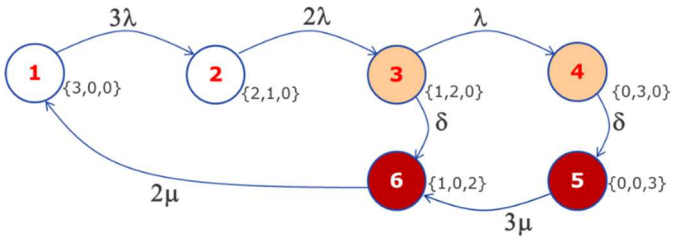

Figure 1 - Markov diagram for Model A of 2oo3 system

In **Figure 1**, states 3 and 4 are the states where the safety system is failed (both channels are down, either detected or undetected), and thus the occurrence of a plant demand at those states lead to the plant hazard states 5 and 6. Therefore, the average plant hazard rate for the 2oo3 configuration of Model A, $\eta_{2oo3\text{-}A}$, can be shown to be given by Equation 1.

$$\eta_{2oo3-A} = \frac{1}{T_1}\int_0^{T_1} \delta.[P_3(t) + P_4(t)]dt \qquad (1)$$

In Equation (1), T_1 is the interval between tests, δ is the demand rate, and $P_3(t)$ and $P_4(t)$ are the probability of the safety system being in states 3 and 4, respectively, at time t.

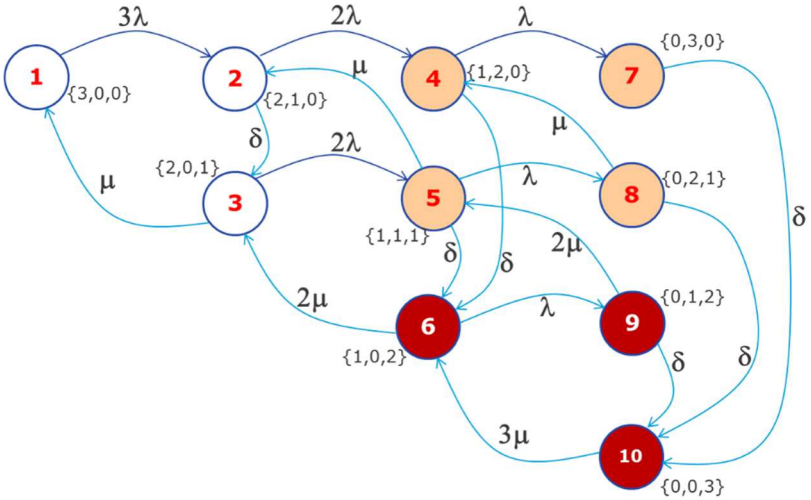

Figure 2 - Markov diagram for Model B of 2oo3 system

In **Figure 2**, states 4, 5, 7 and 8 are the states where the safety system is failed (both channels are down, either detected or undetected), and thus the occurrence of a plant demand at those states lead to the plant hazard states 5 and 6. Therefore the average plant hazard rate for the 2oo3 configuration with Model B can be shown to be given by Equation 1.

:

$$\eta_{2oo3-B} = \frac{1}{T_1}\int_0^{T_1} \delta.[P_4(t) + P_5(t) + P_7(t) + P_8(t)]dt \qquad (2)$$

where the other variables have the same definition as those of Equation (1).

3.4 – Simulation Models

The analysis of intermediate demand mode systems is not straight forward due to the fact that there is a combination of periodic tests and demands. The latter are at least not periodic and are often assumed random, with a constant demand rate, δ. Another complication is given by the component and system level of detail. While failures, repair and proof testing happens on component level, demand and hazards happen on system level. Component level analysis can be performed by Markov Analysis, but the extension to the

system level renders the analysis too complicated because of the large number of states and, in any case, limited to the intrinsic assumptions of the Markov method.

One method which overcomes all the above-mentioned difficulties is that of the Discrete Event Simulation [15]. It is shown here that even the Rare Events Problem, which is often a challenge in very reliable safety system analysis can be solved in a satisfactory way.

As the system to be analyzed here clearly involves states, generalized state modelling represents a good choice for model representation both on the component and on the system level.

State models thus generalized were proposed by Harel (see [16]), which represents also the implementation chosen in this project. The general simulation tool ExtendSim [17] is chosen for modelling and analysis.

On the component level a rather simple repairable component is modelled. Failures happen with a constant rate and are assumed hidden until they are detected by either a demand or a test. In the present article, the time to repair is assumed to be exponentially distributed. The simplicity of the model is mostly triggered by the wish to be able to compare our results with previously published results and with Markov analysis (see Section 3.4). Most assumptions can be made less stringent and more realistic within the framework of the present simulation analysis.

The Harel State Chart model for a 1oo3 system is shown in **Figure 3** together with the component sub-model used in the 'Single Systems'.

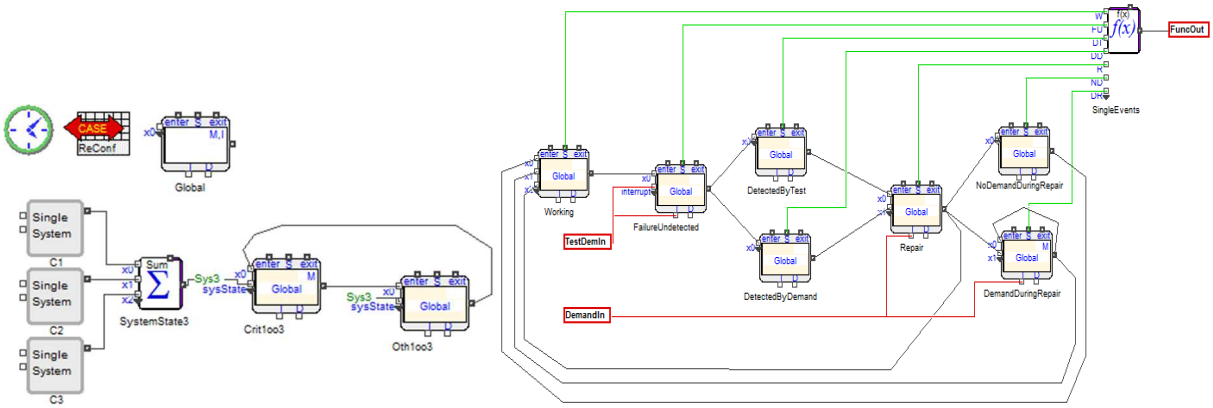

Figure 3 - State model of a 1oo3 system together with component sub-system

This model can be used for direct simulation where all test and demand triggers are generated explicitly. Unfortunately, such direct modelling runs into rare-event problems (see [?]) for high demand rates and for small proof test intervals. This rare event problem is for example caused by the fact that most demands find the system with all components working and only relatively few demands find one component in the failed state - thereby (possibly) detecting this failure and initiating repair actions. Obviously, the system hazard represents the rare event and the many demands which find everything working represent the events which are not really interesting for the analysis, but which use up most of the processing time during a simulation. The problem is overcome through only explicitly generating the test triggers and the demand triggers which are really necessary. Harel State Chart modelling allows to efficiently implement such rules.

4. OBTAINED RESULTS

4.1 Results for the 2oo3 Configuration

The results for the 2oo3 configuration are shown in Figure 4 for models A and B. The following data were used in the calculations: $\lambda = 10^{-2}$/yr, $\mu = 10^{3}$/yr, and T_1 = 1yr, where λ is the dangerous undetected failure rate, μ is the repair rate (μ=1/MRT), and T_1 is the interval between tests.

From Figure 4 it can be seen that for an MRT of around 10 h, a large value for most applications of high reliability systems, the results of the plant hazard rate for Model B are a factor of about one thousand below those of Model A in the high/continuous demand region. This is a clear indication of the importance of configuring the safety system such that any demand causes a detection of failures of individual components of the safety system.

In **Figure 4** the lines are obtained with the Markov methods and the blue crosses and green dots are the results obtained with the simulation method. As can be seen they indicate an almost perfect match

between the results of the two methods for the 2oo3 configuration which is the most demanding one for the Markov method in this paper. The same type of match between the results of the two methods is obtained for the results of all other configurations indicated in this paper.

It is interesting to point out that the asymptotic result for the Model A curve in **Figure 4** coincides with the results obtained with the PFH equation for high demand mode given in IEC 61508 [1]. Therefore, it can be concluded that if a redundant safety is logically configured such that a demand is capable of detecting that an individual component is failed when the system is not and the failed component is repaired upon detection, then the PFH for such safety system is orders of magnitude less than that calculated with the equations from IEC 61508. This is a very relevant finding for the cases of industries that work in the high or continuous demand regions, such as the railway and automotive.

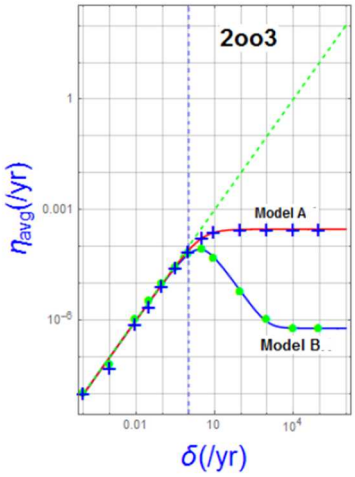

Figure 4 - Plant Hazard Rate as a Function of Demand Rate for the 2oo3 Configuration

4.2 Results for the 1oo2 Configuration with Varying MRT

Values of plant hazard rate, h, as a function of the demand rate for the 1oo2 configuration obtained with Model B are shown on **Figure 5** for different values of the mean repair time (MRT). As can be seen, the no-repair results for Model B coincides with those of Model A, which makes sense because there is no advantage on having the demand identify the failed state of an individual channel of a redundant system if one cannot fix it after detection.

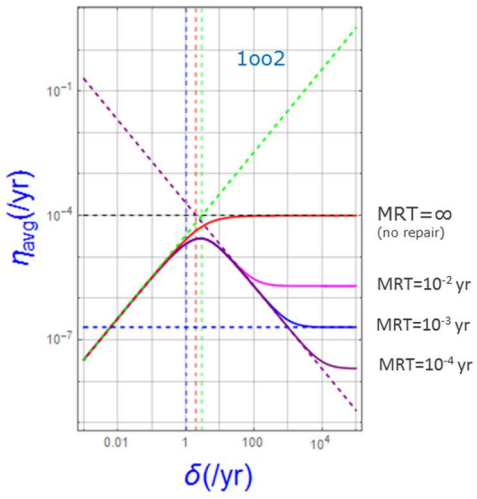

Figure 5 - Effect of reduction of mean repair time on the system hazard rate for 1oo2 system

It can be concluded from **Figure 5** that as the repair times become smaller (higher repair rates), the plant hazard rate in the high/continuous demand region also becomes smaller. The reason is that the probability that a demand finds the two channels in a failed state decreases with the reduced MRT or faster repair rate (a detected failed channel is more often repaired before the second one enters the failed state).

5. CONCLUSIONS AND FINAL COMMENTS

Although the general effect of the demand rate on the system hazard rate has already been studied by some authors after the publication of the IEC 61508 Standard (see Section 2), the novelty of the current paper is that we investigate the effect of the demand on the system hazard rate for two different conditions of redundant SIS, which we labeled as Models A and B. In Model A, the demand is not capable of revealing failed states of individual components when the system itself is in a working state. This assumption has been used in the studies of other authors cited in Section 2. In Model B the demand is capable of detecting the failed states of individual components which can then be repaired before the occurrence of the failure of the redundant safety system.

The results of this paper show that, under this condition (Model B), the system hazard rate exhibits an unexpected behavior in the intermediate to high demand region: it actually reaches a maximum and then goes down with the increase of the demand rate until a point where it levels off. It is also indicated by our results that depending on the SIS repair scheme, the use of Probability of Failure per Hour (PFH) based on the equations for a continuous demand as proposed in IEC 61508 leads to very conservative results in the high and continuous demand regions. This is very important for the industries that rely on safety systems that operate subject to high demands such as the railway industry.

6. REFERENCES

[1] International Electrotechnical Comission (IEC), Functional safety of electrical/ electronic/programmable electronic safety-related systems, IEC 61508 standard, International Electrotechnical Comission (1998).

[2] F. P. Lees, A general relation for the reliability of a single-channel trip system, Reliability Engineering 3 (1982) 1–16.

[3] H. G. Lawley, T. A. Kletz, A high-pressure-trip systems for vessel protection, Chemical Engineering 82 (1975) 81–92.

[4] L. F. Oliveira, J. D. Amaral Netto, Influence of the demand rate and repair rate on the reliability of a single-channel protective system, Reliability Engineering 17 (1987) 267–276.

[5] L. F. Oliveira, R. Youngblood, P. F. F. Frutuoso e Melo, Hazard rate of a plant equipped with a two-channel protective system subject to a high demand rate, Reliability Engineering 28 (1990) 35–58.

[6] F. P. Lees, Loss Prevention in the Process Industries, 2nd Edition, Butterworth-Heinemann Ch. 13, 1996.

[7] P. F. F. Frutuoso e Melo, On the application of semi-markovian processes to the unavailability analysis of protection systems of the voting logic type, Ph.D. thesis, Federal University of Rio de Janeiro, (in Portuguese only) (1992).

[8] Y. Misumi, Y. Sato, Estimation of average hazardous-event-frequency for allocation of safety-integrity levels, Reliability Engineering and System Safety 66 (1999) 135–144.

[9] J. Bukowsky, Incorporating process demand into models for assessment of safety system performance, in: Proceedings of RAMS06 Symposium, Alexandria, VI, USA, 2006.

[10] F. Innal, Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of iec 61508 standard, Ph.D. thesis, University of Bordeaux (2008).

[11] International Electrotechnical Comission (IEC), Functional safety - safety instrumented systems for the process industry sector, IEC 61511 standard, International Electrotechnical Comission (2003).

[12] H. Jin, M. A. Lundteigen, M. Rausand, Reliability performance of safety instrumented systems: a common approach for both low-and high-demand mode of operation, Reliability Engineering and System Safety 96 (2011) 365–373.

[13] K. Tveit, Safety instrumented systems operated in the intermediate demand mode, Master's thesis, University of Bordeaux (2008).

[14] S. Eisinger, L. F. Oliveira, K. Tveit, Safety instrumented systems operated in the intermediate demand mode, in: Proceedings of ESREL 2015, Zurich, Switzerland, 2015.

[15] S.Robinson, Simulation The practice of model development and use, Wiley, 2004.

[16] D. Harel, Statecharts: A visual formalism for complex systems, Science of Computer Programming 8 (1987) 231–274.

[17] I. That, Extendsim. power tools for simulation, Imagine That www.extendsim.com.