



Improvement in Reliability Quantification to Support BS EN 61511 Failure Probability Analysis

Mahesh Kodoth^{a,*}, Tadahiro Shibutani^b

^aGraduate School of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan

^bCenter for Creation of Symbiosis Society with Risk, Yokohama National University, 79-5 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan
 mahesh-kodoth-cd@ynu.jp

Estimation of failure rates provides a key input to quantitative risk assessment (QRA) quantification. International functional safety standard such as BS EN 61511 specifies use of realistic and credible failure data in failure probability analysis. In traditional reliability assessment, mean time to failure is one of the most common approaches to field failure data analysis. Unfortunately, new technology, such as hydrogen failure data is extremely limited. One possible way is to use surrogate failure data from other settings such as commercial nuclear power plants, chemical plants, and offshore oil and natural gas platforms. The proposed Bayesian framework addresses the requirements by allowing industry knowledge about failure rates to be incorporated in a prior gamma distribution and periodic updating process with new survival data as it becomes available. Monte Carlo simulation is adopted which make it practical to solve uncertainty in the failure rate estimation and update these models with many trials in seconds. The result shows that the process of updating failure rate with more samples of new observations and modelling failure data uncertainty using Monte Carlo simulation can be effective in improving reliability quantifications in the existing BS EN 61511 standard.

1. Introduction

Probabilistic risk assessment (PRA) has been widely adopted within the process industries to provide performance based design of the safety instrumented systems (SIS). PRA gained widespread attention since the introduction of the ANSI / ISA S84 (1996) standard. To ensure that the probabilistic calculations in the PRA and SIS design are relevant and meaningful, validation of PRA is necessary. The international standard for functional safety BS EN 61511 (2016) specifies for using credible, traceable and realistic failure rate data in failure probability analysis. However, in reality, these requirements have proven difficult for end-users because of the lack of failure data records and large amount of sample data required for frequentist methods. Lack of failure data leads to uncertainty in risk and reliability quantifications making risk assessment decisions weak. In BS EN 61511 reliability assessment, mean time to failure (MTTF) is one of the most common approaches to field failure data analysis. MTTF and similar metrics are used for situations with a constant failure rate. In other words a piece of equipment has the same chance to failure at any point in time i.e. the chance of failing at 11th hour and the chance of failing at 110th hour is the same. However, this is generally not true for systematic failures encountered in hazardous sites. The most common mechanism of failures in the industry is erosion, corrosion, fatigue, cracks etc. When the right conditions exist, corrosion starts, grows and eventually over time leads to failures. Mahmoodian (2014) describes the older the equipment the more likely it will fail due to corrosion, thus not a constant failure rate. This shows that an overall MTTF may alter the risk assessment results. Over the past several decades, enough information has been collected on MTTF from several sources to estimate failure rates. OREDA (2015), one of the largest data source, combines data from multiple sources. The OREDA data distribution is very wide and uncertainty intervals span 1 or 2 orders of magnitude. One reason for the variability in rates is that these datasets include variations on the environment and service conditions.

Paper Received: 22 October 2018; Revised: 3 May 2019; Accepted: 14 July 2019

Please cite this article as: Kodoth M., Shibutani T., 2019, Improvement in reliability quantification to support BS EN 61511 failure probability analysis, Chemical Engineering Transactions, 77, 571-576 DOI:10.3303/CET1977096

Moreover, new technology or major accident hazards with low probability has limited or no failure data. Under such circumstances, traditional methods are not of much benefit. Even the life data distribution to model the time to failure is not of much use because the time to failure data is not available for new systems. Under such condition, the users are constrained from using traditional approach to reliability engineering.

This paper draws conclusions on how failure rates and failure probability can be controlled in practice. The proposed Bayesian framework addresses the above requirements by providing a periodic updating process that allows industry knowledge about failure rates to be incorporated in a prior distribution and cyclical updated with new survival data as it becomes available. A sensitivity analysis is further carried out to perform uncertainty modelling on failure rate using Monte Carlo simulation. The outcome of this work would help to predict maintenance intervals. The results can be integrated with predictive and preventive maintenance strategies as suggested by Abbassi et al. (2016) whilst maintaining overall system availability and safety.

2. Literature Review

In QRA, risks are calculated from likelihood of scenarios and their consequences. Estimation of failure rates provides a key input to QRA quantification. Unfortunately, hydrogen failure data is extremely limited. One possible way is to collect failure data from other process such as oil and gas or power plants using Oreda (2009). Casamirra et al. (2009) used the fault tree analysis (FTA) to determine frequency of the accident scenarios based on generic failure data. Another way is to employ a Bayesian statistical approach to estimate failure rate from prior data. LaChance et al. (2009) developed a Bayesian model to estimate leak frequency in various components used in a hydrogen refuelling stations.

QRA methods contain a large amount of uncertainty due to the lack of field failure data. The verification and validation of QRA has become a great concern to public acceptance of HRSs. The validity of QRA was reviewed by Goerlandt et. al. (2016). Generic validity approaches such as benchmark tests have been proposed, but it was pointed out that an evidence-based approach is needed to support the validity of QRA results. Pörn (1996) proposed a “two-stage” update of the hierarchical Bayesian process, although the procedure format is quite different since it preceded the widespread availability of computerized Bayesian algorithms. Newer methods for treatments of hierarchical Bayes are covered by Drogue et al. (2006). Hierarchical Bayesian models may also be viewed as a special case of a Bayesian Belief Networks. Khakzad and Reniers (2015) proposed a Bayesian network (BN) methodology to estimate both on-site and off-site risks posed by major accidents in chemical plants.

3. Estimation and interpretation of failure rate using statistical model

The BS EN 61511 standard recognizes the impact of lack of quality reliability data on the PRA result. Justification of failure data is an important measure to provide verification of risk analysis as proposed as reviewed by Goerlandt et al. (2016). The standard demands that:

“Reliability data used in quantifying effect of random failures should be credible, traceable, documented and justified based on field feedback”

BS EN 61508- Part 2 (2010) states that:

“The reliability data uncertainties shall be taken into account when calculating the target failure measure”.

There are basically two types of model that can be applied to reliability modelling. Frequentist approach is commonly used in reliability calculation but one disadvantage is that they do not consider prior knowledge. The Bayesian approach is adopted in this paper to provide more benefits and will be discussed in detail hereafter. As each model has a different application, suitable care should be taken to apply the correct model to the data.

3.1 Estimation of failure rate based on Gamma approximation (Bayesian method)

In reference to the note in Clause 11.9.2 of IEC 61511-1 regarding confidence in reliability data, mean time to failure (MTTF) is typically determined by recording the number of failures (n) which occur in a sample of components during an accumulated number of operating hours (T). However, the failure data can be extremely limited, which in this case, will not be taken into account and can lead to uncertainty in reliability modelling. Japan Nuclear Technology Institute (2017) introduced the Bayesian method to enable the uncertainty width of failure rate to be updateable with data storing, which until then had a fixed value. The nuclear report considers the failure rate as constant over time and the probabilistic variance is updated by new data. Similar approach is adopted in this paper for BS EN 61511 application and discussed in detail hereafter. Data scarcity and constant failure rate uncertainty problem can be addressed using gamma approximation with Bayesian inference to estimate the failure rate. The model presented uses gamma approximation to produce prior distribution with uncertainty. The likelihood function (new observation) is modelled using Poisson

function. Based on the joint likelihood of Poisson distribution and the parameters of the gamma approximation, Bayesian inference is established to analyze survival data. The sensitivity analysis is then performed on the updated failure rate to reduce the uncertainty to as low as possible.

3.1.1 Prior Distribution

There are many techniques and considerations to be taken when selecting a prior distribution. For the purpose of this paper, the main focus is on feasibility, simplicity and mathematical traceability for engineers. For these reasons, a Gamma approximation was chosen as the prior distribution. Prior knowledge will be assigned from external industry data sources. The parameters α and β are estimated using Dutch red book model (1997) as:

$$\alpha = \frac{x^2}{Var} \quad (1)$$

$$\beta = \frac{x}{Var} \quad (2)$$

Where, x - Positive random variable, Var - Variance of the sample data

3.1.2 Likelihood (evidences)

In reality, BS EN 61511 reliability calculations are typically based on the exponential distribution, which is a special case (i.e. where $x = 0$) of the more general Poisson distribution. The Gamma distribution is a "conjugate prior" of the Poisson likelihood function which enables Bayesian equation to be solved analytically and elegantly. Given a constant failure rate (λ), the Poisson distribution gives the probability of failures (x) per time (t), as shown below.

$$P(x_i, t_i | \lambda) = e^{-\lambda t} \frac{(\lambda t)^x}{x!} \quad (3)$$

In the completed model, the variables x and t will take the place of the evidence $f(T_1 | \lambda)$ in Eq. (4). The survival time and number of failures data will be obtained through new observations from failure records.

3.1.3 Sampling of Survival Data using Bayesian Inference

Based on the Bayes' theorem, the relationship between the prior, the posterior, and the likelihood function is written as:

$$f(\lambda | T_1) = \frac{f(T_1 | \lambda) * f_0(\lambda)}{\int_0^\infty f(T_1 | \lambda) * f_0(\lambda)} \quad (4)$$

Note: T_1 is the first occurrence of failure or survival time. In Eq. (4), λ is the unknown parameter of interest distributed with posterior $f(\lambda | T_1)$, $f_0(\lambda)$ is the prior distribution of λ . Subsequently, $f(T_1 | \lambda)$ is the likelihood function that updates a prior distribution. Using the standard equation of Bayesian update from the Dutch Red book (1997), the gamma parameter update is given by,

$$\alpha' = \alpha + n_f, \quad (5)$$

$$\beta' = \beta + T_s, \quad (6)$$

Where, n_f is number of failures and T_s is survival time.

The updated mean and variance can be calculated using Maximum Likelihood method (MLE) with the formula:

$$x = \frac{\alpha'}{\beta} \quad (7)$$

$$Var = \frac{\alpha'}{\beta^2} \quad (8)$$

Using Eqs. (5), (6), (7) and (8), the posterior distribution mean can be expressed as

$$E\{f(\lambda | T_1)\} = \frac{\alpha'}{\beta} \quad (9)$$

In other words, α parameter can be converted to number of failures, β can be converted to the total survival time. The initial prior parameters are denoted as α_0 and β_0 . After the first update of these parameters based on new observation, the parameters are called α' and β' .

4. Practical application of proposed model to BS EN 61511

4.1 Estimating Initial value of Gamma parameters

The prior value of gamma parameters α_0 and β_0 should be carefully chosen as they have large impact on Bayesian updating process. To make this selection, data for valve failure rates was gathered from a variety of

industry data sources such as OREDA (2016). A total of 20 independent dangerous failures for operating valves were collected to produce prior distribution and obtain values for α_0 , β_0 . These data are only used as informative prior to establish prior distribution. Based on the 20 independent failure data for valves, the mean and variance is calculated as:

Mean (x) = 0.0335 failures / year, Variance = 0.0015

Now, the initial values, α_0 and β_0 are calculated using Eq. (1) and Eq. (2) as $\alpha_0 = 0.75$, $\beta_0 = 22.33$.

4.2 Bayesian Update

After describing how to calculate Bayesian model in Section 3, we are presenting some examples to illustrate the application of this model for case specific scenarios. We have obtained case specific data from the Japan Hydrogen and Fuel Cell Demonstration Project – Phase 2 (2011) and Phase 3 (2014). The project analyzed 17 failures that were observed in the various Hydrogen stations operated from FY2002 to FY2013. 6 out of 17 failures were related to process valves. The survival time data chosen are for 6 process valves. The data on valve failures were further analyzed and reliability related information were extracted for use in this paper. The data extracted from the JHFC Phase 2 (2011) project is shown below:

Table 1: Valve survival data from JHFC report

ID	Component	Start Date	Failure Date	Survival (days)	Survival (years)	KHK - ID
1	Check Valve	2003/2/7	2010/6/15	T1 = 2685	7.4	2010-135
2	Suction Valve	2007/8/8	2013/7/30	T2 = 2183	6.0	2013-356
3	Gate Valve	2003/4/1	2007/10/17	T3 = 1660	4.5	2007-532
4	Gate Valve	2010/6/16	2013/2/6	T4 = 966	2.6	2013-037
5	Gate Valve	2012/4/9	2012/10/17	T5 = 191	0.5	2012-314
6	Check Valve	2013/4/19	2013/5/22	T6 = 33	0.1	2013-115

The survival data chosen to demonstrate different aspects of updating in chronological order is: 7.4, 6.0, 4.5, 2.6, 0.5, and 0.1. The six survival time (in years) reported occurs independently and are assumed to follow Poisson distribution (Likelihood function). As illustrated in Section 3.2, the Gamma parameters Alpha and beta are converted to number of failures and survival time respectively. Bayesian update is performed by calculating the parameters of posterior distribution, α' and β' . Table 2 also shows the updated α' , β' , posterior mean and variance for each component based on Eq. (5) and Eq. (6).

Table 2: Bayesian update result

Comp. ID	Component	Survival (in years)	α'	β'	Updated variance	Updated failure rate λ (per hour)
1	Check Valve	7.4	1.75	29.73	2.26×10^{-7}	6.72×10^{-6}
2	Suction Valve	6.0	1.75	28.33	2.49×10^{-7}	7.05×10^{-6}
3	Gate Valve	4.5	1.75	26.83	2.78×10^{-7}	7.45×10^{-6}
4	Gate Valve	2.6	1.75	24.93	3.21×10^{-7}	8.01×10^{-6}
5	Gate Valve	0.5	1.75	22.83	3.83×10^{-7}	8.75×10^{-6}
6	Check Valve	0.1	1.75	22.43	3.97×10^{-7}	8.91×10^{-6}

From Table 2, it can be noticed that there is no significant difference in the failure rates for all six components. All failure rates are within the same order of magnitude. One of the reason could be the updated failure rate is sensitive to generic data uncertainty due to less number of new observation. In order to obtain more realistic data, more observations should be analyzed in order to improve the sensitivity of updated failure rate. For this reason sensitivity analysis using Monte Carlo is performed. Gate valve has minimum three data cases (see Table 2) which is chosen as an example for illustration purpose. In total, three failures occurred at 4.5, 2.6 and 0.5 years respectively. The new values of α' , β' and λ is calculated as:

$$\alpha' = 3.75 \quad \beta' = 29.93 \quad \lambda = 1.43 \times 10^{-5}$$

5. Sensitivity analysis on failure probability using Monte Carlo method

The initial values of α_0 and β_0 can result in uncertainty in the distribution of failure rate due to generic data and therefore a Monte Carlo simulation is adopted in this paper for the uncertainty analysis on the failure rate. In the field of reliability engineering, BS EN 61511 (Ed.2 2016) commonly uses probability of failure on demand (PFD) metric for understanding the performance of safety. The PFD is calculated from the failure rate based

on equation in the BS EN 61508 (2010). The uncertainty analysis on 1oo2 valve system for PFD is shown below:

5.1 Failure Probability Modelling for 1oo2 Final elements Configuration (Valve)

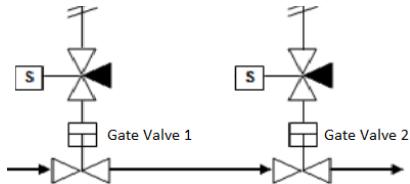


Figure 1: 1oo2 Configuration of final element (Gate valve)

In the process sector industry, the safety function PFD is dominated by the final elements due to relatively higher failure rate and architectural constraint. With 1oo2 valve configuration, the PFD is calculated as:

$$PFD_{1oo2} = (1 - CCF) \frac{\lambda^2 \cdot t_i^2}{3} + \frac{CCF \cdot \lambda \cdot t_i}{2} \quad (10)$$

Where, λ - Failure rate, CCF - Common cause factor (Beta), t_i - Inspection interval in hours.

The total failure rate for gate valve is estimated to be 1.43×10^{-5} failures per hour. The lambda λ is assigned gamma distribution with Mean: 1.43×10^{-5} , Variance: 4.77×10^{-7} . The inspection interval t_i is assigned triangular distribution with minimum value of 8400, likeliest value of 8760 and maximum value of 9000. The inspection period is 8760 hours (annual test). The CCF is assigned uniform distribution with minimum value of 0.01 and maximum value of 0.04. This means the CCF ranges between 1% and 4%. The failure probability calculation computed using Eq. (10) in Monte Carlo simulation after 1000 trials is shown below:

Table 3: Failure probability on demand calculation

Parameter	Value	Distribution	Comment
λ	1.43×10^{-5}	Gamma	Failure rate of dangerous undetected failures (per hour)
M	1	NA	Minimum number of component failures causing system failure
N	2	NA	Number of redundant "channels" of sub function
CCF	0.02	Uniform	Common cause factor
t_i	8760	Triangular	Inspection interval in hours
$PFD(1_{oo2})$	2.51×10^{-3}	Output	Total failure probability on demand

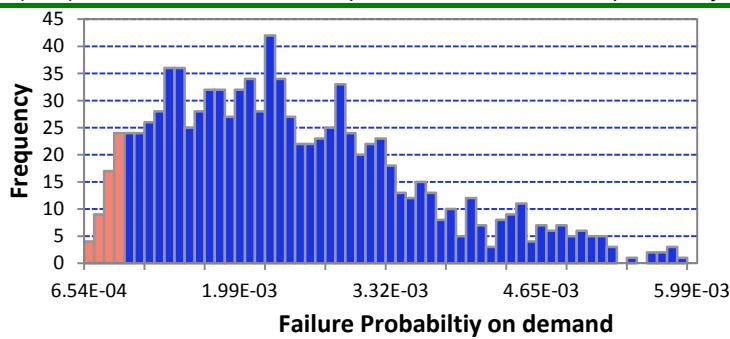


Figure 2: PFD Uncertainty Analysis using Monte Carlo

The PFD forecasts using the Monte Carlo simulation is executed for 1000 number of trials for acceptable uncertainty analysis on failure rate. The blue area in the graph is the certainty range for the estimated value of PFD. The red area is the uncertainty range. Figure 2 shows the PFD certainty range is from 1.00×10^{-3} to 1.00×10^{-2} (SIL 2) based on annual inspection and certainty level of 90%. The base value of PFD for this configuration is estimated to be 0.00251. This is equivalent to SIL 2 classification as per BS EN 61511 SIL classification. The forecasts of failure probability for different inspection intervals is presented in Table 4.

The Monte Carlo simulation allows to model failure probability for all possible values of λ and t_i put together in the calculation. The final PFD certainty range is estimated to be in SIL 2 range with base value of 0.00251 based on 1 year inspection interval and 90% certainty level.

Table 4: Valve Failure Probability Forecast based on failure rate estimation

Failure rate, λ (per hour)	Inspection Interval	Inspection Interval (hours)	Failure Probability on demand	BS EN 61508 SIL Class [Achieved]
1.43×10^{-5} (Gamma function)	Monthly	720	2.06×10^{-4}	SIL 3
	Quarterly	2160	6.18×10^{-4}	SIL 3
	6 months	4320	1.24×10^{-3}	SIL 2
	Yearly	8760	2.51×10^{-3}	SIL 2

6. Conclusion

The Bayes framework expands on the single-stage model and allows data from available sources to be leveraged in the updating process. The Bayesian methodology provides a flexible, coherent framework for managing failure rate data for any component. Monte Carlo simulation make it practical to solve uncertainty in the failure rate estimation and update these models in seconds. The process of updating failure rate with new observations and modelling failure data uncertainty using Monte Carlo simulation will result in lower uncertainty and narrower posterior distribution. It is observed that with less number of new observations, the updated failure rate is sensitive to generic uncertainty data which does not provide realistic result. In order to improve the sensitivity of updated failure rate, more number of observations subject to modelling using Monte Carlo method will be beneficial. The final PFD certainty range for 1002 gate valve is estimated to be in SIL 2 range with base value of 0.00251 based on 1 year inspection interval and 90% certainty level. In order to achieve failure probability in the range of SIL 3, the inspection interval on valve across installations should be carried out at least once in 3-6 months interval. The appropriate base value can be used in design set performance standards for availability and reliability in operation and maintenance of the component.

References

- Abbassi R., Bhandari J., Khan F., Garaniya V., Chai S., 2016, Developing a quantitative risk-based methodology for maintenance scheduling using bayesian network, CET, 48, 235-240 DOI:10.3303/CET1648040
- ANSI/ISA S84.01, 1996, Application of Safety Instrumented Systems for the process control industry, ISA, USA.
- Aven. T., Heide. B., 2009, Reliability and validity of risk analysis, Rel. Eng. & Sys Safe, vol. 94, pp.1862 to 1868.
- BS EN 61511-1 Ed 2, 2016, Functional Safety – Safety Systems for the Process Industry, Geneva, Switzerland.
- BS EN 61508, 2010, Functional Safety of Programmable Electronic Safety-Related Systems: Part 1-4. BS, UK.
- Casamirra M, Castiglia F, Giardina M., Lombarado C., 2009, Safety studies of a hydrogen refuelling station: Determination of the occurrence frequency of the accidental scenarios, International Journal of Hydrogen Energy, Vol. 34, pp. 5846-5854.
- Dutch Red Book, CPR 12E, 1997, Methods for determining and processing probabilities, Committee for the Prevention of Disasters, The Hague, The Netherlands.
- Droguett E.L., Groen F.J., Mosleh A., 2006, Bayesian assessment of variability of reliability measures. Pesquisa Operacional.
- Goerlandt F., Khakzad N., Reniers G., 2016, Validity and validation of safety-related quantitative risk analysis: A review, Safety Science, Vol. 99, pp. 127-139.
- Japan Nuclear Technology Institute, 2016, Estimation of domestic general equipment failure rate considering uncertainty of failure counts, http://www.genanshin.jp/archive/failure_rate/; [accessed Sept 2017].
- Khakzad N., Reniers G., 2016, Application of bayesian network and multi-criteria decision analysis to risk-based design of chemical plants, Chemical Engineering Transactions, 48, 223-228 DOI:10.3303/CET1648038.
- LaChance J., Houf W., Middleton B., Fluer L., 2009, Analysis to Support Development of Risk-Informed Separation Distances for Hydrogen Codes and Standards, Sandia Report, SAND2009-0874.
- Mahmoodian M., Alani A., 2014, A gamma distributed degradation rate model for reliability analysis of concrete pipes subject to sulphide corrosion, International Journal of Reliability and Safety, vol. 8, no. 1, pp. 19-32.
- Oreda Offshore and Onshore Reliability Data Handbook Vol 1, 6th edition, 2015, SINTEF Technology and Society: Department of Safety Research, Trondheim, Norway.
- Pörn K., 1996, The two-stage Bayesian method used for the T-Book application, Reliability Engineering & System Safety, Volume 51, Issue 2, Pages 169-179.
- The Japan Hydrogen and Fuel Cell Demonstration Project (JHFC Phase2), 2011, http://www.jari.or.jp/Portals/0/jhfc/data/report/pdf/tuuki_phase2_01.pdf, Japan.