Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 84 (2014) 2 – 11

Procedia Engineering

www.elsevier.com/locate/procedia

"2014ISSST", 2014 International Symposium on Safety Science and Technology

Challenges in the context of the development and application of risk-informed regulations in the domain of safety technology

Peter KAFKA*

Bureau Veritas Austria GmbH, Habeintenweg 129, A-9710 Feffernitz, Austria

Abstract

Safety regulations have a long historical perspective. Organizations like DIN, German Institute for Standardization (founded in 1917), ISO, International Organization for Standardization (founded in 1947), IEC, International Electrical Commission (founded in 1906) are promoters in that domain. The new era and the main focus of the paper are the transition of regulations from the descriptive format towards to a proactive format considering prognostic elements like: "what can happen if". The transition to risk-informed regulations creates numerous challenges for the development and application on both performers, the inventor of the regulation and the user working at the industry. A successful transition is not only a typical technical and organisational achievement but also a legislative and juristic problem which has to be resolved. In the central part of the paper are typical challenges and drawbacks between the wishes of the regulators and the reality in industries representing the various domains of safety technologies. A substantial challenge is to gain the prerequisite for utilizing risk-infirmed regulations, namely to learn from the past for the prediction into the future. The learning from the past must be realised twofold. First, qualitatively based on verbal descriptions, underlined by physical data of abnormal events, incidents and accidents, perceived in the past, and secondly, quantitatively based on statistical evidence of probabilities of the occurrences. A significant category of statistical information needed is the so-called failure rate Lambda (λ) of a specific failure mode of the component of interest. Obviously, to payback lessons learned and to utilise and publish it in failure reports is in contrary to the strategic attitude of traditional industries. Finally, the paper summarizes some recommendations, were the leading focus of the diverse industrial endeavours should be to apply the selected examples of risk-informed regulations successfully.

Peer-review under responsibility of scientific committee of Beijing Institute of Technology

Keywords: Safety Regulations; Transition to risk-informed regulations; Challenges for utilisation; Analysis of operational experience; Quantitive prediction of future behaviour; Statistical information; Industrial examples

* Corresponding author. Peter Kafka, Tel.: ++43 720 350 335; Fax: ++43 720 350 335
E-mail address: drpkafka@aol.com

Peer-review under responsibility of scientific committee of Beijing Institute of Technology
doi:10.1016/j.proeng.2014.10.404

1. Introduction

Safety regulations have a long historical perspective. Organizations like DIN, German Institute for Standardization (founded in 1917), ISO, International Organization for Standardization (founded in 1947), IEC, International Electrical Commission (founded in 1906) are promoters in that domain. The development and application of safety regulations at the beginning of the last century was driven by so-called "Trial and Error" strategies. Malfunctions, near misses or accidents observed and properly analysed were the initiators to overhaul existing regulations or to establish an advanced one.

Looking at the market place of current regulations one can recognise that the new set of the risk-informed regulations are the transition from the descriptive format towards to a proactive format considering prognostic elements like: "what can happen if".

Standardisation organisations are working hard to harmonise worldwide as best as possible the main regulatory issues across the various standards. But differences in safety culture, financial and technical resources and the existing legislative basics and structures around the globe are drawbacks in that initiative. As a consequence industries and all the safety engineers and safety regulators involved have to consider these inconsistencies between various international standards and have to balance requirements and the technical options.

Obviously, the transition to risk-informed regulations creates numerous challenges for the development and application on both performers, the inventor of the regulation and the user working at the industry. The successful transition is not only a typical technical and organisational achievement but also a legislative and juristic problem in various countries which has to be resolved obviously,

Typical challenges and weaknesses between the wishes of the regulators and the reality in industries representing the various domains of safety technologies are the main focus of this paper. Such as in simple words the "Quantification of Safety" in form of risk-informed numbers based on operational experience in the field and the prognostic estimation of the future behaviour of the functional unit (FU) of interest. Evidently, the prognostic estimation of future behaviour cannot be categorized with "Yes and No Statements"; the term and the meaning of "Probability" came into the game.

The following Table 1 shows important risk-informed regulations for various industrial sectors.

Table 1. The world of risk-informed regulations versus years (not exhaustive).

Year 1980	1985	1990	1995	2000	2005	2010	
Aeronautics	DO 178 DO 178 A			DO 178 B ARP 4754	ARP 4761	DO 264	DO 178C ARP4761A
Rail Transport					EN 50155	IEC 61500 EN 50126- EN 50129	
Generic Standard						IEC 61508	EN DIN 61508
Industrial Automation						IEC 61508 IEC 61511 IEC62061	IEC 61508 Edition3
Automotive						IEC 61508	ISO 26262
Machinery							DIN EN 62061
Medicine							IEC 60601 Edition3

2. The essence of risk-informed regulations

Looking into the risk-informed regulations at the market place which are applicable generically for various products of different industries (e.g. EN DIN 61508, [1]) or specifically for products of a given industry (e.g. ISO 26262; Automotive [2]) the first response of the reader is normally: "so many parts and pages (some hundreds); who should read and understand that at all". In other words it is not an easy task to filter out the normative essence for the daily work at the office. But anyway, risk-informed regulations are in essence:

- Focussed on the avoidance of unwanted consequences created by the use case of the product throughout the life cycle for the user and/or the humans in the hazardous area.
- Structured procedures to attain the risk level below the normative allowable limits.
- Normative for all the specific phases throughout the life cycle of the product. From the concept phase until the decommissioning of the product. Normally, these phases are treated in different "parts" of the regulations.
- To execute two major tasks:
  Firstly, the determination of the inherent risk in the product under consideration the use case, and
  Secondly, the demonstration that the normative requirements, based on the determination of the inherent risk are fulfilled and placed within the allowable limits.
- To perform some tasks "numerically respective quantitative" in the domain of systems reliability by using and estimating well established reliability figures e.g. failure rates Lambda (λ) and relative simple equations to calculate e.g. unavailability of a given system function per demand for a standby system or over time for an operational system. To illuminate these calculations and equations the following Fault Metrics and Target Values from ISO 26262, Part 5 is referenced here below:

  The failure rate λ of each safety-related hardware element can therefore be split up as follows (see equation (1) taken from [2], Part 5):

  a) Failure rate associated to hardware element single point faults: λ_{SPF}
  b) Failure rate associated to hardware element residual faults: λ_{RF}
  c) Failure rate associated to hardware element multiple point faults: λ_{MPF}
     1) Failure rate associated to hardware element perceived or detected multiple point faults: $\lambda_{MPF\,PD}$
     2) Failure rate associated to hardware element latent multiple point faults: $\lambda_{MPF\,L}$
  d) Failure rate associated to hardware element safe faults: λ_{S}

  with the sum of $\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}$ and $\lambda_{MPF} = \lambda_{MPF\,DP} + \lambda_{MPF\,L}$ (1)

  The failure rate assigned to residual faults can be determined using the diagnostic coverage of safety mechanisms which avoid single point faults of the hardware element. The single point faults matric, the latent faults matric and the correlation of the faults matric and the target values of the different ASIL levels are shown in details within the ISO 26262, Part 5 [2].

The determination of the inherent risk is not normative harmonized and frozen across the product type at the various industries and the countries. Some usual methods and tools for that are listed and explained in the regulations. E.g. the so called "Safety Case"has to be analysed via a Hazard Analysis (HA) [3]or a Failure Mode and Effect Analysis (FMEA) [4] and the determined inherent risk level defined by substantial "parameters".

Typically, the substantial parameters are twofold: the estimated amount of consequences and the associated probabilities respective frequencies. Beside this two parameter system there existsa three parameter system with a specific estimate for the possibility to identify the risky case under consideration (diagnose parameter), or to avoid the unwanted consequences, or escaping the hazardous area, or to perform a specific human intervention by the user of the product (see also [2]).

The two parameter system is normally in use in a matrix format and the three parameter system, as a "decision tree" format. Examples are given in Table 2 (matrix format) and Table 3 (decision tree format).

In the following Table 3 the Risk Graph for ASIL determination is shown. The graph-table should be read from left to right, beginning with the estimated parameter S via the parameter E and then the parameter C. Finally, in the respective box the resulting QM or ASIL is shown.

Table 2. A typical Risk Matrix showing Consequences versus Frequencies.

Consequences / Frequencies	Negligible	Marginal	Critical	Catastrophic
Certainly	High	High	Extreme	Extreme
Likely	Moderate	High	High	Extreme
Possible	Low	Moderate	High	Extreme
Unlikely	Low	Low	Moderate	High
Rare	Low	Low	Extreme	High

Table 3. The decision table for determination of a required ASIL level taken from ISO 26262 [2].

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

It means:

S1 to S3 Severity (health impact on the driver)
S1: light and moderate injuries; S2: severe and life-threatening injuries (survival probable);
S3: life-threatening injuries (survival uncertain), fatal injuries.

E1 to E4 Exposure (of the driver to the risky situation)
E1: very low probability, E2: low probability, E3: medium probability, E4: high probability.

C1 to C3 Controllability (by the driver)
C1: simply controllable; C2: normally controllable; C3: difficult to control or uncontrollable.

QM Quality Management sufficient

A, B, C, D resulting ASIL A, B, C, D

Additional to the Table 3 for determination of the required ASIL Level Tables are given to show the required reliability of safety functions related to the SIL/ASIL level. In Table 4 such typical requirementsare listed. These requirements are taken from EN DIN 61508 [1].

Table 4. The required reliability of safety functions related to the required SIL Level taken from [1].

SIL	Small Failure Rate / year failure / demand ≤ 1 times per year	High Failure Rate / year failure/hour ≥ 1 times per year or permanently
1	10E-2 until 10E-1	10E-6 until 10E-5
2	10E-3 until 10E-2	10E-7 until 10E-6
3	10E-4 until 10E-3	10E-8 until 10E-7
4	10E-5 until 10E-4	10E-9 until 10E-8

Based on such risk-informed safety determinations and the respective requirements of functional safety the detailed proof has to follow that the product, normally composed by hardware and software, all the normative requirements of the respective standard are met. Considering the volume of 3 to 4 hundred pages of a typical risk-informed standard this proof is time consuming and not worthwhile here to explain in detail (see ISO 26262 [2]).

3. The challenges at the transition to risk-informed regulations

The normative requirements in risk-informed regulations for hardware units working within the product of interest statistical information from the field to use representative for various types of e.g. failure rates are probably the most significant challenge for the successful adoption of these regulations.

Obviously, for some typical hardware units such statistical information is available in reliability data base handbooks e.g. OREDA Handbook [5], SINTEF Handbook [6], T-Book [7], ZEDB Handbook [8], EXIDA Handbooks [9] and the old MIL Handbook 219F [10]. But the industry itself is mostly the criticiser that these data bases are not representative for their own product. The establishment of a product specific reliability data base would be the way out from this dilemma.

3.1. To collect and to document operational experience of the product in the field

The collection of operational experience for the establishment of a product specific reliability data base needs to pool very specific information from the field which is not routinely in the various available log books regarding field experiences like, systems stops and downtimes, maintenance and repair orders, spare part statistics and all the other costs and investments data sheets.

The type of data needed and therefore should be collected can be categorized as following:

- Product data, e.g. identification data, specification data, boundary conditions of the product;
- Function unit data, e.g. specification data, location data, boundary conditions the FU;
- Operational data, e.g. continuous operation or stand by, operational cycles;
- Malfunction data, e.g. initiating event, number of failures, failure modes, failure consequences, failure detection;
- Maintenance and repair data, e.g. preventive and corrective maintenance, repair or replacement;
- Re-engineering data, e.g. improvement and/or re-engineering of the FU caused by insufficient reliability in the field.

The typical boundary conditions for a FU, like a motor-operated valve is given herewith:

- Valve casing and the internals
- Gearbox including position indicator
- Switch box including power switch, connection relays and the electrical safety features
- Electrical motor
- Drive control unit including priority settings
- Cabling

For illumination what information is needed in the category of malfunction data Table 5 is given.

However, this table can never be exhaustive because the variability of FUs in the great number of products in today's industry is tremendous. Please be aware that all the listed field aspects have some sub-aspects typical for the considered product and FU.

Table 5. Examples of information needed to collect for the establishment of a reliability data base.

Field Aspects	Meaning
Initiating Event	Which event or event chain has triggered/initiated the failure of the FU (FU)?
Failure	Loss of the specified function at a specified point in time
Failure Mode	Type of the loss of the specified function
Failure Consequence	Consequence of the loss of the specified function at various system levels of the product
Main Function	Main function specified for the product
Support Function	Support function for support systems within the product
Maintenance	Specified maintenance actions for the FU
Preventive Maintenance	Performed preventive maintenance actions to hold the FU working
Corrective Maintenance	Performed corrective maintenance actions to restore the FU in working conditions by repair or Replacement
Operation	Is the FU in operation when the product is working?
Stand By	Is the FU stand by and in operation only if the product needs their function?

3.2. To analysethe collected operational experience

The analysis of operational experience with respect to the establishment of a reliability data base can be performed in different ways. Firstly, in the frequentistic coverage and secondly based on the Bayes approach.

The analysis of operational experience needs some basic actions as required in all traditional statistical evaluations. In particular the

- Formation of the statistical universe
- Description of the random sample
- Definition and description of the variables which have to be evaluated e.g. the failure rate Lambda λof a FU

In case of the adoption the frequentistic coverage the Maximum-Likelihood Estimator must be evaluated with the following formula (2) and (3) for the point value of the failure rate Lambda λ:

$$\hat{\lambda} = \frac{k}{\sum_{n=1}^{N} T_n}, \text{ and} \tag{2}$$

$$\sum_{n=1}^{N} T_n = T \tag{3}$$

k…..number of observed failures of a function unit in the statistical universe
N….number of function units in the considered statistical universe
T_n…observation time span

The estimation of the upper and lower limits of the confidence intervall must be executed by the formula (4) and (5) using the Chi-Square Distribution of the observed failures.

$$\bar{\lambda} = \frac{\chi^2(2k; \frac{1-\gamma}{2})}{2T} \tag{4}$$

$$\bar{\lambda} = \frac{\chi^2(2(k+1); \frac{1+\gamma}{2})}{2T} \tag{5}$$

Chi-Quadrat Distribution defines: $2k$ and $2(k+1)$ the degree of freedoms dependant from the number of failures k. The parameter γdefines the confidence interval. Normally 0.9 is chosen; that means with equation (4) and (5) the 5 % and the 95 % confidence limit for the failure rate is calculated.

The unavailability per demand has to be estimated analogies to the failure rate during operation. The model assumed is normally a binominal distributed statistical universe. This is the case if the probability of failure per demand is constant over all the demands.Additionally, it is assumed that the repair or restoration after failure is perfect, that means the FU is after repair "as good as new".The observed random sample should be homogeneous so the unavailability of the FUcomposed in the statistical universe is identical.

The adoption the Bayesian approach has compared to the frequentisticcoverage significant advantages. Thus, it allows the consideration of apriori information gained at other similar products and a mathematical consistent quantification of uncertainties also in case of small numbers of failures. Additional to the uncertainties invented by the small numbers of failures, the approach creates further uncertainties. The model assumption of e.g. a Poison processis an approximation of the real worldand the random sample includes normally similar but not enough similar FUs. The same situation is given with respect to operational and environmental conditions.

The Bayesapproach is customarily executed as anone-stage simulation process, and advanced, a two-stage simulation. In this case the apriori information from similar FUs is combined with the information and state of knowledge observed at the current case.

The elementary Set of Bayes for a failure rate reads as following:

$$f(\lambda|E) = \frac{L(E|\lambda) f(\lambda)}{\int_0^\infty L(E|\lambda') f(\lambda') \mathrm{d}\lambda'} \tag{6}$$

$L(E \mid \lambda)$.....is the likelihood function which describes the probability that the experience E (k failures during observation period) under the condition that thetruth value of λ represents the parameter needed.
$f(\lambda \mid E)$…… is the probability density function.

At the analysis of observations it is assumed that the life time of the FUs is exponential distributed and therefore the failure rate as constant. With this reasonable assumptionthe likelihood function is given as a Poison distribution. This distribution represents the probability that k failures are observed under the condition that $\lambda$is the truth parameter.

$$L(E|\lambda) = \frac{(\lambda T)^k}{k!} \mathrm{e}^{-\lambda T} \tag{7}$$

It means**:**
$L(E \mid \lambda)$ ..Likelihood function
λ.....Failure rate
T…….Observation time

k…….Number of failures

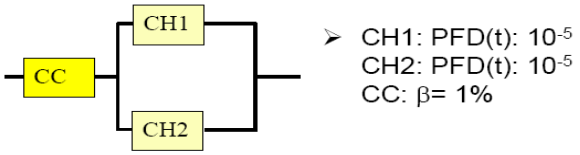
All mathematical and statistical details regarding the one-stage and two-stageBayesian approach are given in the relevant handbooks and in the industrial case study [12] which is availableon the Internet.

3.3. Consideration and quenitification of Common Cause Failures (CCF)

There is ample evidence available from the operational experience that redundant FUs can fail together within a considered small time interval (see also [1], [12]). Such events are called Common Cause Failures (CCFs). The reason for these CCFs can be very manifold. E.g. the similar hidden fault in redundant units is a trigger for a failure or a common unwanted operational condition creates the commonloss of function.

Obviously, such CCFs are relatively rare compared with the typical failure rate of the FU in the range of 10E-5 /hour and 10E-6/hour. But please consider, for a redundant arrangement of two FUs thestatistical independent failure probability would be the multiplication of the single probabilities (AND gate logic). In case of common elements which triggers the common failure anadditional possibility is given namely the common failure additional to the single failures.

Reliability experts have developed a handful different modelsto quantify the CCF effect [11] and have tested these models in the real world with different success. In this contribution one of the simplestmodel which is also referenced informative for use in EN DIN 61508 is shown here below in Figure 1:



$$PFD = PFD_{CH1} \cdot PFD_{CH2} + CC$$

$$PFD = 10^{-10} + 10^{-7}$$

Fig. 1. The principle of the β-Factor Model to quantify CCF probabilities taken from [1].

It means:
CC…..Common Cause
CH1…Channel 1
CH2…Channel 2
PFD… Probability of Failue per Demand

As demonstrated with generic numbers the PFD for the FU is dominated by the Common Cause Failure also if a CCF is relatively rare and estimated with a Beta factor $\beta = 1$ % of the independent PDF of each channel CH1 and CH2.

In some risk-oriented guidance and regulations (e.g. in the Aviation Guidance ARP 4754) it is required to avoid CCFs per se by preventive design features and therefore the quantification of CCFs is not required. Such a guidance is in conflict with the operational experience and anactual accident in aviation (see e.g. the AF 447 in the 2009 accident caused by two frozen redundant Pitot tube sensors). Thus, from the real world we can learn that CCFs are possible also if preventive actions against CCFs are taken at the design of the product.

Additional to this simple Beta factor model the CCF experts developed some other advanced models to simulate as best the real world of common cause failures. As a reference for that developments please consult the literature (e.g. [11]). In [12] many CCF data in form of probabilities for CCFs are given based on real observed CCFs.

3.4. Consqunces for the use and adoption of risk-informed regulations

The main challenge for the use and adoption of risk-.informed regulations namely the quantification of failures of safety function units, represented by sensors, logic device and actuators, needs descriptive reliability figures for hardware units. There are twopossibilities to fulfill these normative requirements:

1) To select and to work with so-called generic data from relevant data systems if the assignability to the case of interest can be certified. If not,
2) To generate a product specific data base originated on the observed failures of the FUs in the field.

It has to bemassively criticizedif large industrial players, like Automotive or Aviation are not willing to spend the resources for the establishment of a product specific reliability data base, and as a consequence, they quantify the normative requirement with dubious reliability data and finally misleading results.

4. Concluding statements

- In the last decade there is a trend in safety technology to move from descriptive regulations towards risk-informed regulations.
- This is valid for so-called generic standards (e.g. EN DIN 61508 [1]) as well as for standards adopted for a specific industrial sector (e.g. ISO 26262 for Automotive[2], [13]).
- The transition creates certainly some challenges for all the users in industries and licensing authorities because some normative requirement are pretty new and therefore the users must be specifically educated and trained.
- The challenges are manifold but the most significant is probably the requirement to quantify numerically some reliability characteristics of the so-called safety function. Specifically, e.g. the failure rates for different type of failure modes of the safety functions and to demonstrate that dangerous failure frequencies are below the limits given by the required safety integrity levels SIL.
- These requirements need to consider and apply reliability figures (e.g. failure rates) for the various FUs either from a generic date base or a product specific one.
- This is a dilemma because generic data are normallycriticised as “non-representative for the considered safety case”, but on the other hand, product specific reliability figures are spars and not easy and cheap to generate.
- A furtherchallenge is given by the facts that many generic reliability date bases show relative small numbers for failure rates in the range of 10E-6/hour and 10E-7/hour and smaller. Compared with real numbers from product specific data bases (e.g. ZEDB [8]) such numbers must be classified as “too optimistic”.
- As a consequence the required unavailability for a safety function in the range of 10E-9/hour (e.g. for SIL 4) needs the installation of redundant FUs.
- From the operational experience in many technologies it is well know that also redundancies have some draw-backs because identical FUs in two channels can fail together with a given probability caused by common inherent faults or common unwanted systems condition (so-called Common Cause Failures, CCF).
- Knowing that some of the risk-informed regulations (e.g. EN DIN 61508 [1]) require to quantify also the effect of CCFs at least with the adoption of the so-called Beta (β) factor model (see part 3.3 above).
- All in all, the new risk-informed regulations create for industries and regulators significant challenges which can be resolved only by hard work, training and some investments.

References

[1] EN DIN 61508, Part 1 - 7, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010
[2] ISO 26262, Part 1-10, Road Vehicles, Functional Safety, 2011
[3] Center for Chemical Process Safety (1992), Guidelines for Hazard Evaluation Procedures, with Worked Examples (2nd Edition ed.). Wiley-American Institute of Chemical Engineers. ISBN 0-8169-0491-X.
[4] Failure Mode andEffect Analysis, DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA), November 2006
[5] OREDA Handbook, http://www.oreda.com/handbook.html
[6] SINTEF Handbook, http://www.sintefbok.no/Product.aspx?sectionId=65&productId=566&categoryId=10
[7] T-Book, Reliability Data of Components in Nordic Nuclear Power Plants,ISBN 91-631-0426-1
[8] ZEDB Handbook, http://www.vgb.org/shop/tw805.html

[9] EXIDA Handbook, http://www.exida.com/Books/Safety-Book-Package
[10] Mil Handbook 217F, http://findebookee.com/m/mil-hdbk-217f
[11] P. Hokstad, M. Rausand, Handbook of Performability Engineering, Springer Verlag, 2008
[12] BfS, Daten zur Probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand August 2008,
http://regelwerk.grs.de/wegweiser2009/RSH/3%20RSH%203-74.3%20PSA%20Datenband.pdf
[13] P.Kafka,The Automotive Standard ISO 26262, the innovative driverfor enhanced safety assessment & technology for motor cars, Paper, ISSST 2012, Nanjing, China.