IGEM/SR/15 Edition 5
COMMUNICATION 1746
2000

The following amendments (November 2015) apply to all copies of IGEM/SR/4 Edition 3 published in May 2010.

Clause 3.1.2.9 **Add new clause Societal Risk**

There is the separate issue of societal risk. An individual risk target reflects the exposure of one individual to multiple events, whereas societal risk reflects the exposure of multiple individuals to the same event. Instead of addressing the risk to an individual, the concern is with the tolerability of multiple fatality events (irrespective of the individual identities of the victims).

The number of potential fatalities should be assessed. This number may vary at different times of the day. The following example shows how a weighted average can be arrived at when overlapping groups of people are at risk over different periods of time:

For 4 hours per day, 60 persons are at risk
For 17 hours per week 10 persons are at risk
For 24 hours per day, 1 person is at risk.

Therefore, the weighted average of exposure is:
4/24 x 60 + 17/168 x 10 + 24/24 x 1 = 12 fatalities.

The next step is to address the Maximum Tolerable Risk. Unlike the Individual Risk criteria (see Table 3), which address the probability as applying to an Individual, the criterion becomes the frequency of a fatal event (irrespective of the individuals concerned). Whereas individual risk addresses a specific person(s), societal risk addresses the risk to a potentially changing group irrespective of their identity (for example the continuously changing occupants of a rail tunnel).

So, the criteria are expressed as frequencies for the event rather than risk to an individual, (see Figure 1). Therefore, for the 12 fatality scenario above a maximum tolerable failure rate for the event of 10^{-3} pa is suggested.

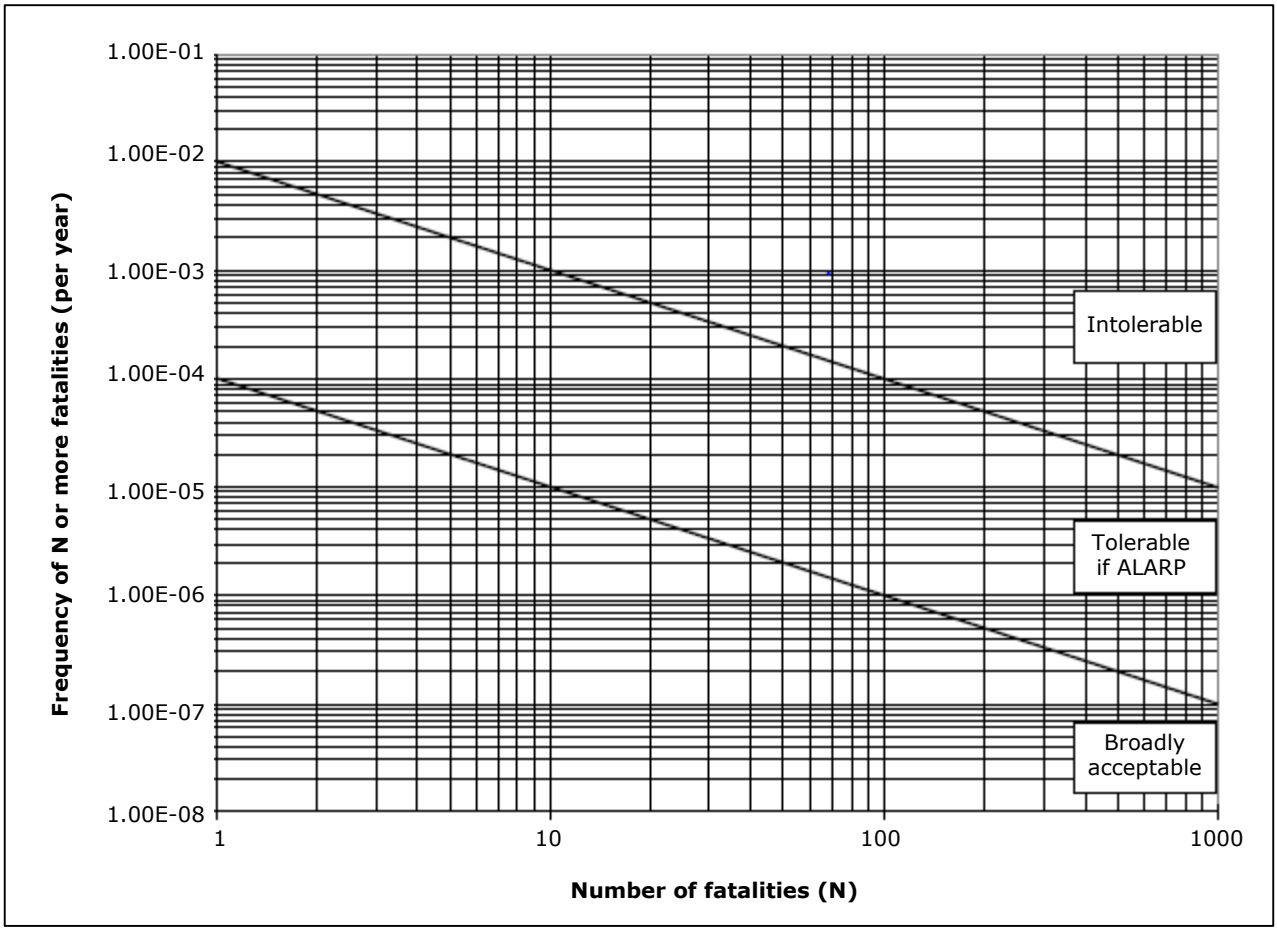

Figure 1 Criteria per number of fatalities

Note 1: This figure has no specific provenance but can be related to HSE document R2P2 by virtue of a 50 fatality target of 1 in 5,000 years (2 10^{-4}) maximum tolerable risk therein.

Note 2: Although expressed in log by log format, it is a relationship which can be summarised (where N is the number of potential fatalities) as:
Maximum Tolerable Frequency (societal) = $10^{-2}pa/N^{-1}$
Broadly Acceptable Frequency (societal) = $10^{-4}pa/N^{-1}$

Note 3: The propagation to fatality of an event is calculated as for Involuntary Risk but ignoring the element which addresses what proportion of the time anyone is at risk, it having been taken account of already in the Societal Risk concept.

Add Clause 3.1.2.10

Environmental and Production loss

Safety-integrity is normally associated with failures that lead to death or injury. BS EN ISO 61508 should be applied to failures leading to environmental damage and loss of production. Reference A2.5 item 1 offers some suggested criteria (see Table 5).

Target max Tolerable Frequency pa	Criteria Environment	Criteria Commercial
10^{-7}	Catastrophic Incident, 5 years effect on water, supply, food chain, or housing	>£500M
10^{-6}	Massive/significant incident (eg 1,000 fish/animals) 1-5 year effect on water, supply, food chain, or housing. Possibly International	<£500M
10^{-5}	Major Offsite Incident (eg Pollution of ground water, impact on fauna/flora). c1 year effect on water, supply, food chain, or housing	<££50M
10^{-4}	Major Offside Incident (eg Reservoir clean up, river remedial action) c1 month effect on water, supply, food chain, or housing	<£5M
10^{-3}	Significant Incident with minor contamination, no effect on water course	<£500,000
10^{-2}	Non-serious 'nuisance'/ odour Incident	<50,000
10^{-1}	Trivial on-site incident/release	<5,000

Table 5: Environmental risk targets

Sub-section 4.3

Add Clause 4.3. Common Cause Failure.

The basic BETA model applies to simple "one out of two" redundancy. This is a pair of redundant items where the "top event" is the failure of both items. However, as the number of voted systems increases (in other words N > 2) the proportion of common cause failures varies and the value of β should be modified.

The original suggestions were from a SINTEF paper (in 2006). The SINTEF paper was revised in 2010 and again in 2013. The IEC 61508 (2010) guidance is similar but not identical and is slightly less pessimistic.

Values for MooN configurations are not based on any empirical data and are a matter of conjecture and never likely to be demonstrated**.** Thu**s** there is no justification for more than single figure accuracy.

Table 9 offers the following compromise:

	M=1	M=2	M=3	M=4	M=5	M=6
N=2	**1**					
N=3	**0.4**	**2**				

N=4	**0.3**	**1**	**3**			
N=5	**0.2**	**0.6**	**1**	**4**		
N=6	**0.1**	**0.5**	**1**	**2**	**5**	
N=7	**0.1**	**0.3**	**0.7**	**1**	**3**	**7**

Table 9: Moon Factor from Betaplus (see A.25 item 3)

Note 1: Moon Factor – to be multiplied by the 1oo2 Beta factor.

Note 2: Values for MooN configurations outside the above table are also a matter of conjecture and the user is encouraged to use judgement.

Clause 4.4.2 **Add:**

Human error probabilities (see Sub-Section 4.3) are often of the order of 10^{-2}. Modifying conditions, such as ergonomics, familiarity, the presence of hazards etc should increase or decrease that figure in the typical range 10^{-1} to 10^{-3} depending upon whether the factor is favourable or unfavourable in respect of its error producing nature.

Regulators and reviewers tend to recommend the use of the pessimistic value of 10^{-1} unless it can be shown that some detailed human error study has been undertaken. A human error study should involve, modelling of the error probability, anecdotal data, written task descriptions and identification of the above modifying factors. It should be recognised that the lower the claim for human error probability then the more rigour is required in operational management to ensure continued and focussed availability of a competent operator commensurate with the error probability claimed.

Clause 5.1 **Delete 2nd paragraph entirely. Substitute:**

The safe failure fraction (SFF) should be calculated from the ratio:

$$\frac{\text{"safe" failures + diagnosed "dangerous" failures}}{\text{total ("safe" failures + "dangerous" failures)}}$$

A "safe" failure is a failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) Results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or
b) Increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.

Clause 10.2.2 **Add:**

Common practice involves calculating the GDF on a logarithmic scale as the individual risk reduces from the maximum tolerable to the broadly acceptable. It also scales the GDF from 10 to a minimum of 2. Table 10 shows the principle and the value calculated is used in the example in Appendix 4.

						IR	GDF					
BA	1.00E-07	2				2.10E-06	**5.80**					
MaxTol	1.00E-05	10										

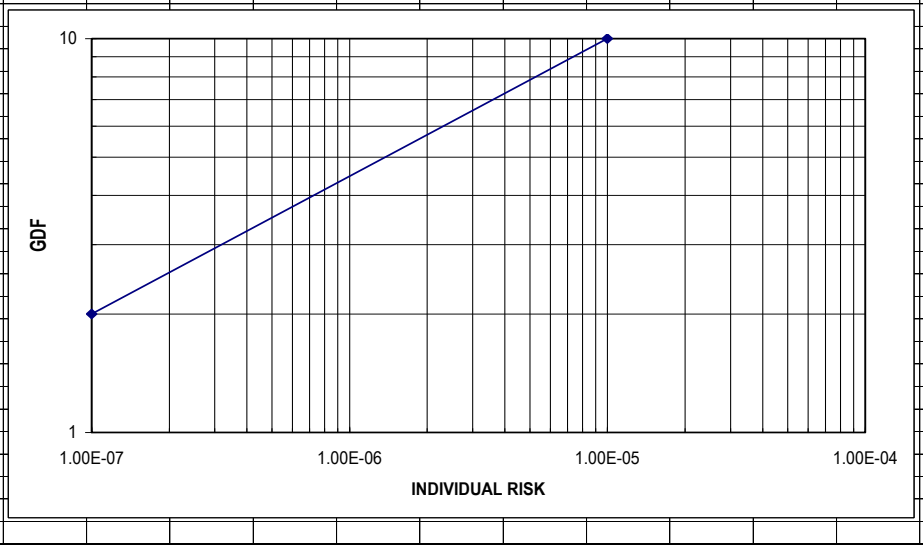

TABLE 10 – INDIVIDUAL RISK

Appendix 2.5 **Delete items 1 and 3 entirely. Substitute:**

Smith, D.J. and Simpson, K.G.L. Functional safety, a straightforward guide to IEC 61508, 4th Edition. Elsevier, 2004, ISBN 0 7506 6269 7.

Smith, D.J. BETAPLUS. User's Manual. Common cause failure package, Version 4.0. 1997, ISBN 0 9516 5625 2.

Appendix 4.3 **Delete cost equation entirely. Substitute:**

5.8x£2,000,000 = (max cost of proposal)/[($2.1 \times 10^{-6} - 1 \times 10^{-7}$) x 2 fatalities x 25 years]

Therefore the maximum cost of any proposal which could be justified on grounds of risk reduction = £1,160.

Appendix 5.2 **Delete Appendix entirely.**

Appendix 5.3 **Delete Appendix entirely.**

END OF AMENDMENTS.