CHAPTER 2

IEC 61508 Modes of Operation, Bernoulli- and Poisson-Process Modelling

We have seen that Bernoulli Processes and Poisson Processes can be used to model the behaviour of software. Bertrand Ricque raised the question how the concepts of Bernoulli and Poisson processes relate to the IEC 61508 notions of “Continuous/high-demand mode" and “low-demand mode". Those concepts of “mode” occur in Tables 2 and 3 of IEC 61508-1:2010 [1, Part 1: General Requirements], which set the safety requirements for safety functions. I explore here the relation between the statistical concepts and the IEC 61508 “modes”.

2.1 Concepts

Tables 2 and 3 of IEC 61508-1:2010 [1] give requirements on average probability of dangerous failure on demand, for “low demand mode” safety functions, and average frequency of dangerous failure per hour, for “high demand / continuous mode” safety functions, for given SIL levels 1-4. They are reproduced in Figures 2.1 and 2.2. (Note that the term PFD_{avg} will be extensively discussed later.) SIL stands for “Safety Integrity Level”. SILs are safety requirements, *the* safety requirements according to the conception of 61508. It follows that only safety functions may have safety requirements, and that these safety requirements specify the allowed probability/likelihood/frequency of a dangerous failure during execution of a safety function. Three oddities can be quickly remarked and clarified.

- There is no SIL 0. Safety functions must operate at least to the reliability of one dangerous failure in ten demands (low-demand mode), or one dangerous failure in 100,000 operational hours (ephors) in high-demand/continuous mode, so they must fulfil at least the requirements of SIL 1. (This is not explicit, and could be.)
- Read literally, SIL 4 seems to *require* that a low-demand safety function fail at least once in 100,000 calls ("$\geq 10^{-5}$") and a continuous-mode/high-demand safety function fail at least once in a billion operational hours ("$\geq 10^{-9}$"). In fact, the standard does not allow any claim of operational reliability more stringent that one failure in 100,000 demands, respectively one failure in a billion operational hours, to be made. These lower bounds reflect that requirement.
- Since continuous-mode SIL 4 specifies a rate of at most one dangerous failure in a period between one hundred million and a billion operational hours, it seems very odd to speak of a "frequency" as in Table 3, Figure 2.2, since the systems to which this might apply come generally nowhere near this number of operational hours. "Frequency" is a term which relates to actual events, not to hypotheticals. "Probability" and "likelihood" do not suffer from this reification, but nevertheless raise the question what they are. Neither IEC 61508, nor I in this essay, attempt to answer this question.

Safety Integrity Level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10{-}4$
3	$\geq 10^{-4}$ to $< 10{-}3$
2	$\geq 10^{-3}$ to $< 10{-}2$
1	$\geq 10^{-2}$ to $< 10{-}1$

Figure 2.1: SIL Definition for Low-Demand-Mode Safety Functions

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function per hour (PFH)
4	$\geq 10^{-9}$ to $< 10{-}8$
3	$\geq 10^{-8}$ to $< 10{-}7$
2	$\geq 10^{-7}$ to $< 10{-}6$
1	$\geq 10^{-6}$ to $< 10{-}5$

Figure 2.2: SIL Definition for High-Demand-/Continuous-Mode Safety Functions

2.2 Random and Systematic Failure

Definition [1, Part 4, Clause 3.6.4] says

> 3.6.4
> failure
>
> termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required
>
> .....
> NOTE 4 Failures are either random (in hardware) or systematic (in hardware or software), see 3.6.5 and 3.6.6.

Definition 3.6.5 concerns “random hardware failure” [1, Part 4, Clause 3.6.5], and 3.6.6 “systematic failure” [1, Part 4, Clause 3.6.6]. In particular, Note 4 to [1, Part 4, Clause 3.6.6] says

> NOTE 4 In this standard, failures in a safety-related system are categorized as random hardware failures (see 3.6.5) or systematic failures.

It follows from these two notes that:

> (†) All SW failures are characterised as systematic failures in IEC 61508.

This assertion is emphasised because it leads to the line of argument that, if all software failures are systematic, randomness and thus statistics plays no role in the analysis of software failures. This line of argument is incorrect. It is correct that SW

failures are systematic in that, if input I is presented to SW S, and S fails on I, S will always fail on I. But the process which presents I to S may well be stochastic, in which case failures-on-I is a stochastic process, which is surely worth investigating. Indeed, in complex systems, despite our attempts to eliminate as many as possible, there remain many sources of uncertainty, for example whether actual operational requirements are faithfully and completely reflected in the requirements specification, and capturing actual system behaviour in conditions of some uncertainty is what appropriate statistical methods do.

2.3 The IEC 61508 Definitions of On-Demand/Continuous Types of Failure

IEC 61508 Part 4 [1] defines the notions of "probability of dangerous failure on demand", "average probability of dangerous failure on demand", and "average frequency of dangerous failure per hour". Tables 2 and 3 of [1, Part 1], Figures 2.1 and 2.2 above, use the second and third of these notions. The definitions from [1, Part 4] are given here in full. Note that the various notions of unavailability now occur in IEC 60050 Part 192 (Dependability) rather than Part 191 (Dependability and Quality of Service) [9].

> 3.6.17
> probability of dangerous failure on demand
> PFD
>
> safety unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system
>
> NOTE 1 The [instantaneous] unavailability (as per IEC 60050-191) is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U (t).
>
> NOTE 2 The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before t. It characterizes an

item which only has to be able to work when it is required to do so, for example, an E/E/PE safety related system working in low demand mode

NOTE 3 If periodically tested, the PFD of an E/E/PE safety-related system is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

3.6.18
average probability of dangerous failure on demand
PFD_{avg}

mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system

NOTE 1 The mean unavailability over a given time interval [t1, t2] is generally noted by U (t1, t2).

NOTE 2 Two kind of failures contribute to PFD and PFD_{avg}: the dangerous undetected failures occurred since the last proof test and genuine on demand failures caused by the demands (proof tests and safety demands) themselves. The first one is time dependent and characterized by their dangerous failure rate DU(t) whilst the second one is dependent only on the number of demands and is characterized by a probability of failure per demand (denoted by .

NOTE 3 As genuine on demand failures cannot be detected by tests, it is necessary to identify them and take them into consideration when calculating the target failure measures.

3.6.19
average frequency of a dangerous failure per hour
PFH

> average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time
>
> NOTE 1 The term "probability of dangerous failure per hour" is not used in this standard but the acronym PFH has been retained but when it is used it means "average frequency of dangerous failure [h^{-1}]".
>
> NOTE 2 From a theoretical point of view, the PFH is the average of the unconditional failure intensity, also called failure frequency, and which is generally designated $w(t)$. It should not be confused with a failure rate (see Annex B of IEC 61508-6).
>
> NOTE 3 When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its unreliability $F(T) = 1 - R(t)$ (see "failure rate" above). When it is not the ultimate safety-related system its PFH should be calculated from its unavailability $U(t)$ (see PFD above). PFH approximations are given by F(T)/T and 1/MTTF in the first case and 1/MTBF in the second case.
>
> NOTE 4 When the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

The notion of "unavailability" is used in both PFD and PFH definitions. Note 3 to the definition of PFH says the the PFH of the "ultimate" safety-related system should be calculated from its unavailability, and refers to the definition of PFD. The definition of PFD says that the PFD is the "safety unavailability (see IEC 60050-191 [9]) of .....". Although IEC 61508 refers to IEC 60050, the reference to Part 191 is no longer apt. The term "availability" occurs twice in Part 191, namely in Definition 191-27-03 *service unavailability per customer served* and Definition 191-27-04 *service unavailability per customer interrupted*. Part 192 contains the appropriate definitions of "instantaneous unavailability", "mean unavailability", and "steady state unavailability", as follows.

192-08-04
Symbol $U(t)$
instantaneous unavailability

probability that an item is not in a state to perform as required at a given instant
192-08-06
Symbol $\bar{U}(t_1,t_2)$
mean unavailability
average unavailability

average value of the instantaneous unavailability over a given time interval (t1, t2)

Note 1 to entry: The mean unavailability is related to the instantaneous unavailability $U(t)$ as:

$$\bar{U}(t_1,t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U(t)dt$$

192-08-08
Symbol U
steady state unavailability
asymptotic unavailability

limit, if it exists, of the instantaneous unavailability when the time tends to infinity

Note 1 to entry: Under certain conditions the steady state unavailability may be expressed as the ratio of the mean down time to the sum of the mean up time and mean down time. See IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms.

There is no definition of "safety unavailability" available in the on-line version of IEC 60050.

2.4 A Textbook Explanation

Marvin Rausand's book [9] considers probability of failure on demand in Section 7.5.1 and average frequency of a dangerous failure per hour in Section 7.5.2. The book specifically "*focuses on IEC 61508 and ..... IEC 61511.*" His concepts are meant to be the same as those defined in [1, Part 4, Clauses 3.6.17-19]. Rausand defines:

> The average probability of (dangerous) failure on demand, PFD_{avg}, is the average probability that the item (SIS, subsystem, voted group, or channel) is not able to perform its specified safety function if a demand should occur.

He says it is

> the same as the average unavailability of the item (see Appendix A) and is equal to the long-term average proportion of time where the item is not able to perform its safety function.

He defines "average unavailability" in Appendix A.5.1. Note that Appendix A.5 is concerned with "Repairable Items". He defines the availability of the item $A(t)$ in Equation (A.44) as

$$A(t) = Pr(X(t) = 1) = Pr(\text{ The item is able to function at time } t)$$

and its unavailability in Equation (A.45) as

$$\ldots 1 - A(t) = Pr(\text{ The item is not able to function at time } t)$$

The average unavailability is defined in Equation (A.46) as the integral of the unavailability over a time interval, divided by the length of the time interval. Let the interval be $(t, t + \tau)$. Then the average unavailability is

$$\frac{1}{\tau} \int_{t}^{t+\tau} (1 - A(t))\, dt$$

Clearly this definition is consonant with that in IEC 60050 Part 191 and in IEC 61703:2016 [3]. Rausand's definition of average frequency of dangerous failures per

hour in his section 7.5.2 is synonymous with the IEC 61508-4:2010 definition. He refers to his Chapter 9 for further consideration of PFH. Chapter 9 is entitled Average Frequency of Dangerous Failures. Section 9.2.1 is entitled Nonrepairable Items, and Section 9.2.2 Repairable Items.

2.5 SW as a Non-Repairable Item

Concerning non-repairable items, Rausand defines the probability density function of time-to-failure $f(t)$ as a function of time t in the usual fashion, and the failure rate function $z(t)$ by means of the explanation that $z(t).\delta t$ is the conditional probability of failure in a small time interval $(t, t + \delta t)$, given that an item has survived up to time t. The average failure rate over a time interval τ is then defined (p274) as the integral from 0 to τ of $z(t)$ divided by τ:

$$\frac{1}{\tau}\int_0^\tau z(t)\,dt$$

Here, it is considered that the item is subject to a proof test, and the length of the proof test interval is τ. If the item is indeed subjected to proof testing at intervals τ, then this formula is obviously appropriate for the unavailability of an item between proof tests. If we are to take into consideration the length of time it takes to perform the proof test, say δ, and the item is unavailable during the proof test, then the average unavailability of the item over all time surely includes the time for the proof test as well:

$$\frac{1}{\tau}\int_0^\tau z(t)\,dt + \frac{\delta}{\tau}$$

We shall just consider using the first formula, that is, the availability/unavailabilty of the item between proof tests. Using the homogeneity assumption for Poisson Processes or the memoryless assumption for Bernoulli Processes, by means of which the probability of failure at a time point (Poisson) or demand occurrence (Bernoulli) is independent of previous process history, the first formula is appropriate for any time interval $(t, t + \tau)$.

For Poisson processes, the failure rate function is constant. For Bernoulli processes, the failure rate function is given by the (Bernoulli) pfd combined with the stochastic process SP1 of demands in continuous time. Let us assume that

(*) Bernoulli demands occur sufficiently sparsely in time that the software is reinitialised between demands.

It follows from the assumption (*) that, as required, the pfd is constant. Then the probability of failure over a given time interval $(t, t+\tau)$ is

$$\sum_{n=0}^{N(\tau)} pfd \times Pr(\text{ n demands occur in } (t, t+\tau))$$

where $N(\tau)$ is an upper bound to the number of demands which can occur in $(t, t+\tau)$. Let the reinitialisation time for the SW be δ, and let us assume

(**) that the reinitialisation time δ is constant and that the SW is unavailable while being reinitialised.

Then $N(\tau)$ could be $\lceil(\tau/\delta)\rceil$, which is independent of t under the assumption (*). The average failure rate over the time interval $(t, t+\tau)$ is then

$$\frac{1}{\tau}\sum_{n=0}^{N(\tau)} pfd \times Pr(\text{ n demands occur in } (t, t+\tau))$$

which is clearly dependent upon $Pr(\text{ n demands occur in } (t, t+\tau))$, which is associated with the process SP1. We may say nothing further about this until we know the stochastic properties of SP1.

However, concerning unavailability, the SW is only unavailable if two demands occur within a time period δ, during which the software will be unavailable to respond to the second demand because it is reinitialising according to assumption (**). Under assumption (*), this never occurs. It follows under assumption (*), therefore, that the SW is never unavailable, otherwise expressed, that the unavailability is 0. It follows from this that the average unavailability under assumption (*) is also 0. So if, according to Rausand, "[t]he average probability of (dangerous) failure on demand, PFD_{avg}, is ..... the same as the average unavailability of the item", then, under assumption (*), $\text{PFD}_{avg} = 0$. It follows, since $pfd \neq 0$, that $PFD_{avg} \neq pfd$.

2.6 SW as a Repairable Item

Concerning repairable items, Rausand defines in Section 9.2.2 the notion of ROCOF, rate of occurrence of failures, $w(t)$. He says (p277) that

$$w(t) \approx Pr(\text{Failure in } (t, t + \Delta t))/\Delta t$$

In Example 9.2, he considers an item with constant failure rate λ and says that "the ROCOF is in this case $w(t) = ... = \lambda$ " which is Equation (9.9).

In Section 9.3, Average Frequency of Dangerous Failures, subsection 9.3.1 Definition and Interpretation of PFH, the first sentence says "The frequency of dangerous failures (PFH) is the same concept as the ROCOF, which was introduced in Section 9.2.2."

2.7 Software and Its Failure Behaviour

Software-based systems can fail. One of the ways in which they may fail is because the software causes them to behave in such a way that they fail to fulfil their function, even though the rest of the system remains intact and fully capable. In such a case, we may speak of a "software failure" and "software... failing" and that "software ... fails...", to emphasise the fact that the fault lies somewhere in the software logic. Suppose software implementing a safety-related function fails dangerously (that is, a safety function implemented by the software fails). Then three situations traditionally considered in engineering reliability can pertain, namely if the item is repairable or non-repairable, and how the repair time factors in.

Assumption 1: The SW is repairable with repair time 0.

In this case, we consider that the software has failed and can be reset (reinitialised) in zero time.

Alternatively, we can consider that the software takes some time to be reinitialised. It seems reasonable to consider an upper bound $\delta \neq 0$ to the reinitialisation time, assuming the HW remains available:

Assumption 2: The SW is repairable with repair time δ.

The SW behaviour we are considering is that we observe a long (sequence or time) of operation of the SW and reliably observe no failure. This is the technical basis on which the long-term reliability of the software is estimated. It is consistent with this view that software is non-repairable. Indeed, this is often the case in practice – when a dangerous failure occurs in software, then the software is changed to avoid or mitigate a recurrence. The changed software constitutes a new item; a change in design is not a "repair" in the usual technical-reliability sense. Hence we also consider

Assumption 3: The SW is non-repairable.

The three Assumptions 1, 2, and 3 are mutually exclusive. Together, they cover all cases.

2.8 The Failure Behaviour of Software Implementing an On-Demand Function as a Bernoulli Process

Notice that no parameter of a Bernoulli Process involves time. Notice also that the concept of PFD$_{avg}$, as explained above, essentially involves the notion of time. There are thus two approaches which can be used to relate the IEC 61508 notion of PFD$_{avg}$ to a Bernoulli process.

Under Assumption 1, the repair time of the SW is zero; it follows that the software is always available and never unavailable, and thus PFD$_{avg}$ is 0. Since the pfd of a Bernoulli process may be anything, it follows that, unless the SW is perfect and never fails,

Under Assumption 1, $pfd \neq PFD_{avg} = 0$

If the SW has a finite repair (reinitialisation) time δ after failure, then the unavailability will be non-zero: measured from time 0, the software progresses to failure at t_f and then takes δ to be reinitialised to be available again, during which it is unavailable. The unavailability in this period $(0, t_f + \delta)$ is $\delta/(t_f + \delta)$ and the average unavailability in a period in which $N(\tau)$ failures occur will be

$$\frac{\sum_{i=0}^{N(\tau)} \delta/(t_{f_i} + \delta)}{\sum_{i=0}^{N(\tau)} t_{f_i}}$$

To calculate this, it seems we would need the values of the times to failure. Time to failure is not a parameter of a Bernoulli Process, because time is not a parameter of a

Bernoulli Process. It would be necessary in this case to consider the stochastic process of demands occurring in time, which we have called process SP1, and combine this with the Bernoulli Process in order to calculate average unavailability. It follows that, under Assumption 2, as things are, the process SP1 of demands occurring in time must be known in order to calculate PFD$_{avg}$.

The Bernoulli Process is a separate stochastic process from SP1. Therefore no exact relation can be expected or anticipated between the parameters of the Bernoulli Process and those of process SP1. It follows that no exact relation can be expected or anticipated between pfd, a parameter of the Bernoulli process, and PFD$_{avg}$, a quantity calculated from stochastic parameters of SP1.

The discussion concerning SW as a non-repairable item also yielded the conclusion that, under Assumption 3 and assumption (*), $pfd \neq PFD_{avg} = 0$. In all these cases, then, the Bernoulli parameter pfd is different from the IEC 61508 notion of PFD$_{avg}$.

Rausand also says (p197, Section 8.3.1 Probability of Failure on Demand) that

> The PFD$_{avg}$ can be interpreted in two different ways:
>
> 1. If a demand for the safety function of the item occurs at a random time in the future, the PFD$_{avg}$ is the average probability that the item is not able to react and perform its safety function in response to the demand.
> 2. The PFD$_{avg}$ is equal to the mean proportion of time the item is not able to perform its safety function.

Both of these interpretations speak of performing the safety function simpliciter, not of performing the safety function successfully or unsuccessfully. Intuitively, unavailability is not the same as available-but-unsuccessful. Lack of performance is not the same thing as unsuccessful performance.

I conclude that the Bernoulli parameter pfd is not the same as the IEC 61508 notion of PFD$_{avg}$.

2.9 The Failure Behaviour of Software Implementing a Function as a Poisson Process

It follows from Rausand's explanation above that the IEC 61508 concept average frequency of dangerous failures per hour for a Poisson Process is exactly the Poisson parameter λ.

Table 3 of IEC 61508-1:2010, Figure 2.2, thus gives the permissible values of λ per SIL. Figure 1.2 gives the failure-free observation time required to attain a certain level of confidence that a particular value-range of λ pertains, and this may be directly related to SIL as given in Table 3 of IEC 61508-1:2010, Figure 2.2.

2.10 Conclusions

The Bernoulli parameter pfd is not the same as the IEC 61508 notion of PFD_{avg}, and cannot strictly be compared.

PFD_{avg} concerns availability and unavailability of the item to perform its function, and under assumption (*) that demands do not occur closer together than the reinitialisation time of the SW, $\text{PFD}_{avg} = 0$.

pfd concerns unsuccessful performance of a function, in this case a safety function. The function is prima facie available if it is performed, whether successfully or unsuccessfully.

The Poisson parameter λ is exactly the IEC 61508 concept average frequency of dangerous failures per hour.

Bibliography

[1] International Electrotechnical Commission, IEC 60050, *International Electrotechnical Vocabulary*, on-line at www.electropedia.org . Part 192 is at http://www.electropedia.org/iev/iev.nsf/index?openform&part=192

[2] International Electrotechnical Commission, IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2nd edition, 7 parts, 2010.

[3] International Electrotechnical Commission, IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*, 2016.

[4] Marvin Rausand, *Reliability of Safety-Critical Systems*, John Wiley & Sons, 2014.