

THE SAFETY ANALYSIS OF REDUNDANT SAFETY INSTRUMENTED FUNCTIONS (SIF) WITH INCOMPLETE OR PARTIAL TESTING.

Harry Cheddie P.Eng., CQE, CRE, CFSE
Exida.com
Sarnia, Ontario, Canada

KEYWORDS

Safety Instrumented Function, PFD_{avg} , FMEA, Fault trees, Safety Integrity Levels, SIL Verification, Redundancy.

INTRODUCTION

A common definition of a Safety Instrumented Function (SIF) as defined in Functional Safety Standards is "Function to be implemented by a Safety Instrumented System (SIS) to mitigate or prevent a specific hazardous event." The performance based standards (IEC61508/61511) require that we demonstrate quantitatively that each SIF satisfy its Risk Reduction requirements.

To achieve the Risk Reduction requirements, SIF's need to be tested periodically. This article provides an understanding and some examples as to how the Average Probability of Failure on Demand (PFD_{avg}), which is the inverse of the Risk Reduction required, can be calculated when one or several components that are part of the SIF are:

- (1) Never tested
- (2) The testing is incomplete or
- (3) Partial testing is carried out

How to Calculate PFD_{avg}

Before looking at how to calculate PFD_{avg} , let's first define what PFD_{avg} means. As per the definition of a SIF, we expect the function, which normally consists of sensor(s), logic solver, and final element(s), to respond to a process demand. A process demand would be a process variable reaching a potentially dangerous value. There is always a probability that the function will not operate as specified and a hazardous event will occur. The PFD_{avg} defines the average probability that the function will fail to respond to the demand. The Probability of failure of a system when a demand occurs is its "Unavailability", because it is the probability of failure at a specific point in time. The PFD_{avg} is therefore the average unavailability of the system or function.

If we were to test a system periodically and completely, and at the end of the test we assume that the system has been restored to its original day one state, then from a reliability life analysis point of view, all we have to be concerned with is the test interval, because this is, theoretically,

the life of the system. (Again, we are assuming that it is back to day one conditions at the end of the test. This is of course a big assumption).

What is Reliability/Availability from a SIF Point of View?

The reliability of a system can be defined as the probability that it will perform its function successfully under stated conditions for a specific period of time. Looking at how this definition applies to a Safety Instrumented Function that is tested periodically and restored to day one condition, the following applies:

- The probability refers to the probability that the function will operate satisfactorily
- Success is the hazardous event being prevented or mitigated when a demand occurs
- The period of time is the test interval

The availability of a system can be defined as the probability that it will perform its function successfully under stated conditions at a certain point in time. This assumes that the system is repaired periodically. Assuming that our SIF is not repaired during the test interval then its

$$\begin{aligned} \text{Reliability} &= \text{Availability} \\ &\text{and} \\ \text{Unreliability} &= \text{Unavailability} \end{aligned}$$

Simplified Equations for Reliability and Unavailability

For systems with a constant failure rate, which is typical for Electronic Safety Instrumented Systems, the Reliability can be calculated from the following equation.

$$R(t) = e^{-\lambda t}$$

Where, t = period of time for successful operation
 λ = failure rate

$$\text{The Unreliability} = 1 - e^{-\lambda t}$$

$$\text{If } \lambda t \text{ is small } (< 0.1), \text{ then } 1 - e^{-\lambda t} \approx \lambda t$$

Relating the above equation to a Safety Instrumented Function as per our previous discussion:

$$\text{The Unavailability} = \lambda t$$

where t = test interval, and λ = average failure rate of component or system.

It is very unlikely that the Safety Function will always fail at the end of the test interval, i.e. just before the next test. Failure can occur just after a test is completed, or at any point in time during the test interval. It therefore makes more sense for us to assume that on the average failures will occur at that middle of the test interval; hence we calculate the average unavailability by using $t/2$ instead of t . The average unavailability is the PFD_{avg}.

What about the PFD_{avg} for the complete function?

We indicated earlier that a Safety Instrumented Function usually consists of a sensor, logic solver, and a final element. If we assume that the dangerous failure rates for the sensor/logic solver/ final element are λ_S , λ_{LS} , and λ_{FE} , and the test intervals are T_S , T_{LS} , and T_{FE} then the PFD_{avg} for each component will be:

Sensor	$\frac{\lambda_S T_S}{2}$
Logic Solver	$\frac{\lambda_{LS} T_{LS}}{2}$
Final Elements	$\frac{\lambda_{FE} T_{FE}}{2}$

The Safety Instrumented Function will fail to operate as specified if the sensor, OR the logic solver, OR the final element fail to perform.

This is as per the fault tree in Fig. 1 below.

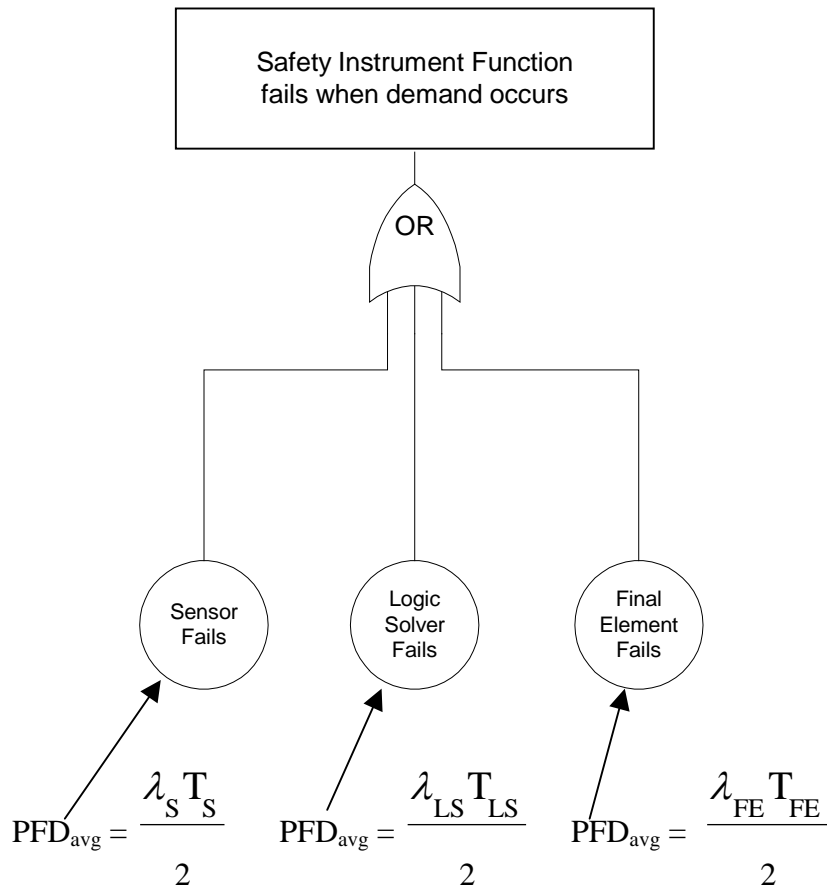


Figure 1

From the above fault tree diagram, if the PFD_{avg} values are small then the probability that the system will fail when a demand occur.

$$PFD_{avg (system)} = \frac{\lambda_S T_S}{2} + \frac{\lambda_{LS} T_{LS}}{2} + \frac{\lambda_{FE} T_{FE}}{2}$$

What if we never test one or several components?

Lets assume that the sensor is never tested, but the logic solver, and the final element are tested periodically. In this case the test interval for the sensor would be the life of the unit, i.e. the number of years until the unit is decommissioned. If the unit is shutdown for major repairs, say every 5 years, and the sensors were then thoroughly tested, then the 5 years can be used as the test interval. To demonstrate the impact of never testing a sensor lets first assume that a sensor ($\lambda^D = 0.013$ failures/yr) is tested annually.

$$PFD_{avg} = 0.0065 \qquad RRF = 153.8 \rightarrow \text{SIL 2 (Sensor only).}$$

If the sensor is never tested and the life of the unit is 25 years then:

$$PFD_{avg} = 0.013 * 25 / 2 = 0.1625 \qquad RRF = 6.1 \rightarrow \text{SIL 0 (Sensor only)}$$

In this case the sensor alone will not allow the complete function to be rated higher than SIL 0.

What about incomplete testing?

Lets now assume that the sensor is a pressure transmitter and the process line connection to the transmitter manifold is only tested during the plant major turnaround (every 10 years), but the transmitter (manifold, etc.) is tested every year. To calculate the PFD_{avg} for the complete sensing system we would split the system into two separate components, i.e. leg line and the transmitter. We then split the failure rate of the sensing system into the two separate components, i.e.:

if λ_{SS} = Failure rate of complete sensing system.

and λ_{RT} = Failure rate of sensing system without leg lines.

and λ_{LL} = Failure rate of leg line.

$$\text{then } \lambda_{SS} = \lambda_{LL} + \lambda_{RT}.$$

If we define E_T , as the testing efficiency when the annual test is carried out

then, $E_T = \frac{\lambda_{RT}}{\lambda_{SS}}$ i.e. the test only addresses failures associated with the sensing system without the leg lines.

hence, $\lambda_{RT} = E_T \lambda_{SS}$

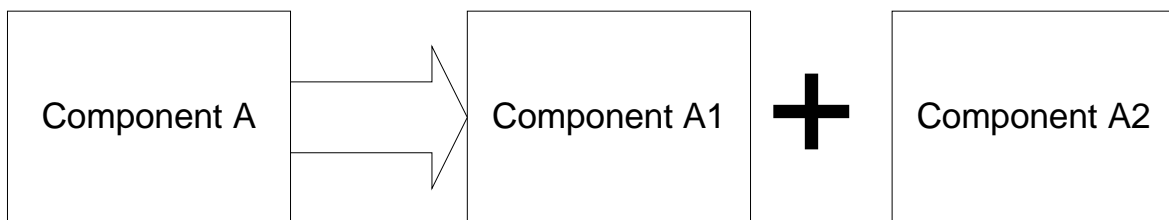
and, $\lambda_{LL} = (1 - E_T) \lambda_{SS}$

If the Proof test interval is T1 and the Plant Turnaround interval is T2, then for the sensing system:

$$\begin{aligned} \text{PFD}_{\text{avg}} &= \frac{\lambda_{RT} T_1}{2} + \frac{\lambda_{LL} T_2}{2} \\ &= \frac{E_T \lambda_{SS} T_1}{2} + \frac{(1 - E_T) \lambda_{SS} T_2}{2} \end{aligned}$$

(Note: The OR logic still applies).

For the incomplete testing we therefore split the component into 2 separate components in series and calculate the PFD_{avg} for each component based on its individual testing interval, then add the PFD_{avg} values to obtain the PFD_{avg} value for the series components i.e.:



The testing efficiency is based on the failure rate associated with each component.

$$\text{i.e. } \lambda_A = \lambda_{A1} + \lambda_{A2}.$$

To identify the failure rate split, the failure modes and effects analysis technique (FMEA) can be used.

Example

We saw that for a transmitter in which $\lambda^D = 0.013$ failures/yr.

$$\begin{aligned} \text{PFD}_{\text{avg}} &= 0.0065 \text{ if TI} = 1 \text{ yr.} \\ &= \text{SIL 2} \end{aligned}$$

If $E_T = 60\%$ and the plant turnaround interval is 10 years,

$$\begin{aligned} \text{then, } \text{PFD}_{\text{avg}} &= \frac{0.6 * 0.013}{2} + \frac{0.4 * 0.013 * 10}{2} \\ &= 0.0039 + 0.026 \\ &= 0.0299 \\ &= \text{SIL 1 (Sensor only)} \end{aligned}$$

What about Partial Stroke Testing (PST) of Valves?

Partial Stroke Testing of valves is an example of incomplete testing and can be treated mathematically in the same manner. With partial stroke testing, the valve is partially stroked, i.e. not allowed to close fully. The valve plug, seats and other components are therefore not tested. In the case of Partial Stroke Testing, it is also recommended that a failure mode and effect analysis (FMEA) be carried out to accurately determine the failure rates of the portions of the valve that will be tested with partial testing and the remaining portion. This will allow the efficiency of the partial test to be accurately determined.

Note: If the Partial Stroke Testing is done at a frequency that is 10 times greater than the demand rate, then as per IEC 61508, a diagnostic coverage factor C^D of 0.6 can be used for calculating the dangerous undetected failure rate. The normal PFD_{avg} calculation method can be used in lieu of the method described above. This method can also be used for the PFD_{avg} calculations for Partial Stroke Testing of valves.

What about incomplete testing of redundant systems?

Lets first look at a redundant system consisting of two valves connected in series in which the voting is 1oo2, and the testing is 100% effective, i.e.:

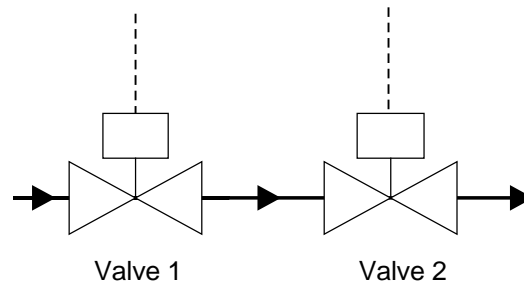


Figure 2

During normal operation both valves are open. In the case of a 1oo2 system as shown in Fig.2 above, common cause failures have a significant impact on the PFD_{avg} calculations. Common cause failures can be modeled using a simple "Beta" model in which,

$$\beta = \frac{\lambda_{\text{common cause}}}{\lambda_{\text{single valve}}}$$

β represents the split between the common cause and the total failure, i.e.

$$\lambda_{cc} = \beta\lambda$$

The total failure rate is therefore split into independent failures and common cause failures.

$$\lambda = \lambda_{\text{independent}} + \lambda_{\text{common cause}}$$

A fault tree showing common cause is:

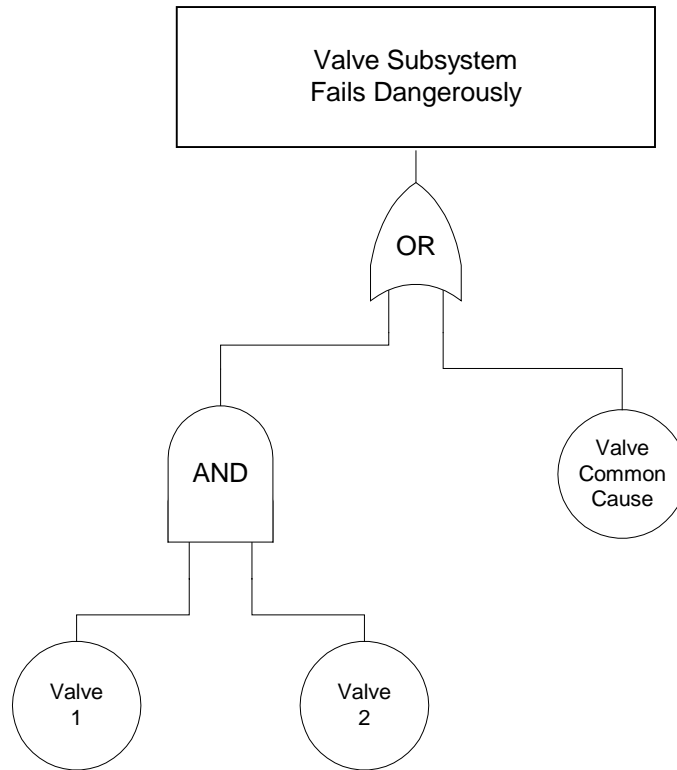


Figure 3

For the Fault Tree shown in Fig. 3 above:

$$\text{The } PFD_{avg} = \frac{\lambda_I^2 T^2}{3} + \frac{\beta \lambda T}{2}$$

λ_I = Valve dangerous failure rate independent of the common cause failure

T = Test Interval.

Where $\frac{\lambda_I^2 T^2}{3}$ represents the PFD_{avg} of the 1oo2 components and $\frac{\beta \lambda T}{2}$ represents the PFD_{avg} of the common cause component.

Example:

If $\lambda_{valve}^D = 0.02$ failures/yr.

$\beta = 0.05$

TI = 1 year



If λ = dangerous failure rate for valve
 T_1 = Proof Test frequency
 T_2 = Major turnaround frequency of unit
 β = Beta factor
 E_T = Proof Testing efficiency

Then for Proof Test frequency T_1 ,

$$\text{PFD}_{\text{avg}(T_1)} = \frac{E_T^2 \lambda^2 T_1^2}{3} + \frac{E_T \beta \lambda T_1}{2}$$

For major turnaround testing,

$$\text{PFD}_{\text{avg}(T_2)} = \frac{(1 - E_T)^2 \lambda^2 T_2^2}{3} + \frac{\beta(1 - E_T) \lambda T_2}{2}$$

PFD_{avg} (Valve Subsystems) = $\text{PFD}_{\text{avg}(T_1)} + \text{PFD}_{\text{avg}(T_2)}$.

Example:

If $\lambda = 0.02$
 $T_1 = 1$ year
 $T_2 = 25$ years
 $\beta = 0.05$
 $E_T = 75\%$
 $\lambda_{\text{CC}} = 0.001$



$$\text{PFD}_{\text{avg}} = \frac{0.75^2 \cdot 0.02^2}{3} + \frac{0.75 \cdot 0.05 \cdot 0.02}{2} + \frac{0.25^2 \cdot 0.02^2 \cdot 25^2}{3} + \frac{0.05 \cdot 0.25 \cdot 0.02 \cdot 25}{2}$$

$$= 0.00878$$

$$\text{RRF} = 113.9$$

For T_2 = 5 years instead of 25 years,

$$\text{the } \text{PFD}_{\text{avg}} = 0.00128$$

$$\text{with RRF} = 780$$

The above analysis for the incomplete testing of redundant systems was carried out for a valve. The same concept and equations can be applied to redundant sensors and logic solvers.

For example:

Two temperature transmitters are used to sense an abnormal process condition and are arranged in a one-out-of-two voting arrangement. Each transmitter has a dangerous failure rate of $\lambda^D = 0.05$ failures per year, and the beta factor of 10%. What is the PFD_{avg} of this subsystem if a periodic inspection is done once a year that detects 90% of the failures? The transmitter subsystem is operated for ten years between major overhauls.

The solution would be:

$$\begin{aligned}\lambda^D &= 0.05 \\ T_1 &= 1 \text{ year} \\ T_2 &= 10 \text{ years} \\ \beta &= 0.1 \\ E_T &= 90\% \\ \lambda_{\text{CC}} &= 0.005 \\ \lambda_r^D &= 0.045\end{aligned}$$



The PFD_{avg} values will therefore be: (For this solution we used λ_r^D instead of λ^D)

- (1) 1002 portion that is tested at Proof test frequency (T_1).

$$\text{PFD}_{\text{avg}} = 0.9^2 \cdot 0.045^2 / 3 = 0.00547$$

- (2) Common Cause portion that is tested at Proof test frequency (T_1).

$$\text{PFD}_{\text{avg}} = 0.9 \cdot 0.1 \cdot 0.005 / 2 = 0.00225$$

- (3) 1002 portion that is tested during major overhaul (T_2).

$$\text{PFD}_{\text{avg}} = 0.1^2 \cdot 0.045^2 \cdot 10^2 / 3 = 0.000675$$

- (4) Common Cause portion that is tested during major overhaul (T_2).

$$\text{PFD}_{\text{avg}} = 0.1 \cdot 0.1 \cdot 0.05 \cdot 10 / 2 = 0.0025$$

$$\text{PFD}_{\text{avg (for the system)}} = 0.00547 + 0.00225 + 0.000675 + 0.0025 = 0.005972$$

$$\text{RRF} = \frac{1}{0.005972} = 167$$

REFERENCES:

1. Exida Safety Engineering II Course Notes.