

Determining the Probability of Failure on Demand for Heterogeneous, Combined BPCS and SIS Systems

Markus Weber
Principal Consultant
System Safety, Inc.
San Diego, CA 92131

KEYWORDS

Safety Integrity Level, BPCS, Safety System

ABSTRACT

Determining the Safety Integrity Level (SIL) for homogeneous architectures is simple and can be achieved using simple equations or models. However when the Basic Process Control System (BPCS) and the protective Safety Integrated System (SIS) share common components and the channels of a multi-channel protection system are comprised of different components, the estimation of the Probability of Failure on Demand (PFD) becomes much more challenging. Using Markov modeling and model variation based on failures of BPCS components initiating a shutdown situation, the overall risk reduction under these 'internal demand' scenarios can be calculated. This allows deriving an equivalent SIL level for the safety function. Using a turbine overspeed protection system the steps for this methodology will be illustrated.

Heterogeneous Architectures

Most published examples of multi-channel SIS architectures are based on the assumption that matching components in all channels are identical and exhibit identical failure rates and failure modes. For many off-the-shelf safety PLCs this may be the case, but very often more sophisticated implementations use different equipment or even technologies to implement a multi-channel safety system. This approach does not only have economical advantages but carries the added benefit of reducing the common mode failure rate (especially the common mode contribution caused by identical software running on each channel of the SIS.)

If one of these heterogeneous architectures is used, the published simple equations, fault tree or Markov models, cannot be used to determine the PFD or SIL. A model tailored to the specific implementation has to be developed. An example for such a heterogeneous architecture is illustrated in Figure 1.

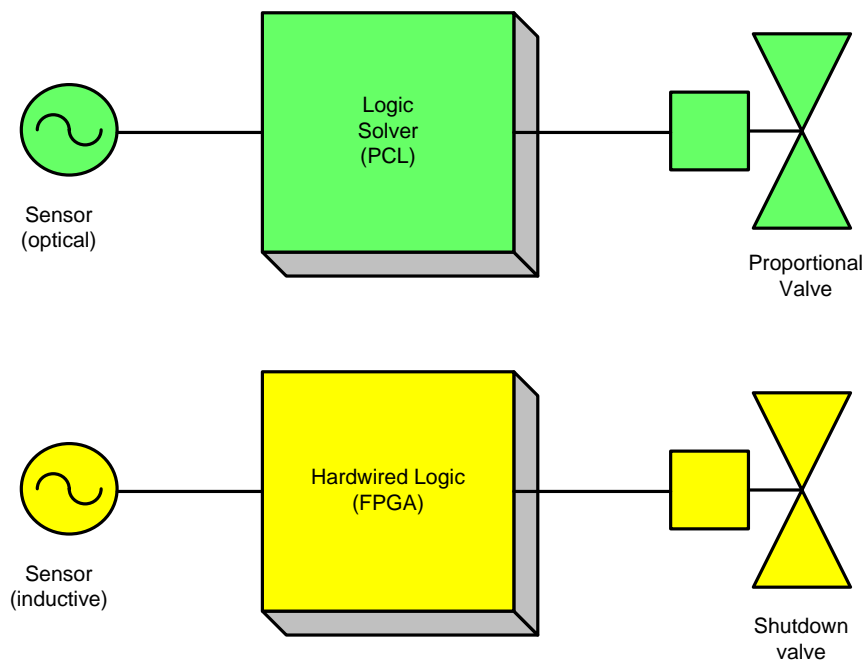


Figure 1 – Heterogeneous System Architecture

Fault Containment Architectures

Another assumption often made in simple models is that all channels of a SIS are independent and do not share information between each other. In practical implementations this is not always the case and often not desired. Interconnecting parts of a multi-channel system can be advantageous to increase the overall safety availability and to isolate defective parts of a channel without degrading the entire channel function. Figure 2 shows a 1oo2 system without channel cross-connects, and it can easily be seen that a failure for a single component in one of the channels will disable the entire channel.

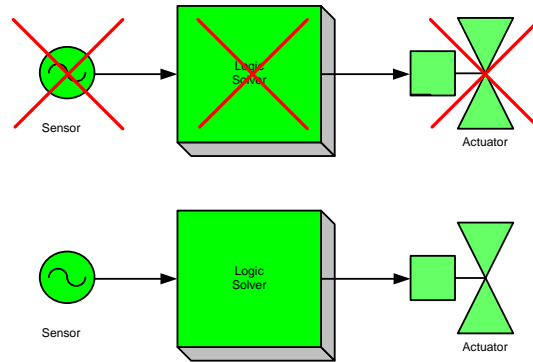


Figure 2 – Independent Channels

Figure 3 shows a typical 1oo2 sensor and actuator cross-connect with inter-logic-solver communication. It is obvious that a dangerous fault in any of the 6 modules can be isolated and contained within a zone and will not impair the function of the remaining system. For instance, if one sensor fails, both control units and both shutdown valves are still available to process a demand. The same is true for a failure of one logic solver (both sensors and actuators are still available) and for the failure of an actuator (both sensors and controllers remain available).

Using such an interconnected architecture allows containing the component fault to only a section of the degraded channel and will maintain a higher level of safety availability und single fault conditions.

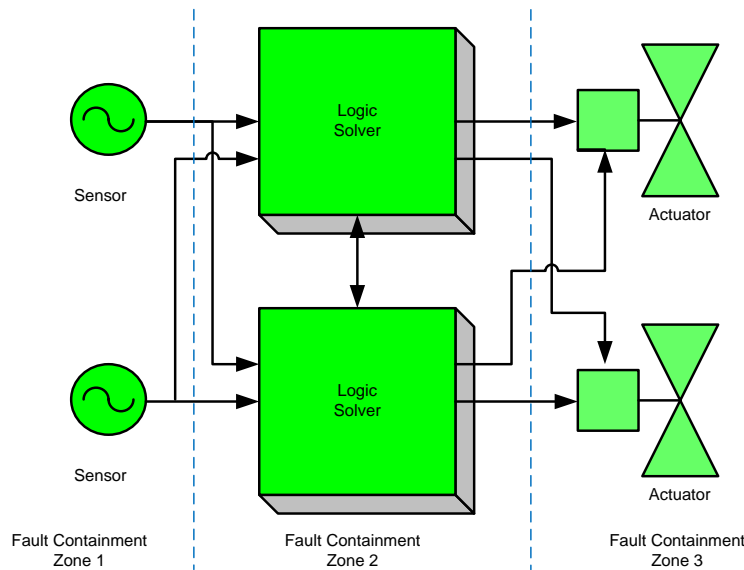


Figure 3 – Fault Containment Architecture

Combination of BCPS and SIS Components

Sometimes it is not possible to entirely separate BCPS and SIS functions due to process constraints or integration issues. In general it is desirable to separate the two systems to avoid faults within the BCPS system to propagate into the SIS or partially disable SIS functions. Most published scenarios and models therefore do not account for possible interactions between the control and safety systems. If the implementation does not allow for a full separation additional modeling will be necessary to determine the safety integrity level and PFD values. Figure 4 shows a system in which the control function and the safety function are integrated into one of two channels. It is assumed that the safety function is a separate software function within the control system and is logically independent from the control logic. A dangerous failure of the sensor, controller or actuator will not only result in the generation of a demand for the safety system, but will at the same time disable a part of the safety system and degrade it to a single channel architecture. This illustrates why a separation of control and safety system is easier to assess and model if the architecture is reduced to a single channel.

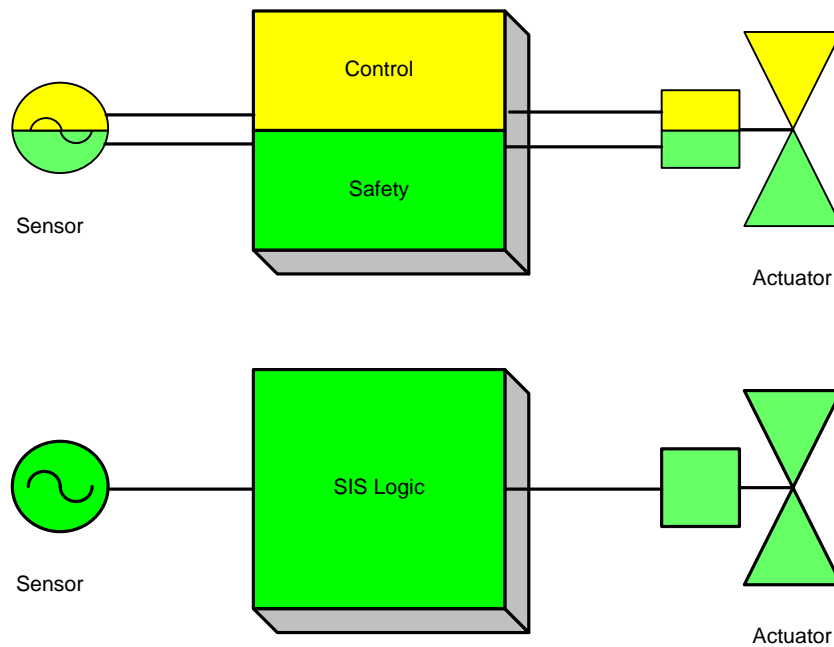


Figure 4 – BCPS/SIS Combined Components

Example: Gas Turbine Overspeed Protection

The following example uses the overspeed protection of a gas turbine control system to show how the three basic challenges - Heterogeneous Channels, Fault Containment Architectures, and combination of BCPS and SIS functions – can be used to design a safety interlock system with a high level of safety integrity and PFD. The modeling uses a combination of Markov models and elements of a Level of Protection Analysis (LOPA) to derive a numerical value for the PFD that can be expected.

Gas turbines have to be very responsive and manage the combustion process with a high level of coordination. Safety functions often need to be closely integrated with the turbine control system. Clause 7.3.4 of ANSI/ISA-S8.01:1996 specifically exempts gas turbines from requiring a separation of control and safety functions.

SIS Architecture

The combined BPCS/SIS is illustrated in Figure 5. The critical process parameter is measured by two independent sensors. Both are connected to a programmable controller (PLC) as well as to a discrete logic processor (backup safety system (BSS)). Both the PLC and the BSS can independently actuate the control and the shutoff valves. The sensor information is processed within the PLC using two separate software paths: The control path actuates the control valve proportionally, based on the implemented control algorithm, and a second software path compares the sensor readings to a shutdown threshold and actuates the control and shutoff valves through two independent paths. The shutdown signal (Out D) to the control valve overrides any analog positioning signal (Out A). The entire system uses a de-energized-to-trip configuration, including spring loaded valves, to assert the safe state in case of loss of connection or power.

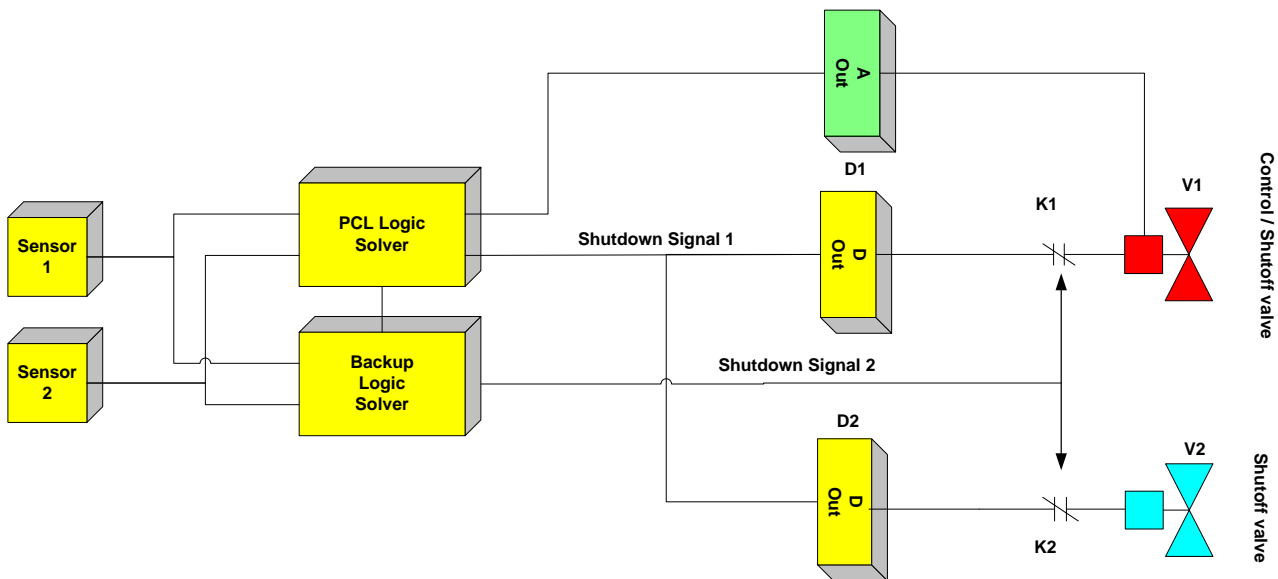


Figure 5 - System Architecture

This architecture is not only feasible to protect a gas turbine from overspeed (the sensors are inductive speed sensors and the backup logic solver is a frequency-dependent trip logic) but it can also be applied to level, pressure, or temperature control loops (i.e. if 4-20 mA pressure sensors feed a trip amplifier.)

To evaluate the probability of failure on demand, this system has to be evaluated using characteristic failure rates for the sensors, logic solvers, and actuators involved. It is easily conceivable that failures of the digital output modules and the shutdown relays can be neglected since at least 3 simultaneous components have to fail dangerously. The failure rates of the PLC input modules are combined with the PLC logic solver rates. For the purpose of this paper the following failure rates are assumed:

Failure Rates											
Function	FIT	MTTF	Safe	Nsafe	Diag	S	D	SD	SU	DD	DU
		{h}				FIT	FIT	FIT	FIT	FIT	FIT
Sensor 1	1500	666667	50%	50%	20%	750	750	150	600	150	600
Sensor 2	1500	666667	50%	50%	20%	750	750	150	600	150	600
Logic Solver	4000	250000	51%	62%	95%	1200	1490	1010	190	1450	200
Backup Logic	10000	100000	96%	4%	94%	14209	629	13650	559	345	284
Control Valve	5000	200000	14%	86%	60%	680	4320	408	272	2592	1728
Shutoff Valve	9000	111111	32%	68%	0%	2900	6100	0	2900	0	6100

FIT = Failure rate (10⁻⁹) hours / MTTF = Mean time to fail (hours)
Safe = Safe failure fraction / NSafe = Unsafe failure fraction / Diag = Diagnostic coverage / S = Safe failures (FIT)
D = Dangerous failures (FIT) / SD = Safe detected failures (FIT) / SU = Safe undetected failures (FIT)
DD = Dangerous detected failures (FIT) / DU = Dangerous undetected failures (FIT)

Table 1 - Failure Rates

These failure rates reflect currently-used industry data such as in [i]. The control valve is continuously modulated by the control branch of the PLC systems and therefore a limited degree of diagnostic coverage can be assumed.

Probability of Failure on Demand (PFD)

To determine the PFD value of this system the easiest approach would be to ignore the PLC channel and only evaluate the backup channel consisting of a single sensor, the backup logic solver and the shutdown valve. For the purpose of this paper, a proof test interval of 1 year = 8,766 hours and a beta factor of 1% are assumed.

Using the simple equation approach of IEC 61508-6: 1998 *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3* the PFD calculates to:

$$PFD_{1oo1}(T_P, \lambda_{DU}) := \left(\lambda_{DU} \frac{T_P}{2} \right)$$

Using the above failure rates the resulting PFD is:

$$PFD_S = 31 \times 10^{-3} \quad SIL_D(PFD_S) = 1$$

This corresponds to a risk reduction factor of:

$$RRF := \frac{1}{PFD_S} \quad RRF = 33$$

The value is the worst case scenario and does not take any of the voting and redundancy of functions into account.

An alternative way to determine the PFD value is to ignore the control function of the sensor, the PLC, and the control valve, and model the system as a dual channel emergency shutdown (ESD) system. In this case simple equations cannot be applied, since the failure characteristics in both channels are not identical. To accurately predict the PFD, the more complex approach of Markov modeling has to be employed. To simplify the model, it is assumed that any detected fault will result in an immediate shutdown of both valves. This is common practice in gas turbine applications and simplifies the models, because no safe or dangerous detected states exist, and online repair does not need to be considered.

The cross-connection of sensors, logic solvers, and actuators segments the system into fault containment zones. A failure of a component in one of the components does not propagate into the remaining channel and the functionality of the remaining component remains unaffected. The model in Figure 6 shows the clustering of states caused by these fault containment zones. The fault containment zones are clearly identifiable in the model and depicted by the blue dotted lines.

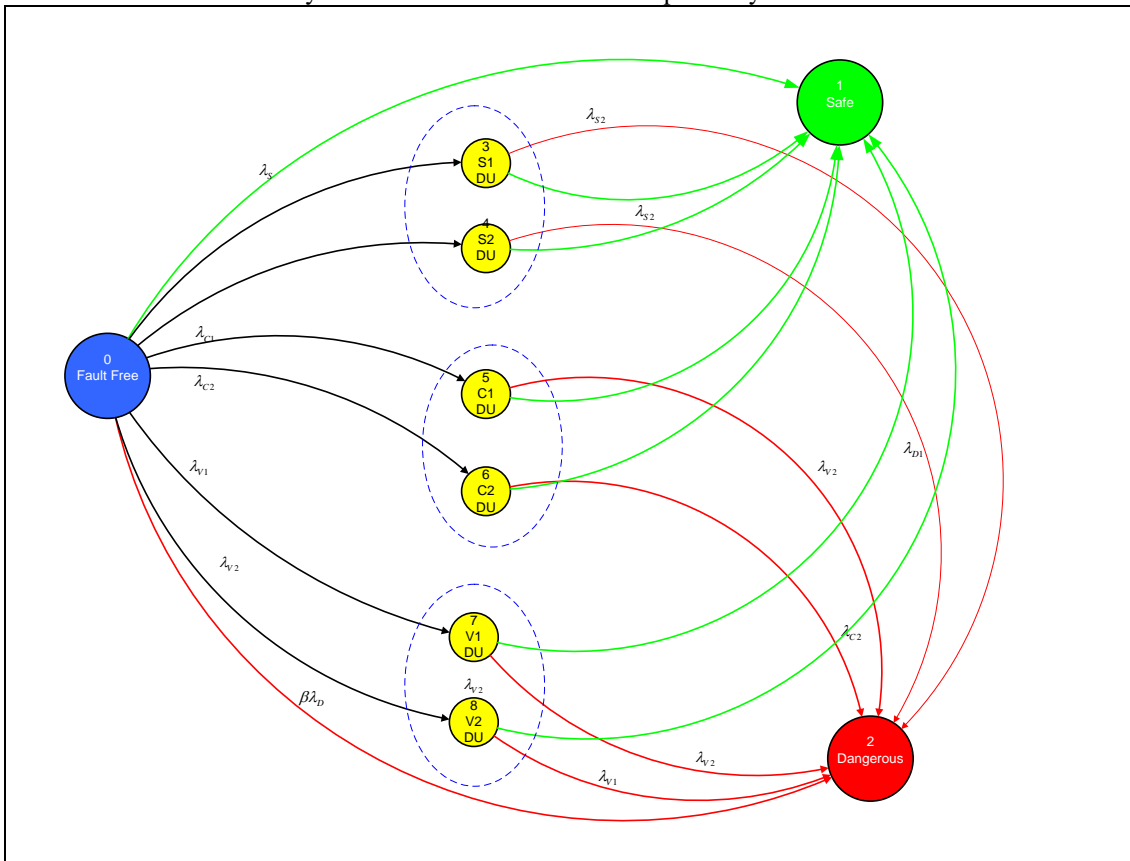


Figure 6 – Markov Model

$$T = \begin{pmatrix} 10 \times 10^8 & 25176 & 95 & 594 & 594 & 198 & 281 & 1711 & 1711 \\ 0 & 1 \times 10^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 \times 10^9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 24276 & 600 & 10 \times 10^8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 24276 & 594 & 0 & 10 \times 10^8 & 0 & 0 & 0 & 0 \\ 0 & 22526 & 594 & 0 & 0 & 10 \times 10^8 & 0 & 0 & 0 \\ 0 & 10622 & 281 & 0 & 0 & 0 & 10 \times 10^8 & 0 & 0 \\ 0 & 21904 & 0 & 0 & 0 & 0 & 0 & 10 \times 10^8 & 0 \\ 0 & 21904 & 1711 & 0 & 0 & 0 & 0 & 0 & 10 \times 10^8 \end{pmatrix} \text{FIT}$$

Table 2 – Transition Matrix

This model accurately describes the safety system behavior for external demands. Using the above failure rates, the probability of failure on demand, the SIL level, and the risk reduction factor (RRF) under commonly used assumptions (proof test interval = 8,766 hours, beta factor 1%), calculates to:

$$pfd_{dS} = 425.9848 \times 10^{-6} \quad SIL_D(pfd_{dS}) = 3 \quad RRF := \frac{1}{pfd_{dS}} \quad RRF = 2348$$

These values represent a significant improvement over the simple approach using a single channel calculation method. Additionally the non-linear slope of PDF over time as shown in Figure 7 can be calculated more exactly by evaluating:

$$pfd_{dS} := \frac{\sum_t pfd(T, t)}{T_p}$$

The difference between this integration method and the conventional calculation of 50% of PFD at 8,766 hours can be up to 20% depending on the model.

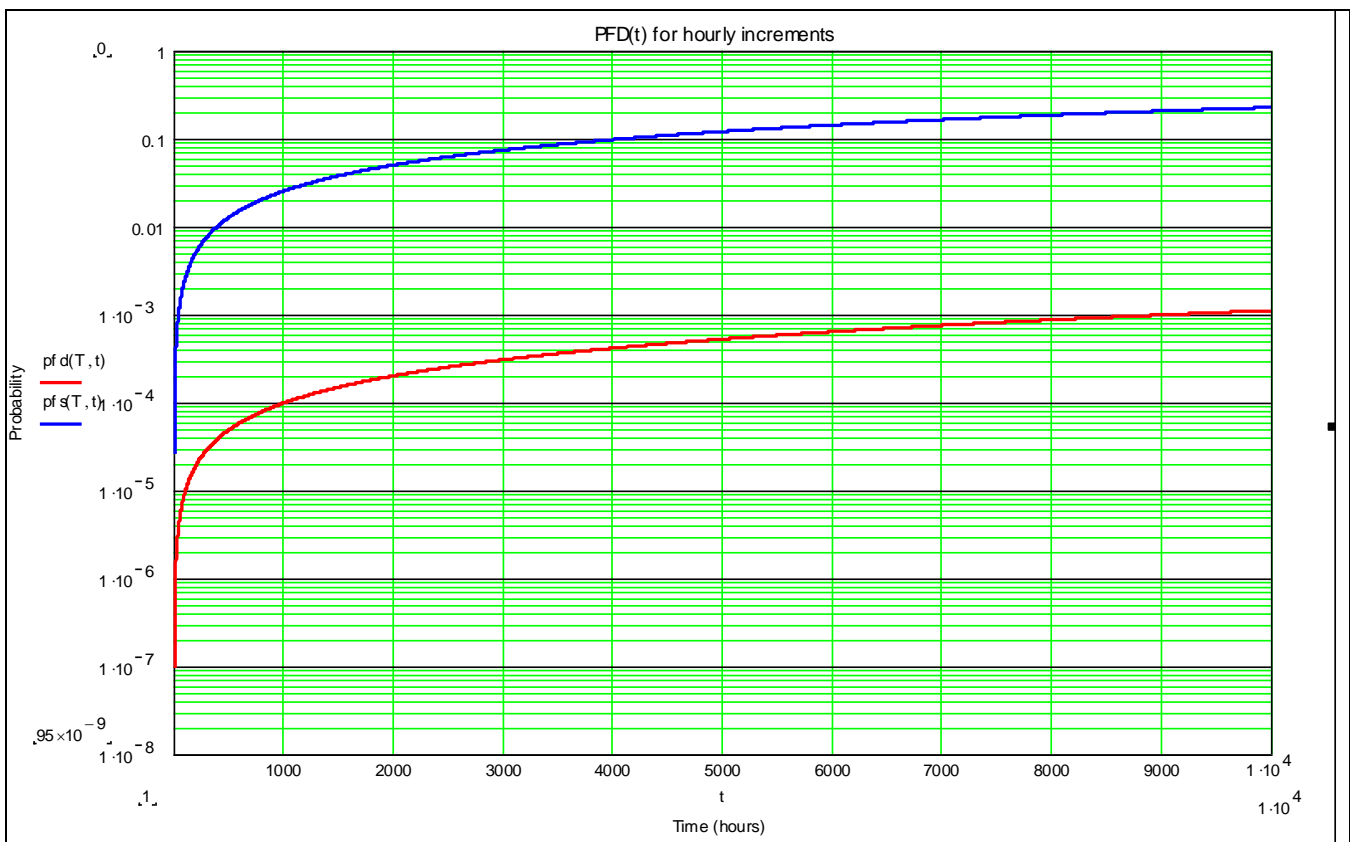


Figure 7 – PFD as Function of Time

BPCS Effects on the SIS System

In our example several components are shared between the BPCS and the safety system. Sensor 1 is used for both, process control and sensing of safety critical parameters. The PLC and the control valve are also shared. It is assumed however that the software within the PLC used for the control loop is separate and independent from the software module used for the safety function and that no software resources are shared.

These shared hardware resources illustrate why in many cases a separation of BPCS and SIS is not advisable, because a failure of a shared resource can lead to a demand on the safety system. However, with a fault containment design, since the demand was generated by an internal fault of a shared resource, a degraded safety system is still available to react to the demand and mitigate the impending hazard. If, for example, the control valve fully opens due to a dangerous fault within the valve, this valve is unavailable for the safety system. If the sensors and controllers are not cross-connected this will result in one of the two safety channels becoming unavailable resulting in a degradation of the safety integrated function (SIF) from SIL 3 to SIL 1. This level of degradation may not be acceptable for the safety loop.

Our system compares the sensor values as well as the results of the safety logic. Therefore the entire second channel is not degraded, but as in the case of a control valve failure, we still have dual sensors and dual logic solvers connected to a single shutdown valve. This architecture can be modeled and the achievable PFD can be quantitatively determined. To evaluate the system we have to consider four scenarios:

Scenario	Demand	Available SIS Components
1	External	2 sensors, 2 logic solvers, 2 shutdown valves
2	Control valve failure	2 sensors, 2 logic solvers, 1 shutdown valve
3	PLC failure	2 sensors, 1 logic solver, 2 shutdown valves
4	Sensor 1 failure	1 sensor, 2 logic solvers, 2 shutdown valves

Table 3 – Failure Scenarios

This requires developing 3 additional Markov models. These have less states due to the already failed component.

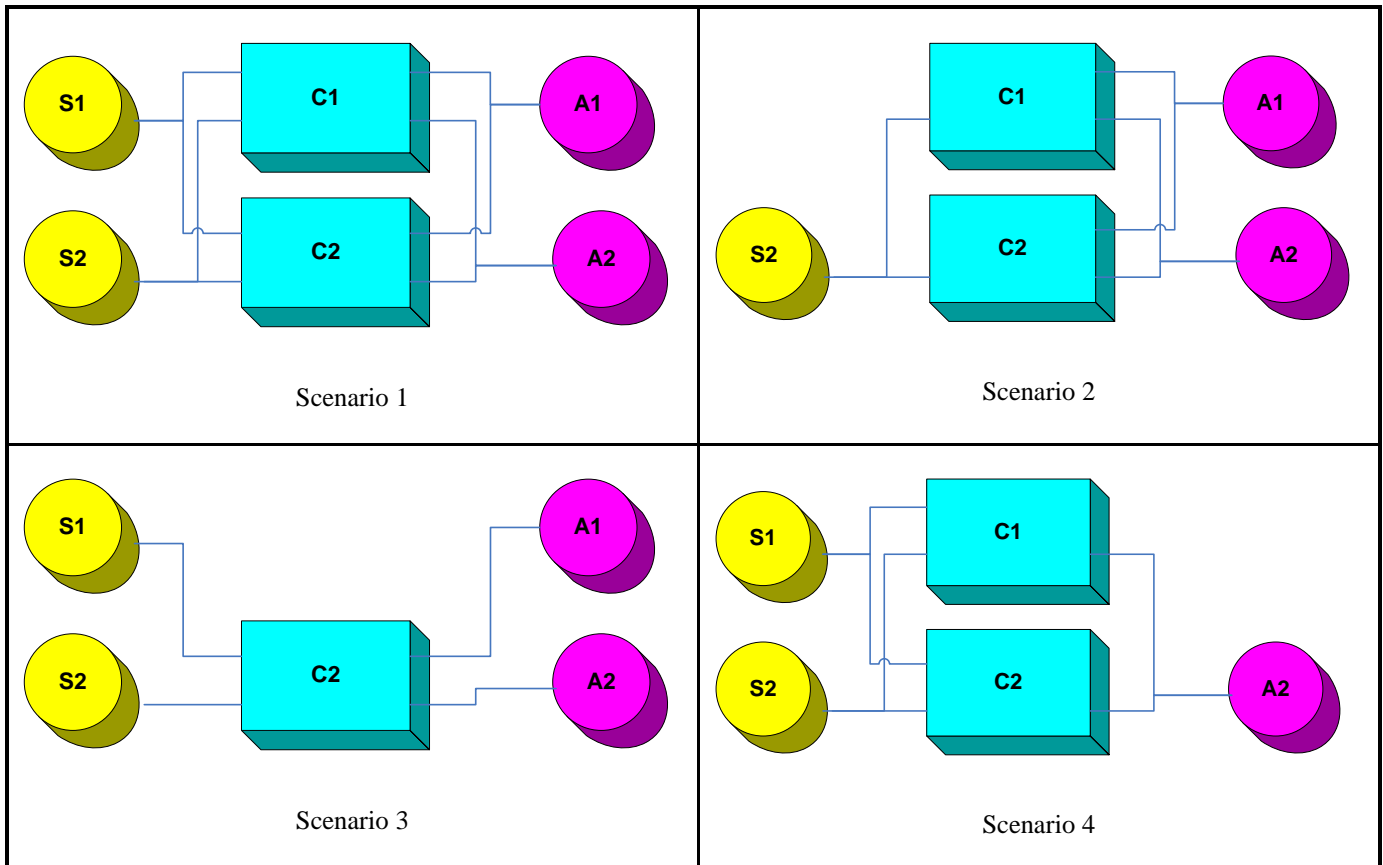


Figure 8 – Scenario Architectures

These three models omit the failed component, and due to the single remaining matching component, the failure of this component now leads to the immediate dangerous state. An example of the Markov model for Scenario 2 is shown below.

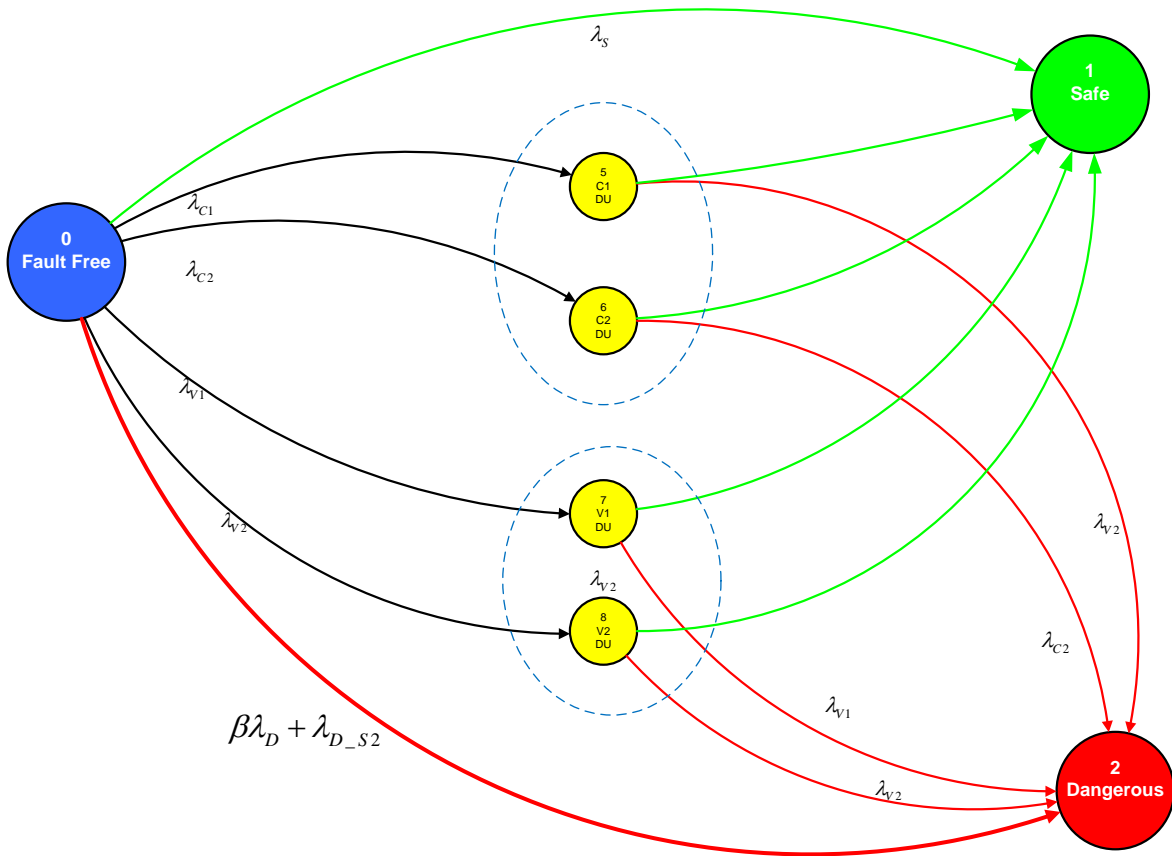


Figure 9 – Markov Model Scenario 2

If each Markov model is solved for the sample failure rate data and standard conditions (1 year proof test interval) the following results can be calculated and compared to the 1oo1 case:

Scenario	Architecture	Demand Cause	PDF _{avg}	SIL	RRF
	1oo1	External event	$3.06 \cdot 10^{-02}$	1	33
1	1oo2	External event	$4.25 \cdot 10^{-04}$	3	2348
2	1oo2	Sensor 1 failure	$3.01 \cdot 10^{-03}$	2	332
3	1oo2	PLC failure	$1.77 \cdot 10^{-03}$	2	565
4	1oo2	Control valve failure	$2.48 \cdot 10^{-02}$	1	40

Table 4 – Scenario Risk Reductions

The results show, that depending on the cause of the demand, a wide variation of probability of failure (PFD) results. It should also be noted that all 1oo2 models show a better risk reduction than the simplified 1oo1 calculation.

Combination of Analysis Results

So far widely varying results have been calculated for risk reduction capabilities of the same instrumentation under different scenarios. How do we consolidate the results? What is the real probability that a unsafe condition will occur?

A method used to derive a single PFD and risk reduction factor is called “Initiator Analysis” to illustrate that the effects of various demand initiators on the overall safety integrity of the SIF are analyzed.

To combine the different results a way has to be derived to combine the Risk Reduction Factors of all three scenarios into a single value, representing the overall risk reduction achieved by the system. This can be done using the probability of the occurrence of each scenario as a weighing factor. For the un-degraded system the standard demand rate of once per year can be used as a worst case scenario. The event probabilities of the other three scenarios are also known, because the event is caused by a failure of a module with known failure rates and failure mode. These rates were used in modeling the un-degraded system and are quantified by the dangerous failure rate of the component causing the degradation and the demand.¹

Based on these failure rates the average demand rate for each of the scenarios can be determined. For each of these events the risk reduction is known and therefore the probability of all mitigated events can be calculated. As we see in Table 5 the system reduced the dangerous event frequency of 1.022 per year to 0.00082 events per year. Since the risk reduction of the overall system is known, the Probability of Failure on Demand can be determined as the inverse of the risk reduction.

Since all initiating events are statistically independent, the frequency of their occurrence can be determined by adding the corresponding initiating frequencies. The unmitigated hazard frequencies are also independent and can be summed.

The demand rates for internal failures of the SIF are known, because they are defined by the dangerous failure rate of the initiating component. By combining these failure rates with any external demand rates, we can derive the equivalent frequency with which a fault initiated or external demand occurs.

The results of this operation are shown in Table 5:

Scenario	Architecture	Demand Cause	Demands per year	Years between ²	RRF ³	Hazards per year	Years between ⁴
1	1oo2	External event	1.000000	1	2347.5	0.000426	2348
2	1oo2	Sensor 1 failure	0.005260	190	331.8	0.000016	63086
3	1oo2	PLC failure	0.001753	570	565.1	0.000003	322324
4	1oo2	Control valve failure	0.015148	66	40.4	0.000375	2667
	Total		1.022160	1		0.000820	1220

Table 5 – Initiator Analysis

The combined demand rate and resulting hazard rate are linked by the SIS specific risk reduction.

By dividing the demands per year by the hazardous events per year, the combined risk reduction can be calculated to:

$$pf_{d_2} = 802.1409 \times 10^{-6} \quad SIL_D(pf_{d_2}) = 3 \quad RRF := \frac{1}{pf_{d_2}} \quad RRF = 1247$$

¹ The method used is similar to the level of protection analysis (LOPA) can be used. In a LOPA SIL determination a risk evaluation determines the target event frequency. The SIL required after external mitigation is then determined from the risk reduction needed from that target event frequency mitigating events and the demand rate.

² Years between unmitigated dangerous events

³ Risk Reduction Factor

⁴ Years between mitigated dangerous events

Conclusion

Even if it appears to be counter-intuitive, the example shows that for certain SIFs, the BPCS and safety integrated function can be combined without compromising the safety of the protected process. In the above example the decrease of risk reduction is only approximately 50%, resulting in the same SIL category as an entirely separated 1oo2 system would achieve. However caution is advised since the above method is only viable for well-defined and low complexity SIF architectures. Combining a complex DCS with SIF functions is still not advisable. This fact should not lead to codifying a general requirement for separation of BPCS and SIS, since for certain systems requiring fast responses and high level of coordination between control and safety functions, such as shown above, the combination of control and safety functions using shared resources is feasible and justifiable.

ⁱ Exida LLC - Safety Equipment Reliability Handbook (Second Edition)