HOW SHOULD SHARED ELEMENTS BE TREATED IN ESTIMATING FAILURE PROBABILITY FOR A 'TRIP GROUP'?

By Mirek Generowicz FS Expert (TÜV Rheinland #183/12) - I&E Systems Pty Ltd

In this context a 'trip group' is a set of safety instrumented functions (SIFs) that activates a common set of shared final elements.

If two SIFs each respond to distinctly different hazardous events with independent causal events then the SIFs are effectively independent. The risk reduction achieved by the SIS for one hazardous event is independent of the risk reduction for other events.

If several SIFs in one common trip group all respond to **common or related hazardous events** then the overall risk reduction achieved must consider all of the related SIFs in the SIS as a whole.

Take the example of a large gas-fired heater or furnace. The most obvious scenario requiring risk reduction relates to the hazardous consequences of re-ignition of unburnt fuel after a flame-out (i.e flame failure, loss of combustion).

The following (hypothetical) functions are closely related and **not** independent because they all relate to the scenario of re-ignition of unburnt fuel following flame failure or flame instability:

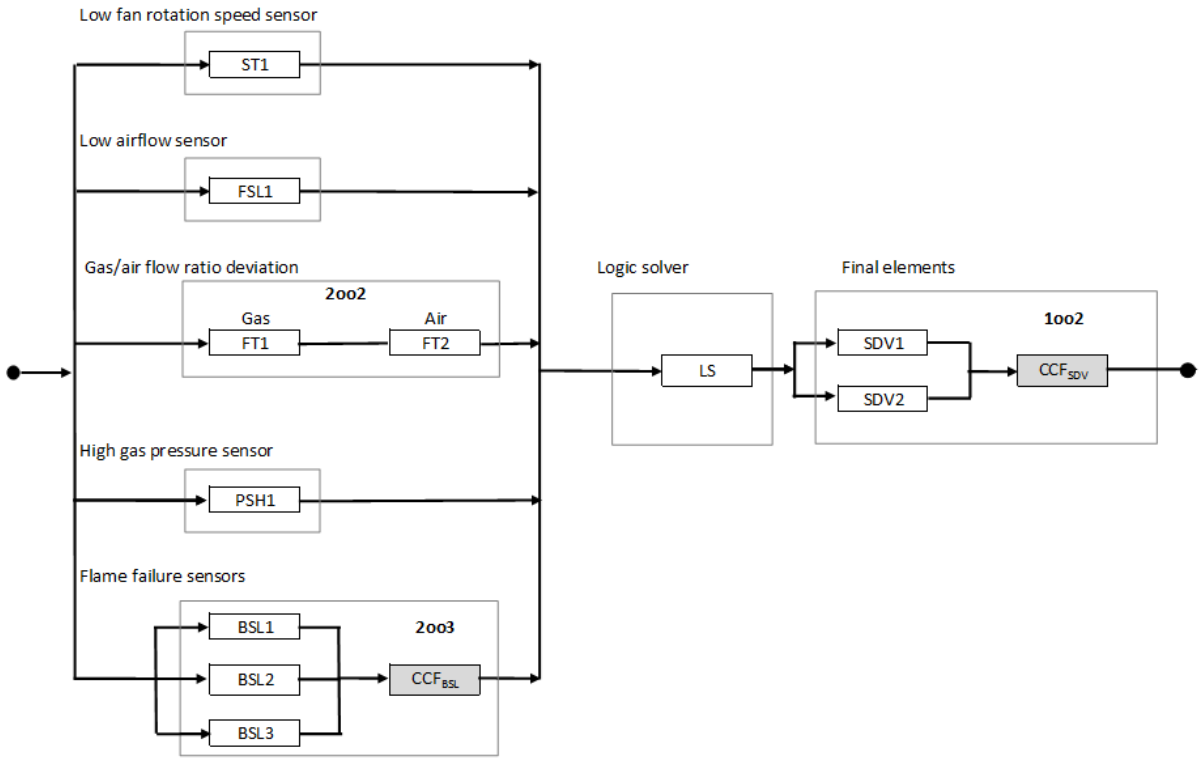
- Flame failure, tripping the master fuel valves
- Burner fan low speed ('fan failure'), tripping the master fuel valves
- Low air flow, tripping the master fuel valves
- Gas/air flow ratio deviation from setpoint, tripping the master fuel valves
- High gas pressure, tripping the master fuel valves.

We cannot take risk reduction credit separately for these SIFs as if they were completely independent.

They may be other separate SIFs responding to high tube temperature or high exhaust stack temperature. Those would be completely unrelated and would represent unrelated demands on the master fuel valve.

The risk reduction required for these five flame failure SIFs comes from the consequence of re-ignition of unburnt fuel and the expected frequency of flame failure ***from all possible causes***.

- The five SIFs related to flame failure all rely on the master fuel valves.
- In the calculation of failure probability, the five SIFs need to be treated as a single system sharing one common final element subsystem, one shared logic solver subsystem and having five separate sensor subsystems (voted in a '1oo5' arrangement).
- The contribution to the overall probability of failure on demand (PFD) of each sensor subsystem needs to be factored by the proportion of causal events to which that sensor subsystem will respond.



The factoring can be achieved by identifying four 'sub-functions', each of which will respond to the individual causal events identified in the LOPA.

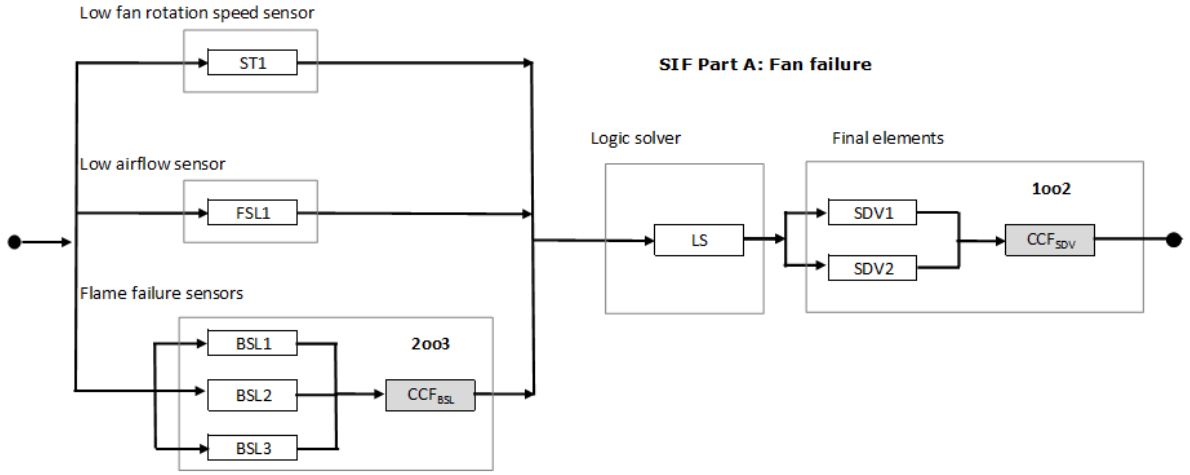
The first step is to identify the causal events and their relative contribution to the hazardous event frequency, for example:

Causal Event	**Frequency (from LOPA)**	**Frequency Proportion**
Fan failure	0.03 pa	10%
Gas pressure regulator fails open	0.1 pa	30%
Gas control valve stuck	0.1 pa	30%
Other events	0.1 pa	30%
Overall	**0.33 pa**	**100%**

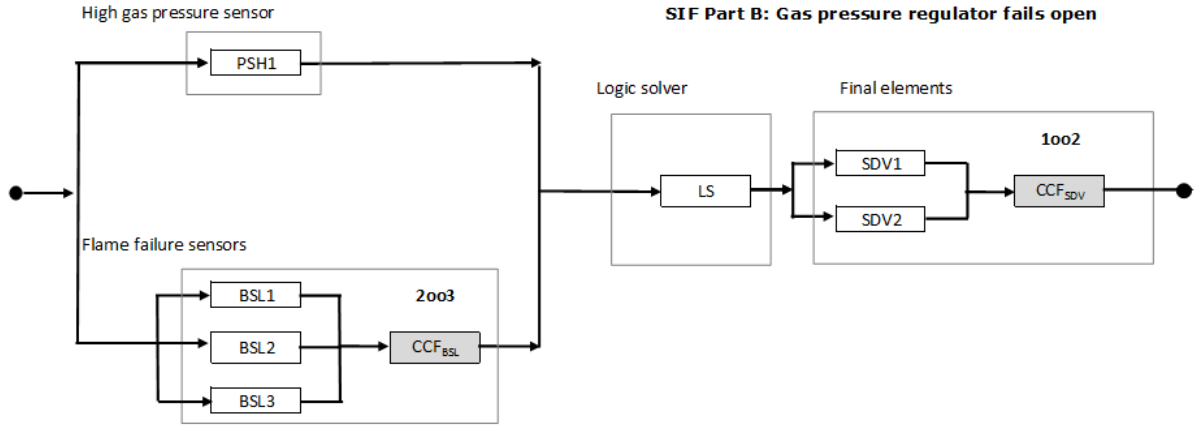
In this example fan failure causes about 10% of flame out scenarios. Fan failure could be detected by three different sensor subsystems in a 1oo3 voting architecture: fan speed, low air flow and flame failure. The reliability block diagram for the fan failure sub-function combines the 1oo3 sensors with the logic solver and the final elements.

Note that in this example there are no common cause failures that would affect a speed sensor, flow senor and flame sensor at the same time. Common cause failure is considered only for the three

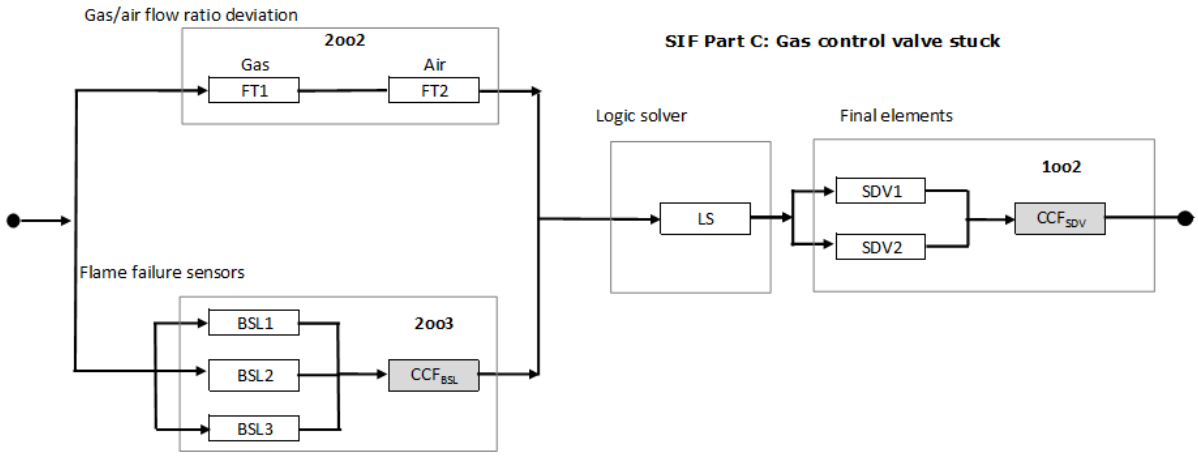
identical flame failure sensors voted 2oo3. The overall 1oo3 voting of diverse technologies results in a comparatively low PFD for the sensor subsystem.



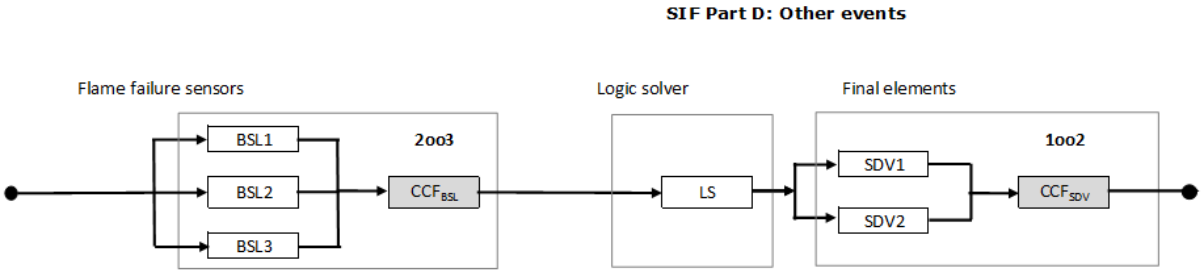
The gas pressure regulator failing open might be detected by a 1oo2 arrangement of the high gas pressure sensor and the flame failure sensors.



Problems with the fuel/air ratio control might be detected by measuring the gas flow and air flow. The flame failure sensor would also respond to loss of flame caused by loss of fuel/air ratio control.



The remaining events might only detected by the flame failure sensors.



In this example the logic solver and final elements are common to the four sub-functions. Only the sensor subsystems need to be factored.

The PFD of the sensor subsystem of each sub-function is factored by the proportion of causal events.

Sub-functions by Causal Event	**Frequency Proportion**	**Sensor Part PFD**	**Factored PFD**
SIF Part A: Fan failure (detected by fan speed, low air flow or flame failure in 1oo3 voting)	10%	2×10^{-9}	2×10^{-10}
SIF Part B: Gas pressure regulator fails open (detected by high gas pressure or flame failure in 1oo2 voting)	30%	2×10^{-6}	6×10^{-7}
SIF Part C: Gas control valve stuck (detected by gas/air flow ratio deviation or flame failure in 1oo2 voting)	30%	3×10^{-6}	9×10^{-7}
SIF Part D: Other events (detected only by flame failure in 1oo1 voting)	30%	3×10^{-5}	1×10^{-5}
Overall sensor sub-system PFD	**100%**	**Total**	**1×10^{-5}**

The total overall PFD of the SIF sensor subsystem is calculated by summing the factored PFD for the individual sub-function sensor subsystems.

The factored PFD is strongly dominated by Part D, because it is the only part without diverse sensor technologies. This is the usually the case. Completely diverse sensor technologies in a voted architecture will always achieve a very low PFD.

The PFD of the logic solver and final elements are then added to the PFD of the sensor subsystem.

The PFD of the logic solver might be 1×10^{-6} and the PFD of the final elements might be 1×10^{-3}.

The overall PFD of this example SIF is dominated by the final elements (master fuel valves). It is usual for the shared final elements to dominate the PFD of a composite function. Correct function of the final element subsystem is essential, no matter what causes the flame failure.

The same final elements may also need to provide risk reduction for scenarios involving failure of tubing carrying the heat transfer fluid. Those scenarios may be completely unrelated to flame failure. The risk reduction required for those scenarios would then be completely independent of the flame failure scenarios.