HOW SHOULD SHARED ELEMENTS BE TREATED IN THE CALCULATION OF FAILURE PROBABILITY FOR A ‘TRIP GROUP’?

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

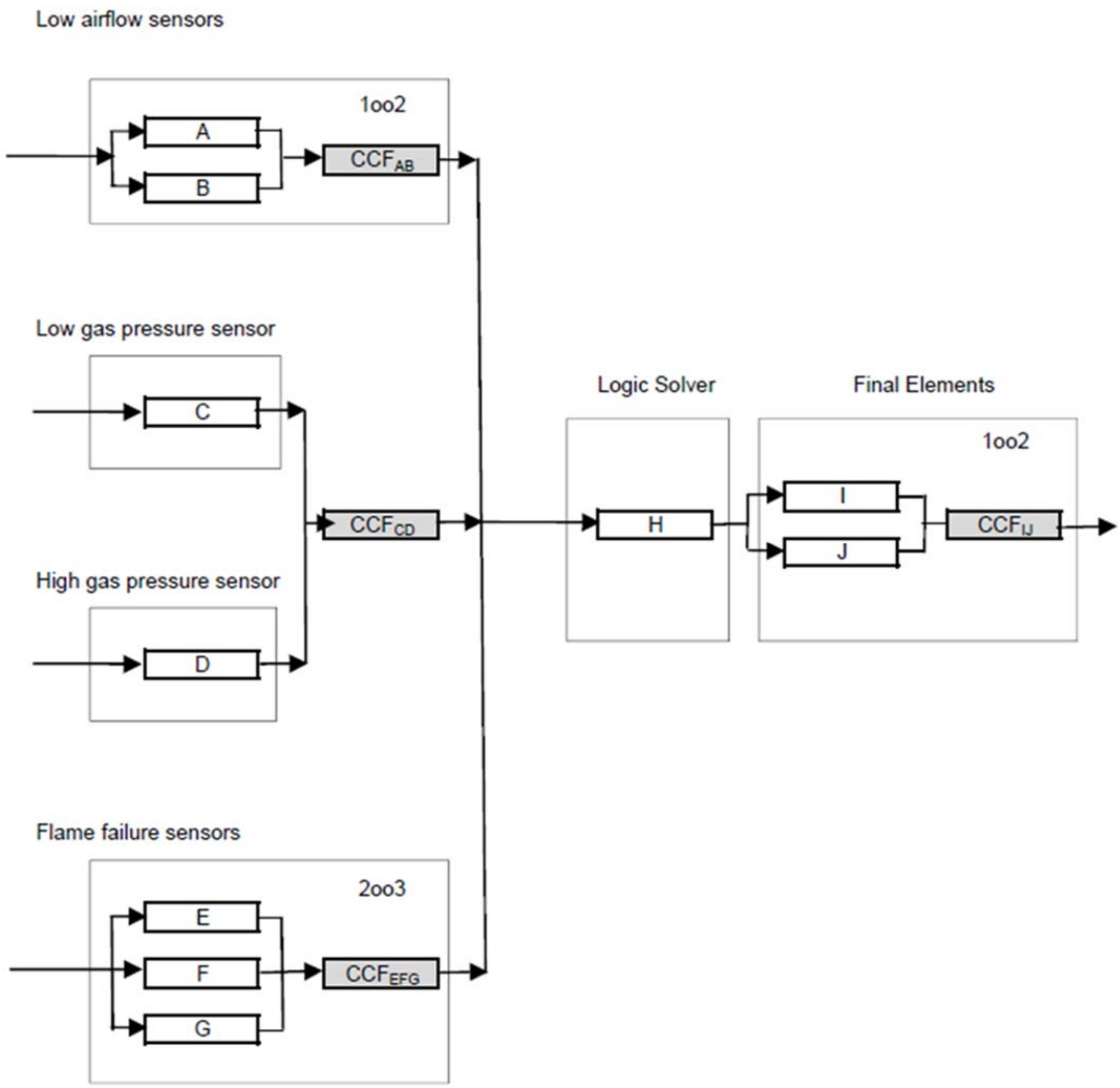
- Flame failure, tripping the master fuel valves
- Low air flow, tripping the master fuel valves
- Low gas pressure, tripping the master fuel valves
- High gas pressure, tripping the master fuel valves.

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 the four flame failure SIFs comes from the consequence of re-ignition of unburnt fuel and the expected and the expected frequency of flame failure ***from all possible causes***.

- The four SIFs related to flame failure all rely on the master fuel valves.
- In the calculation of failure probability the four SIFs need to be treated as a single system sharing one common final element subsystem, one shared logic solver subsystem and having four separate sensor subsystems (voted in a ‘1oo4’ 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.



Assume for example:

- The flame failure sensors are required to respond to 100% of flame failure scenarios.
- Approximately 30% of flame failure is caused by low airflow
- Approximately 10% of flame failure is caused by undetected failure of the gas control valve
- Approximately 30% of flame failure is caused by low gas pressure
- Approximately 30% of flame failure is caused by high gas pressure

The gas pressure sensors are completely independent of the flame failure sensors so for the appropriate proportion of relevant events it might be justifiable to multiply the probability of failure of the pressure sensors by the probability of failure of the flame sensors.

Clearly the low gas pressure sensor is relevant only for low gas pressure events and the high gas pressure sensor is relevant only for high gas pressure events. These gas pressure sensor subsystems may share some common cause failures (CCF) that affect both in the same way (such as relating to the design of the process connections).

Similarly the probability of failure of the low airflow sensor may be multiplied by the probability of failure of the flame failure sensors.

In this example:

$$PFD_{SYS} \approx 0.3 \times \left(PFD_G^{AB} \times \ PFD_G^{EFG}\right) + 0.3 \times \left(PFD_G^{C} \times \ PFD_G^{EFG}\right) + 0.3 \times \left(PFD_G^{D} \times \ PFD_G^{EFG}\right) \\ + 0.6 \times \left(PFD_{CCF}^{CD} \times \ PFD_G^{EFG}\right) \ + 0.1 \times \left(\ PFD_G^{EFG}\right) + PFD_G^{H} + \ PFD_G^{IJ}$$

Clearly the overall PFD of the system is strongly dominated by the PFD of the final elements, as they need to function correctly for all flame failure events.

The 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 can then ignore the demand on the final elements due to flame failure.