Simplified PFD formulae for complex architectures

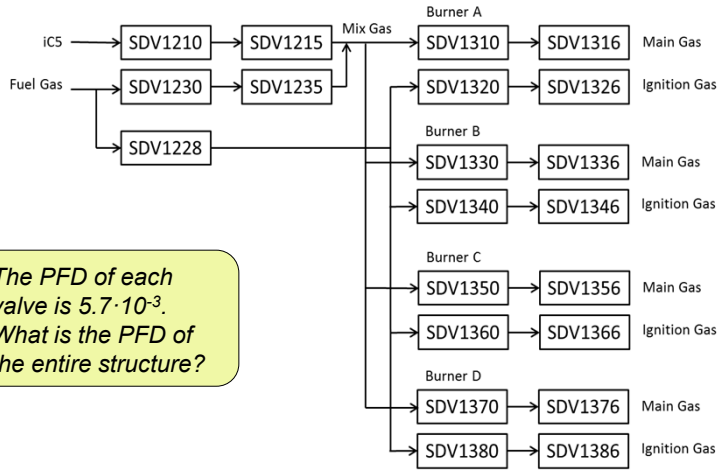
5 February 2025

Arnold Groot MSc MBA

arnold.groot.66@gmail.com

1

The Challenge



The PFD of each valve is $5.7 \cdot 10^{-3}$. What is the PFD of the entire structure?

2

λ_{du} revisited

Failure state	Means of detection	Failure mode
Safe	Proof test	Safe undetected
Safe	Built-in diagnostics	Safe detected
Dangerous	Proof test	Dangerous undetected
Dangerous	Built-in diagnostics	Dangerous detected

λ_{du}= frequency of dangerous and undetected failures [hr^{-1}]

3

PFD revisited

Parameter	Formula
Frequency of dangerous and undetected failure	λ_{du}
Frequency of dangerous, but detected failure	λ_{dd}
Proof Test Interval (say, six months)	T_P
Mean Time to Repair (say, one day)	T_R
Probability of Failure on Demand (PFD)	$\lambda_{du} \cdot \left(\frac{T_P}{2} + T_R\right) + \lambda_{dd} \cdot T_R$

½ T_p is the expectated remaining time to discovery of the failure

4

Simplified formulae revisited

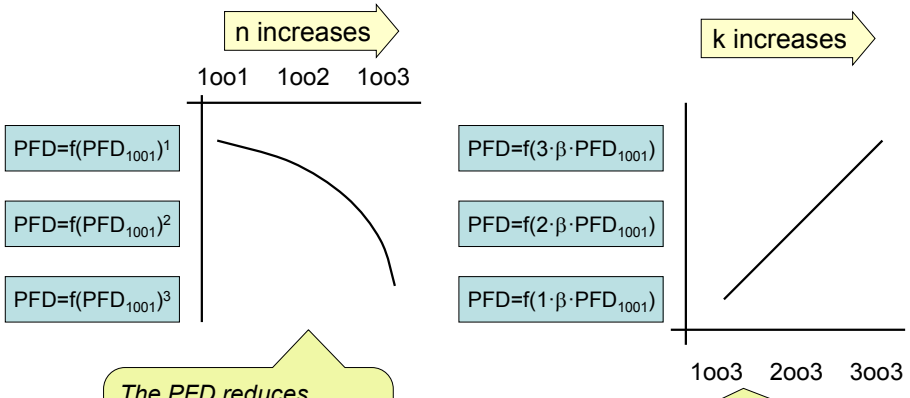
PFD for 1oo1 voting	$PFD_{1oo1} \approx \frac{1}{2} \cdot \lambda_{du} \cdot T_p$
PFD for 1oo2 voting	$PFD_{1oo2} \approx \frac{4}{3} \cdot PFD_{1oo1}^2 + \beta \cdot PFD_{1oo1}$
PFD for 2oo2 voting	$PFD_{2oo2} \approx 2 \cdot PFD_{1oo1} + 2 \cdot \beta \cdot PFD_{1oo1}$
PFD for 2oo3 voting	$PFD_{2oo3} \approx 4 \cdot PFD_{1oo1}^2 + 2 \cdot \beta \cdot PFD_{1oo1}$

Definition of Norwegian University of Science & Technology

λ_{du} = dangerous undetected failure rate [hr^{-1}]
Tp = proof test interval [hrs]
β = fraction of dangerous undetected failures that have a common cause

5

Analysing the patterns

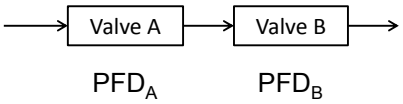


The PFD reduces exponentially as the number of channels increases

The Common Cause Factor increases as the number of combinations of common causes (k) increases

6

Network approach



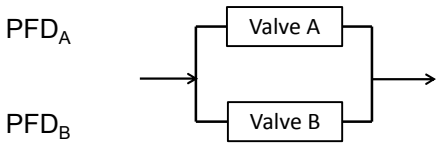
Two different valves A and B in series with PFD_B>PFD_A yield:

$$PFD_{1oo2} \approx \frac{4}{3} \cdot PFD_A \cdot PFD_B + \beta \cdot PFD_A \approx \beta \cdot PFD_A$$

*The safety performance of the **best** valve is further improved by adding a poorer valve in series.*

7

Network approach



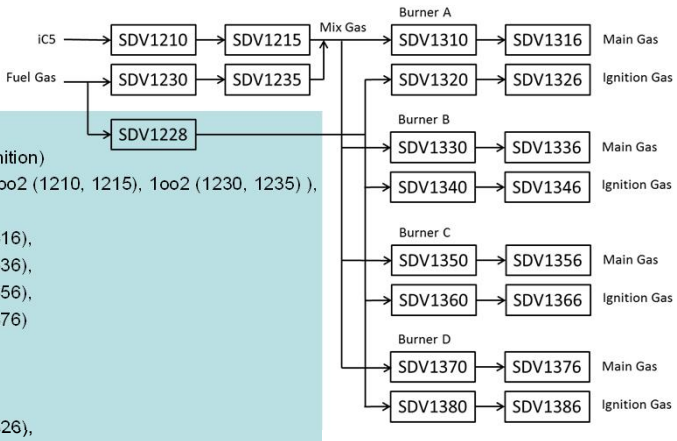
Two different valves A and B in parallel yield:

$$PFD_{2oo2} \approx PFD_A + PFD_B + \beta \cdot (PFD_A + PFD_B)$$

The PFD's of two independent failure sources can be added together.

8

From P&ID to reliability logics



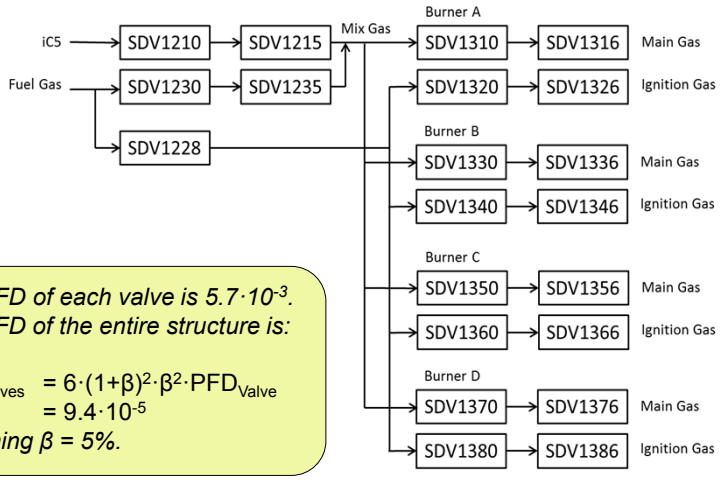
Valves = 2oo2 (Main, Ignition)
Main = 1oo2 (2oo2 (1oo2 (1210, 1215), 1oo2 (1230, 1235)),
4oo4 (
1oo2 (1310, 1316),
1oo2 (1330, 1336),
1oo2 (1350, 1356),
1oo2 (1370, 1376)
))
Ignition = 1oo2 (1228,
4oo4 (
1oo2 (1320, 1326),
1oo2 (1340, 1346),
1oo2 (1360, 1366),
1oo2 (1380, 1386)
))

From reliability logics to PFD

Valves = 2oo2 (Main, Ignition)
Main = 1oo2 (2oo2 (1oo2 (1210, 1215), 1oo2 (1230, 1235)),
4004 (
1oo2 (1310, 1316),
1oo2 (1330, 1336),
1oo2 (1350, 1356),
1oo2 (1370, 1376)
))
Ignition = 1oo2 (1228,
4oo4 (
1oo2 (1320, 1326),
1oo2 (1340, 1346),
1oo2 (1360, 1366),
1oo2 (1380, 1386)
))

PFD_{Valves} $= (1+\beta)\cdot(Main + Ignition)$
Main $= \beta \cdot Min\ (4\cdot(1+\beta)\cdot\beta\cdot PFD_{Valve},\ 2\cdot(1+\beta)\cdot\beta\cdot PFD_{Valve})$
$= 2\cdot(1+\beta)\cdot\beta^2\cdot PFD_{Valve}$
Ignition $= \beta \cdot Min\ (4\cdot(1+\beta)\cdot\beta\cdot PFD_{Valve},\ PFD_{Valve})$
$= 4\cdot(1+\beta)\cdot\beta^2\cdot PFD_{Valve}$
so PFD_{Valves} $= 6\cdot(1+\beta)^2\cdot\beta^2\cdot PFD_{Valve}$

Problem solved



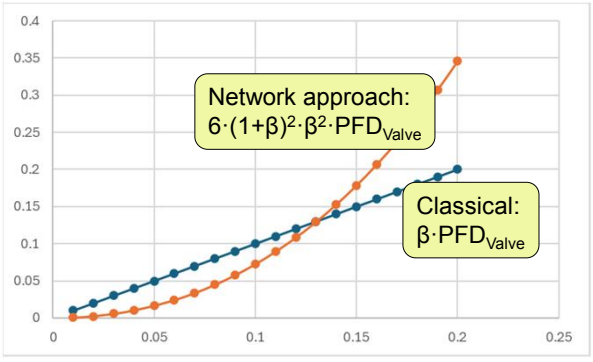
The PFD of each valve is $5.7 \cdot 10^{-3}$. The PFD of the entire structure is:

$PFD_{Valves} = 6 \cdot (1+\beta)^2 \cdot \beta^2 \cdot PFD_{Valve}$
$= 9.4 \cdot 10^{-5}$

assuming $\beta = 5\%$.

11

Problem solved?

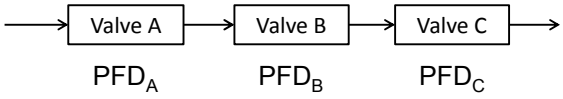


Why is the minimum CCF of a network often defined as $\beta \cdot PFD_{1001}$?

Why can the PFD of a network not be improved by adding additional valves in series (or transmitters in parallel)?

12

Is the network approach wrong?



Generic formula for 1oo3 of three identical valves:

$$PFD_{1oo3} \approx \beta \cdot PFD_{1oo1}$$

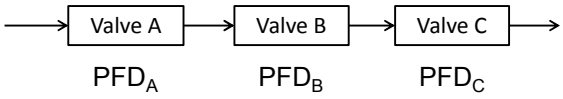
Network of A and B in series (with PFD_A<PFD_B):

$$PFD_{1oo2} \approx \beta \cdot PFD_A$$

Network of (A and B) and C in series:

$$PFD_{1oo3} \approx \beta^2 \cdot PFD_A$$

Independent probabilities



Generic formula for 1oo3 of three identical valves:
"Rolling the same dice three times"
If the CCF between A and B equals X, then the CCF between A and C is X, and the CCF between B and C is also X.

Network of A, B and C in series:
"Rolling three different dices"
If the CCF between A and B equals X, then the CCF between A and C, and between B and C, may be quite different
The CCF between A and B may relate to FTC (failure to close), whereas the CCF between B and C may relate to LCP (leaking in closed position)

and finally...

The Functional Safety community overemphasizes the use of software tools and underemphasizes the definition of β.