MANAGING RISK

Evaluating the PFD of Safety Instrumented Systems with Partial Stroke Testing

Luiz Fernando Oliveira
Vice-President
DNV Energy Solutions South America

How did I get to writing this paper?

MANAGING RISK

- Started doing SIL analysis in Brazil in 1999
- Looked at the analytical equations given in IEC 61508
  - Given only for four possible configurations (1oo1, 1oo2, 2oo2, 2oo3)
  - Used them but did not pay too much attention to them
- In 2004 got funds to develop a SIL analysis software for DNV internal use throughout the world
  - Had to include a much larger number of possible configurations
    - Why not all of them? KooN?
- Several choices to calculate them
  - Fault tree engine? Markov engine? Analytical equations? Numerical Integration?
- Chose to use analytical equations: simpler and faster
- Then came the problem: a generic KooN equation is not difficult to obtain
  - But had to revert to those given in IEC 61508
  - Clients always ask if the calculations are in accordance with the Standard

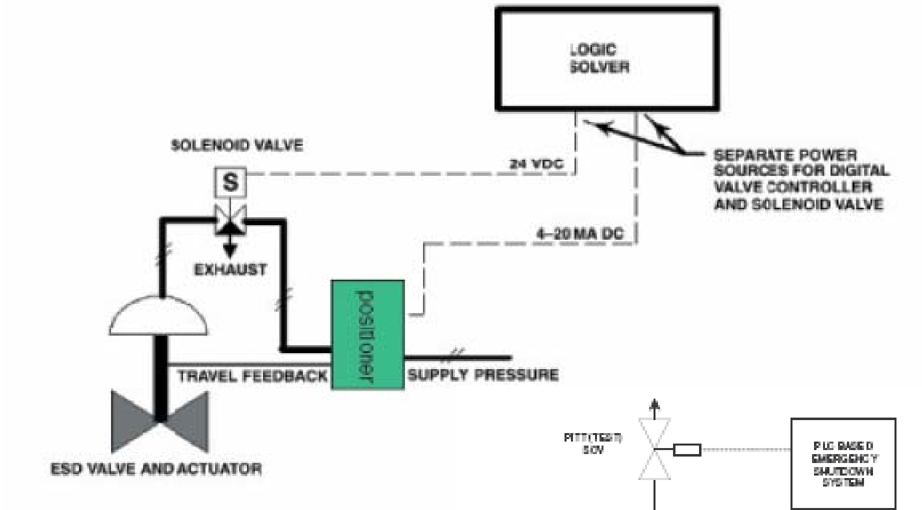
How did I get to writing this paper?

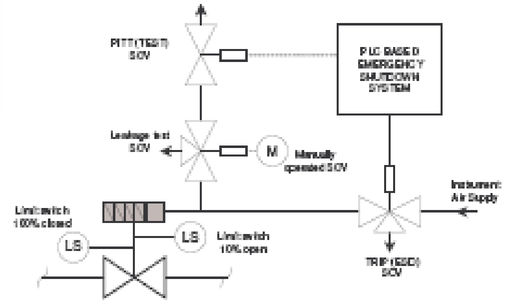
- First task was to derive the equations in IEC 61508
  - This proved not so simple
  - Not enough details are given in the Standard
    - Assumptions and approximations
  - Could not find anywhere else
  - Biggest difficulty: uses both detected (revealed) and undetected (unrevealed) dangerous failure rate – which one to assume?
- And the Partial Stroke Testing problem?
  - Recognized as a very good solution in many situations
  - Had to be solved together
  - Not given in IEC 61508 (only one equation for non-perfect testing - could use the same equation?)
- Whole problem solved after several tries
  - Deduction of PFD equation for KooN configuration without and with PST capabillity

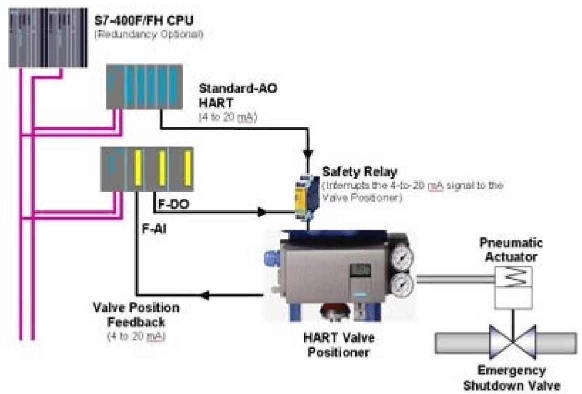
What is Partial Stroke Testing?

MANAGING RISK DNV

- Ability to test some failure modes of a block valve without any significant variation in plant throughput
- Several makers and models
- Apply small torque and monitor corresponding valve movement
- Tests failure mode “valve stuck open”
- Do not test the whole blocking function
  - Latter is only tested in a full test
- Advantages
  - Less plant shutdowns for testing
  - Lower PFD value

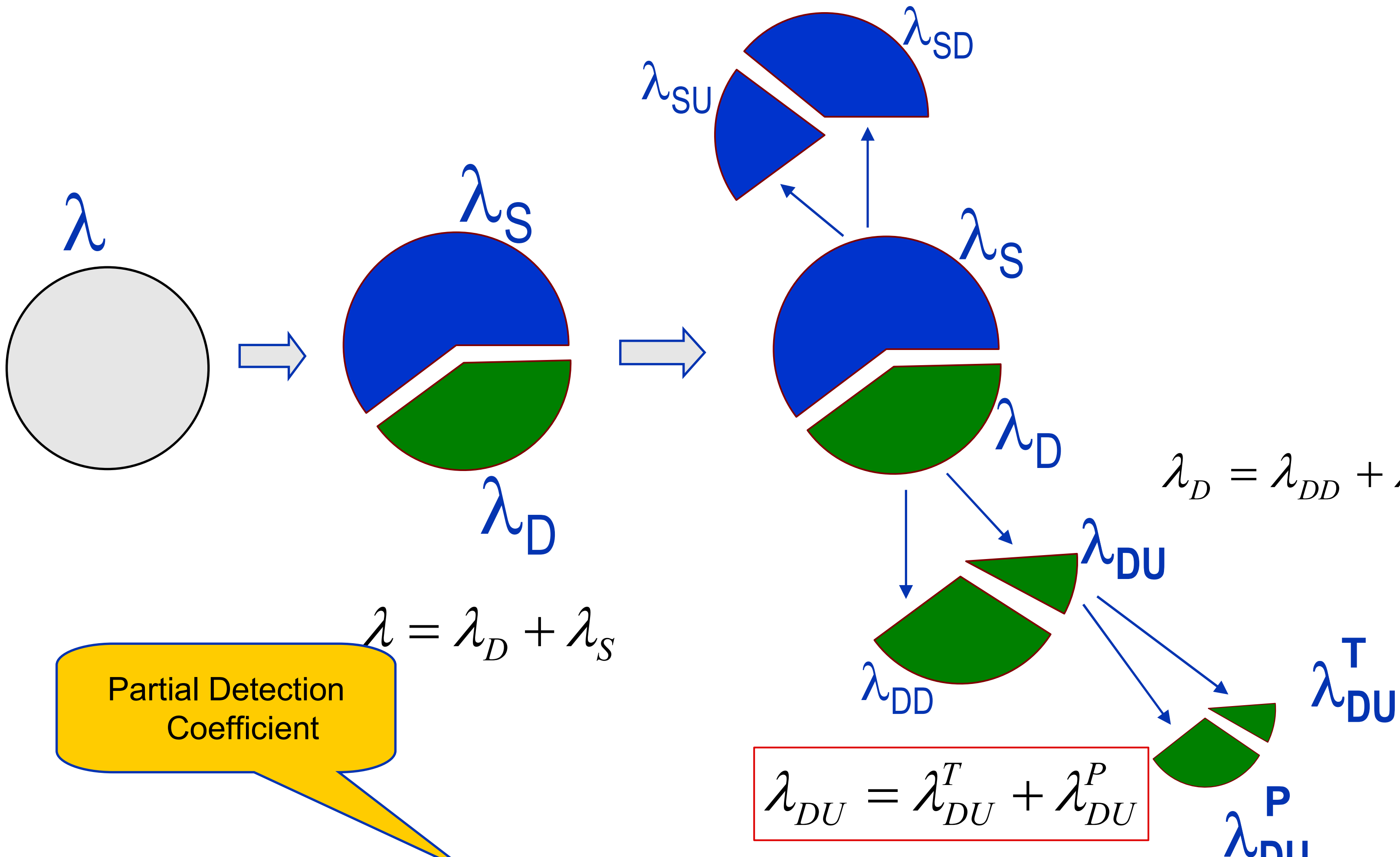






Failure Rate Taxonomy without and with PST

MANAGING RISK DNV



$$\lambda = \lambda_D + \lambda_S$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

$$\boxed{\lambda_{DU} = \lambda_{DU}^{T} + \lambda_{DU}^{P}}$$

$$\boxed{\lambda_{DU} = PDC \times \lambda_{DU} + (1 - PDC) \times \lambda_{DU}}$$

KooN System without PST

MANAGING RISK DNV

- Average value of PFD can be written as the product of
  - Frequency of entering the failed state, and
  - Time it remains in the failed state

$$PFD_{koon} = \Phi_{koon} * T_{koon}$$

- Average value of PFD can be written as the product of
  - Frequency of entering the failed state, and
  - Time it remains in the failed state

- Dangerous failure rate has two contributions: detected (revealed) and undetected (unrevealed)

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

- Two possible approaches:
  - Behaves as “revealed”
  - Behaves as “unrevealed”

KooN System without PST

MANAGING RISK DNV

- Two possible approaches:
  - Behaves as "revealed"
  - Behaves as "unrevealed"
- In both cases:
  - the mean duration the channel spends in a failed state is taken approximately as a weighted average of the two contributions
  - For a single channel (IEC 61508)

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

  - For two channels (IEC 61508)

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

  - Generalizing for KooN channels

$$T_{koon} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

1st Analytical Approach: "Revealed Failure"

MANAGING RISK

- For koon system:
  - Frequency of entering the failed state: n-k already and (n-k+1)th failed

$$\Phi_{koon} = K_{koon} \times \lambda_D \times (\lambda_D t_{CE})^{n-k}$$

$$K_{koon} = k \times C_n^{n-k} = k \times \frac{n!}{k!(n-k)!}$$

$$\Phi_{koon} = \frac{n!}{(k-1)!(n-k)!} \lambda_D^{n-k+1} t_{CE}{}^{n-k}$$

Reproduces the equations in IEC 61508

$$PFD_{koon} = \frac{n!}{(k-1)!(n-k)!} \lambda_D^{n-k+1} t_{CE}{}^{n-k} \times \left[\frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{n-k+2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right]$$

2nd Analytical Approach: "Unrevealed Failure"

- For koon system:
  - Frequency of entering the failed state: (a little more laborious)

$$\Phi_{koon} = \frac{n!}{(k-1)!\,(n-k+1)!}\lambda_D^{n-k+1}T_1^{\,n-k}$$

$$PFD_{koon} = \frac{n!}{(k-1)!\,(n-k+1)!}\lambda_D^{n-k+1}T_1^{\,n-k} \times \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR\right]$$

For $T_1 \approx 2t_{CE}$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

Reproduces the equations in IEC 61508

when $\lambda_{DD} << \lambda_{DU}$

and $MTTR << T_1$

PFD with PST ("Revealed Failure")

MANAGING RISK DNV

Test interval for total test

Test interval for partial test

- For 1oo1 system:

$$PFD_{1oo1PST} = (1-PDC)\times\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)+PDC\times\lambda_{DU}\left(\frac{T_2}{2}+MTTR\right)+\lambda_{DD}MTTR$$

- For 1oo2 system:

$$PFD_{1oo2PST} = 2\lambda_{DU}^2 t_{CE-PST}\cdot t_{GE-PST}$$

$$t_{CE-PST} = \frac{(1-PDC)\times\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{PDC\times\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{GE-PST} = \frac{(1-PDC)\times\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3}+MTTR\right)+\frac{PDC\times\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{3}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

PFD with PST ("Revealed Failure")

MANAGING RISK DNV

- Generalizing for a koon configuration:

$$PFD_{koon-PST} = \frac{n!}{(k-1)!\,(n-k)!}\lambda_D^{n-k+1}\left(t_{CE-PST}\right)^{n-k} \times T_{koon-PST}$$

$$t_{CE-PST} = \frac{(1-PDC)\times\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{PDC\times\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

Test interval for total test

Test interval for partial test

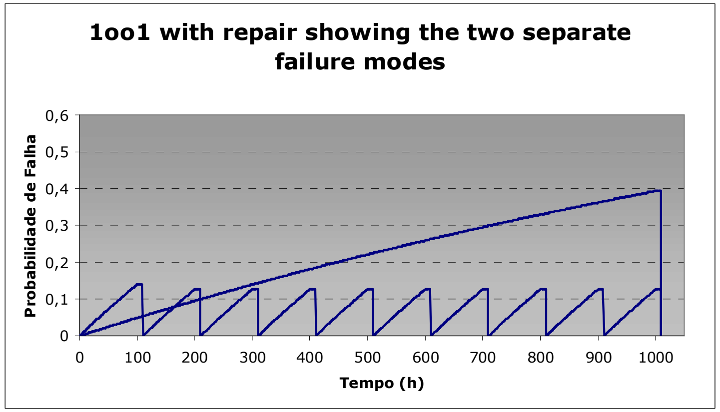
$$T_{koon-PST} = \frac{(1-PDC)\times\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2}+MTTR\right)+\frac{PDC\times\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{n-k+2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

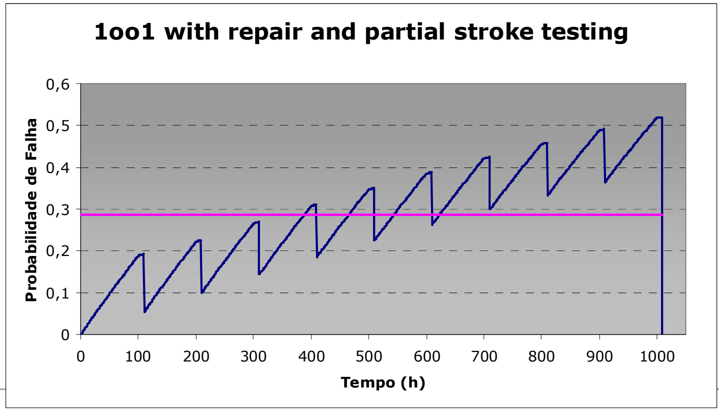
Numerical Approach

MANAGING RISK

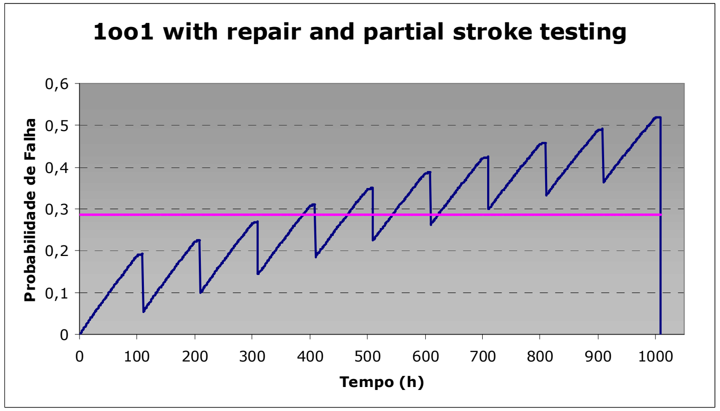
- Numerical evaluation of system unreliability function
  - Unreliability function described as numerical function
- Numerical integration of unreliability function over test interval
  - Obtain average PFD value

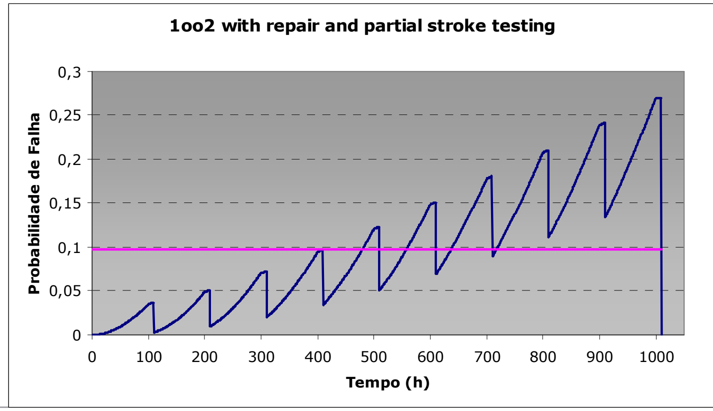
1oo1





1oo2





Some Comparisons

MANAGING RISK DNV

Data Used

Description	Value
Interval between complete tests [(T$_1$ (h)]	43800
Interval between partial tests [T$_2$ (h)]	730/365
Dangerous failure rate [λ_D (/h)]	2,70E-06
Diagnostic coverage coefficient [DC$_D$]	0,25
Partial test detection coefficient [PDC]	0,8
Beta factor for undetected dangerous failures [ß]	0,05
Beta factor for detected dangerous failures [ß$_D$]	0,05
Mean time between restoration [MTTR (h)]	24,0

Some Comparisons

MANAGING RISK

The two analytical equations and the numerical approach with PST (T_2=730 h)

Architecture	Equation 17	Equation 18 (with $T_1=2t_{CE\text{-}PST}$)	Numerical Approach
1oo1	9.53E-03	9.53E-03	9.42E-03
1oo2	1.21E-04	1.21E-04	1.15E-04
2oo2	1.91E-02	1.91E-02	1.87E-02
1oo3	1.31E-06	1.74E-06	1.57E-06
2oo3	3.64E-04	3.64E-04	3.41E-04
3oo3	2.86E-02	2.86E-02	2.79E-02
1oo4	1.33E-08	2.66E-08	2.29E-08
2oo4	5.22E-06	6.96E-06	6.21E-06
3oo4	7.28E-04	7.28E-04	6.76E-04
4oo4	3.81E-02	3.81E-02	3.70E-02

Some Comparisons

MANAGING RISK DNV

The two analytical equations and the numerical approach with PST (T_2=730 h)

Architecture	Eq.(17) w/o PST	Eq.(17) w PST (730 h)	Eq.(17) w PST (365 h)
1oo1	4,44E-02	9,53E-03	9,23E-03
1oo2	4,60E-03	5,86E-04	5,64E-04
2oo2	8,88E-02	1,91E-02	1,85E-02
1oo3	2,33E-03	4,77E-04	4,63E-04
2oo3	9,35E-03	8,05E-04	7,70E-04
3oo3	1,33E-01	2,86E-02	2,77E-02
1oo4	2,23E-03	4,76E-04	4,62E-04
2oo4	2,67E-03	4,81E-04	4,66E-04
3oo4	1,65E-02	1,13E-03	1,08E-03
4oo4	1,78E-01	3,81E-02	3,69E-02

Some Comparisons

MANAGING RISK DNV

The two analytical equations and the numerical approach with PST (T_2=730 h)

Architecture	Eq.(17) w/o PST	Eq.(17) w PST (730 h)	Eq.(17) w PST (365 h)
1oo1	4,44E-02	9,53E-03	9,23E-03
1oo2	4,60E-03	5,86E-04	5,64E-04
2oo2	8,88E-02	1,91E-02	1,85E-02
1oo3	2,33E-03	4,77E-04	4,63E-04
2oo3	9,35E-03	8,05E-04	7,70E-04
3oo3	1,33E-01	2,86E-02	2,77E-02
1oo4	2,23E-03	4,76E-04	4,62E-04
2oo4	2,67E-03	4,81E-04	4,66E-04
3oo4	1,65E-02	1,13E-03	1,08E-03
4oo4	1,78E-01	3,81E-02	3,69E-02

De SIL 0 para SIL 1

Some Comparisons

MANAGING RISK DNV

The two analytical equations and the numerical approach with PST (T_2=730 h)

Architecture	Eq.(17) w/o PST	Eq.(17) w PST (730 h)	Eq.(17) w PST (365 h)
1oo1	4,44E-02	9,53E-03	9,23E-03
1oo2	4,60E-03	5,86E-04	5,64E-04
2oo2	8,88E-02	1,91E-02	1,85E-02
1oo3	2,33E-03	4,77E-04	4,63E-04
2oo3	9,35E-03	8,05E-04	7,70E-04
3oo3	1,33E-01	2,86E-02	2,77E-02
1oo4	2,23E-03	4,76E-04	4,62E-04
2oo4	2,67E-03	4,81E-04	4,66E-04
3oo4	1,65E-02	1,13E-03	1,08E-03
4oo4	1,78E-01	3,81E-02	3,69E-02

De SIL 1 para SIL 2

Some Comparisons

MANAGING RISK DNV

The two analytical equations and the numerical approach with PST (T_2=730 h)

Architecture	Eq.(17) w/o PST	Eq.(17) w PST (730 h)	Eq.(17) w PST (365 h)
1oo1	4,44E-02	9,53E-03	9,23E-03
1oo2	4,60E-03	5,86E-04	5,64E-04
2oo2	8,88E-02	1,91E-02	1,85E-02
1oo3	2,33E-03	4,77E-04	4,63E-04
2oo3	9,35E-03	8,05E-04	7,70E-04
3oo3	1,33E-01	2,86E-02	2,77E-02
1oo4	2,23E-03	4,76E-04	4,62E-04
2oo4	2,67E-03	4,81E-04	4,66E-04
3oo4	1,65E-02	1,13E-03	1,08E-03
4oo4	1,78E-01	3,81E-02	3,69E-02

De SIL 2 para SIL 3

Final Comments

MANAGING RISK DNV

- Two different analytical equations for koon systems with PST were presented
  - Considering revealed or unrevealed failure
- “Revealed” seems to be the approach used in IEC 61508
- Results of both equations are similar
- Results compare very well to those of a numerical approach
- Ability to undergo PST generally increases the SIL value by one
- PST significantly reduces the number of plant shutdowns
- Analytical equations can be used even for very reduntdant configurations and large proof test intervals

And to finish …

I will give you a one-minute test …

If you already knew it, please don´t answer it, thank you.

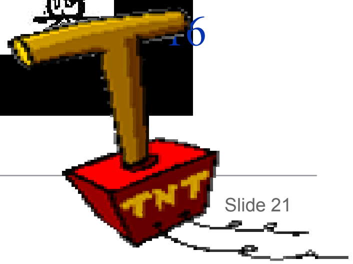
What are the two squares with the same symbols In different orders? You have one minute

MANAGING RISK DNV

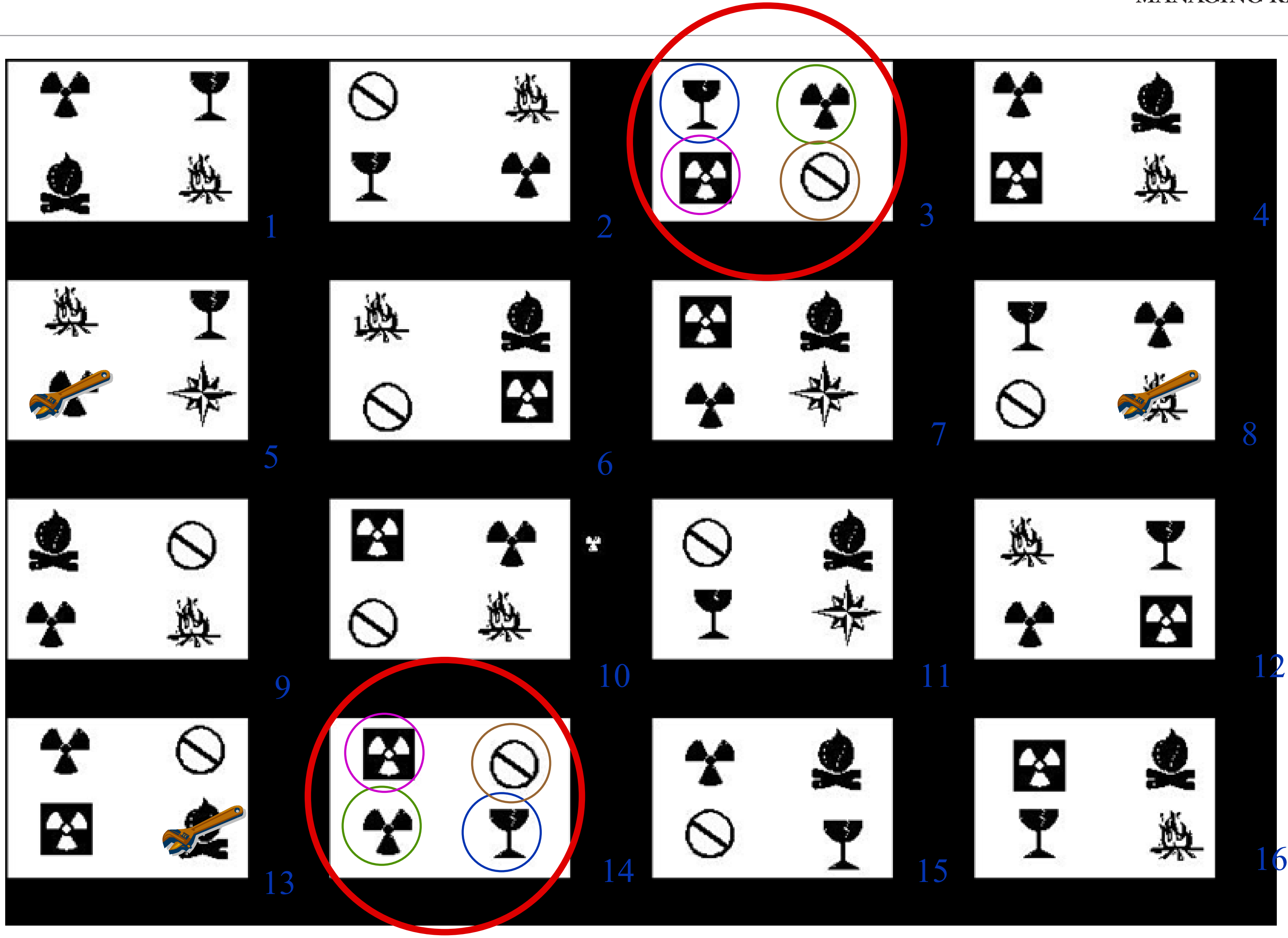
55 s ..

30 s ..

1 s



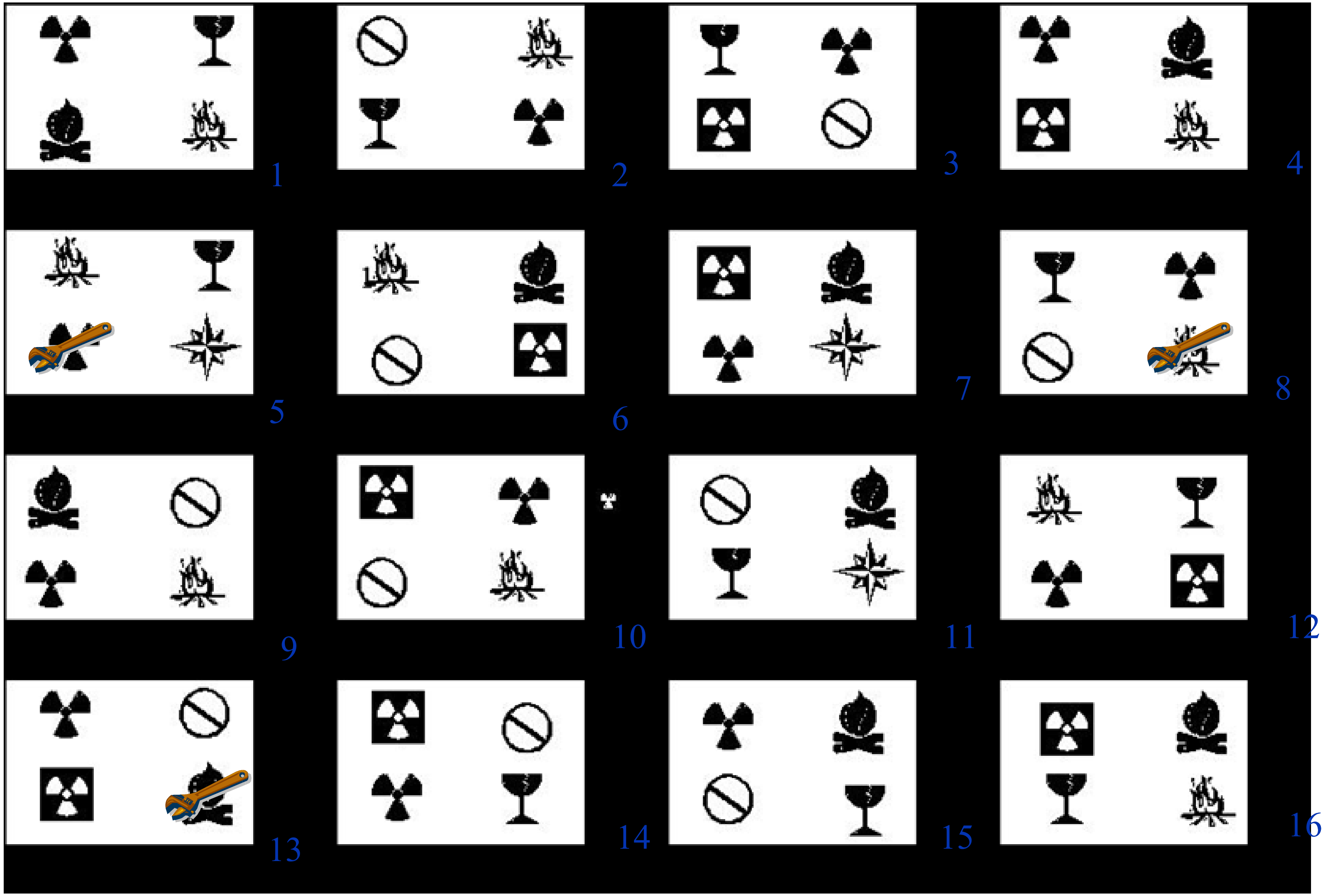
And here is the answer…


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

And now look again…

Can you find them now?

MANAGING RISK DNV



Moral of the story?

MANAGING RISK DNV

Everything looks easy after it is solved.

Many thanks, everyone!!!