ISO/TR 12489: Reliability modelling & calculation of safety systems. Presentation and applications

Jean-Pierre SIGNORET
ISO/TR 12489 project leader
Reliability expert, TOTAL

TC67
WG4

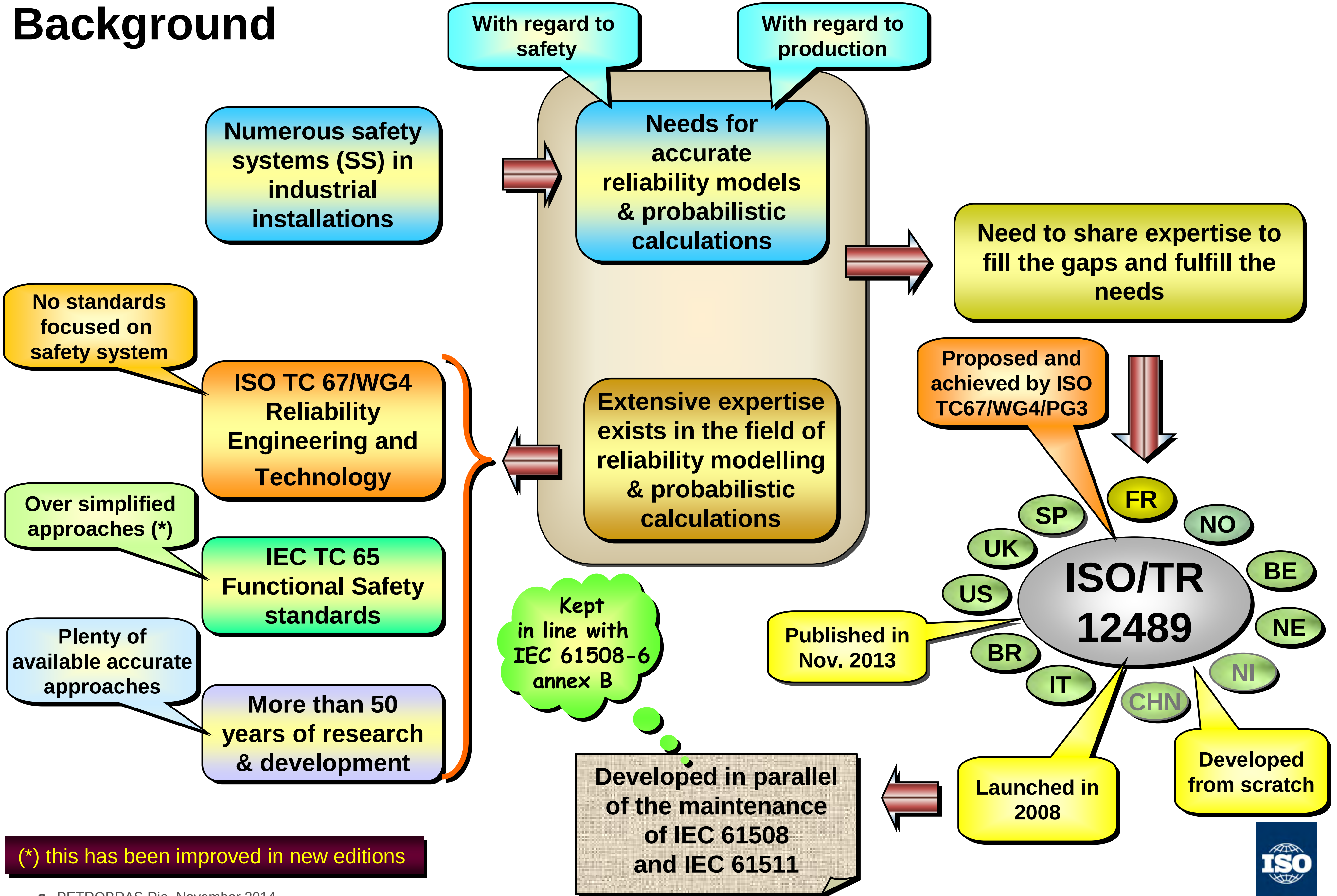
PETROBRAS Rio, November 2014

Presentation of ISO/TR 12489

TR prepared by ISO TC67 WG4/Project Group 3
PG3 leader : Jean Pierre Signoret (Total)
WG4 Convenor: Runar Østebø (Statoil)

TC67
WG4

Background



(*) this has been improved in new editions

ISO TC67/ WG4

ISO/TR 12489 outline

This is a Technical Report

Only **informative** matters

Aims to provide guidelines

A technical report is obviously "technical"!

Mathematical development of formulae

Not explained elsewhere

Implementation of systemic approaches

Not developed elsewhere

Reliability data collection (ISO 14224)

This document deals with reliability modelling & calculations

Simplified & non-simplified approaches

Reliability modelling & calculation of safety systems

Simple & complex systems

This document deals with safety systems

Ordinary Safety Systems

Safety Instrumented Systems (SIS)

Failure of safety actions

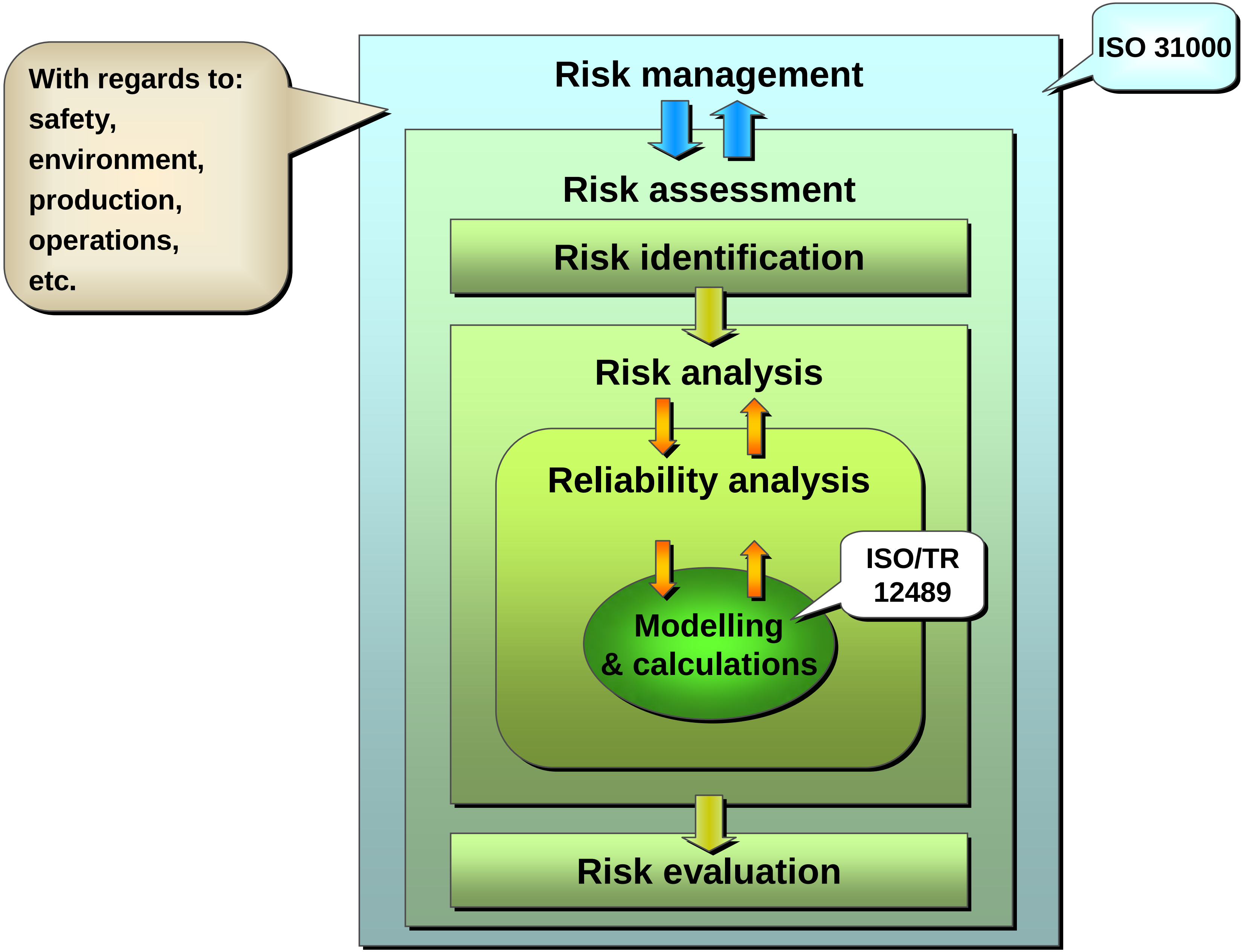
Impact on safety

Spurious actions

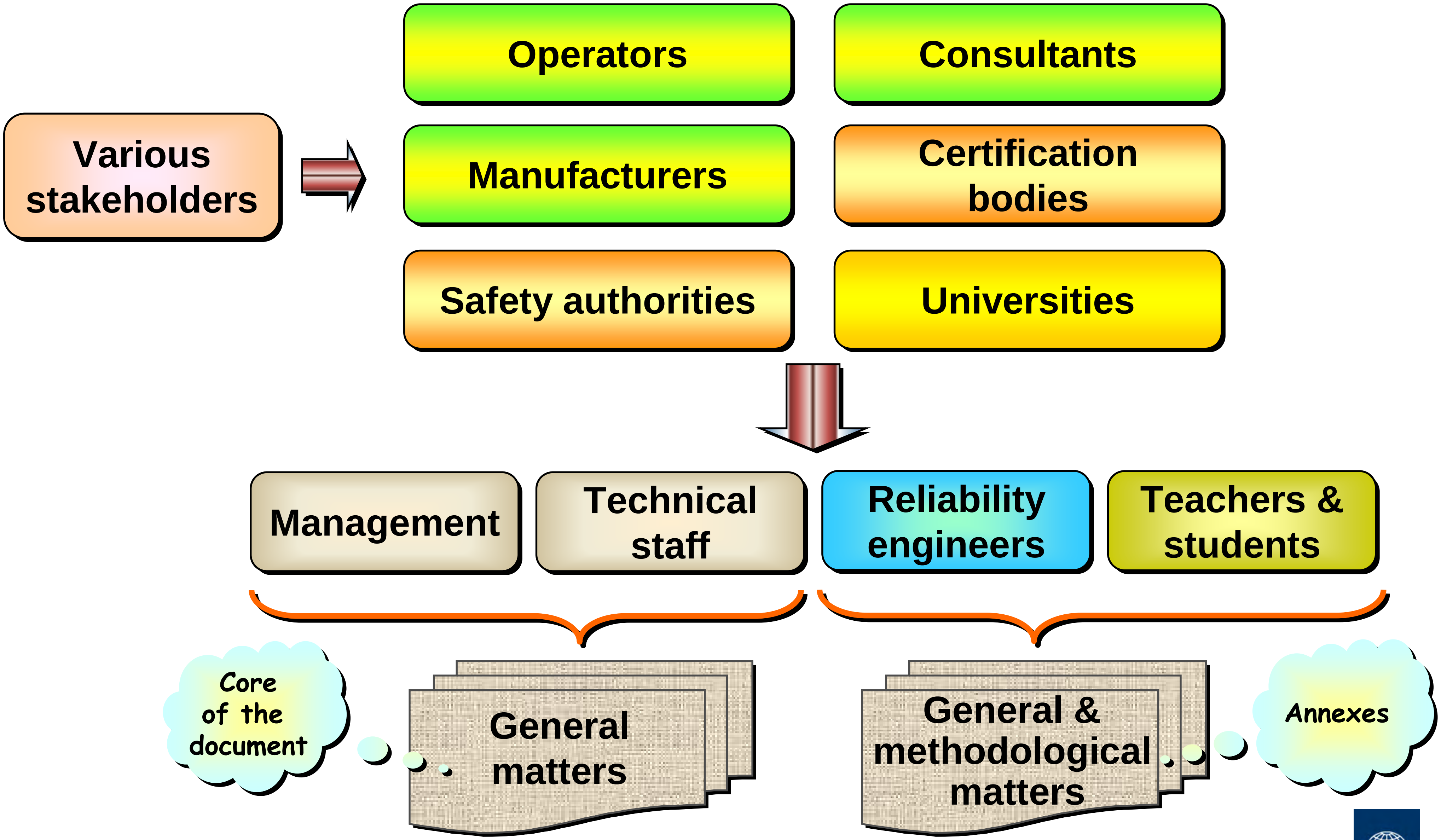
Impact on Dependability

Production availability (ISO 20815)

Overall framework of ISO/TR 12489

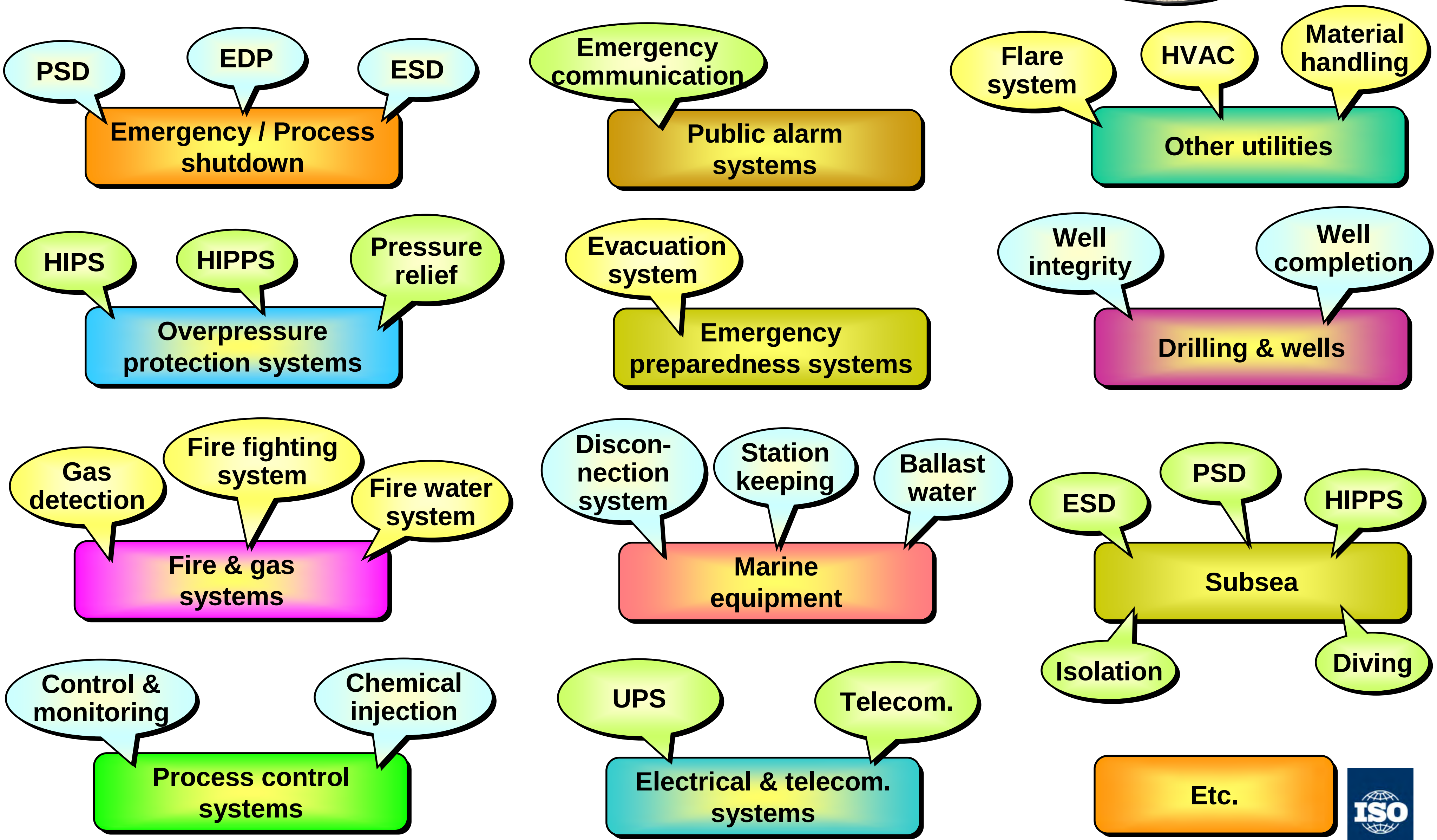


Target users of ISO/TR 12489

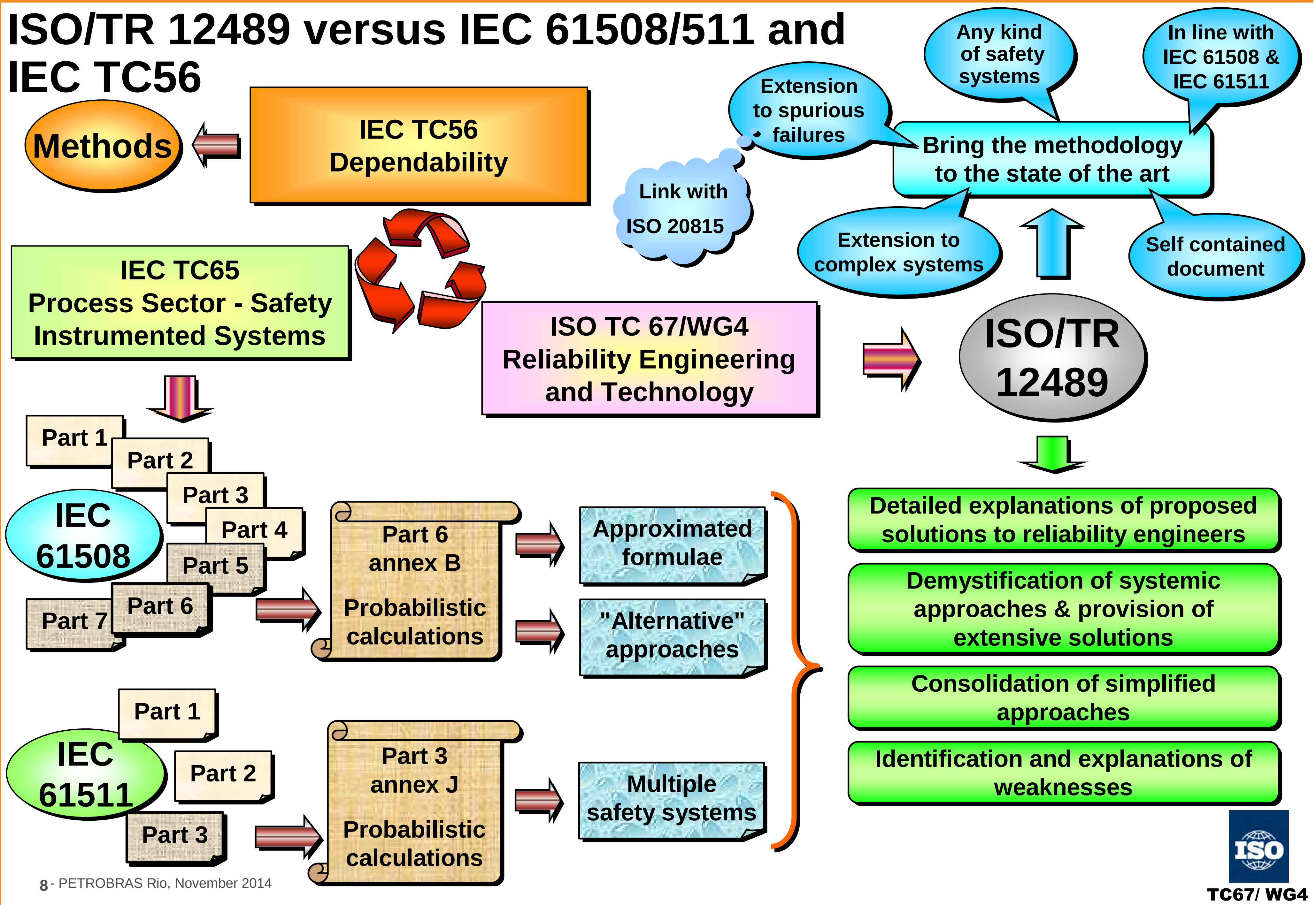


Some examples of safety systems covered by ISO/TR 12489 (instrumented or not)

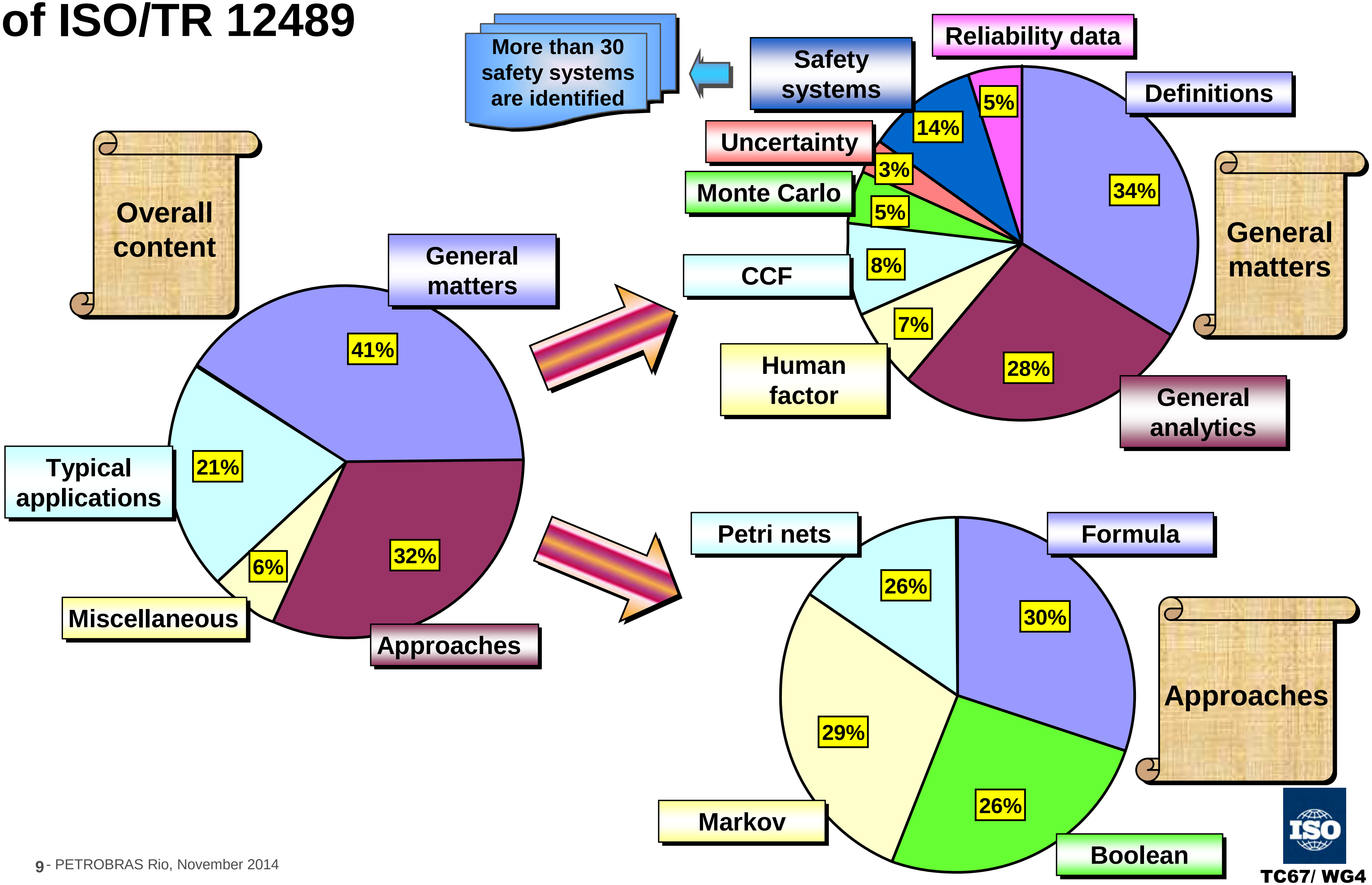
31 systems identified in the TR



ISO/TR 12489 versus IEC 61508/511 and IEC TC56



Distribution of the topics within the 260 pages of ISO/TR 12489

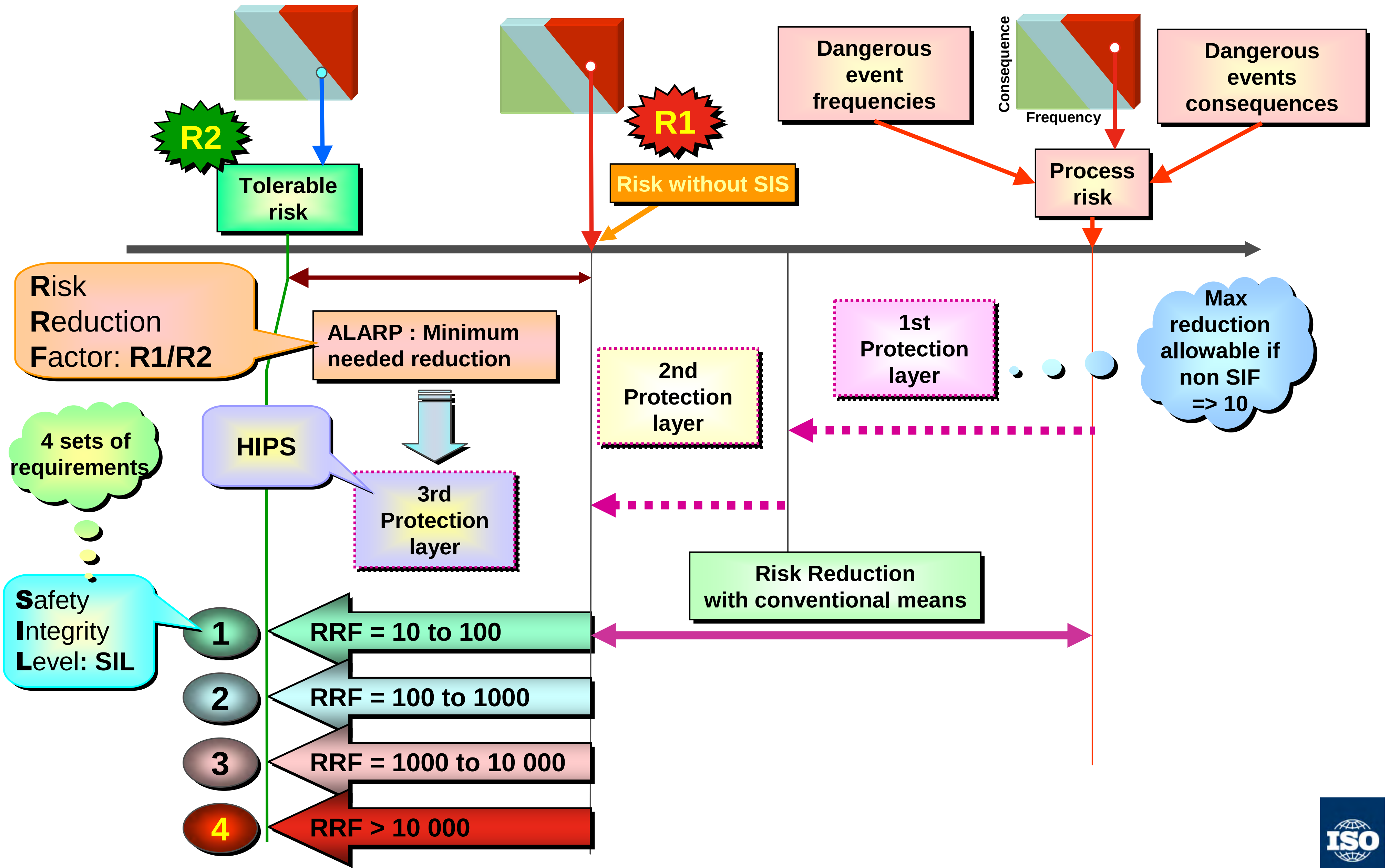


Introduction to functional safety concepts

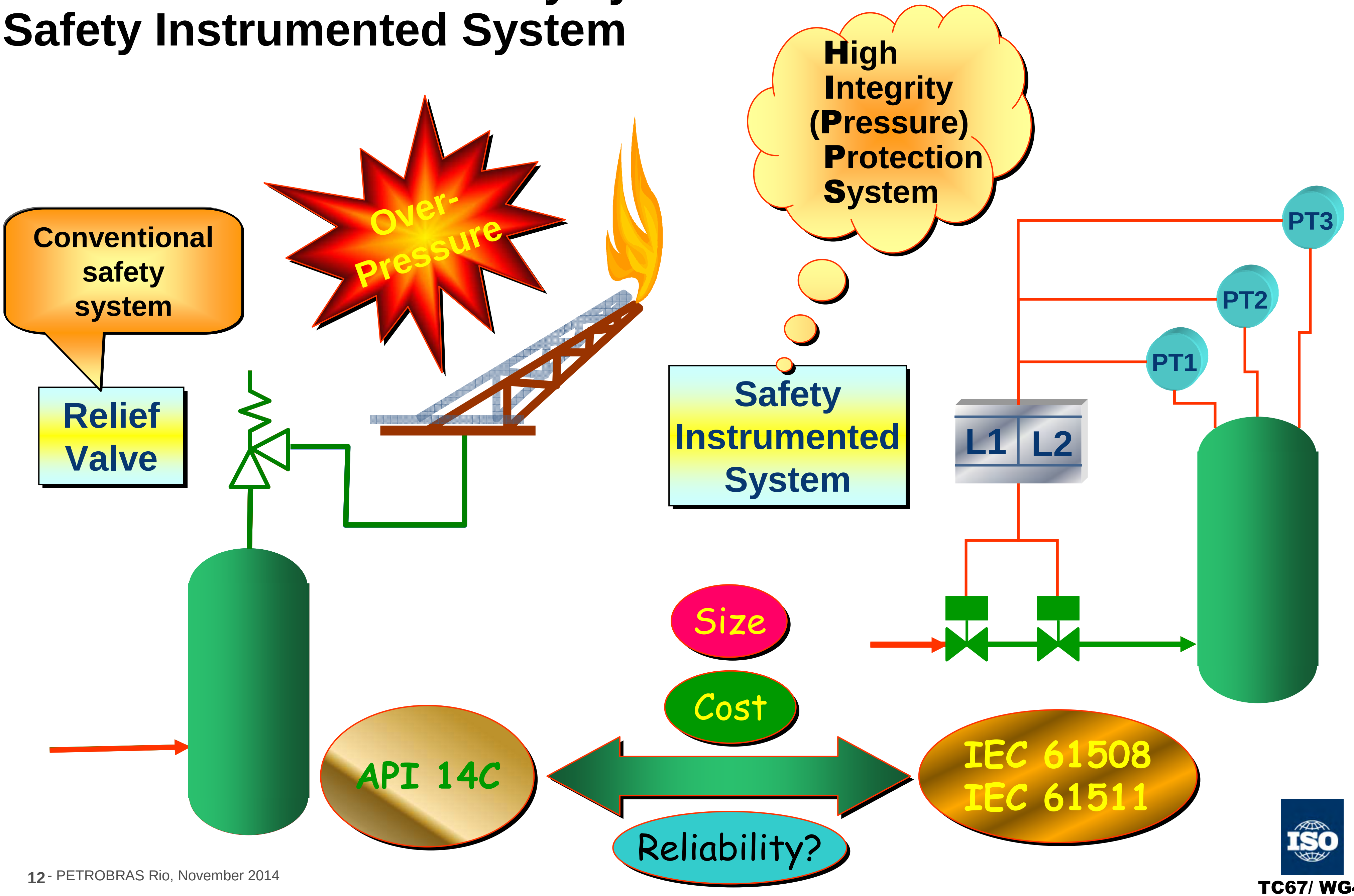
PETROBRAS Rio, November 2014

TC67
WG4

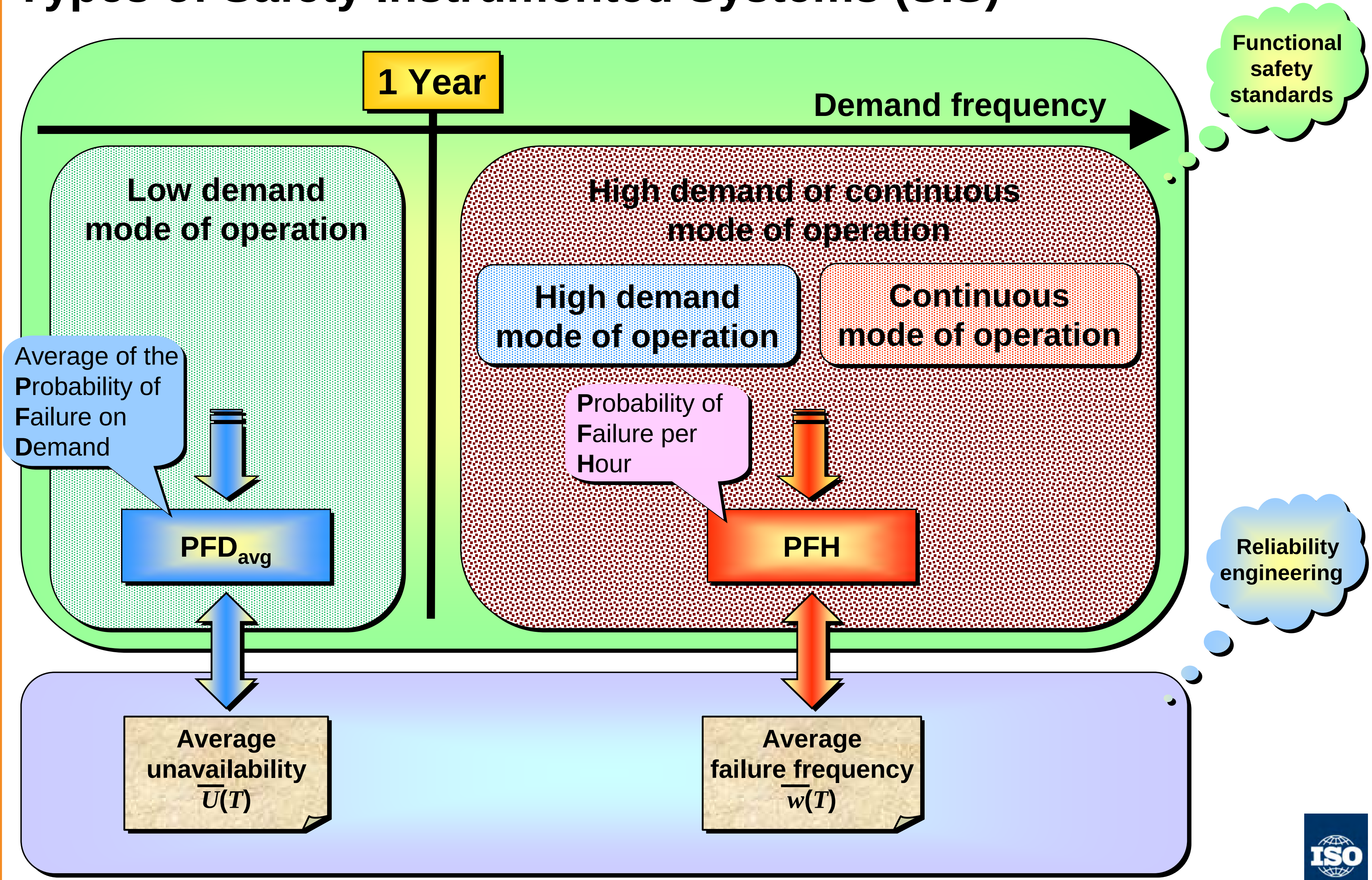
SIL Principle: identification of *Risk Reduction* needed



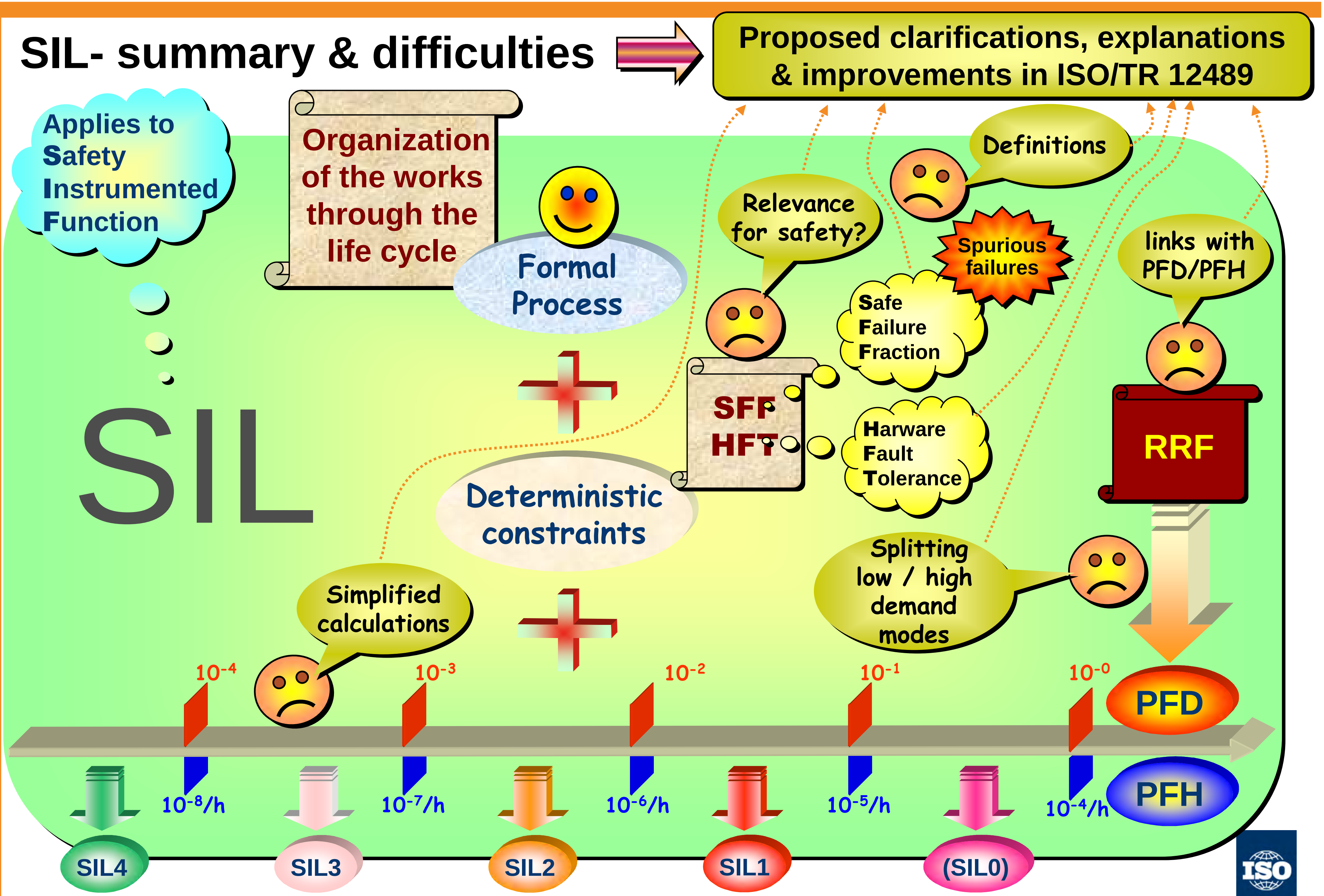
From conventional Safety system to Safety Instrumented System



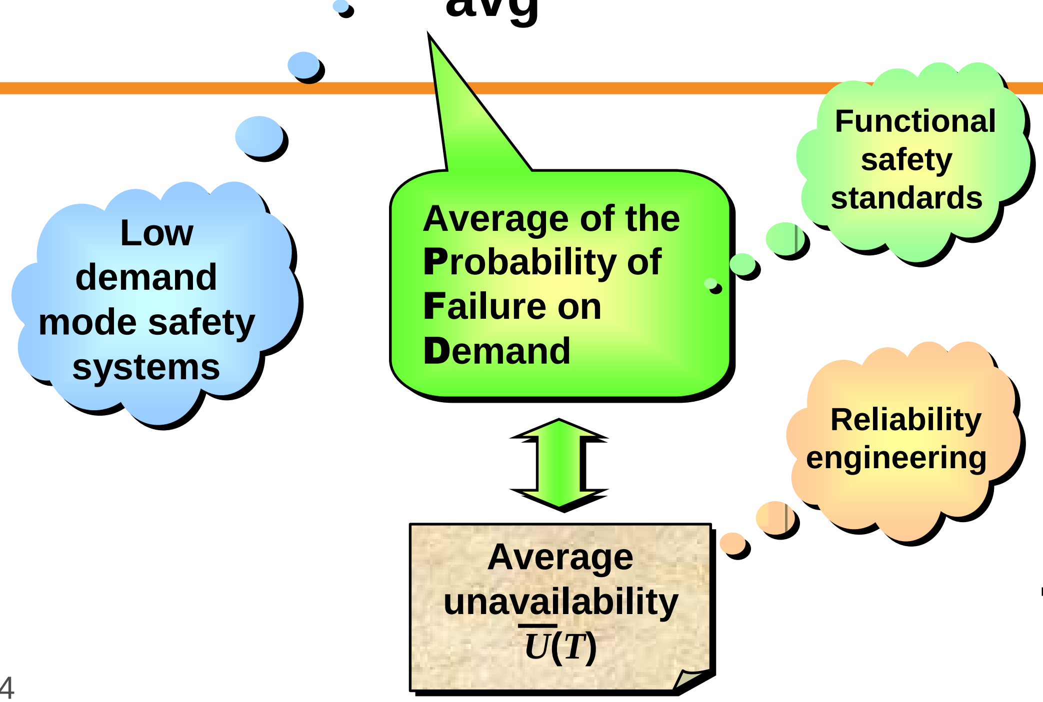
Types of Safety Instrumented Systems (SIS)



SIL- summary & difficulties



Introduction to the methods developed into ISO/TR 12489 for PFD_{avg} calculations

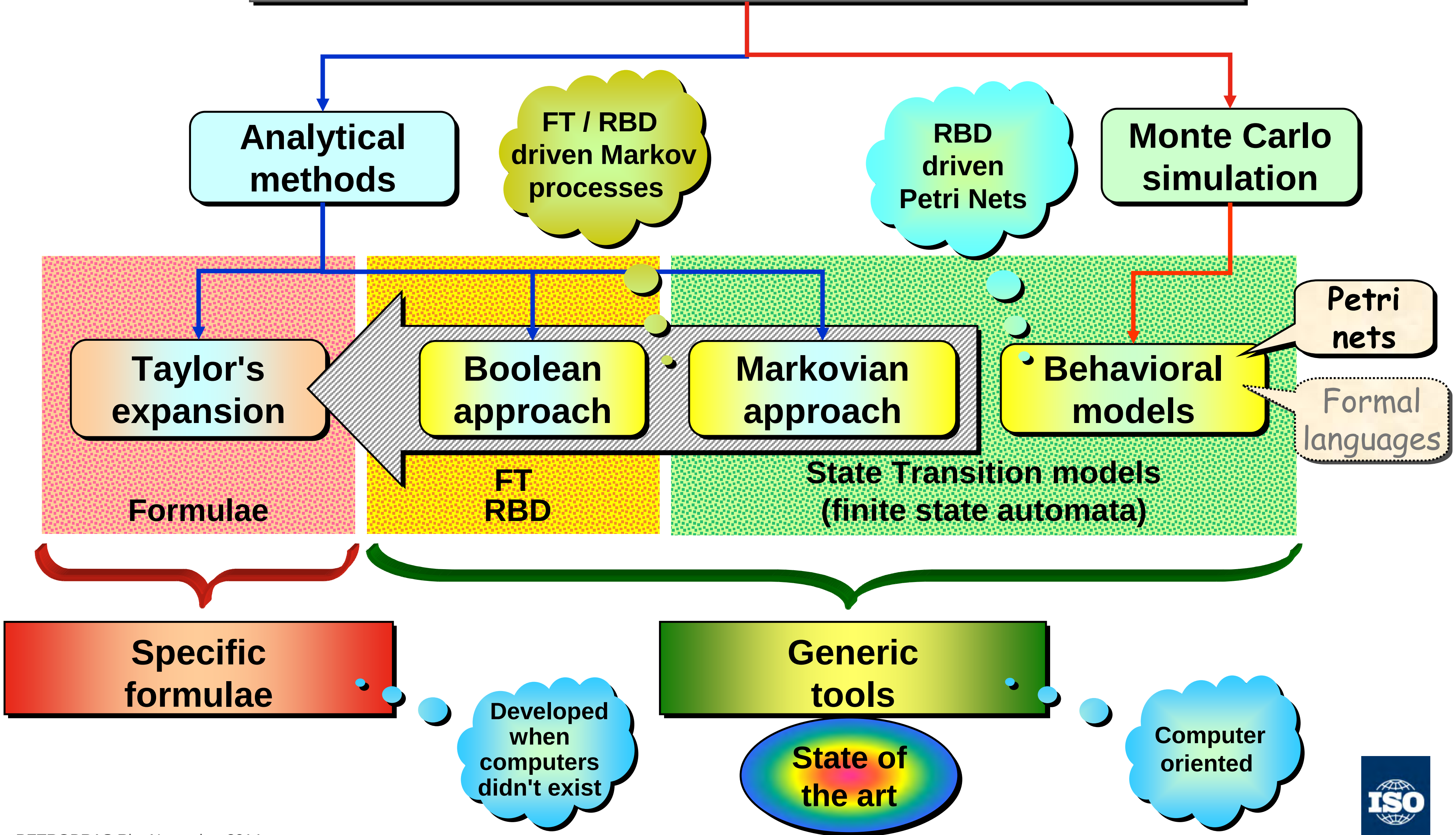


TC67 WG4

PETROBRAS Rio, November 2014

50 years of experience

Probabilistic models overview



Simplified analytical approach

TC67
WG4

PETROBRAS Rio, November 2014

Simplest approximation of the PFDavg

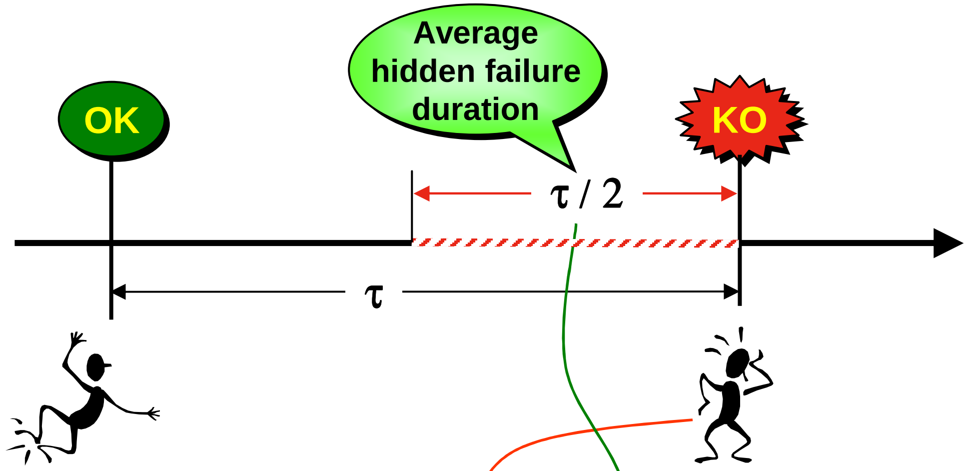
A

$$PFD_{avg} = \overline{U}(\tau) \approx \frac{1}{\tau}\int_0^{\tau} \lambda\delta . d\delta = \frac{1}{\tau}\frac{\lambda\tau^2}{2} = \frac{\lambda\tau}{2}$$

$\tau << 1/\lambda$

2 parameters:
- λ : Failure rate
- τ : test interval

$$U(\delta) = 1 - \exp(-\lambda\delta) \approx \lambda\delta$$



Not realistic!

$$\lim_{\tau \to 0} PFD_{avg} = 0$$

But

Unavailability duration

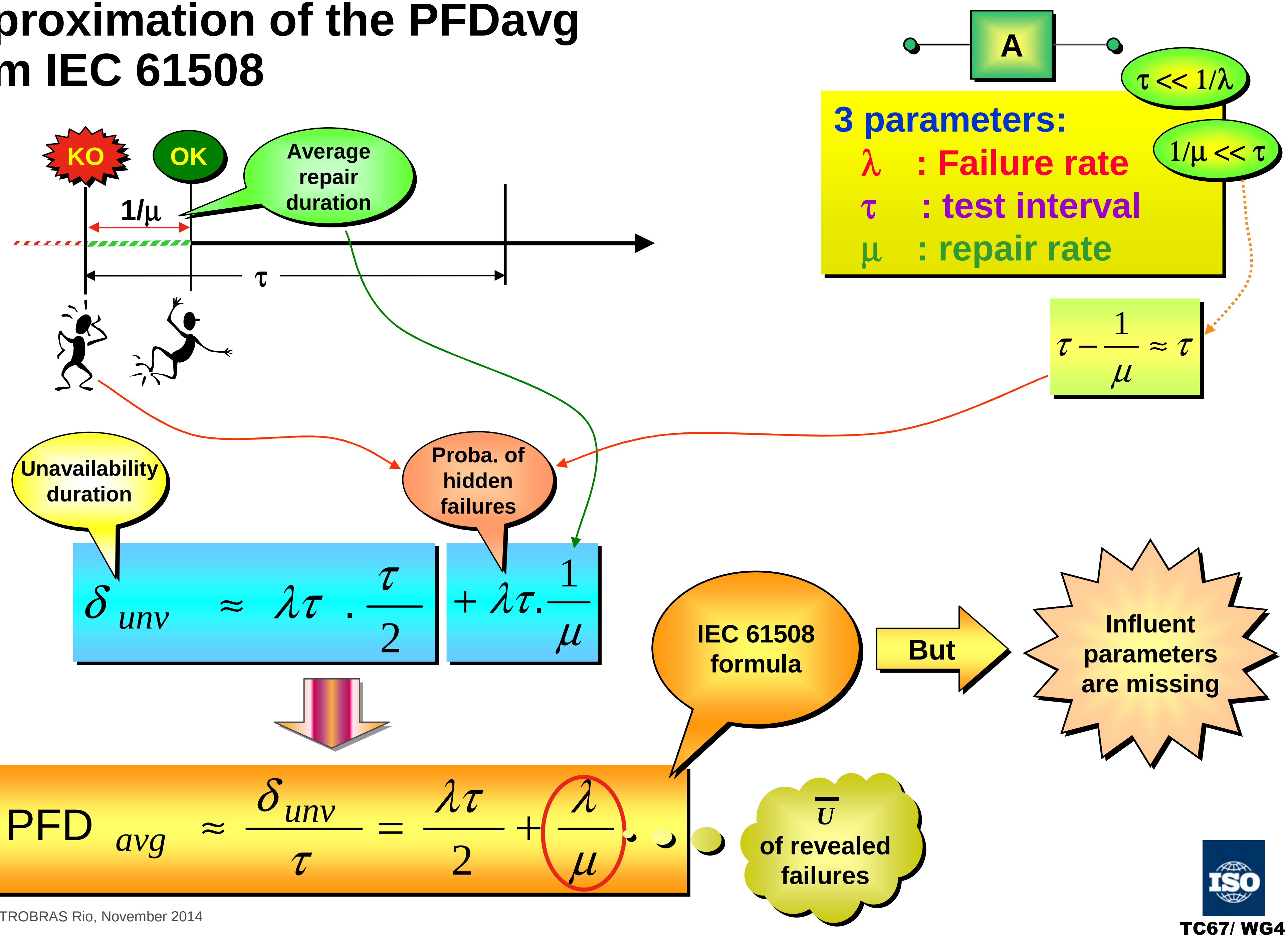
Proba. of hidden failures

$$\delta_{unv} \approx \lambda\tau . \frac{\tau}{2}$$

$$PFD_{avg} \approx \frac{\delta_{unv}}{\tau} = \frac{\lambda\tau}{2}$$

The most famous formula in functional safety

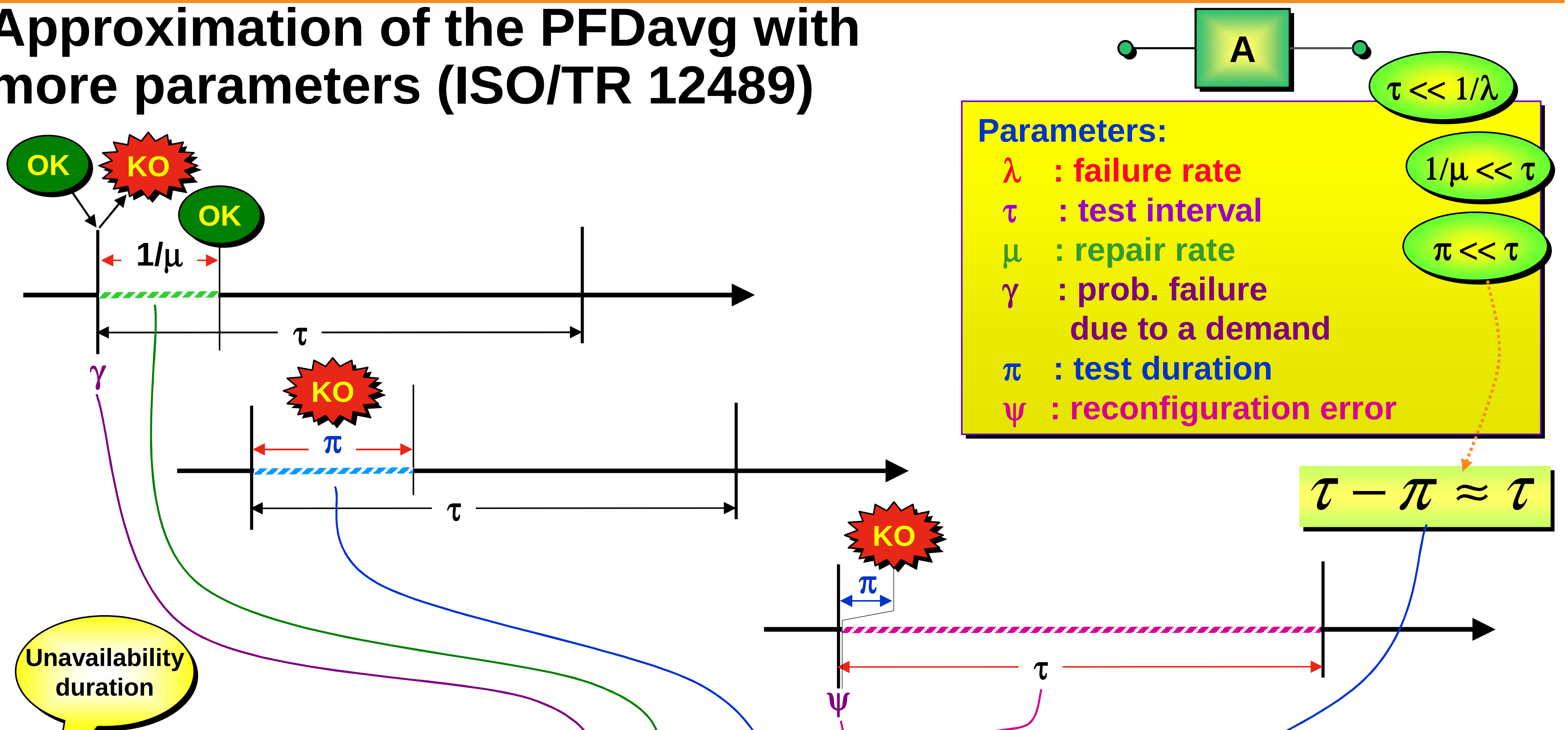
Approximation of the PFDavg from IEC 61508



Approximation of the PFDavg with more parameters (ISO/TR 12489)

Parameters:

- λ : failure rate
- τ : test interval
- μ : repair rate
- γ : prob. failure due to a demand
- π : test duration
- ψ : reconfiguration error



$$\tau - \pi \approx \tau$$

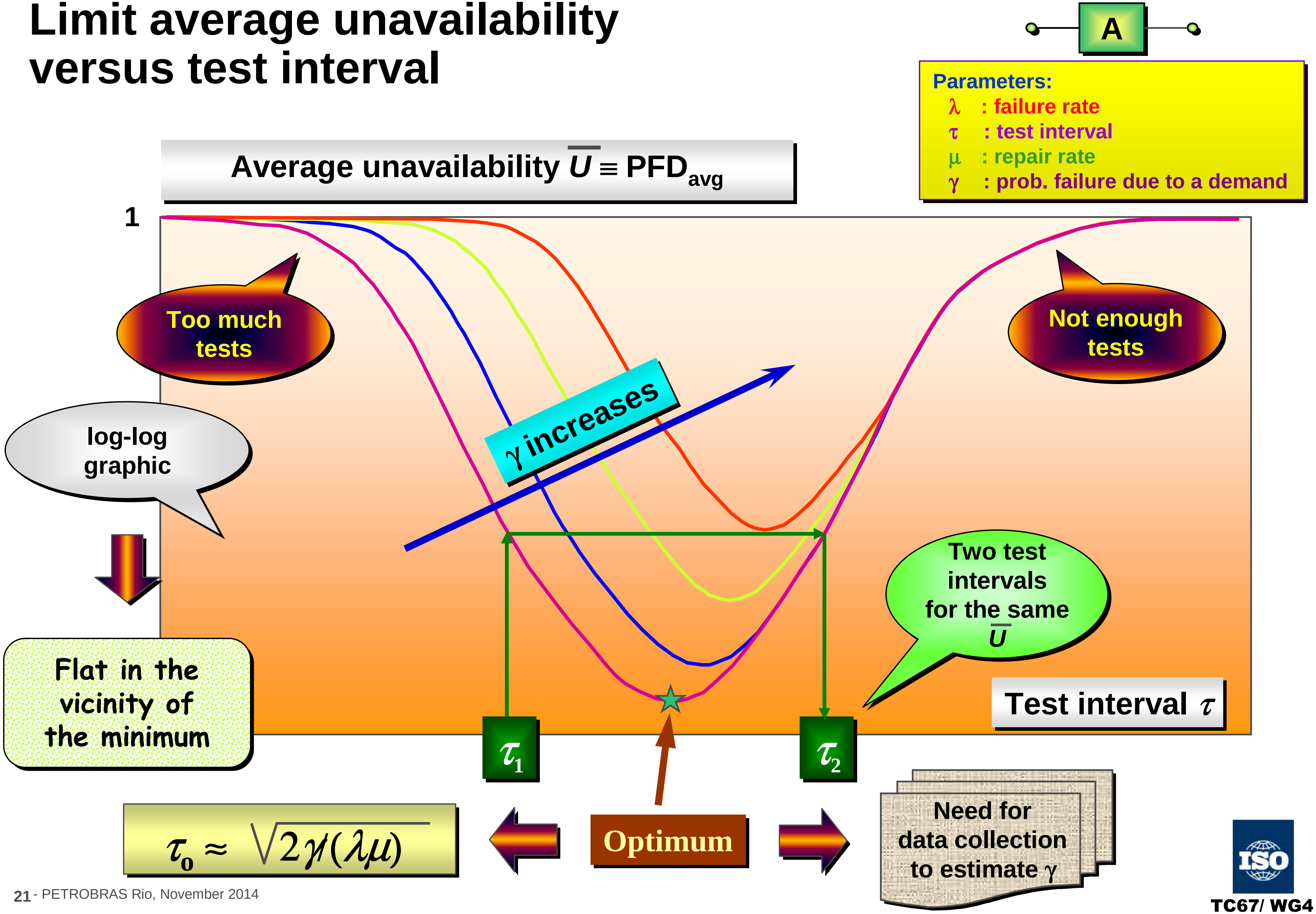
$$\delta_{unv} \approx \lambda\tau \,.\, \frac{\tau}{2} + \lambda\tau \frac{1}{\mu} + \gamma \,.\, \frac{1}{\mu} + \pi + \psi \,.\tau$$

$$PFD_{avg} \approx \frac{\delta_{unv}}{\tau} = \frac{\lambda\tau}{2} + \frac{\lambda}{\mu} + \frac{\gamma}{\mu.\tau} + \frac{\pi}{\tau} + \psi$$

etc.

Taylor expansion for more complex cases

Limit average unavailability versus test interval

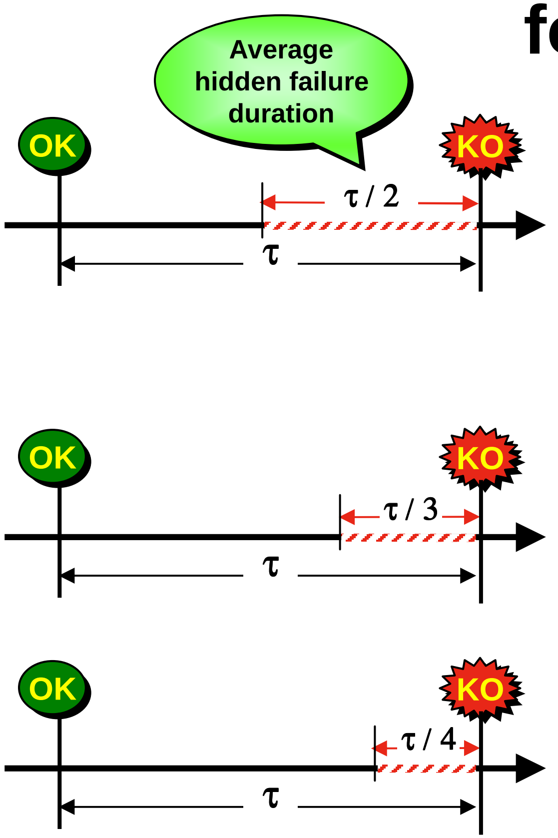


$$\tau_0 \approx \sqrt{2\gamma/(\lambda\mu)}$$

Simplest approximation of the PFDavg for redundant systems

2 parameters:
- λ : Failure rate
- τ : test interval

$\tau << 1/\lambda$

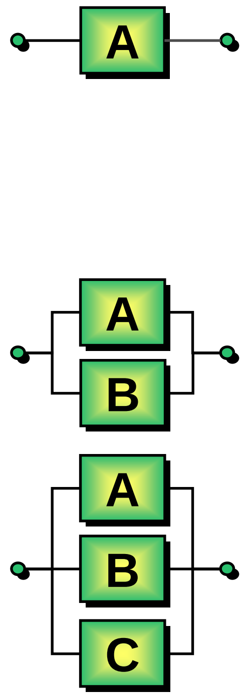


$$PFD_{avg} = \overline{U}_A(\tau) \approx \frac{1}{\tau}\int_0^{\tau}\lambda.\delta.d\delta = \frac{1}{\tau}\frac{\lambda\tau^2}{2} = \frac{\lambda\tau}{2}$$

Taylor expansion $\lambda\delta << 1$

$$PFD_{avg} = \overline{U}_{AB}(\tau) \approx \frac{1}{\tau}\int_0^{\tau}(\lambda.\delta)^2 d\delta = \frac{1}{\tau}\frac{\lambda^2\tau^3}{3} = \frac{(\lambda\tau)^2}{3}$$

$$PFD_{avg} = \overline{U}_{ABC}(\tau) \approx \frac{1}{\tau}\int_0^{\tau}(\lambda.\delta)^3 d\delta = \frac{1}{\tau}\frac{\lambda^3\tau^4}{4} = \frac{(\lambda\tau)^3}{4}$$



Effect of systemic dependencies

$$\overline{U}_{AB}(\tau) \neq \overline{U}_A(\tau).\overline{U}_B(\tau), \quad \overline{U}_{ABC}(\tau) \neq \overline{U}_A(\tau).\overline{U}_B(\tau).\overline{U}_C(\tau)$$

Not possible to combine formulae!

Even for simplest systems, each case implies specific Taylor expansion development

Catalog of ad hoc formulae

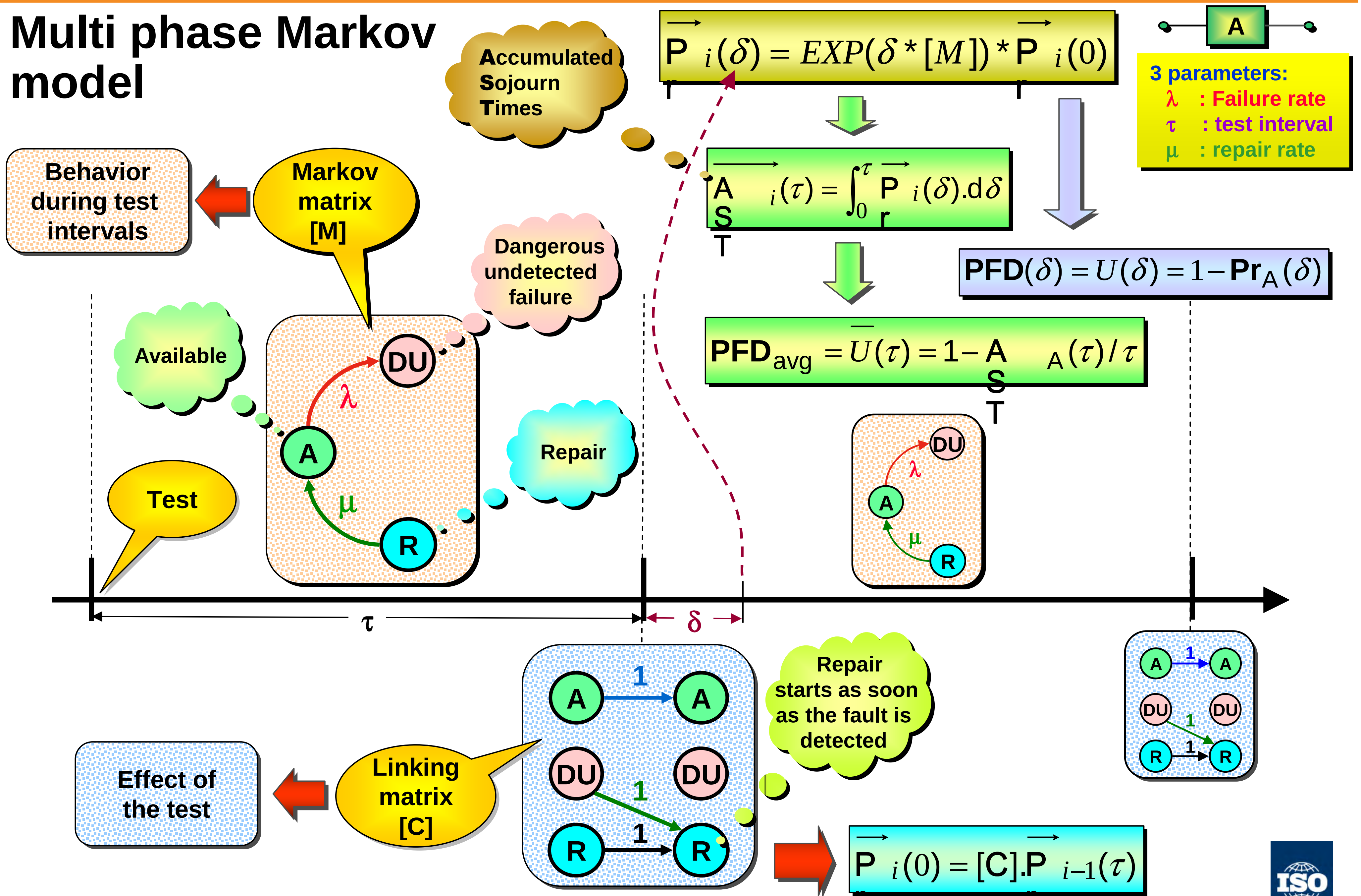
Not in line with reliability analysis philosophy

Multi-phase Markovian approach

PETROBRAS Rio, November 2014

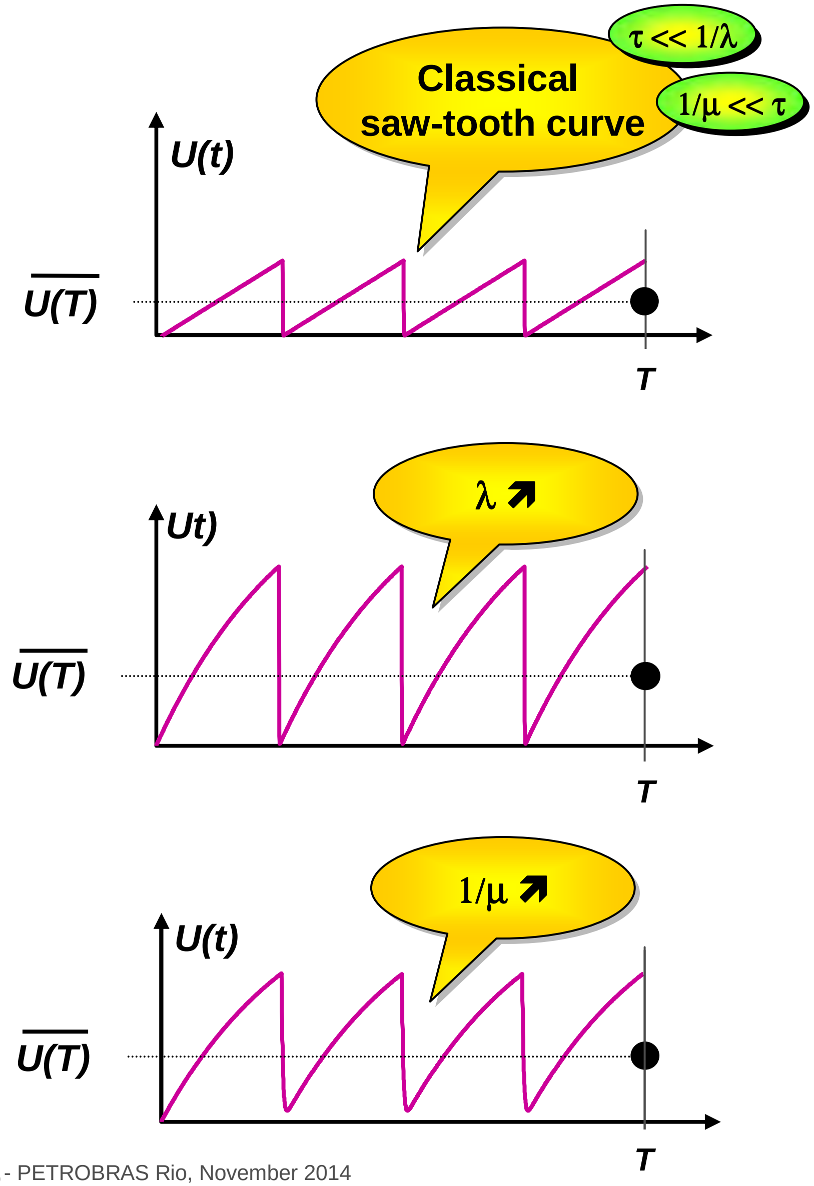
TC67
WG4

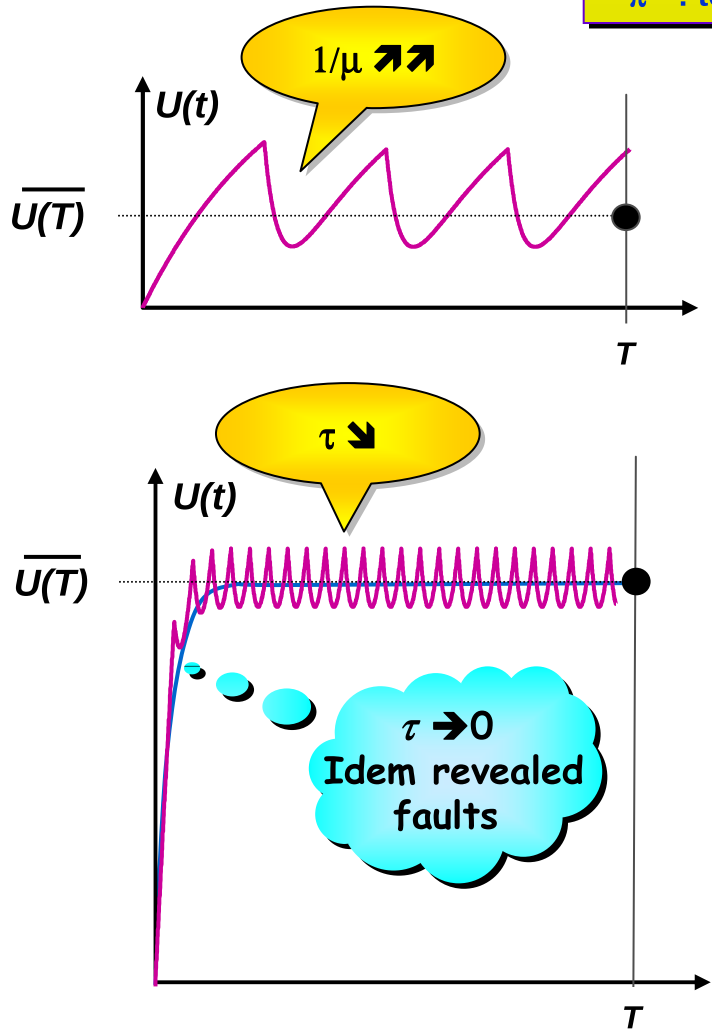
Multi phase Markov model



Typical saw-tooth curves for a single periodically tested component

Parameters:
- λ : failure rate
- τ : test interval
- μ : repair rate
- γ : prob. failure due to a demand
- π : test duration

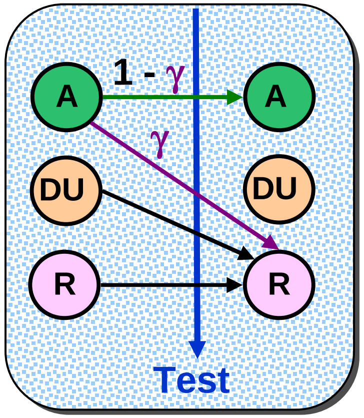


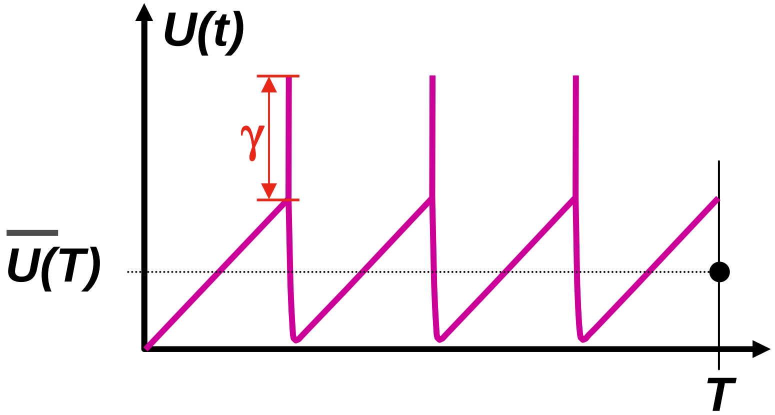


TC67/ WG4

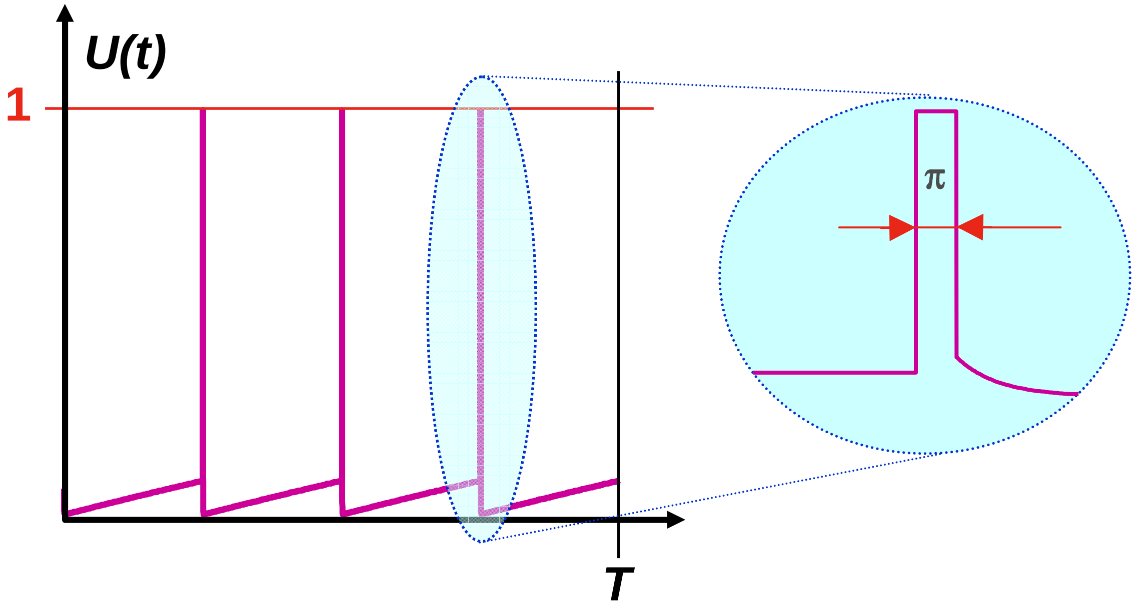
Modeling the probability of failure due to the demand itself and the test duration

Failure due to tests (γ)





Test duration

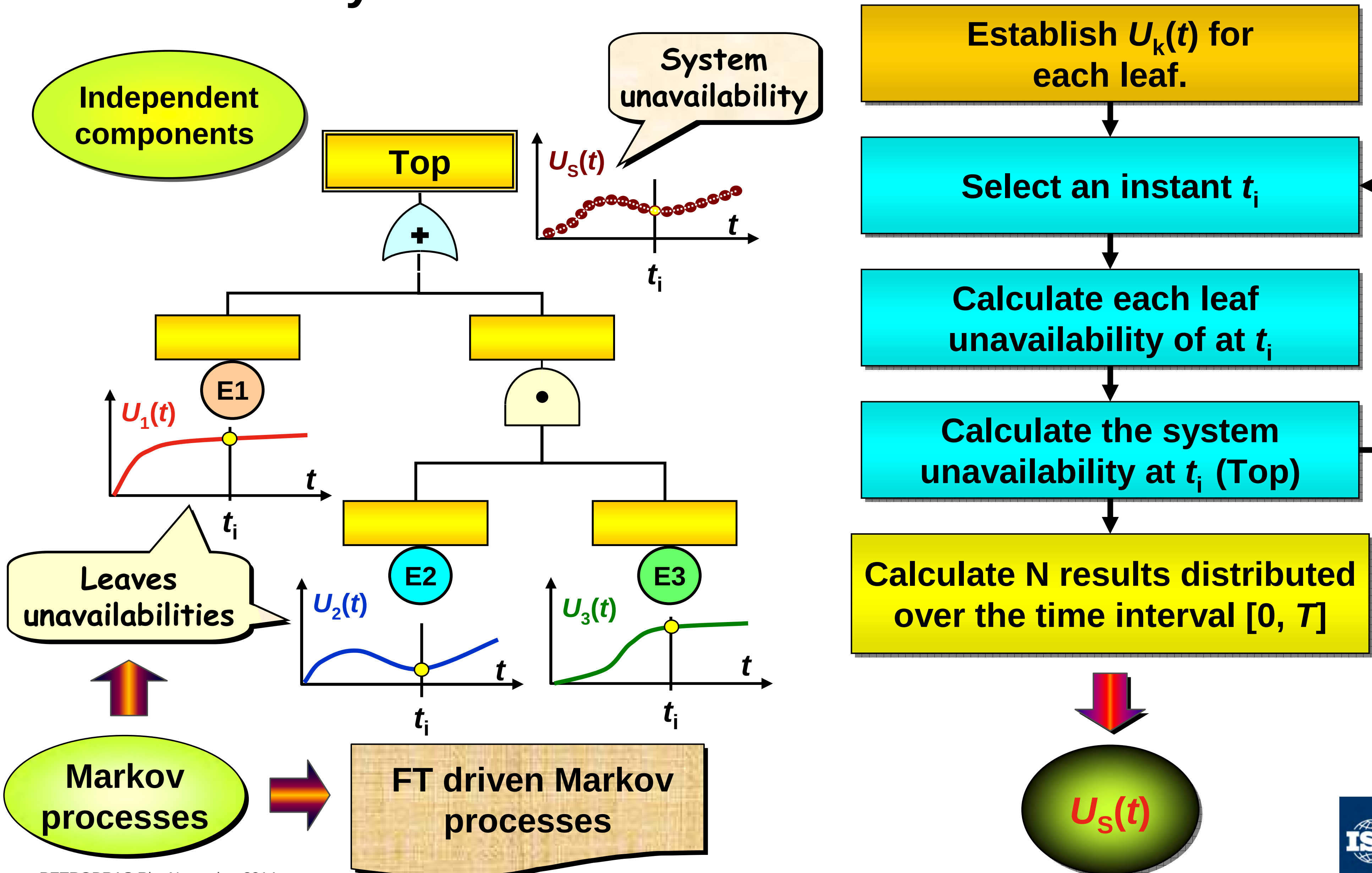


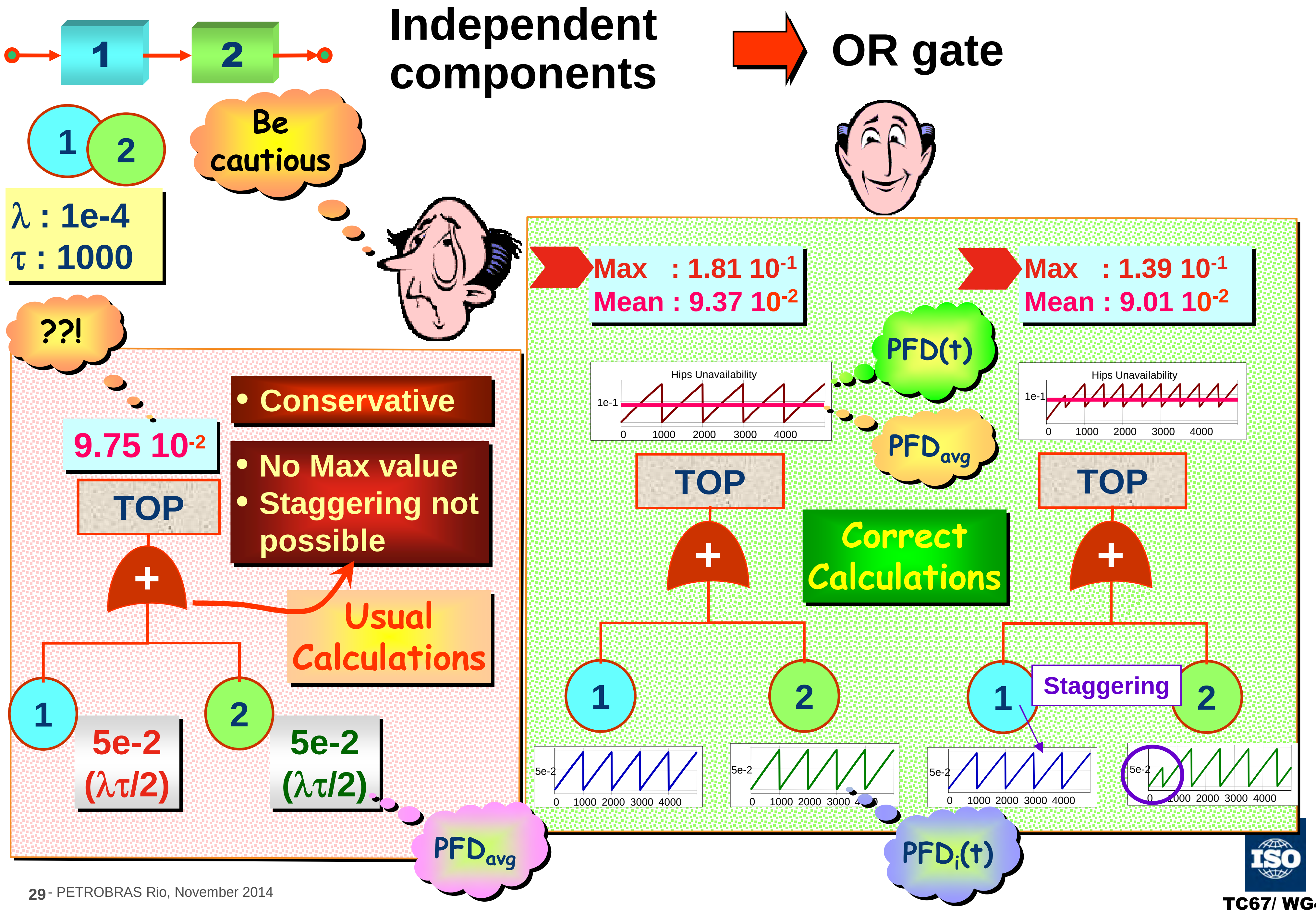
Fault tree approach

TC67
WG4

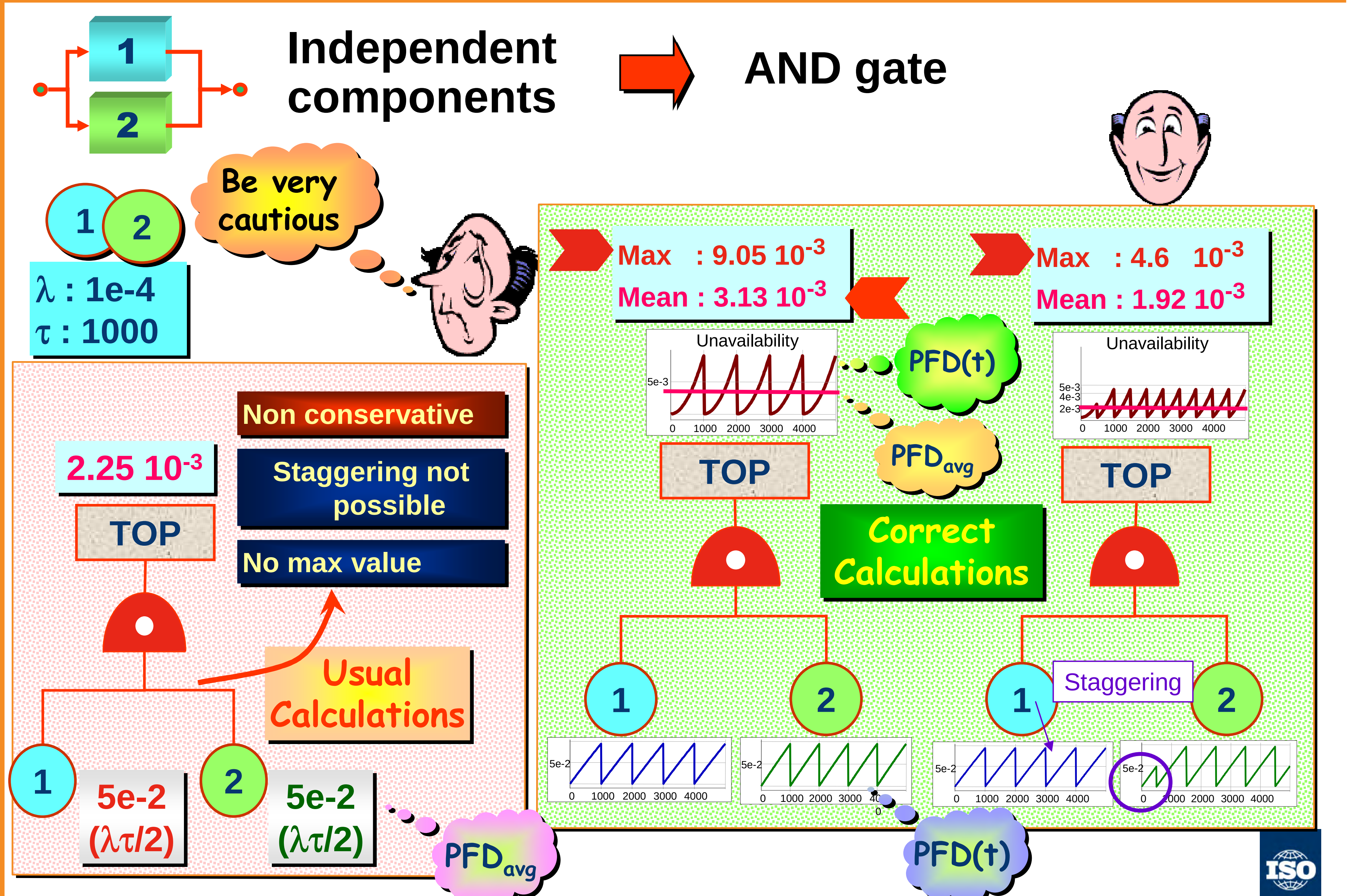
PETROBRAS Rio, November 2014

Fault tree driven Markov processes: principle for unavailability calculation.



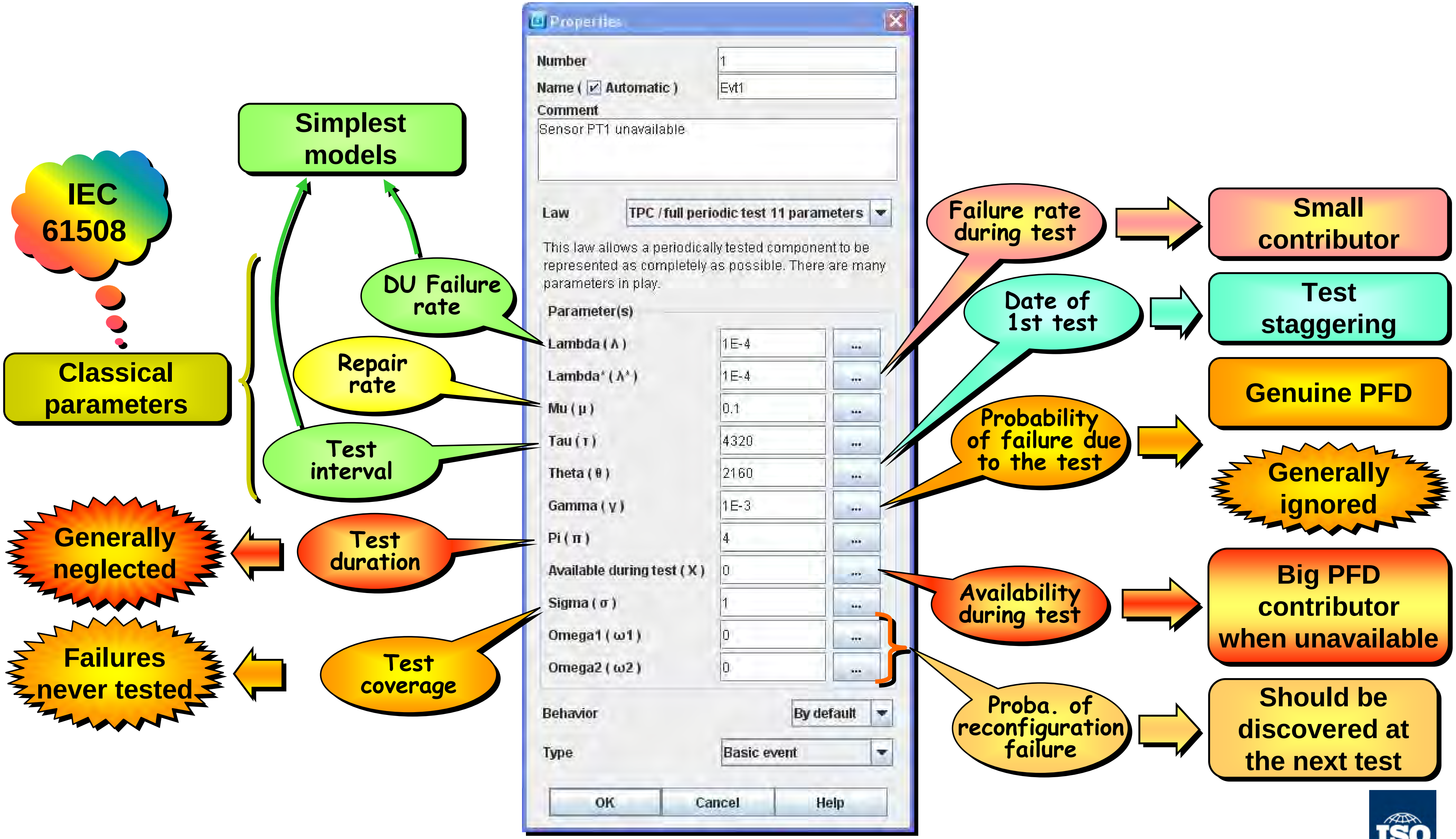


1
2
Independent components
OR gate
1
2
Be cautious
λ : 1e-4
τ : 1000
??!
9.75 10-2
TOP
+
• Conservative
• No Max value
• Staggering not possible
Usual Calculations
1
5e-2 (λτ/2)
2
5e-2 (λτ/2)
PFDavg
Max : 1.81 10-1
Mean : 9.37 10-2
Max : 1.39 10-1
Mean : 9.01 10-2
PFD(t)
PFDavg
Hips Unavailability
1e-1
0 1000 2000 3000 4000
TOP
+
Correct Calculations
1
2
Staggering
5e-2
PFDi(t)



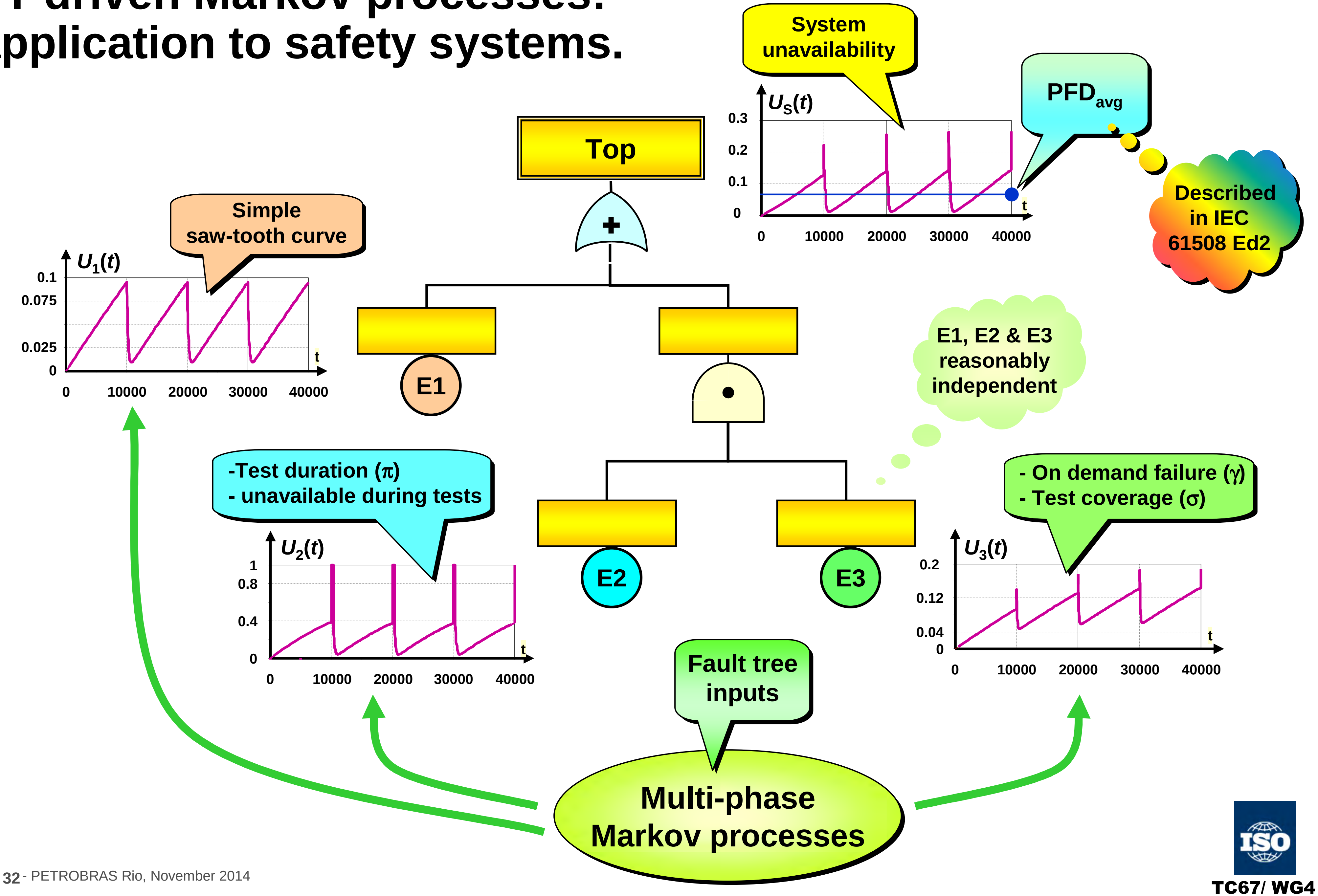
1
2
Independent components
AND gate
Be very cautious
λ : 1e-4
τ : 1000
Non conservative
Staggering not possible
No max value
2.25 10-3
TOP
Usual Calculations
1
5e-2 (λτ/2)
2
5e-2 (λτ/2)
PFDavg
Max : 9.05 10-3
Mean : 3.13 10-3
Unavailability
5e-3
0 1000 2000 3000 4000
PFD(t)
PFDavg
TOP
Correct Calculations
1
2
Max : 4.6 10-3
Mean : 1.92 10-3
Unavailability
5e-3
4e-3
2e-3
TOP
Staggering
PFD(t)

Parameters of a periodically tested component (dangerous undetected failures)



ISO TC67/ WG4

FT driven Markov processes: application to safety systems.



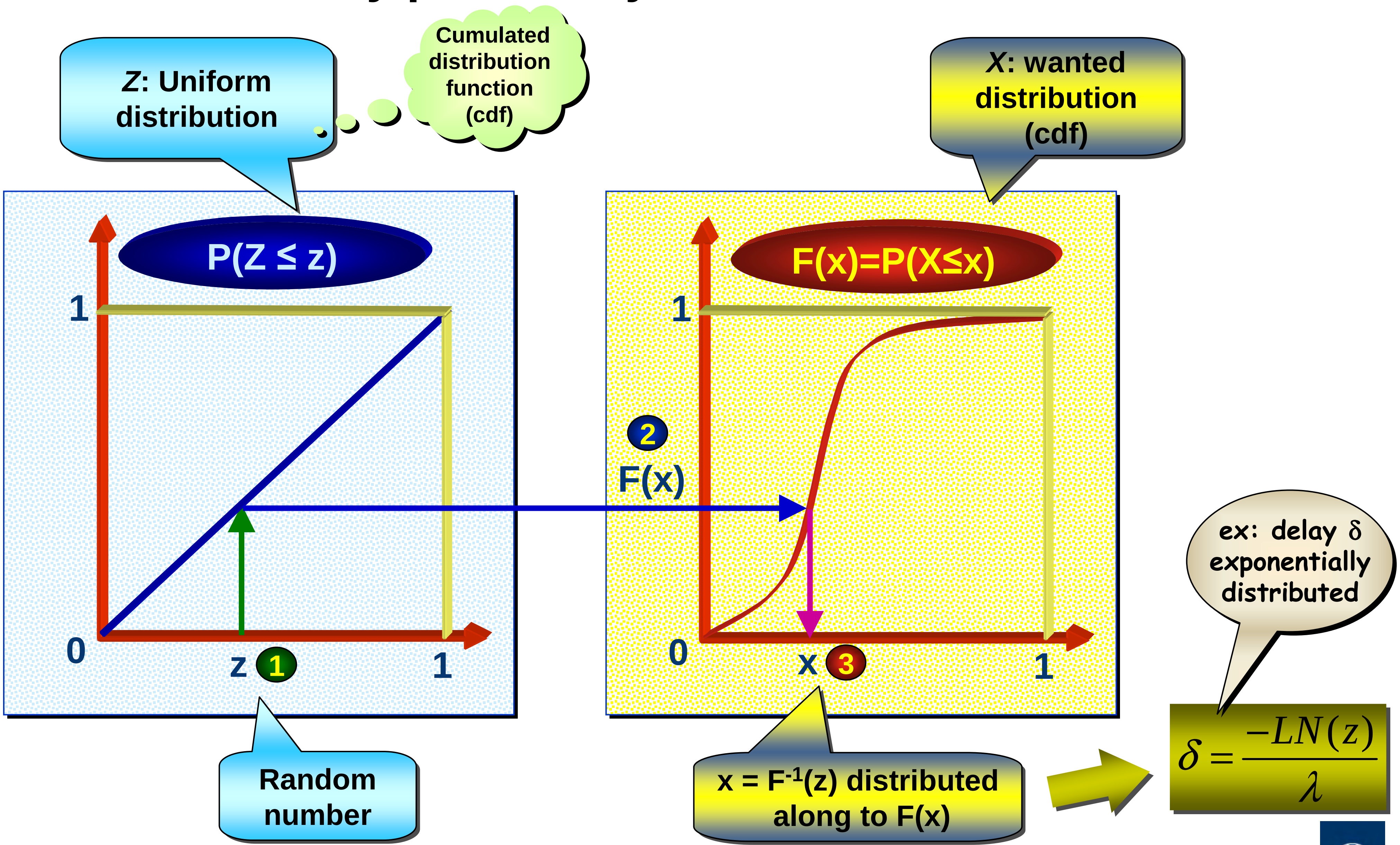
RBD driven Petri net and Monte Carlo simulation approaches

TC67
WG4

ISO

PETROBRAS Rio, November 2014

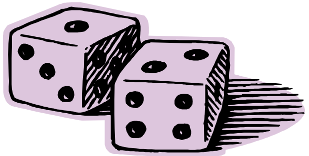
Simulation of any probability law



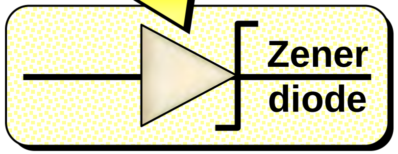
$$\delta = \frac{-LN(z)}{\lambda}$$

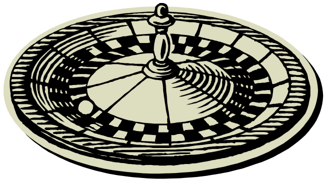
Random number generators

Physical methods



Thermal noise





Several billons are known

Decimals of π

3,14159265358979323846264338327950288419716939937510
58209749445923078164062862089986280348253421170679
82148086513282306647093844609550582231725359408128 ...

Widely used

J. Von Neumann

Pseudo random number generators

Linear congruential generators

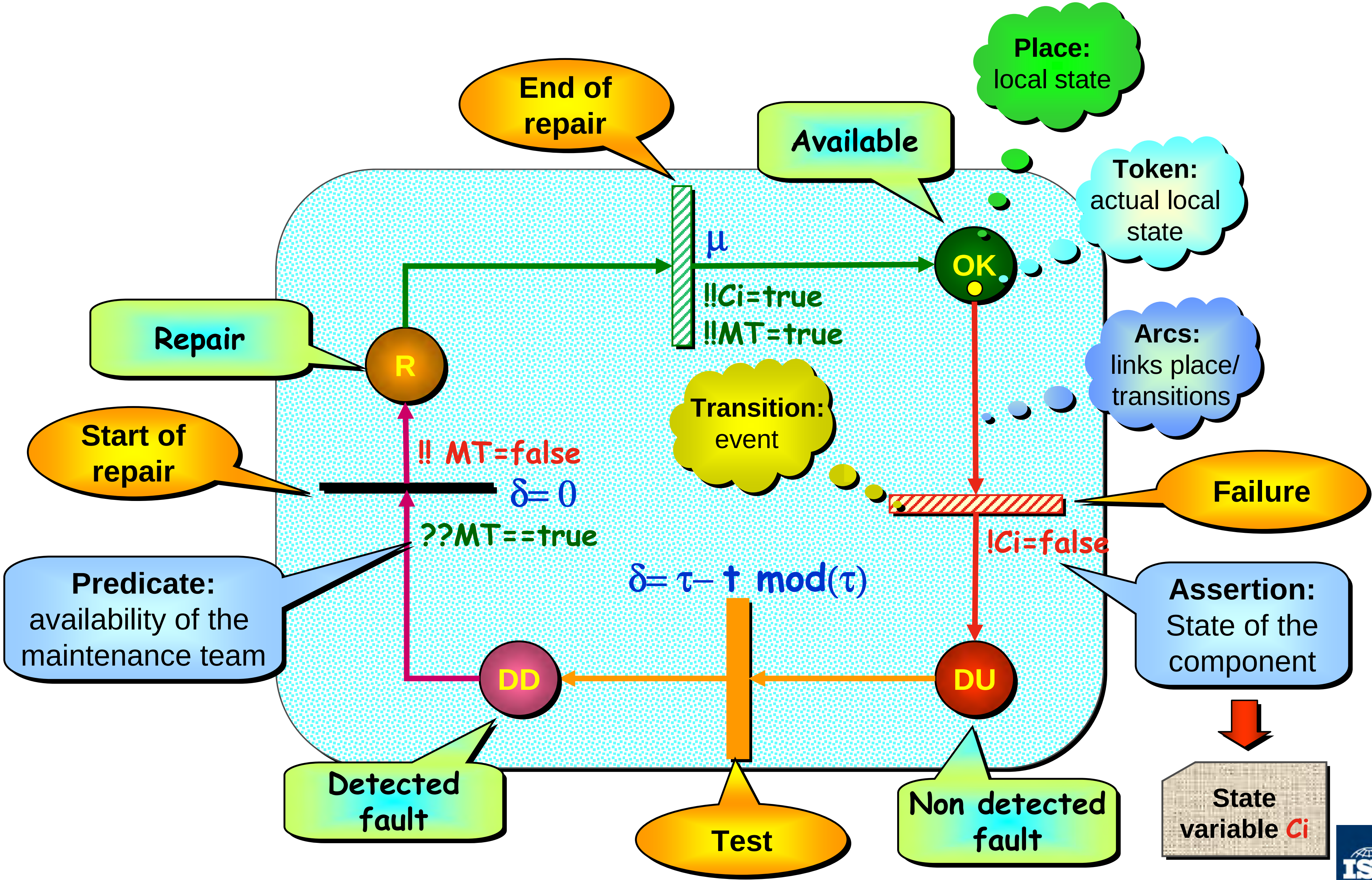
$$X_{n+1} = (a.X_n + b) \bmod m$$

Trajectory of the boule

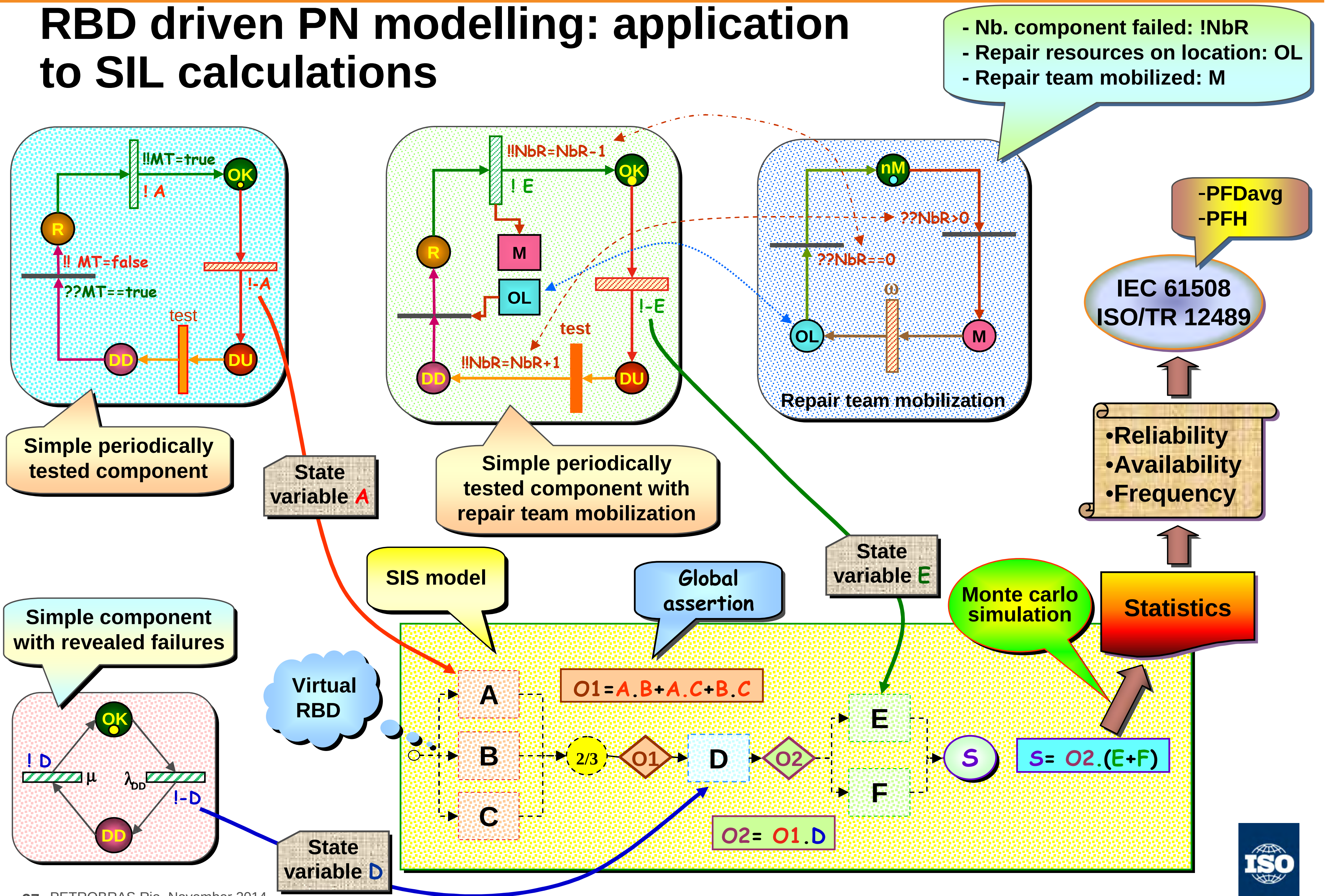
Length of one revolution

Computer

Periodically tested component



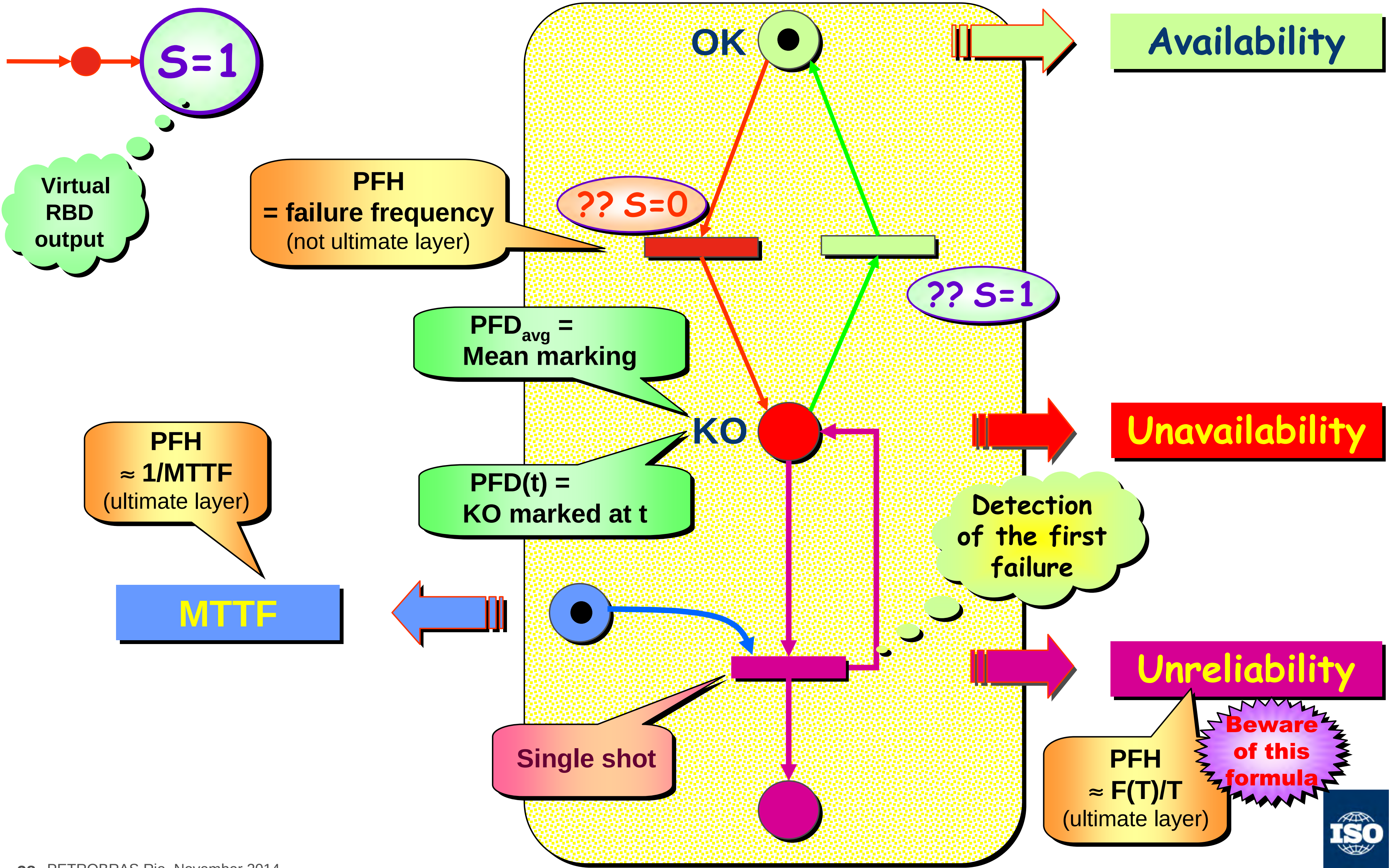
RBD driven PN modelling: application to SIL calculations



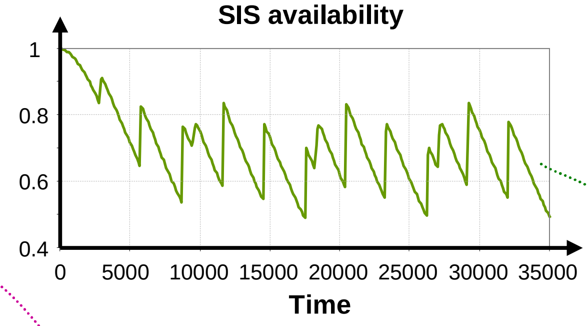
ISO

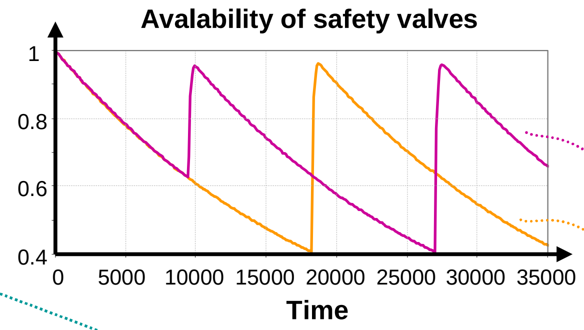
TC67/ WG4

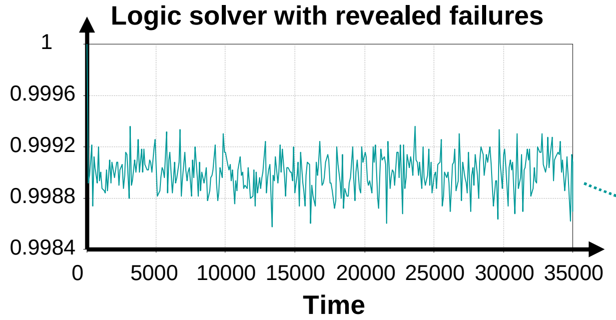
Parameter calculations: The *magic* sub PN!

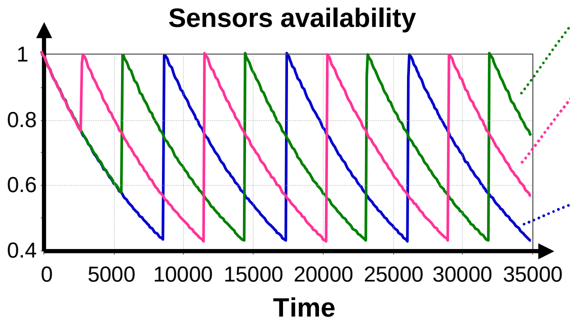


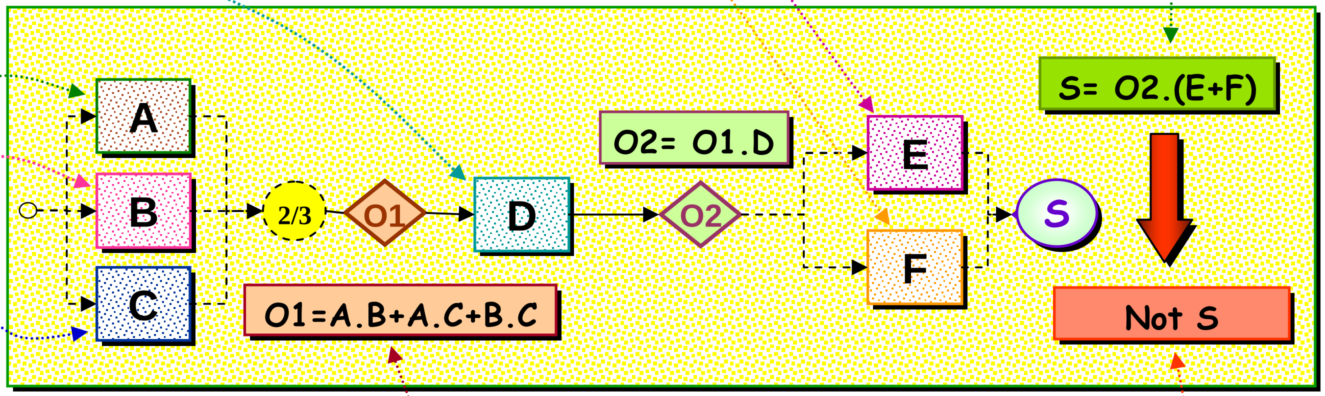
Example of Monte Carlo output (50 000 histories)

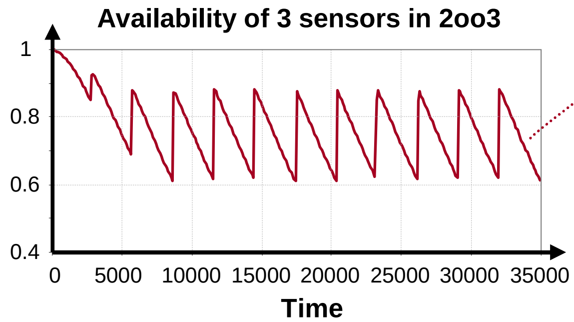


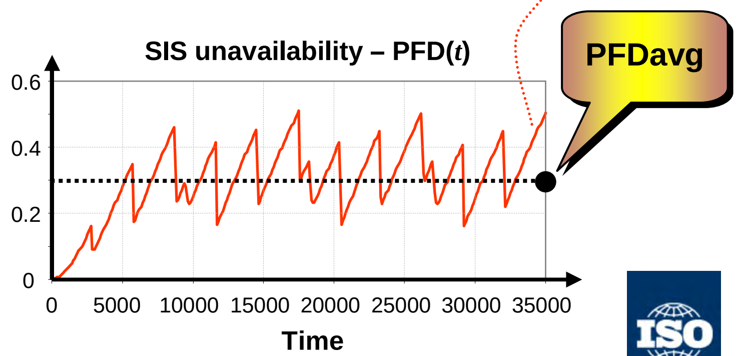






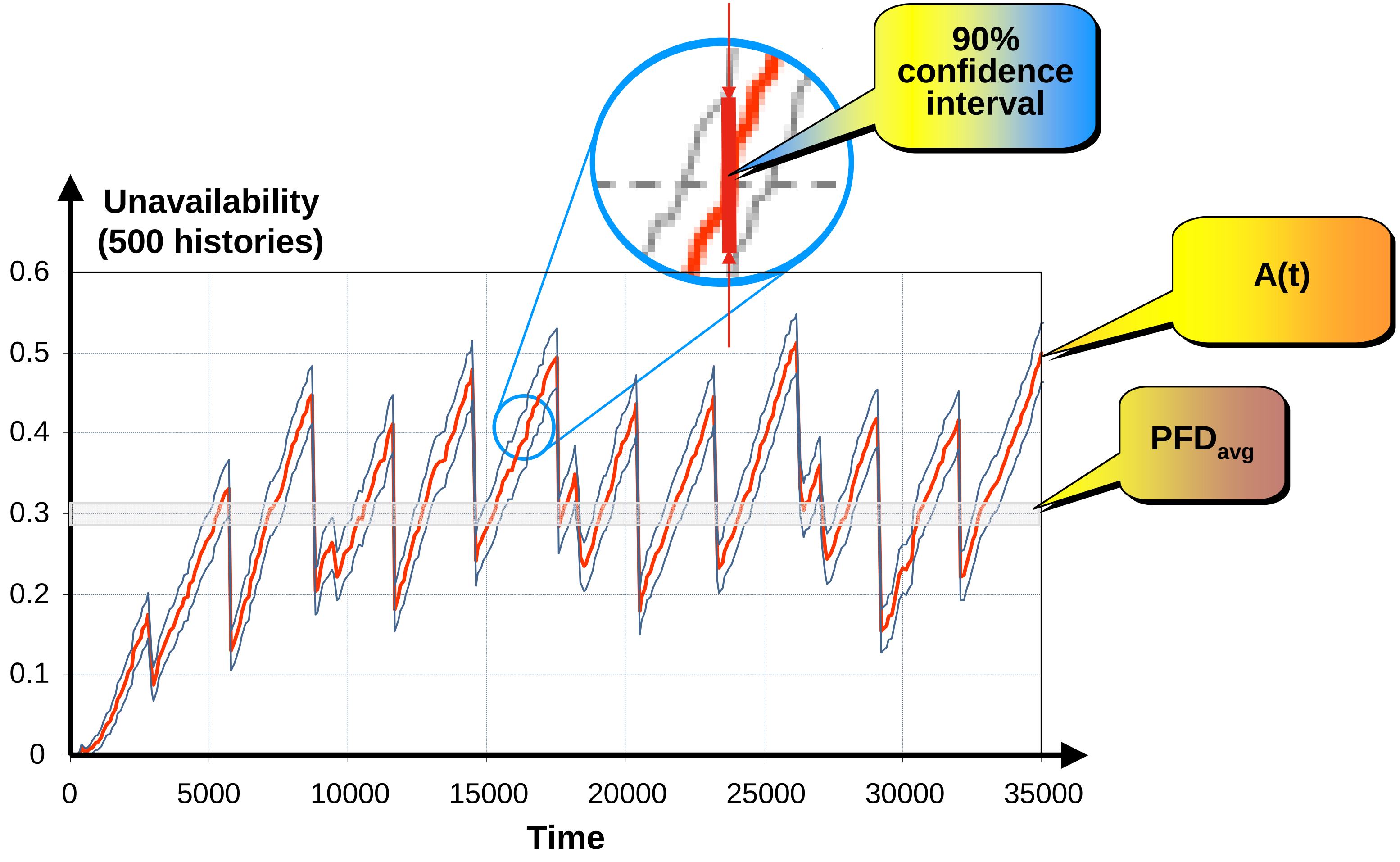




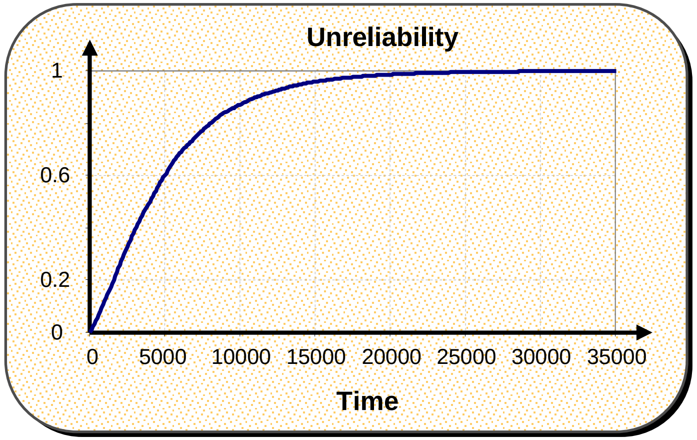


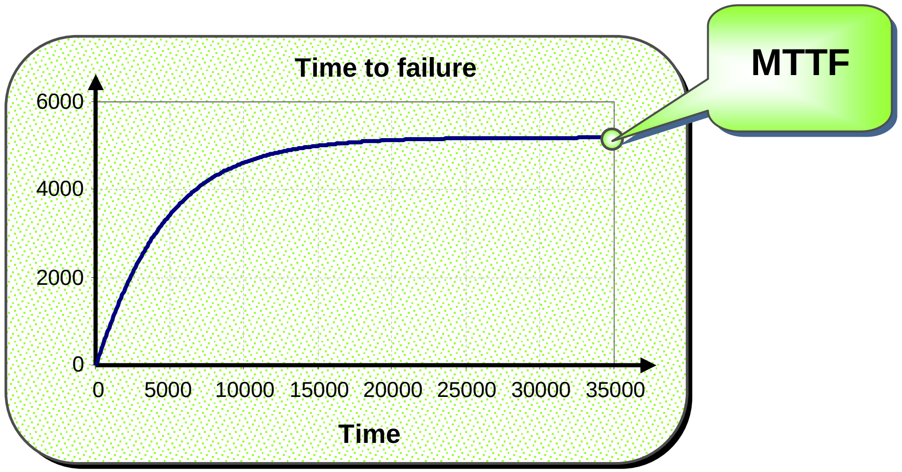
TC67/ WG4

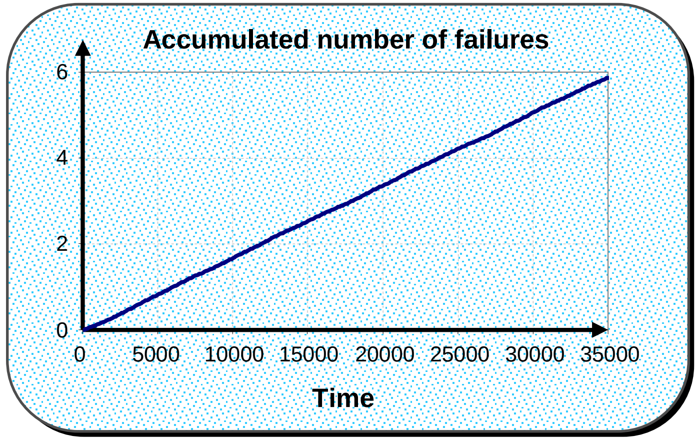
Monte Carlo simulation uncertainties

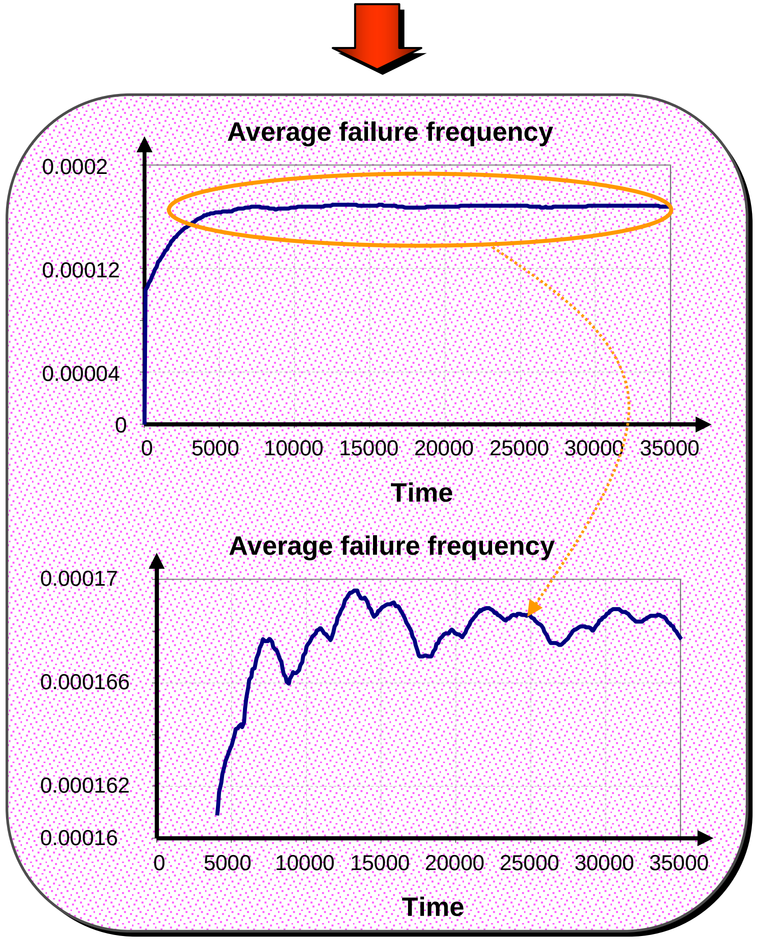


Other possible outputs







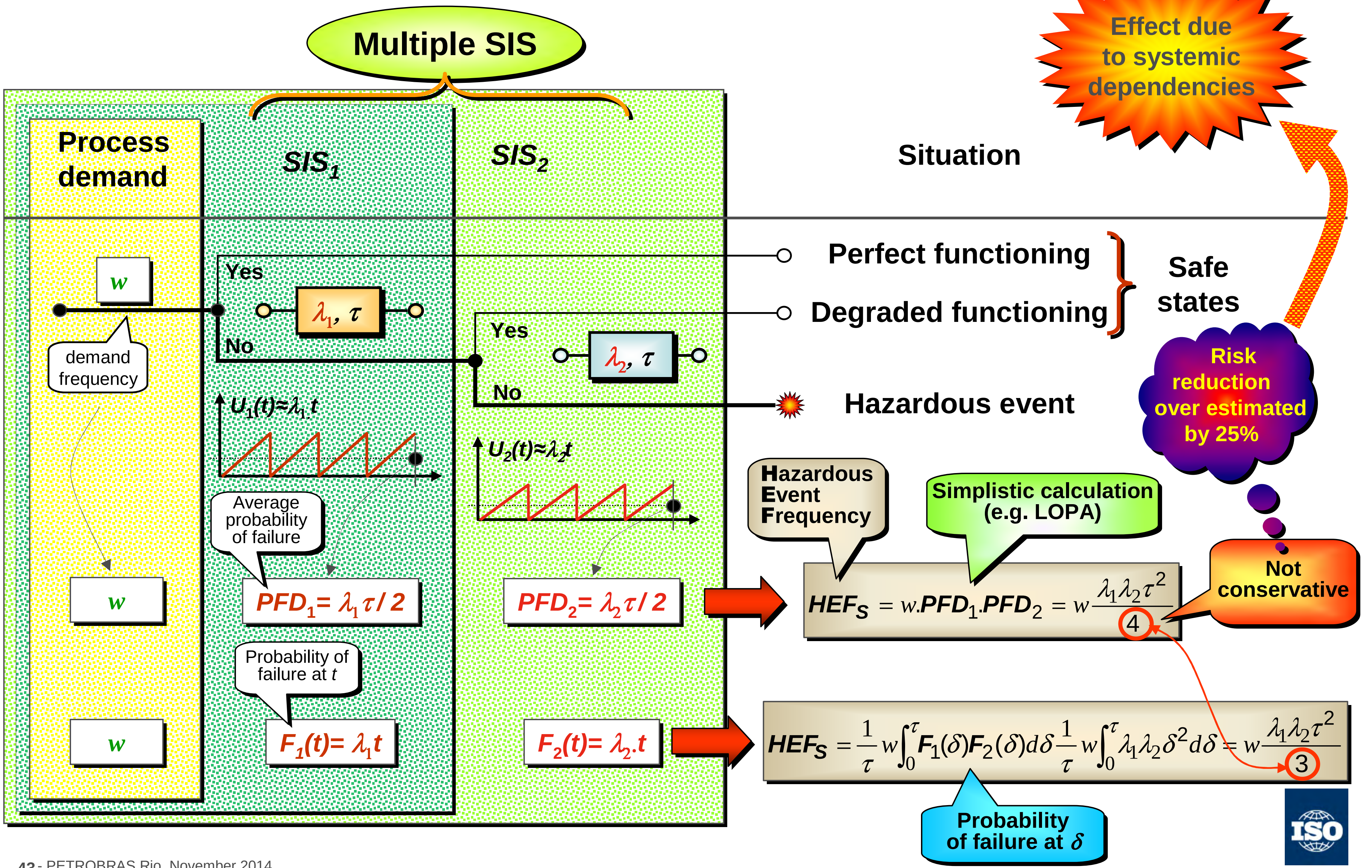


Multiple safety systems

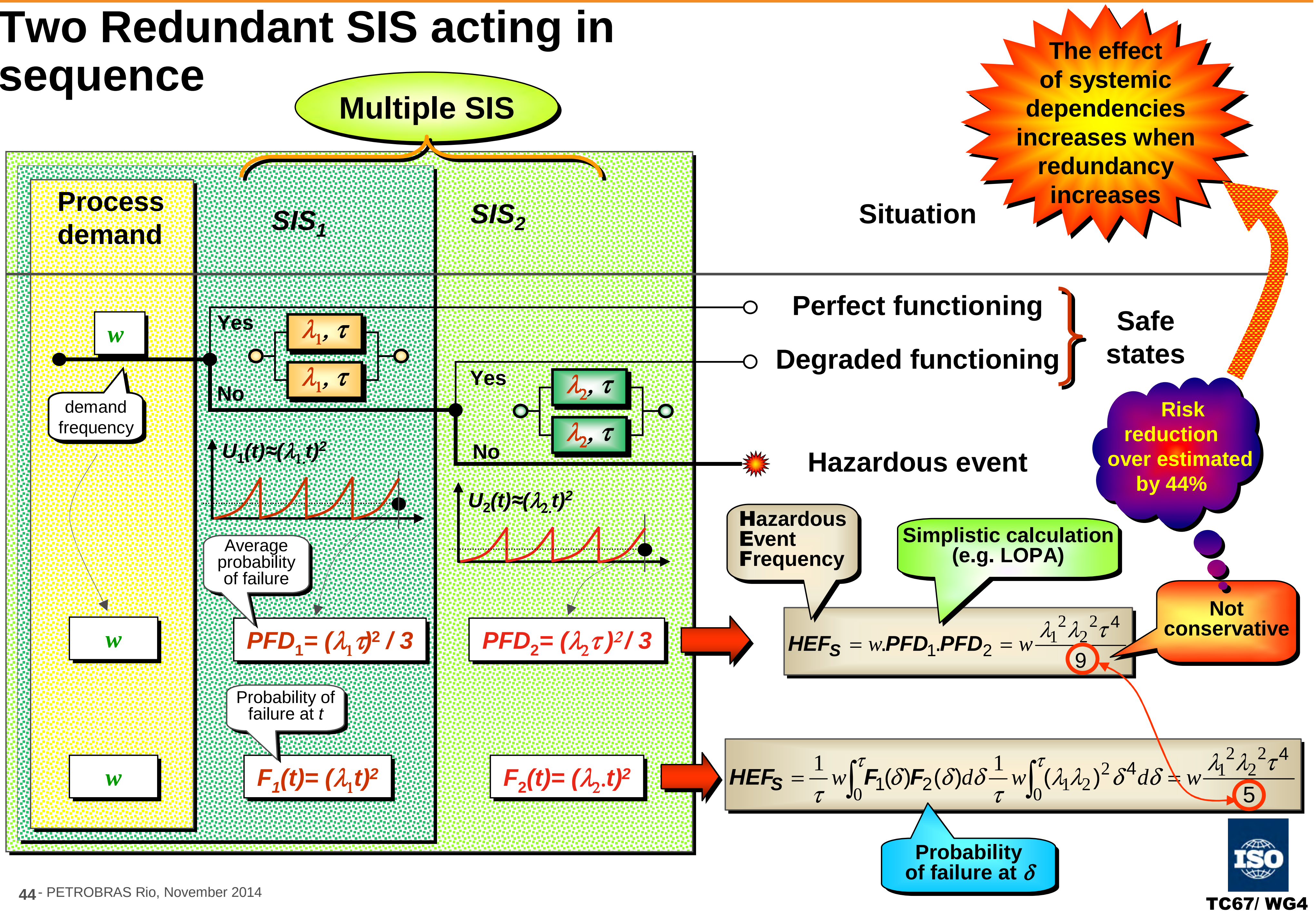
TC67
WG4

PETROBRAS Rio, November 2014

Two simple SIS acting in sequence

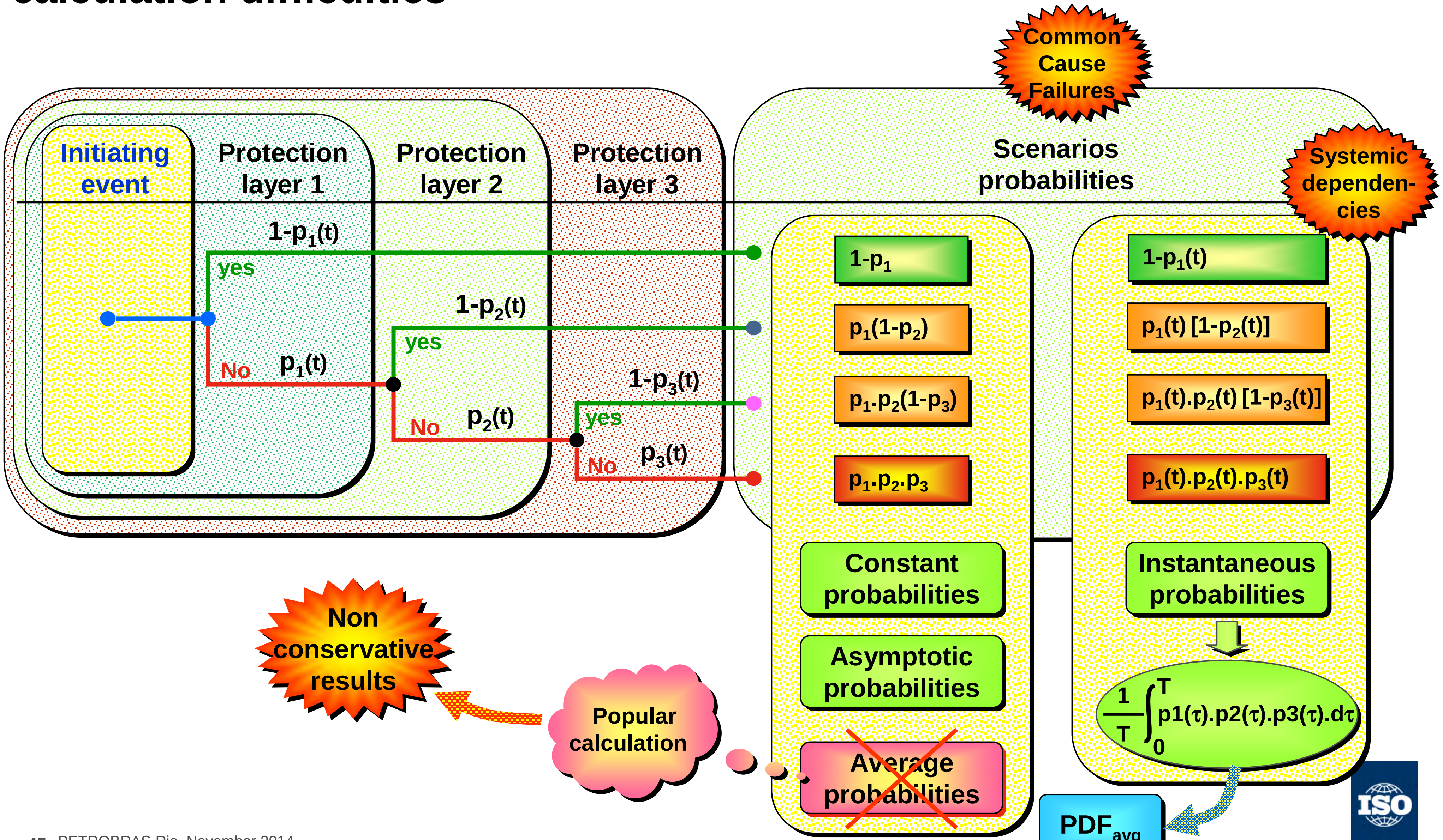


Two Redundant SIS acting in sequence



Event tree (multiple SIS) or fault tree (redundant SIS) calculation difficulties

Explained in IEC 61511 and ISO/TR 12489



TC67/ WG4

Any questions ?...

SIL Bridge !

PFDavg is not really a good indicator for worker in operation