TOTAL
COMMITTED TO BETTER ENERGY

ISO/TR 12489 - RELIABILITY MODELING AND CALCULATION OF SAFETY SYSTEMS: BUSINESS CASE APPLICATION BY TOTAL

By **Nicolas Clavé** (France), Total S.A., Specialist in Reliability & Production availability

& **Jean-Pierre Signoret**, Reliability expert, Project leader for ISO/TR 12489

International ISO standardization seminar for the reliability technology and cost area, Statoil Business Centre, Stavanger, Norway, 26 April 2016.

Field Operations

TABLE OF CONTENTS

1. ISO/TR 12489: STAKES AND OBJECTIVES

Stakes:

The first issue of the *International Standard IEC 61508* *"Functional safety of Electrical / electronic / programmable electronic safety-related systems"* part-6 annex B proposed only a catalogue of **simplified analytical formulas** to perform the probabilistic calculations (PFD_{avg}/PFH) related to Safety Instrumented Systems (SIS).

No explanations are provided about how these formulas had been developed. Therefore this make them **difficult to understand** and properly apply. **Their extension to important missing parameters** (e.g. potential effect of test durations, probability of failure due to the demand itself, human errors, etc.) is also **almost impossible**.

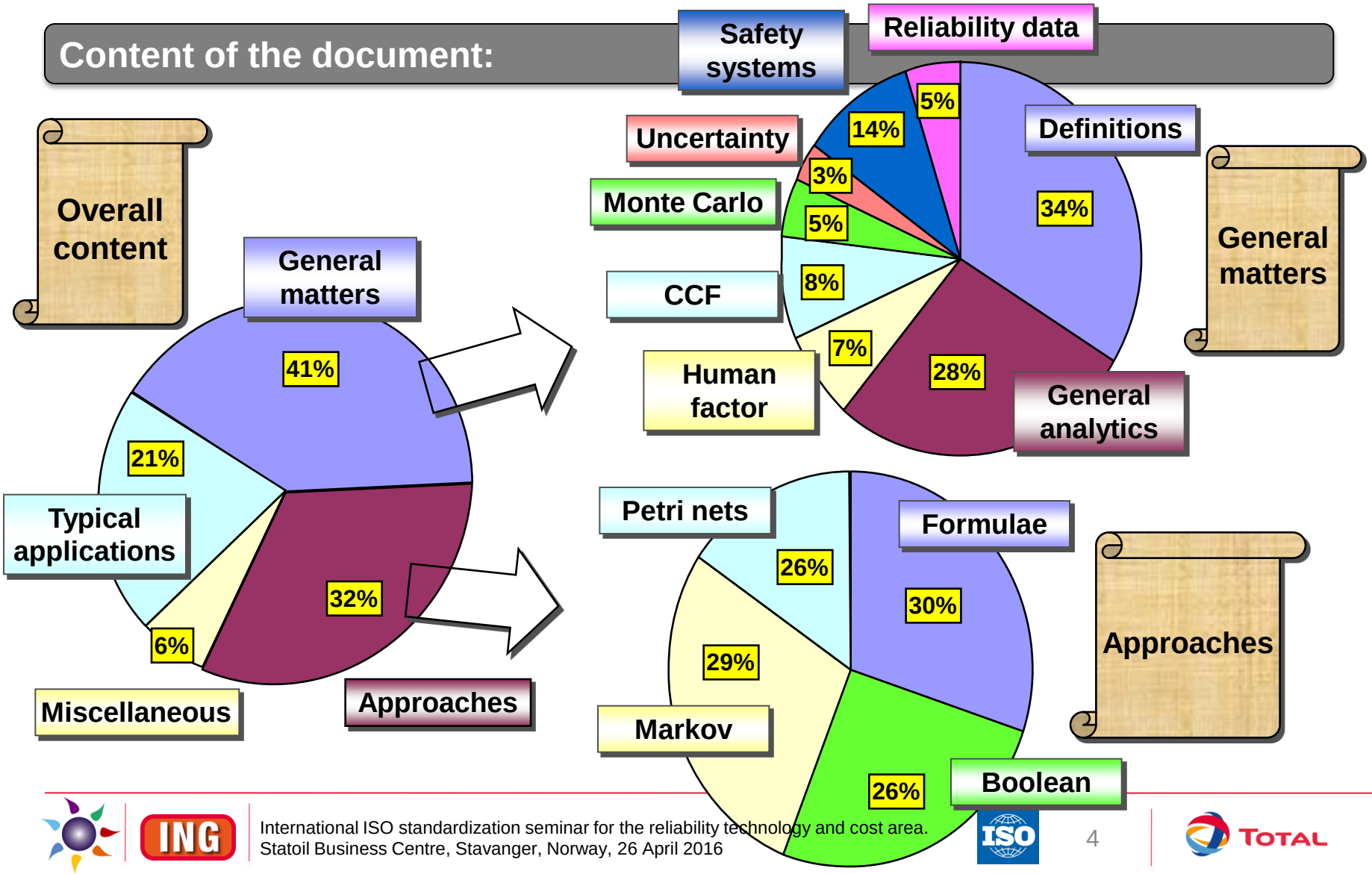
Objectives:

In 2008, the gap with the state of the art in the dependability field was so obvious that it was decided by the ISO TC67/WG4 to develop a *Technical Report* to identify the challenges related to probabilistic calculations related to SIS and provide a sound background to perform them in order to close this gap.

Note: the second issue of the IEC 61508-6 annex B has briefly introduced alternative approaches in line with the ISO/TR 12489.

1. ISO/TR 12489: STAKES AND OBJECTIVES

Content of the document:



2. FIRST EDITION AND DISSEMINATION

First issue:

The first edition has been issued on **November 1, 2013** (with the majority of the document worked out by Jean-Pierre SIGNORET).

In addition, a **CEN version** has been issued early **February, 2016**.

Dissemination:

- **Articles:** OGP Highlights, AFTP bulletin (France), λμ conferences (France)
- **Seminars:** ESRA Norge (Stavanger, Norway), TUV (Köln, Germany), PETROBRAS (Rio, Brazil), PDS forum (Trondheim, Norway), GEP-AFTP (Paris, France), etc.
- **Courses:** Universitad Central de Venezuela (Caracas), École Centrale (Beijing, China), ENIM (Rabat, Morocco), University of Technology of Troyes (France), University of Stavanger (Norway), etc.

3. BUSINESS CASE APPLICATION

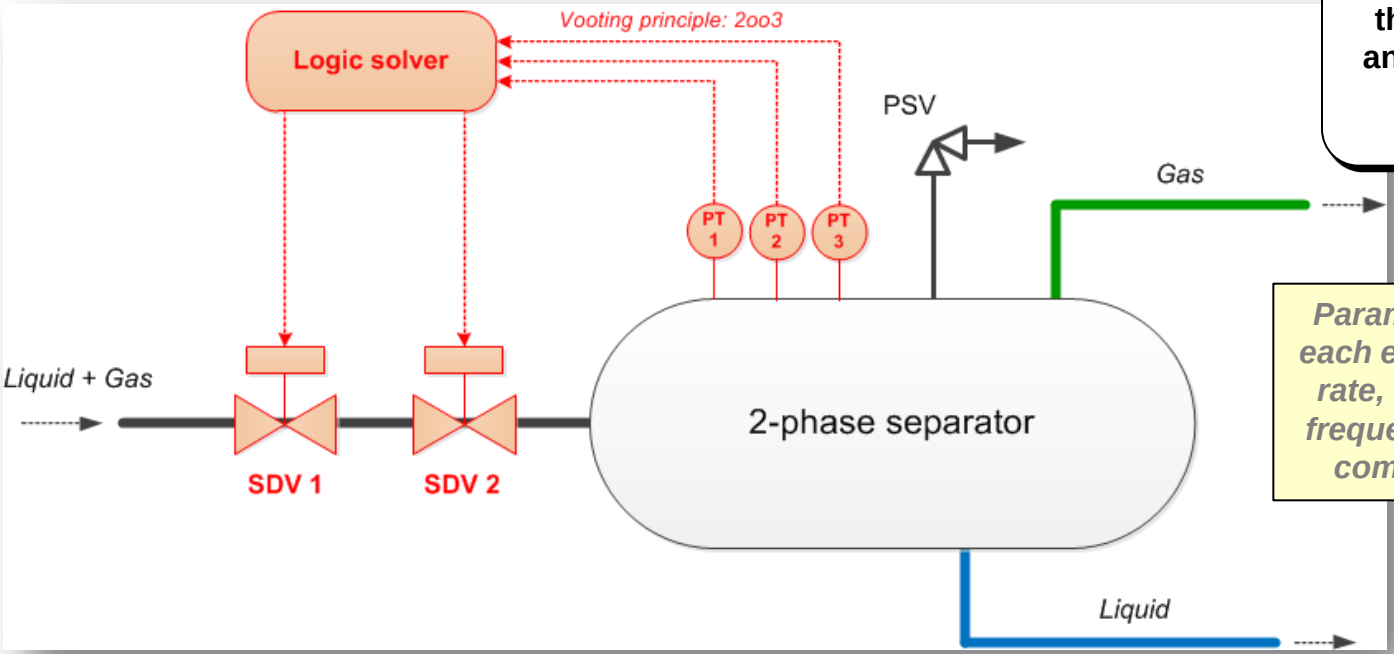
Example chosen to be simple enough to be explained but not trivial

Presentation:

The objective is to assess the PFD_{avg} of the SIS below made up of 3 sensors in 2oo3, a dedicated logic solver and 2 redundant shutdown valves to close.

For the purpose of this paper, it was decided to perform the calculations with 3 different modelling techniques: Fault trees, Markov graphs and Petri nets.

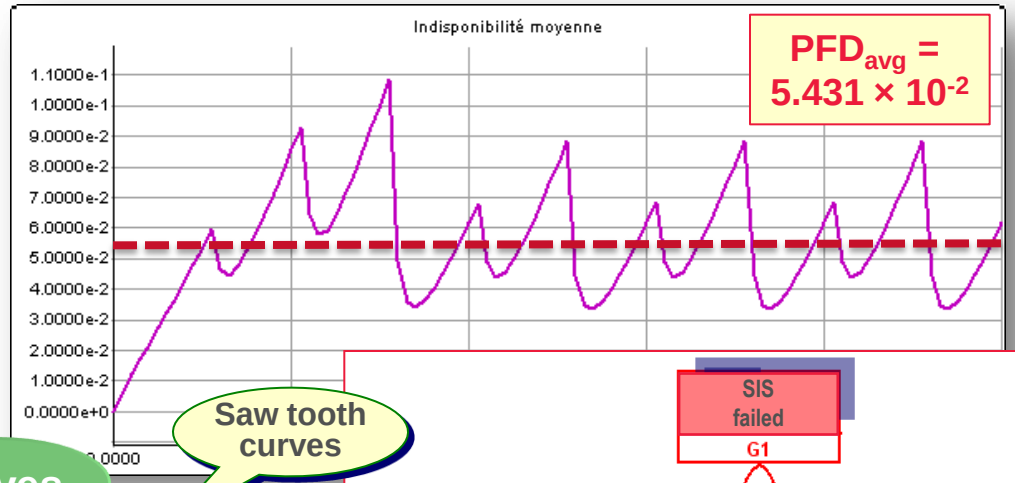
Parameter chosen to make the calculations difficult and verify that the results do not depend on the modeling technique



Parameters to consider for each equipment type: failure rate, repair rate, proof test frequency and duration and common cause failures.

3. BUSINESS CASE APPLICATION

Fault tree analysis (ISO/TR 12489, § 8.3):



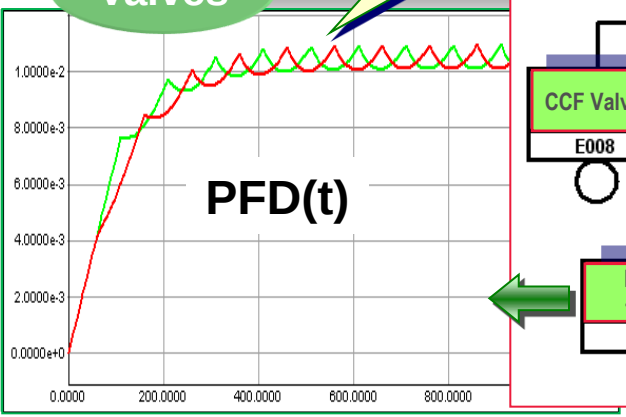
$PFD_{avg} = 5.431 \times 10^{-2}$

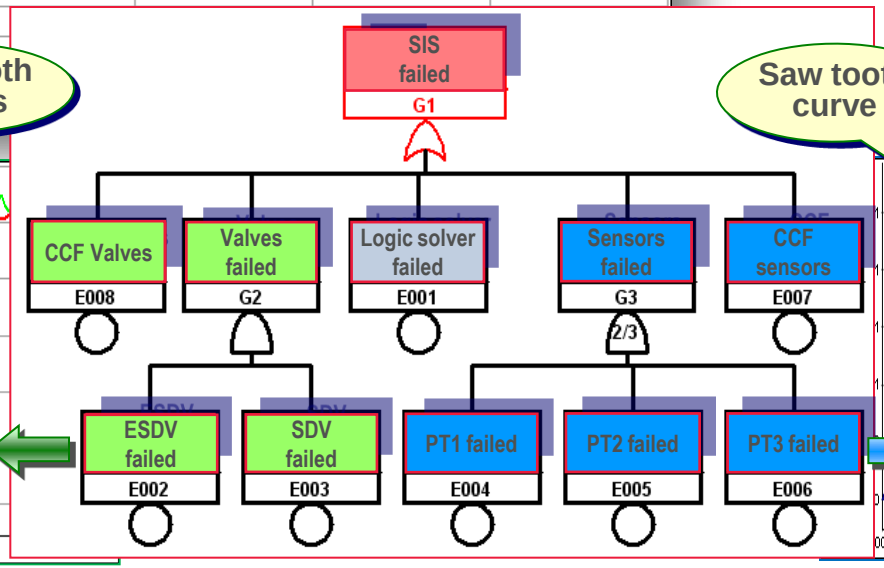
- Modeling tool:
  GRIF-Tree module *(© Total)*
- Computation engine:
  ALBIZIA = BDD tool *(© Total)*

Computation time < 1s

Saw tooth curves

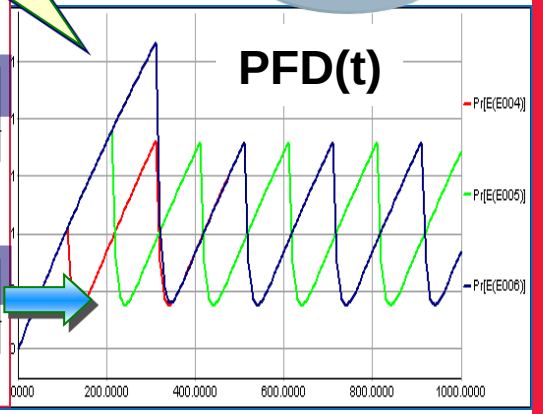
Valves





Saw tooth curve

Sensors



3. BUSINESS CASE APPLICATION

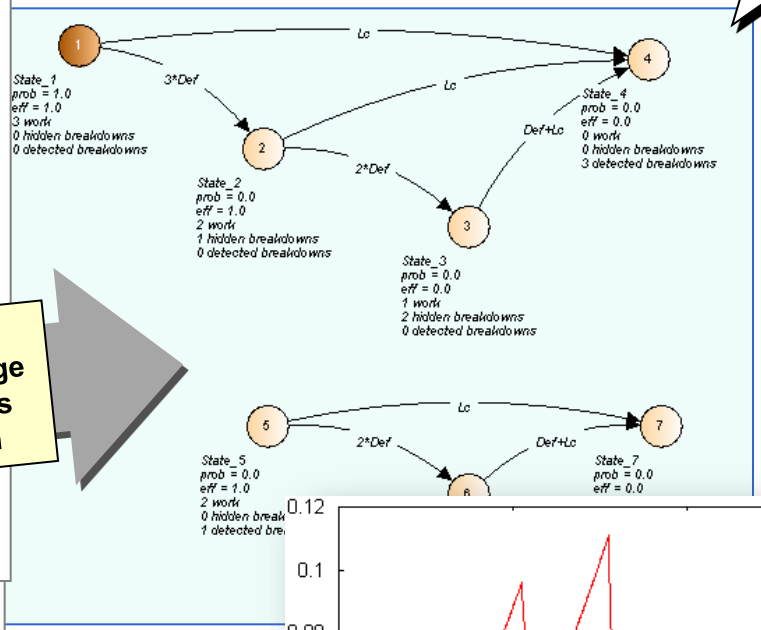
Multiphase Markov model (ISO/TR 12489, § 9):

Actual Markov model generated = several hundred of states

```
node unitTEST
  state s:{W,F,R}; p:{I,T,O};
  event fail, repair, firstTest, startTest, endTest;
  init
    s:=W, p:=I;
  trans
    (s=W) |- fail      -> s:=F;
    (s=R) |- repair    -> s:=W;
    (p=I) |- firstTest -> p:=T;
    (p=O) |- startTest -> p:=T;
    (p=T) |- endTest   -> p:=O, s:=if (s=F) then R else s;
  extern
    law <event fail>      = exponential(lambda);
    law <event repair>    = exponential(mu);
    law <event firstTest> = Dirac(theta);
    law <event startTest> = Dirac(tau);
    law <event endTest>   = Dirac(pi);
edon

node unitNONTEST
state s:{W,R};
  event fail, repai
  init
    s:=W;
  trans
    (s=W) |- fail
    (s=R) |- repair
  extern
    law <event fail>      = exponential(lambda);
    law <event repair>    = exponential(mu);
edon
```

COMBAVA: Interface that automatically generates large multi-phase Markov graphs from a formal description

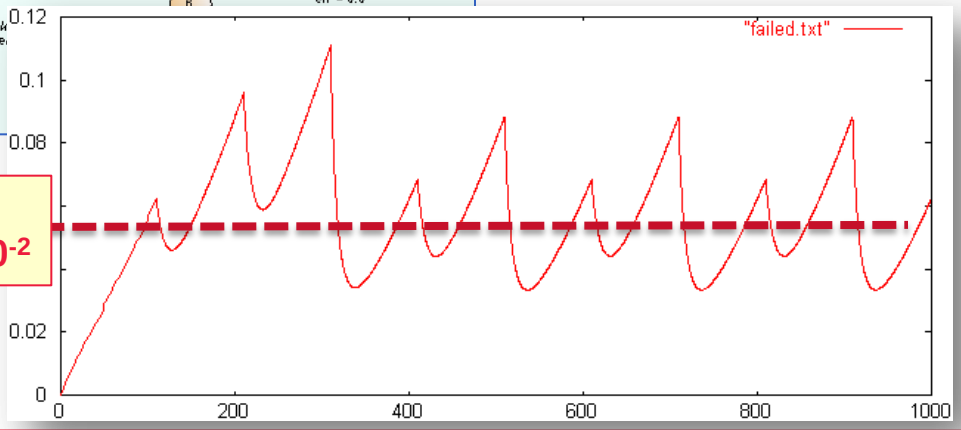


Modeling tool:
Combava / Altarica data flow

Computation time ≈ 20 min

```
    parameter SV.mu      = 0.01;
    parameter SV.theta   = 50;
    parameter SV.tau     = 100;
    parameter SV.pi      = 10;
    parameter SDV.lambda = 0.00007;
    parameter SDV.mu     = 0.01;
    parameter SDV.theta  = 100;
    parameter SDV.tau    = 100;
    parameter SDV.pi     = 10;
    property  PT1failed  = <term (PT1.s#W)>;
    property  PT2failed  = <term (PT2.s#W)>;
    property  PT3failed  = <term (PT3.s#W)>;
    property  LSfailed   = <term (LS.s#W)>;
    property  SVfailed   = <term (SV.s#W)>;
    property  SDVfailed  = <term (SDV.s#W)>;
    property  failed     = <term (((PT1.s#W) and (PT2.s#W))
edon
```

$PFD_{avg} = 5.306 \times 10^{-2}$

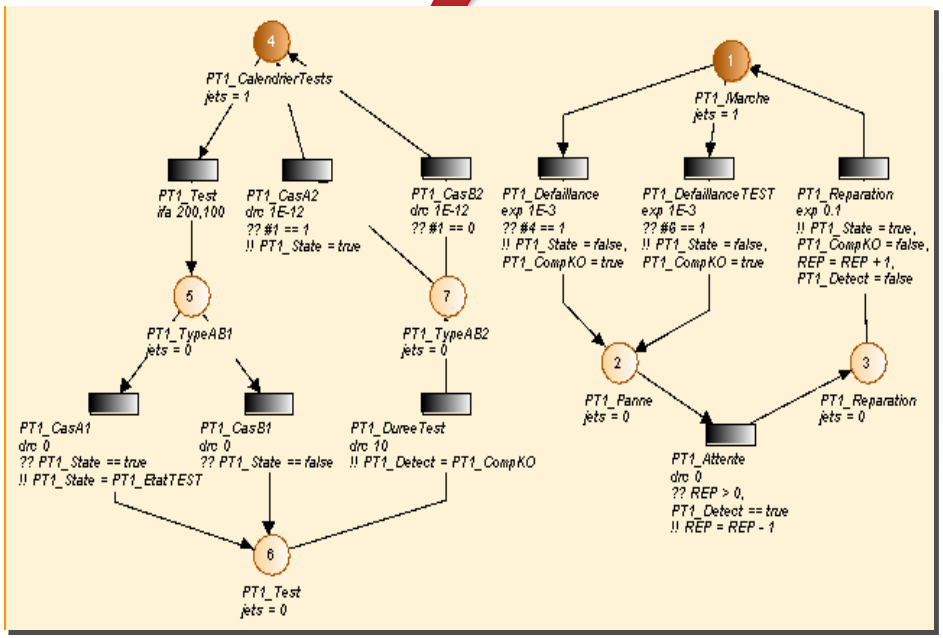


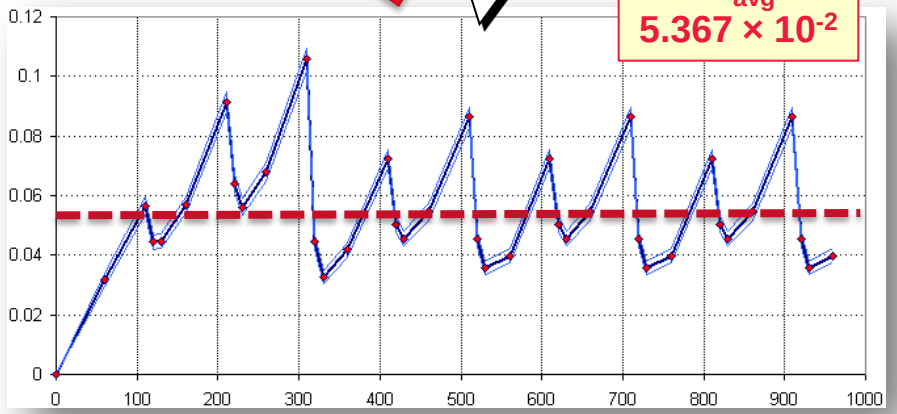
3. BUSINESS CASE APPLICATION

Petri nets (ISO/TR 12489, § 10):

Monte-Carlo simulation
(about 60,000 histories)

It is possible to obtain a smoother curve but it is useless as the average is obtained without using this curve.





$PFD_{avg} = 5.367 \times 10^{-2}$

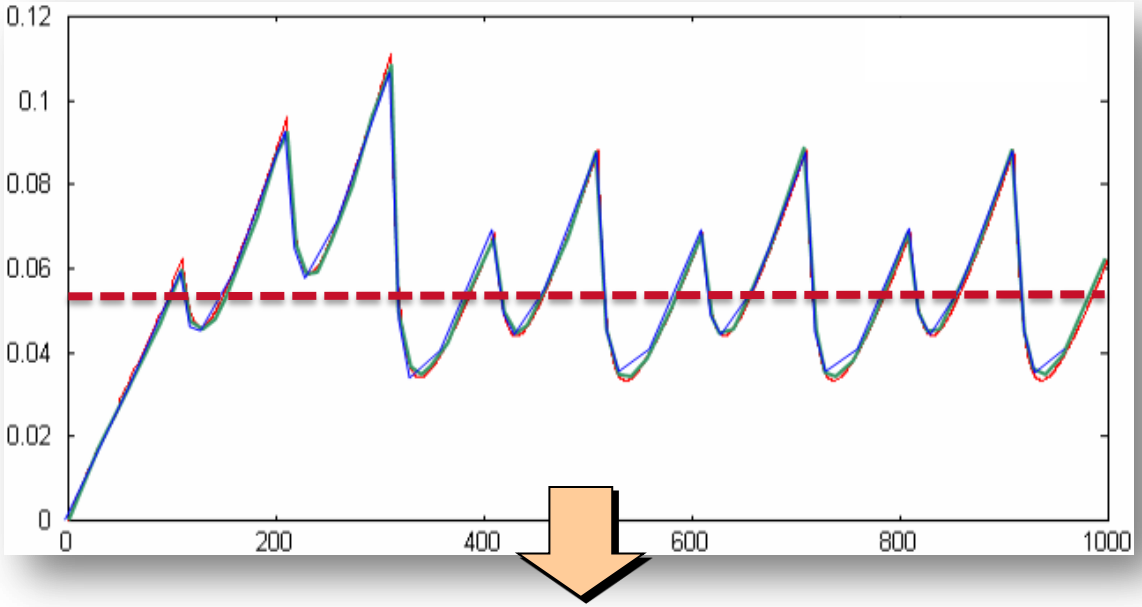
- Modeling tool:
  GRIF-Petri module *(© Total)*
- Computation engine:
  MOCA-RP *(© Total)*

Computation time < 1s

3. BUSINESS CASE APPLICATION

Comparison between results:

The graph below shows the curve obtained for each method:



Fault tree analysis:

$PFD_{avg} = 5.431 \times 10^{-2}$

Multiphase markov graph:

$PFD_{avg} = 5.306 \times 10^{-2}$

Petri nets:

$PFD_{avg} = 5.367 \times 10^{-2}$

The threes techniques provide the same results

3. BUSINESS CASE APPLICATION

All applications in Total:

- Emergency shutdown (ESD loops) and blowdown
- Fire fighting
- Gas and fire detection
- Overpressure detection/protection (top riser, pipeline, separator, compressor…)
- Overflow protection
- Prevention of flare spill-over
- Sour gas arrival prevention
- Subsea Isolation Valve (SSIV) module
- Subsea preservation
- Oil offloading

4. CONCLUSIONS

The business case application shows that **the three methods give very close curves** for **PFD(t)** and **very close final results** for **PFD_{avg}**.

ISO/TR 12489 provides different methods and techniques to **accurately assess reliability parameters**.

The **most suitable method** is to be selected according to the number, the nature/type, the level of details and the complexity of the assumptions that are to be considered.

If the Reliability engineer in charge of the study can choose from among several methods/techniques that could be applied, **he will obtain rigorously the same results** if he uses the same assumptions.