Review of the calculation methods of ISO/TR 12489 for the probability of failure of safety-related systems

Florent Brissaud, Sr. Research Engineer (GRTgaz)
and ISO/TC67/WG4/PG3 Interim Leader

5th ISO Seminar on International Standardization in the Reliability Technology and Cost Area

Hosted by TotalEnergies, Paris, France - 1 December 2022

Industrial and standardization background

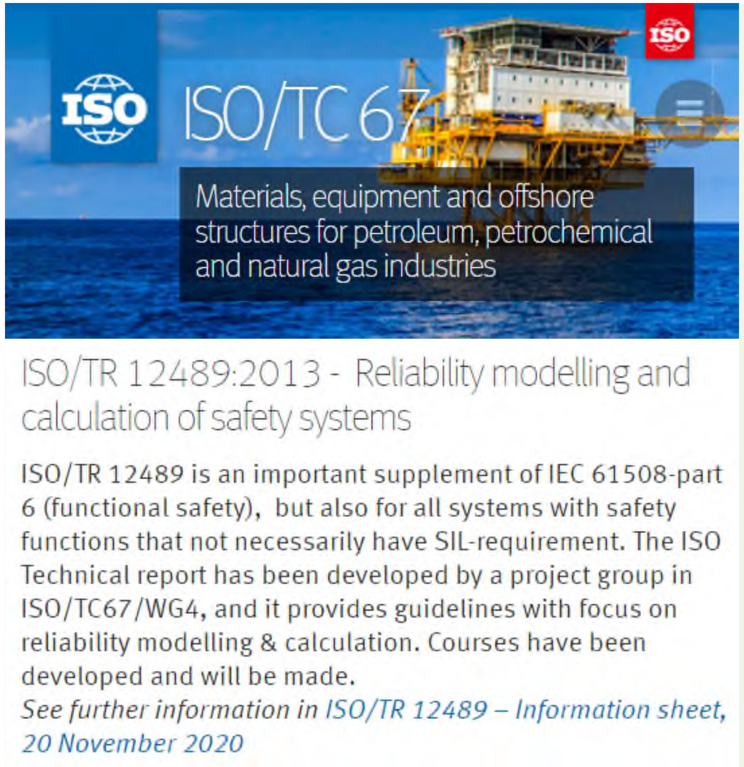
ISO/TR 12489 to fill the gaps for reliability of safety-related systems

- More than 50 years of research & development on safety-related systems
  → numerous methods for reliability calculation
- IEC/TC65: Functional Safety standards
  → oversimplified calculation (improved in IEC 61508:2010)
- ISO/TC67/WG4: Reliability Engineering and Technology
  → standards with relevance to safety-related systems

- Several countries involved in the development of the ISO/TR 12489 from 2008 and 2013
  → Belgium, Brazil, France, Netherlands, Norway, Italy, Spain, UK, USA
- Issued by ISO in 2013 and approved by CEN
  → officially adopted by more than 20 countries in Europe
- Interim phase of the ISO/TC67/WG4/PG3
  → additional countries involved (Australia, Denmark)

ISO/TR 12489

In a few words…



Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries

ISO/TR 12489:2013 - Reliability modelling and calculation of safety systems

ISO/TR 12489 is an important supplement of IEC 61508-part 6 (functional safety), but also for all systems with safety functions that not necessarily have SIL-requirement. The ISO Technical report has been developed by a project group in ISO/TC67/WG4, and it provides guidelines with focus on reliability modelling & calculation. Courses have been developed and will be made.
See further information in ISO/TR 12489 – Information sheet, 20 November 2020

https://committee.iso.org/sites/tc67/home/working-groups/wg4---reliability-engineering--t.html

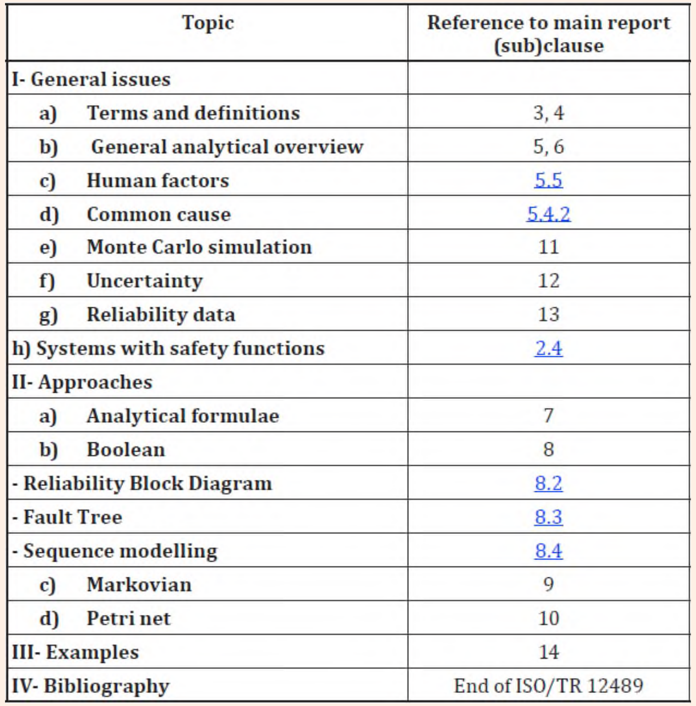
Technical report

- Informative (guideline)
- General and methodological matters
- Simplified formulae plus more advanced approaches

Safety-related systems

- Simple or complex systems
- "Ordinary" or instrumented
- Safety ("dangerous failures")
- Production ("safe failures")

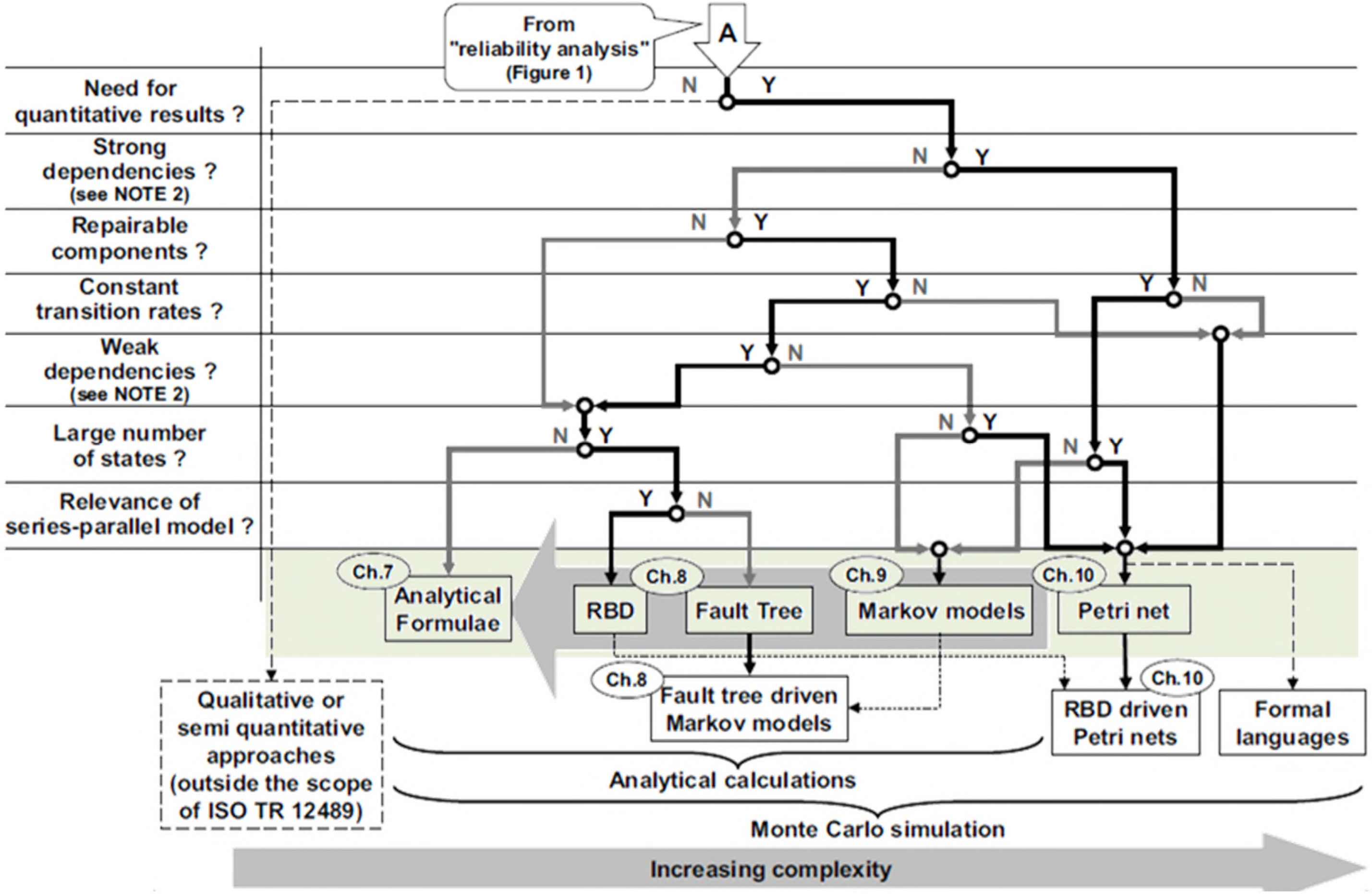
Content



Topic	Reference to main report (sub)clause
I- General issues	
a) Terms and definitions	3, 4
b) General analytical overview	5, 6
c) Human factors	5.5
d) Common cause	5.4.2
e) Monte Carlo simulation	11
f) Uncertainty	12
g) Reliability data	13
h) Systems with safety functions	2.4
II- Approaches	
a) Analytical formulae	7
b) Boolean	8
- Reliability Block Diagram	8.2
- Fault Tree	8.3
- Sequence modelling	8.4
c) Markovian	9
d) Petri net	10
III- Examples	14
IV- Bibliography	End of ISO/TR 12489

Reliability modelling and calculation

Overview of the approaches as per ISO/TR 12489



Measures of reliability

Targets and inputs for reliability modelling and calculation

- **PFDavg: average probability** of failure on demand of the safety function (i.e. average unavailability)
  → target failure measure for safety functions performed **on demand, once per year or less**

- **PFH: average frequency** of failure of the safety function (i.e. average unconditional failure intensity)
  → target failure measure for safety functions performed **more than once per year**

- system architecture (e.g. M-out-of-N)
- dangerous failures detected online (λ_{DD})
- dangerous failures only revealed by proof tests (λ_{DU})
- period of proof tests (T_1)
- common cause failures (β factor)
- repair times (MRT)
- human errors
- …

Simplified equations

…simple, but restrictive

Concepts

- Reliability equations are approximated by formula that only contain “basic” operations
- IEC 61508 proposes simplified equations for basic architectures (1oo1, 1oo2, 2oo2, 2oo3, 1oo3) with identical elements (i.e. same failure rates, proof tested at the same time…)
- Example with a 1oo2 system:

$$PFDavg = 2 \times [((1 - \beta_D) \times \lambda_{DD} + (1 - \beta) \times \lambda_{DU})]^2 \times [(\lambda_{DD} / \lambda_D) \times MRT_{DD} + (\lambda_{DU} / \lambda_D) \times ((T_1 / 2) + MRT_{DU})]$$
$$\times [(\lambda_{DD} / \lambda_D) \times MRT_{DD} + (\lambda_{DU} / \lambda_D) \times ((T_1 / 3) + MRT_{DU})] + \beta_D \times \lambda_{DD} \times MRT_{DD} + \beta \times \lambda_{DU} \times ((T_1 / 2) + MRT_{DU})$$

Limitations

- These equations are not fully explained… and doubtful!
- These equations are developed under specific assumptions and applying them outside their limits can lead to wrong results

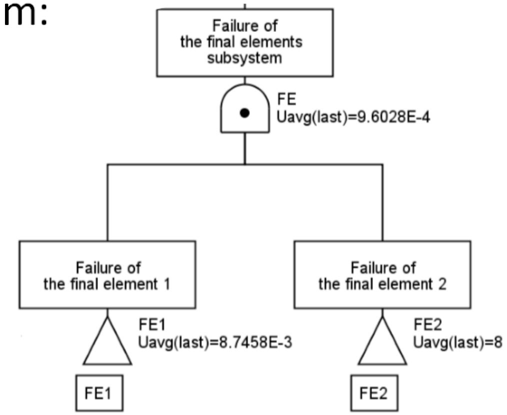
→ **ISO/TR 12489 provides explanations of these equations**

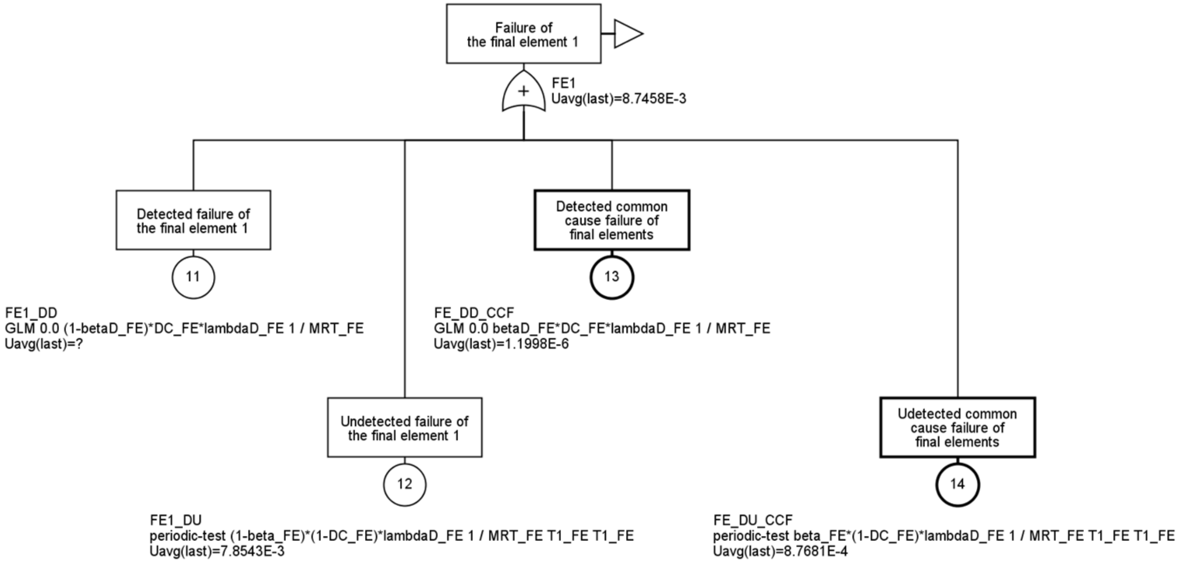
Fault trees

…a basic tool for reliability engineers

Concepts

- Express a top event (e.g. loss of the safety function) by combinations of basic events (e.g. dangerous failures of elements), using logic gates
- Exact analyses are performed using Boolean algebra
- Example with a 1oo2 system:


Failure of the final elements subsystem
FE
Uavg(last)=9.6028E-4
Failure of the final element 1
FE1
Uavg(last)=8.7458E-3
FE1
Failure of the final element 2
FE2
Uavg(last)=8
FE2


Failure of the final element 1
FE1
Uavg(last)=8.7458E-3
+
Detected failure of the final element 1
11
FE1_DD
GLM 0.0 (1-betaD_FE)*DC_FE*lambdaD_FE 1 / MRT_FE
Uavg(last)=?
Undetected failure of the final element 1
12
FE1_DU
periodic-test (1-beta_FE)*(1-DC_FE)*lambdaD_FE 1 / MRT_FE T1_FE T1_FE
Uavg(last)=7.8543E-3
Detected common cause failure of final elements
13
FE_DD_CCF
GLM 0.0 betaD_FE*DC_FE*lambdaD_FE 1 / MRT_FE
Uavg(last)=1.1998E-6
Udetected common cause failure of final elements
14
FE_DU_CCF
periodic-test beta_FE*(1-DC_FE)*lambdaD_FE 1 / MRT_FE T1_FE T1_FE
Uavg(last)=8.7681E-4

Limitations

- Basic events must be independent (e.g. no “stand-by” elements)
- The model is static (e.g. no reconfiguration of the architecture)

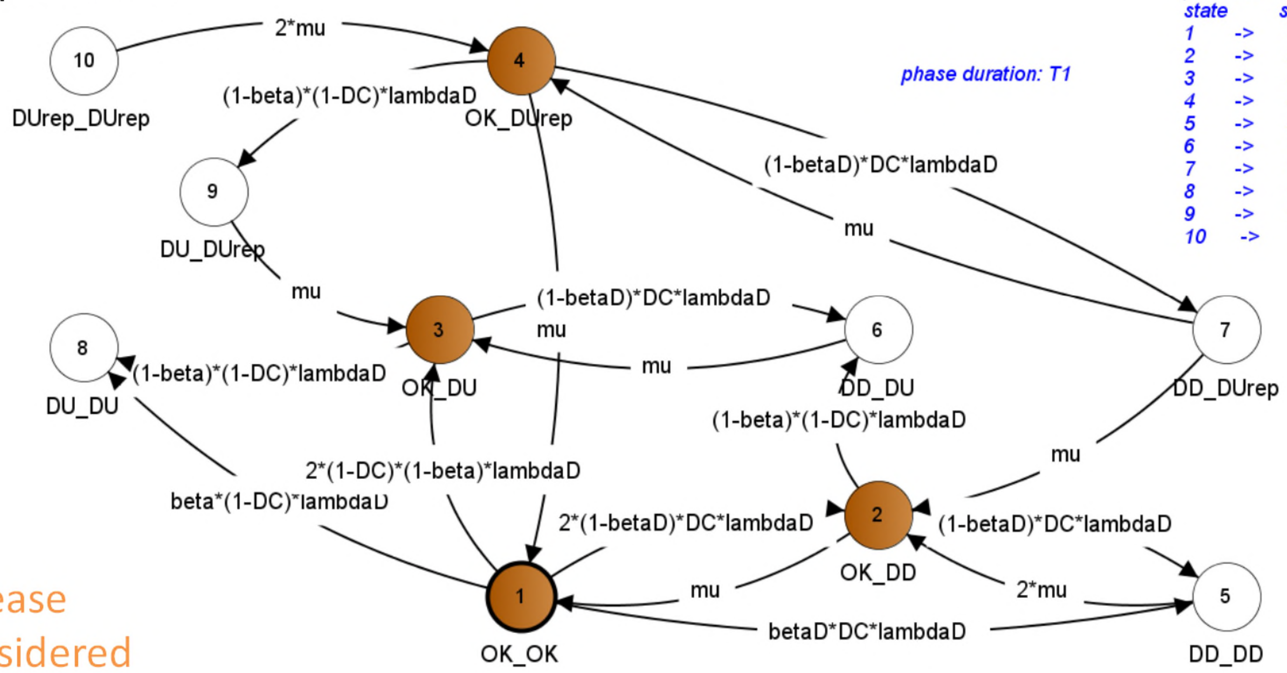
→ ISO/TR 12489 provides a guideline to use fault trees

Multiphase Markov graphs

…powerful, but complex

Concepts

- State-transition modelling of a system, with constant rates
- Multi-phase feature is required to model proof tests
- Exact analyses are performed using mathematical theories
- Example with a 1oo2 system:



phase duration: T1

Linking matrix (between p.

previous state		*next state*	*probability*
1	*->*	*1*	*1.0*
2	*->*	*2*	*1.0*
3	*->*	*4*	*1.0*
4	*->*	*4*	*1.0*
5	*->*	*5*	*1.0*
6	*->*	*7*	*1.0*
7	*->*	*7*	*1.0*
8	*->*	*10*	*1.0*
9	*->*	*10*	*1.0*
10	*->*	*10*	*1.0*

Limitations

- The size of the model can drastically increase according to the characteristics to be considered

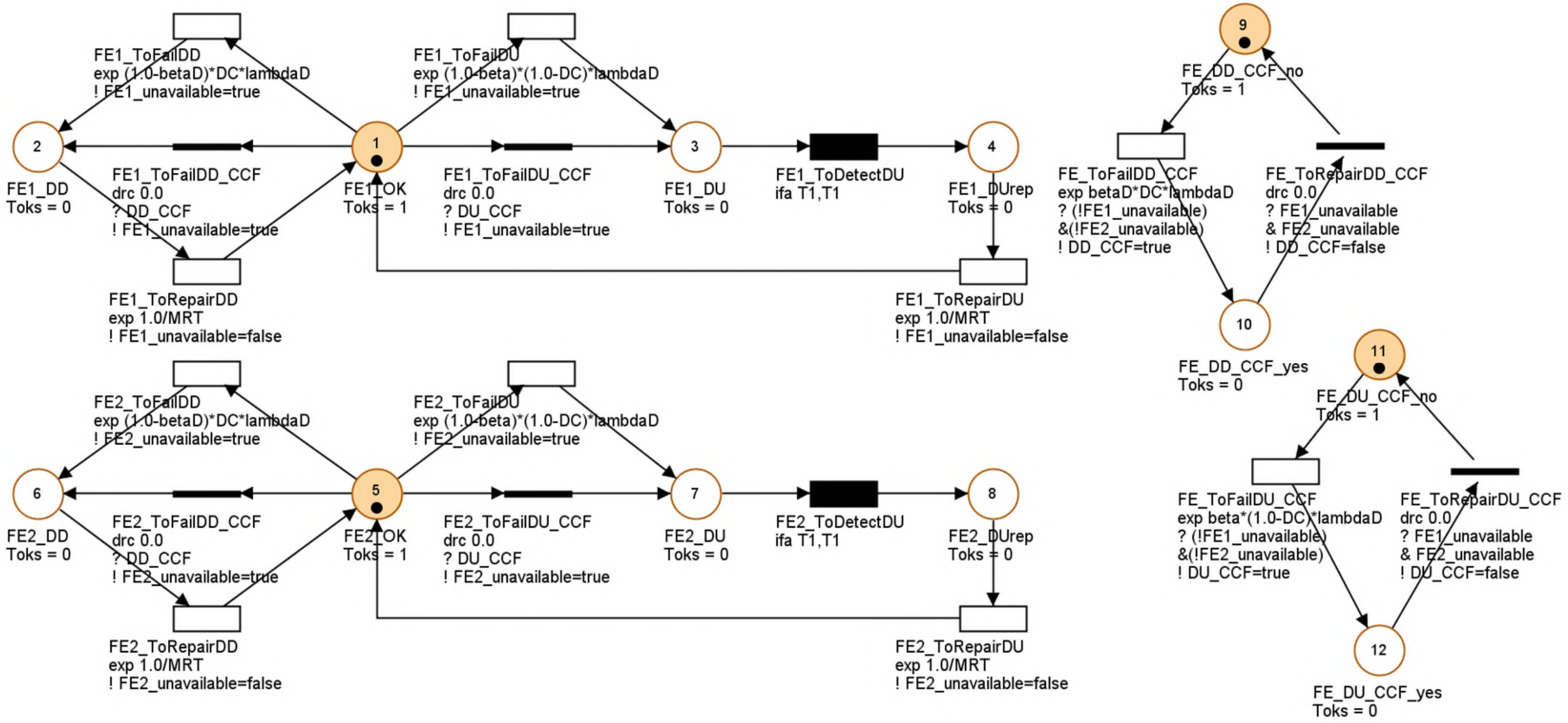
→ **ISO/TR 12489 provides a guideline to use Markov models**

Stochastic Petri nets

…the most flexible

Concepts

- State-transition modelling of a system (with "tokens")
- Analyses are performed using Monte Carlo simulations
- Example with a 1oo2 system:



Limitations

- The simulations can be quite time-consuming for large models or when the probabilities are very low

→ **ISO/TR 12489 provides a guideline to use Petri nets**

Recommendations

Which method to use?

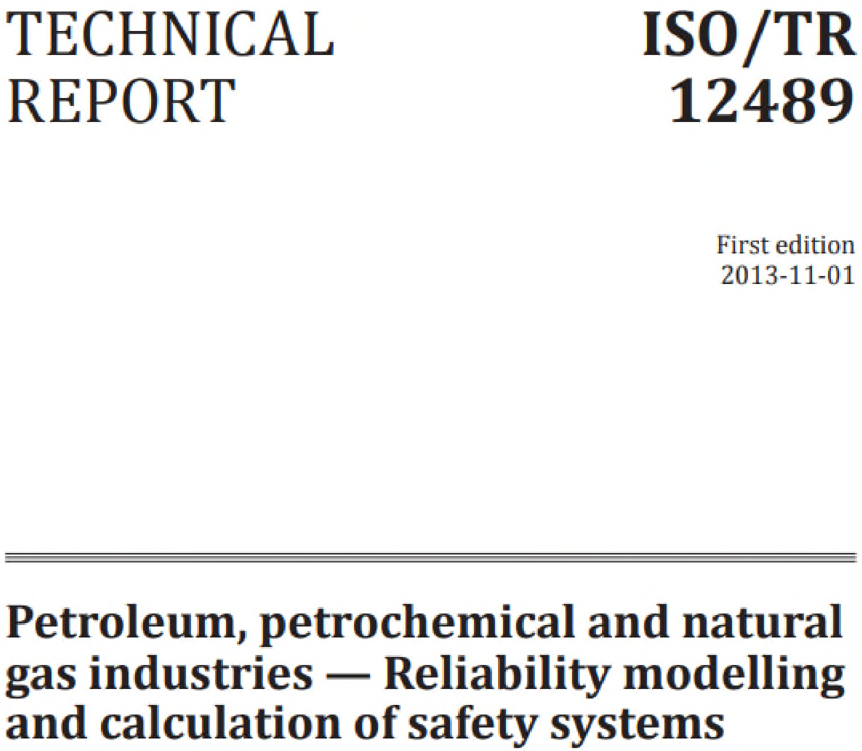
ISO/TR 12489 requirements

- *"Using a software package as a black box or a formula as a magic recipe is likely to lead to inaccurate, often non-conservative, results."*
- *"In all cases the reliability engineers should (...) have a minimum understanding of the mathematics behind the calculations and a good knowledge of the nature of the results that they obtain (...)"*
- *"Working with time constraints leading to (over)simplifications (...) encourages practitioners to think that reliability modelling and calculations can be properly made just by applying analytical formulae or using black boxes without really understanding."*

Proposed recommendations

- **Avoid using simplified equations, which are not flexible and often used without any cautions with regards to the underlying assumptions**
- **Prefer fault trees for classical systems (i.e. without dynamic features), because they carry most of the advantages for engineers: easy to apply and to read, allow extended modelling and powerful analyses**
- **Use Petri nets for other cases, because of the most flexible method**

Acknowledgements / Thank You / Questions?



TECHNICAL REPORT

ISO/TR 12489

First edition
2013-11-01

Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems