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

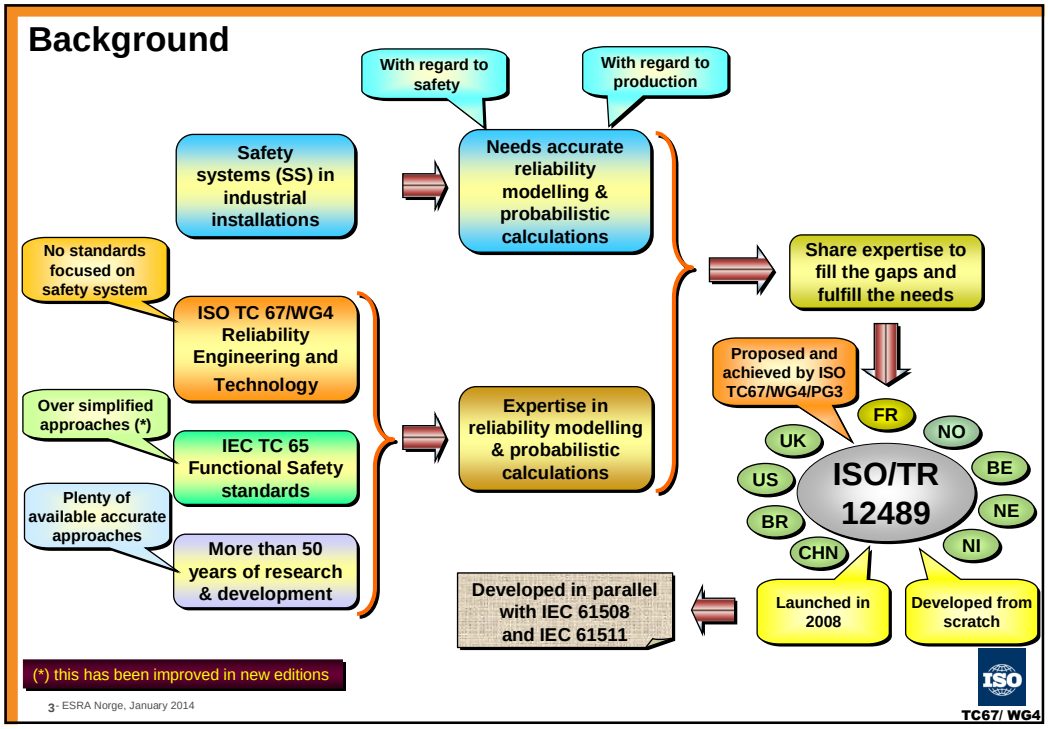
ESRA Norge, January 2014

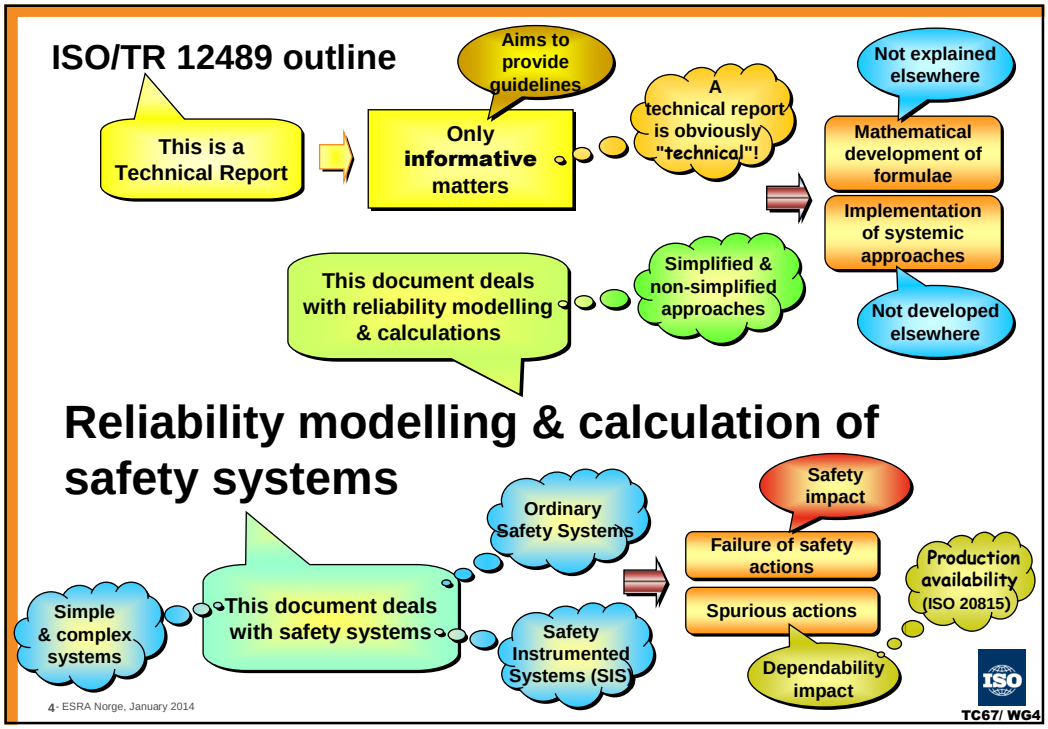
Presentation of ISO/TR 12489

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

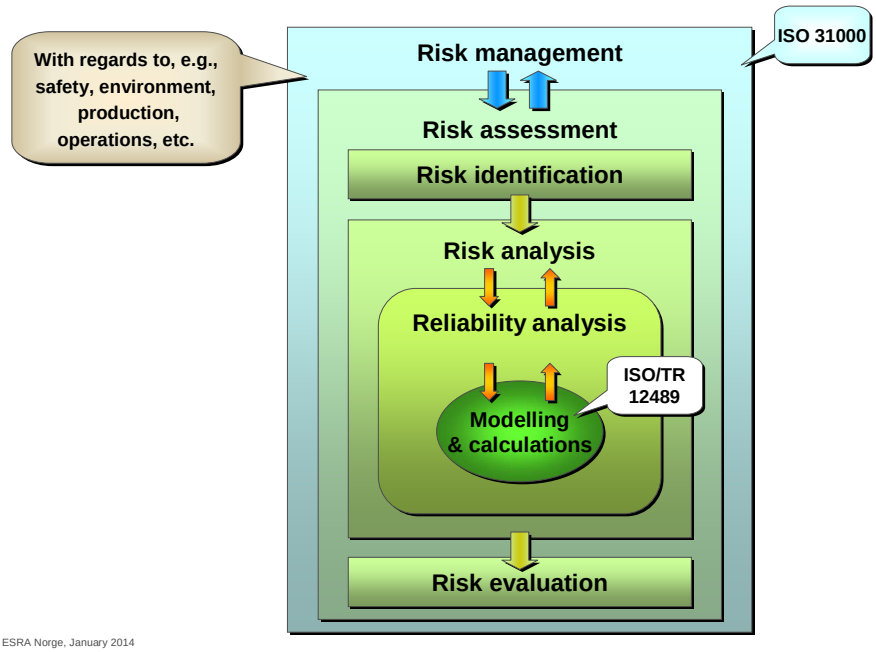
TC67
WG4

ESRA Norge, January 2014


Background
With regard to safety
With regard to production
Safety systems (SS) in industrial installations
Needs accurate reliability modelling & probabilistic calculations
Share expertise to fill the gaps and fulfill the needs
No standards focused on safety system
ISO TC 67/WG4 Reliability Engineering and Technology
Over simplified approaches (*)
IEC TC 65 Functional Safety standards
Plenty of available accurate approaches
More than 50 years of research & development
Expertise in reliability modelling & probabilistic calculations
Proposed and achieved by ISO TC67/WG4/PG3
FR
NO
UK
BE
US
ISO/TR 12489
NE
BR
NI
CHN
Launched in 2008
Developed from scratch
Developed in parallel with IEC 61508 and IEC 61511
(*) this has been improved in new editions
3 - ESRA Norge, January 2014
TC67/ WG4

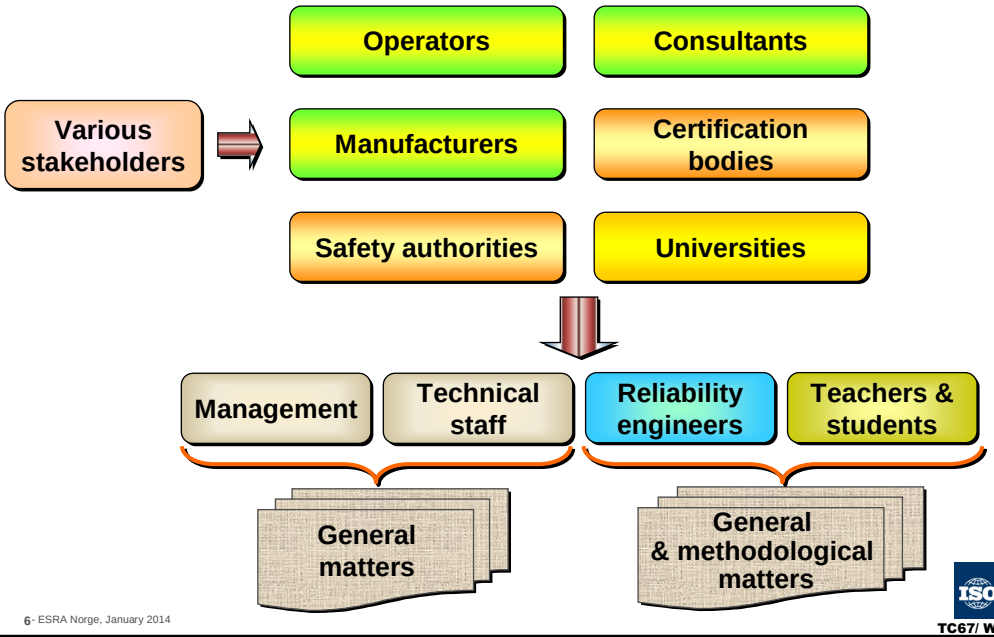

ISO/TR 12489 outline
Aims to provide guidelines
This is a Technical Report
Only informative matters
A technical report is obviously "technical"!
Not explained elsewhere
Mathematical development of formulae
Implementation of systemic approaches
Not developed elsewhere
This document deals with reliability modelling & calculations
Simplified & non-simplified approaches
Reliability modelling & calculation of safety systems
Ordinary Safety Systems
Safety impact
Failure of safety actions
Simple & complex systems
This document deals with safety systems
Spurious actions
Production availability (ISO 20815)
Safety Instrumented Systems (SIS)
Dependability impact
4 - ESRA Norge, January 2014
TC67/ WG4

Overall framework of ISO/TR 12489

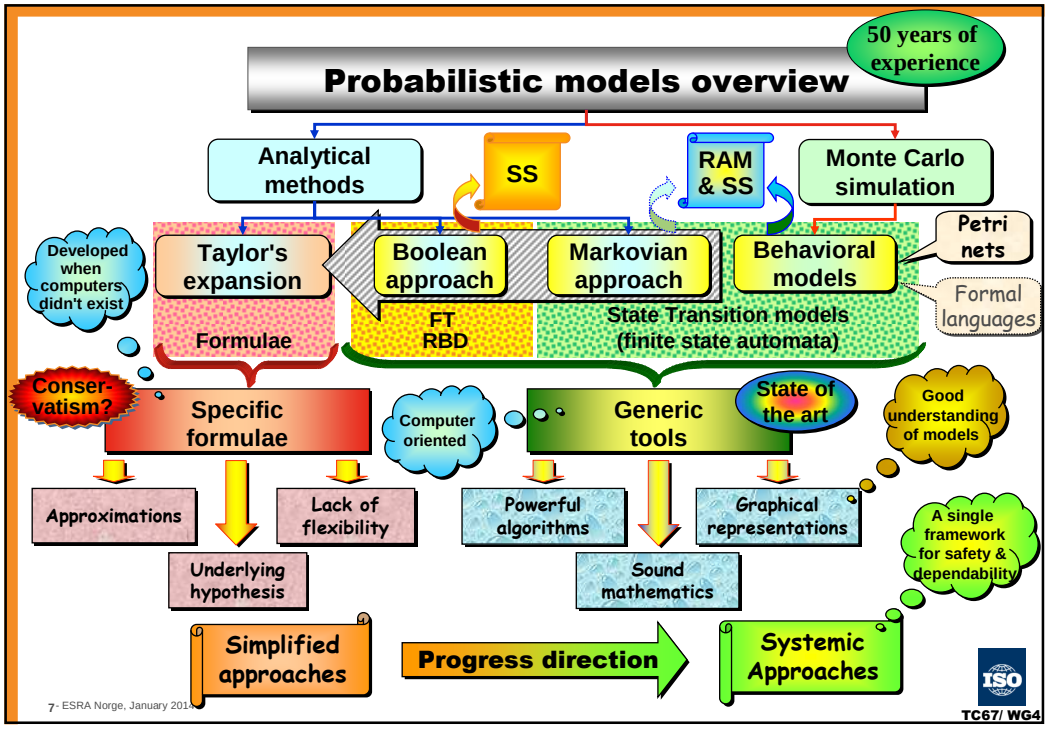


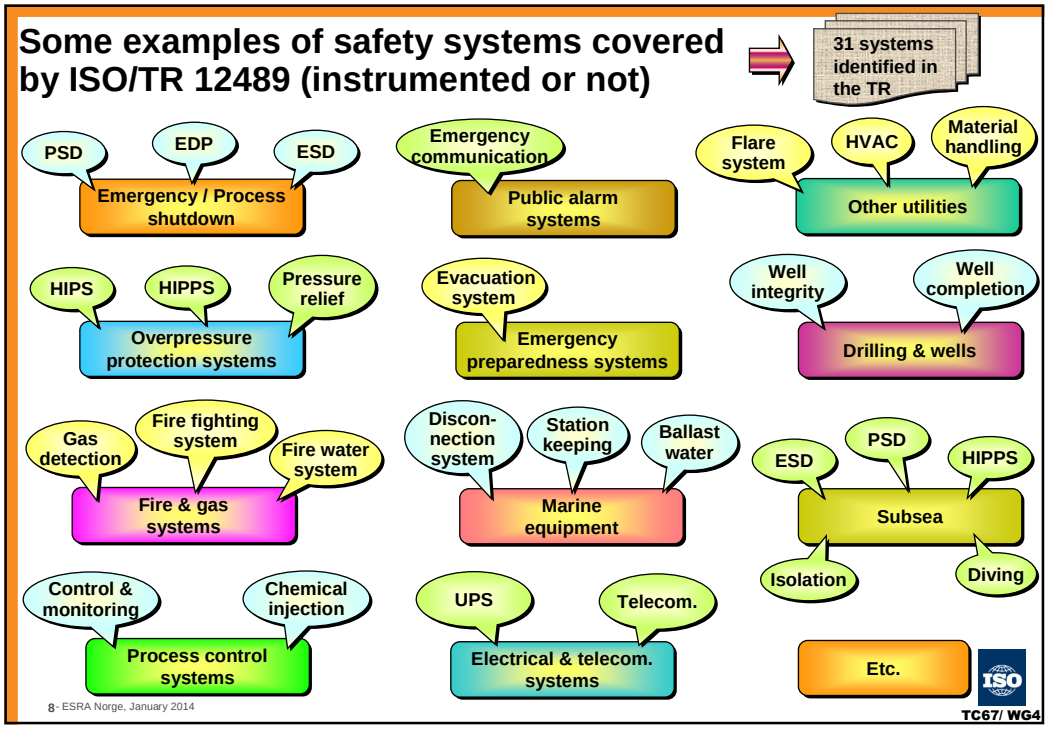
TC67/ WG4

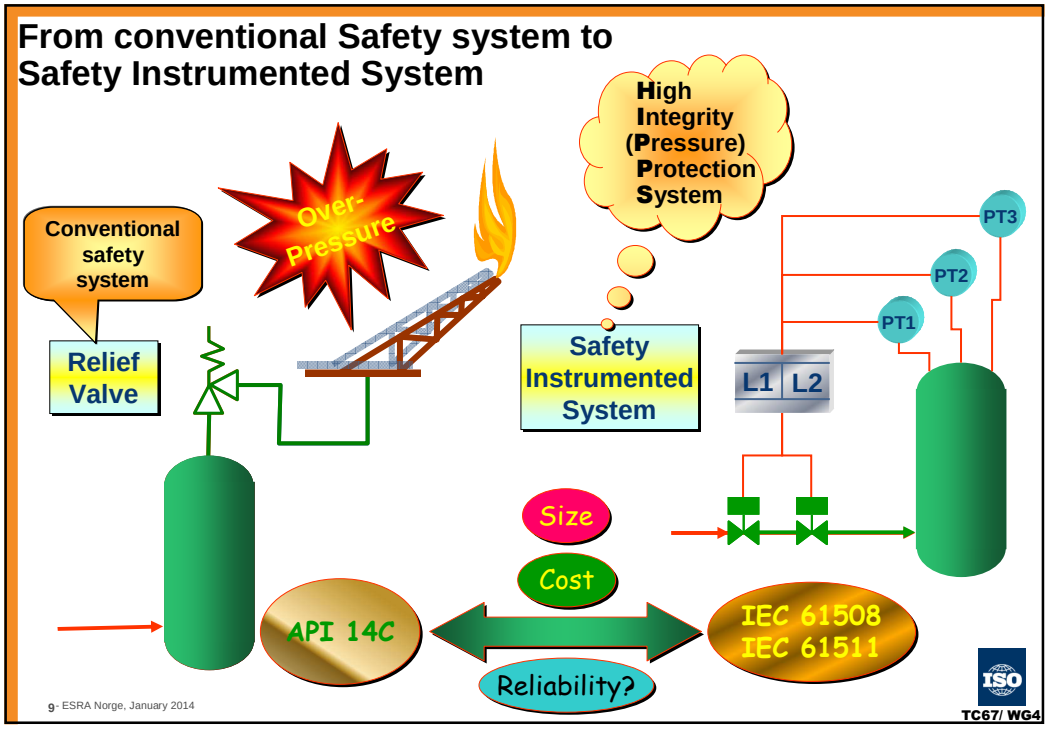
Target users of ISO/TR 12489

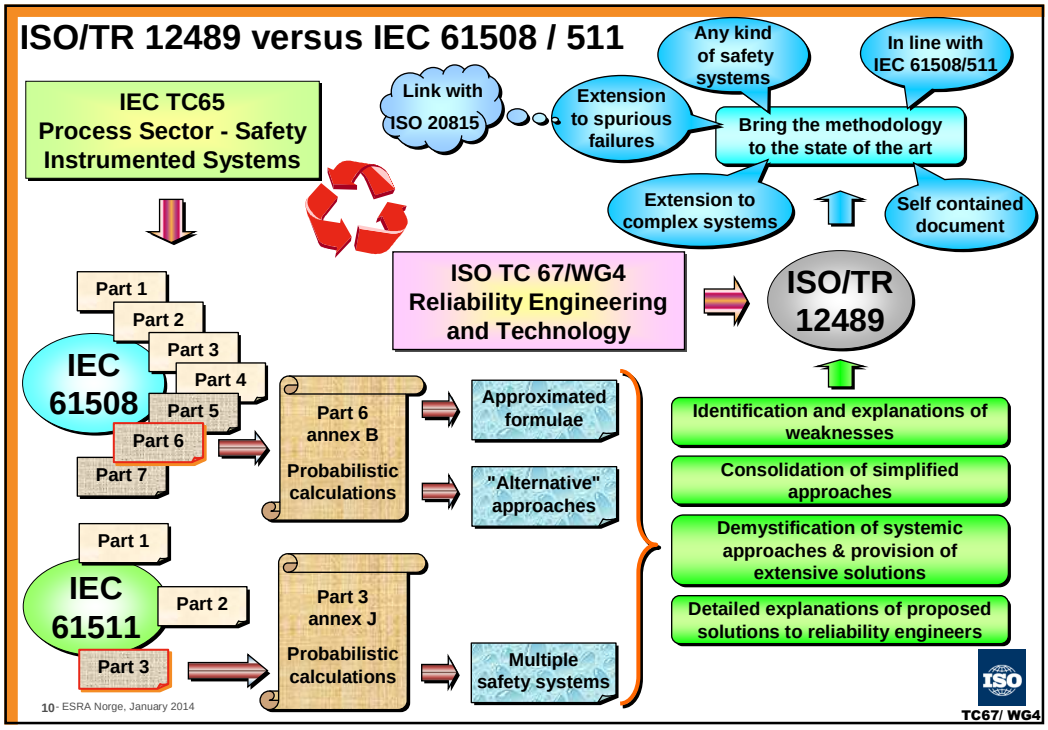


TC67/ WG4


Probabilistic models overview
50 years of experience
Analytical methods
SS
RAM & SS
Monte Carlo simulation
Developed when computers didn't exist
Taylor's expansion
Boolean approach
Markovian approach
Behavioral models
Petri nets
Formal languages
Formulae
FT
RBD
State Transition models (finite state automata)
Conser-vatism?
Specific formulae
Computer oriented
Generic tools
State of the art
Good understanding of models
Approximations
Lack of flexibility
Powerful algorithms
Graphical representations
A single framework for safety & dependability
Underlying hypothesis
Sound mathematics
Simplified approaches
Progress direction
Systemic Approaches
7 - ESRA Norge, January 2014
TC67/ WG4


Some examples of safety systems covered by ISO/TR 12489 (instrumented or not)
31 systems identified in the TR
PSD
EDP
ESD
Emergency / Process shutdown
Emergency communication
Public alarm systems
Flare system
HVAC
Material handling
Other utilities
HIPS
HIPPS
Pressure relief
Overpressure protection systems
Evacuation system
Emergency preparedness systems
Well integrity
Well completion
Drilling & wells
Gas detection
Fire fighting system
Fire water system
Fire & gas systems
Discon-nection system
Station keeping
Ballast water
Marine equipment
ESD
PSD
HIPPS
Subsea
Isolation
Diving
Control & monitoring
Chemical injection
Process control systems
UPS
Telecom.
Electrical & telecom. systems
Etc.
8 - ESRA Norge, January 2014
TC67/ WG4


From conventional Safety system to Safety Instrumented System
High Integrity (Pressure) Protection System
Over-Pressure
Conventional safety system
Relief Valve
Safety Instrumented System
PT3
PT2
PT1
L1
L2
Size
Cost
API 14C
IEC 61508
IEC 61511
Reliability?
9 - ESRA Norge, January 2014
TC67/ WG4


ISO/TR 12489 versus IEC 61508 / 511
IEC TC65 Process Sector - Safety Instrumented Systems
Link with ISO 20815
Extension to spurious failures
Any kind of safety systems
In line with IEC 61508/511
Bring the methodology to the state of the art
Extension to complex systems
Self contained document
ISO TC 67/WG4 Reliability Engineering and Technology
ISO/TR 12489
IEC 61508
Part 1
Part 2
Part 3
Part 4
Part 5
Part 6
Part 7
Part 6 annex B
Probabilistic calculations
Approximated formulae
"Alternative" approaches
IEC 61511
Part 1
Part 2
Part 3
Part 3 annex J
Probabilistic calculations
Multiple safety systems
Identification and explanations of weaknesses
Consolidation of simplified approaches
Demystification of systemic approaches & provision of extensive solutions
Detailed explanations of proposed solutions to reliability engineers
10 - ESRA Norge, January 2014
TC67/ WG4

Core of ISO/TR 12489

- Foreword
- Introduction
- 1-Scope → Framework, users and overview of the ISO/TR 12489 content
- 2-Analysis framework
- 3-Terms & definitions → Consolidation and explanations of definitions.
- 4-Symbols & abbreviations
- 5-Overview & challenges
- 6-Introduction to modelling & calculations

→ General considerations
Introduction to modelling & calculations
Difficulties & Warnings

TC67/ WG4

Core of ISO/TR 12489 (cont')

- 7- Analytical formulae → Mathematical development and explanations of approximate formulae
- 8- Boolean approach
- 9- Markovian approach
- 10- Petri Net approach
- 11- Monte Carlo simulation approach

What must be understood to use them in a relevant way

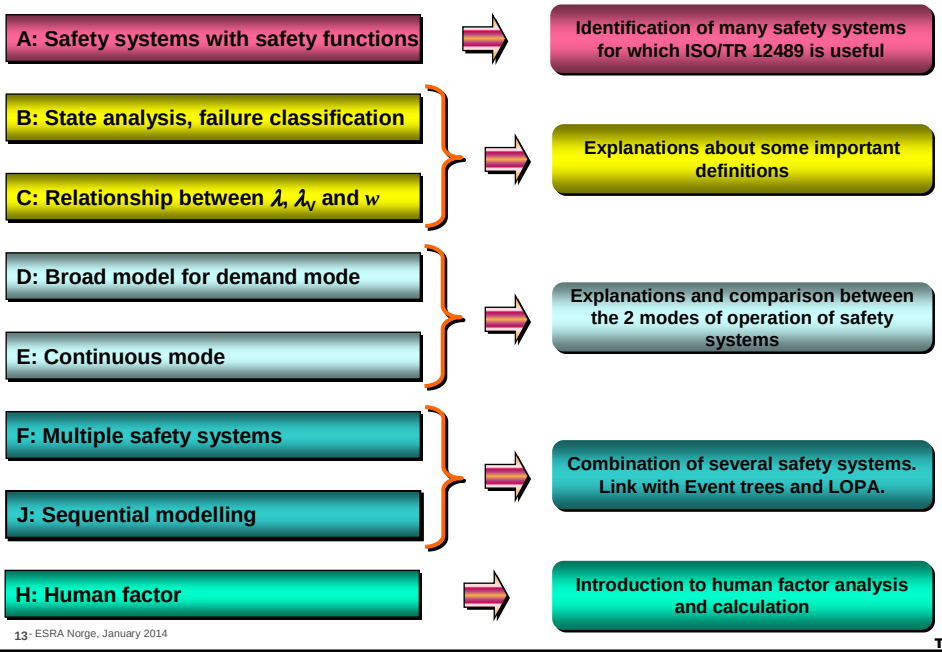
Comparisons

→ General description of systemic approaches. Main results

- 12- Numerical uncertainty handling → Introduction to numerical uncertainty handling
- 13- Reliability data considerations → Data sources, data collection, data needed. Link with ISO 14224
- 14- Typical applications → Comprehensive set of examples
- Bibliography → Comprehensive set of relevant documents

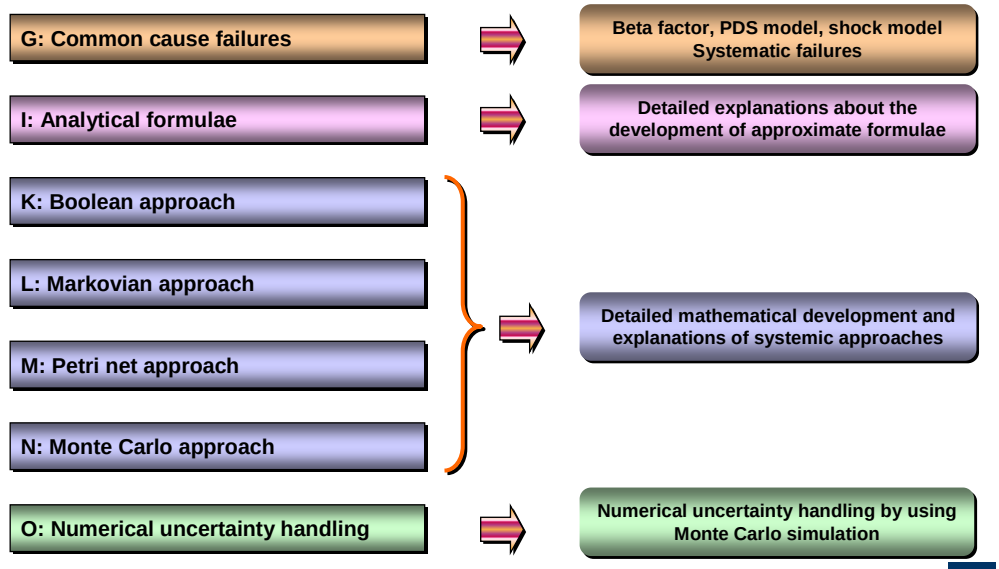
TC67/ WG4

Detailed annexes of ISO/TR 12489



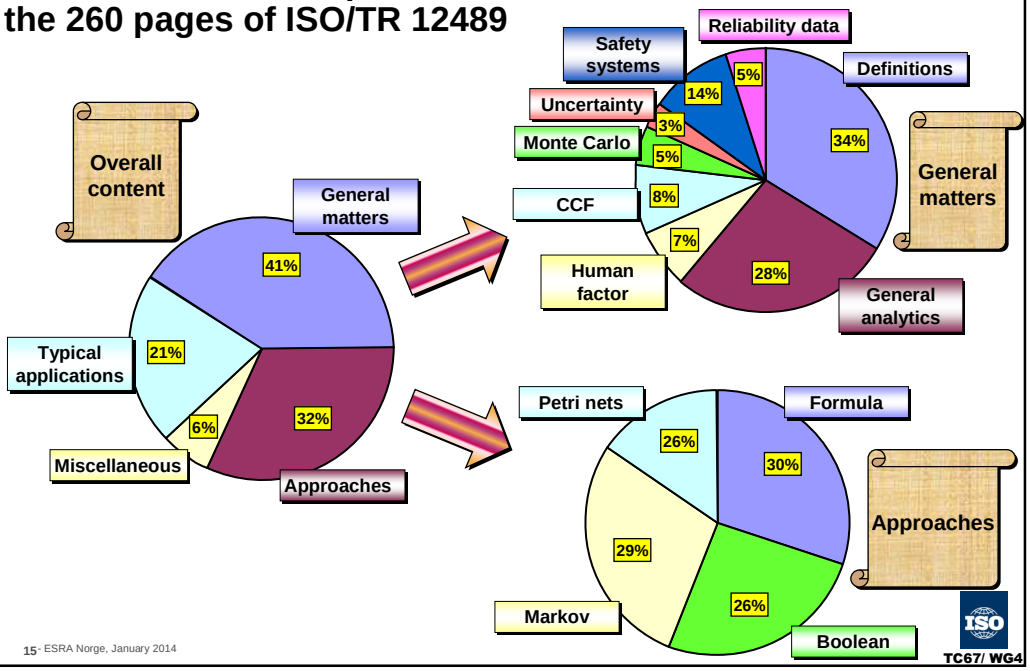
TC67/ WG4

Detailed annexes of ISO/TR 12489 (cont')



TC67/ WG4

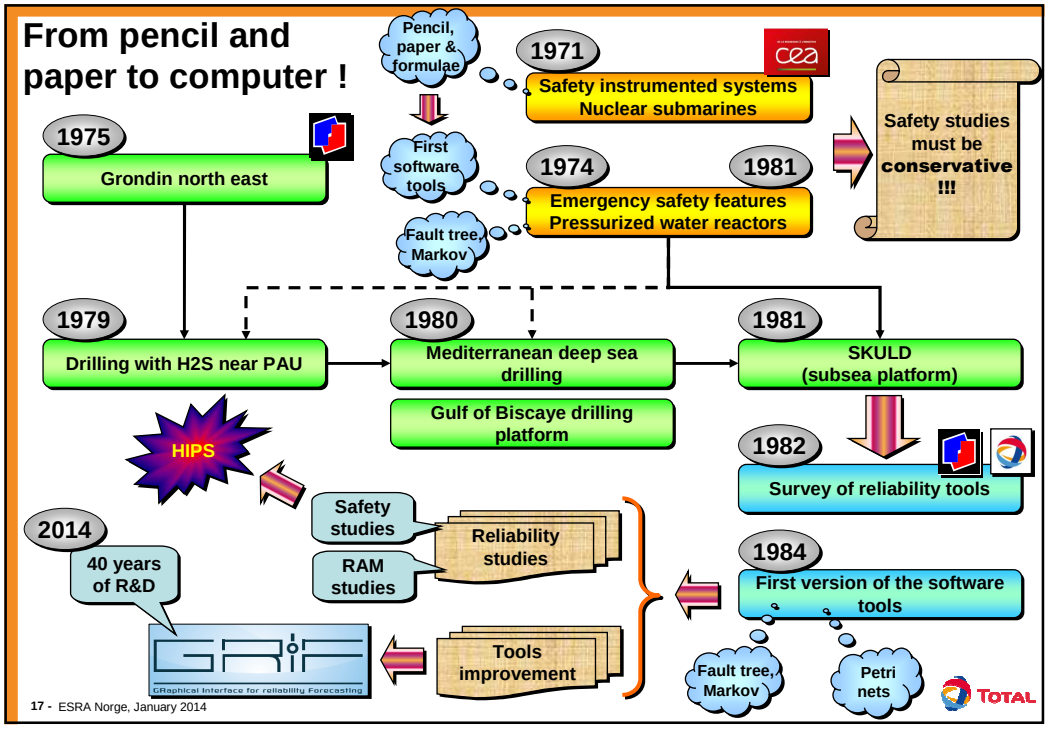
Distribution of the topics within the 260 pages of ISO/TR 12489

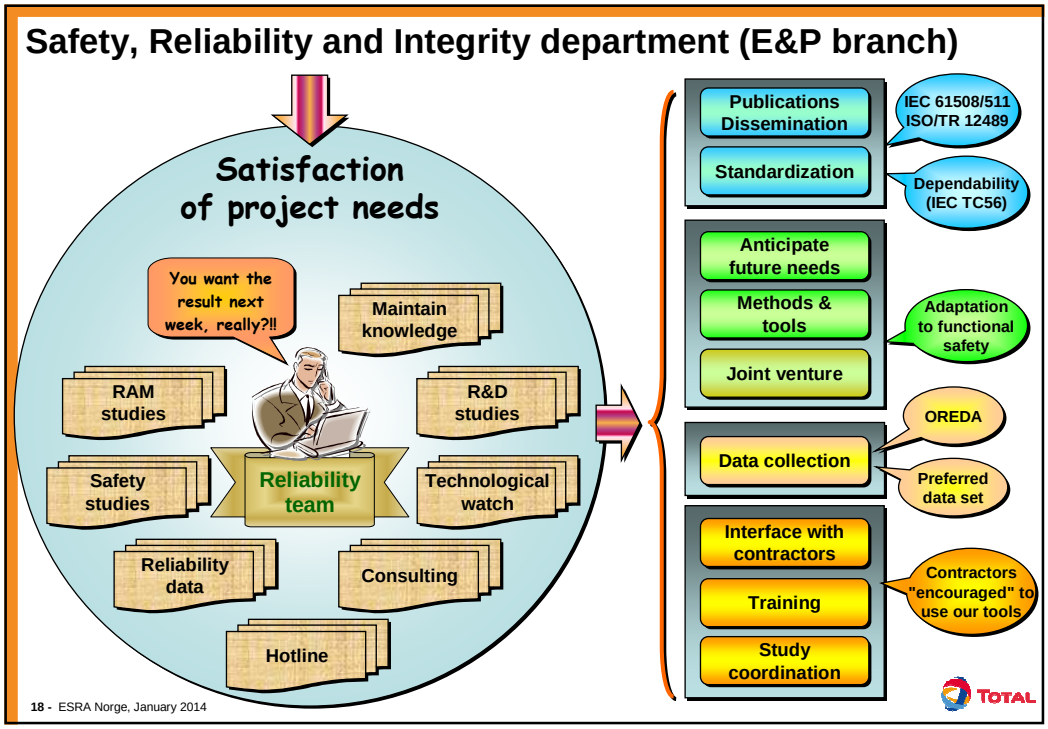


Application in TOTAL

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

Pierre-Joseph CACHEUX
Reliability expert, TOTAL


From pencil and paper to computer !
Pencil, paper & formulae
1971
Safety instrumented systems
Nuclear submarines
Safety studies must be conservative !!!
First software tools
1974
1981
Emergency safety features
Pressurized water reactors
Fault tree, Markov
1975
Grondin north east
1979
Drilling with H2S near PAU
1980
Mediterranean deep sea drilling
Gulf of Biscaye drilling platform
1981
SKULD (subsea platform)
HIPS
1982
Survey of reliability tools
2014
40 years of R&D
Safety studies
RAM studies
Reliability studies
1984
First version of the software tools
Tools improvement
Fault tree, Markov
Petri nets
GRaphical Interface for reliability Forecasting
17 - ESRA Norge, January 2014


Safety, Reliability and Integrity department (E&P branch)
Satisfaction of project needs
You want the result next week, really?!!
Maintain knowledge
RAM studies
R&D studies
Safety studies
Reliability team
Technological watch
Reliability data
Consulting
Hotline
Publications Dissemination
IEC 61508/511 ISO/TR 12489
Standardization
Dependability (IEC TC56)
Anticipate future needs
Methods & tools
Adaptation to functional safety
Joint venture
Data collection
OREDA
Preferred data set
Interface with contractors
Training
Study coordination
Contractors "encouraged" to use our tools
18 - ESRA Norge, January 2014

Examples of HIPS studies

Most of these HIPS are HIPPS

Classical studies

- ABK
- AL KHALIJ
- L4G
- OFON 2
- OML 100 WH
- MOHO BILONDO
- SP 11
- TP1 by pass
- AL JURF
- GIRASSOL
- etc.

Studies managed by Headquarters

Atypical studies

- AKPO anti surge
- OFON2
- OML 58
- BUFALO
- PECIKO
- BULISAA
- KAOMBO
- etc

KO-Drum overflow

Expertise & advices

- AKPO
- DALIA
- FORVIE
- HILD
- JAFRA
- ROSA-LIRIO
- KHARIR
- TIGF
- SHAH DENIZ
- etc.

TOTAL

Examples of RAM studies

Managed by Headquarters

- ADC
- AL JURF
- CLOV
- EGINA
- K5
- KCTS
- NKARIKA
- NKOSSA
- OML 100
- OML 58
- PAZFLOR
- PECIKO
- TIGF
- USAN
- YLNG
- PECIKO

- ABK
- AHNET
- ANGUILLE
- BUL HANINE
- DALIA
- KAOMBO
- KHARYAGA
- MARTIN LINGE
- MLJ
- MOHO
- MTPS
- PNGF
- South SULIGE
- TEMPA ROSSA
- VEGA PLEYADE

Expertise & advices

- KASHAGAN
- MOHO BILONDO
- QATAGAS
- DOLPHIN
- FLNG
- ICHTHYS
- JOSLYN
- LAGGAN
- TORMORE
- YAMAL LNG
- etc.

TOTAL

Why participating to functional safety standardization?

2005

Bad safety studies coming in Headquarters for advice

Discussions

Our studies **are very good:** they follow the standards !!

Your studies **are not good !!!**

Full development of reliability modelling & calculations

Project leader

Improvements in IEC 61508:2010

Participation to ISO/TR 12489 committees

Participation to IEC 61508 & 511 committees

Was not the state of the art in probabilistic calculations

Analysis of IEC 61508 and IEC 61511

"*Common cause failure*": IEC 61508-6 Annex B Edition 1

Adaptation of our software tool GRIF

TOTAL

Calculations : IEC 61508 Part 6 ed1

stop !!!

It is "informative" not "normative"

Who really understand those formulae ?

Correct but ...

A catalogue is not really a "method"

Introduced in IEC 61508 Ed2

Nothing about developing formulae

Not general

Difficult to use

Difficult to improve

Hypotheses ignored

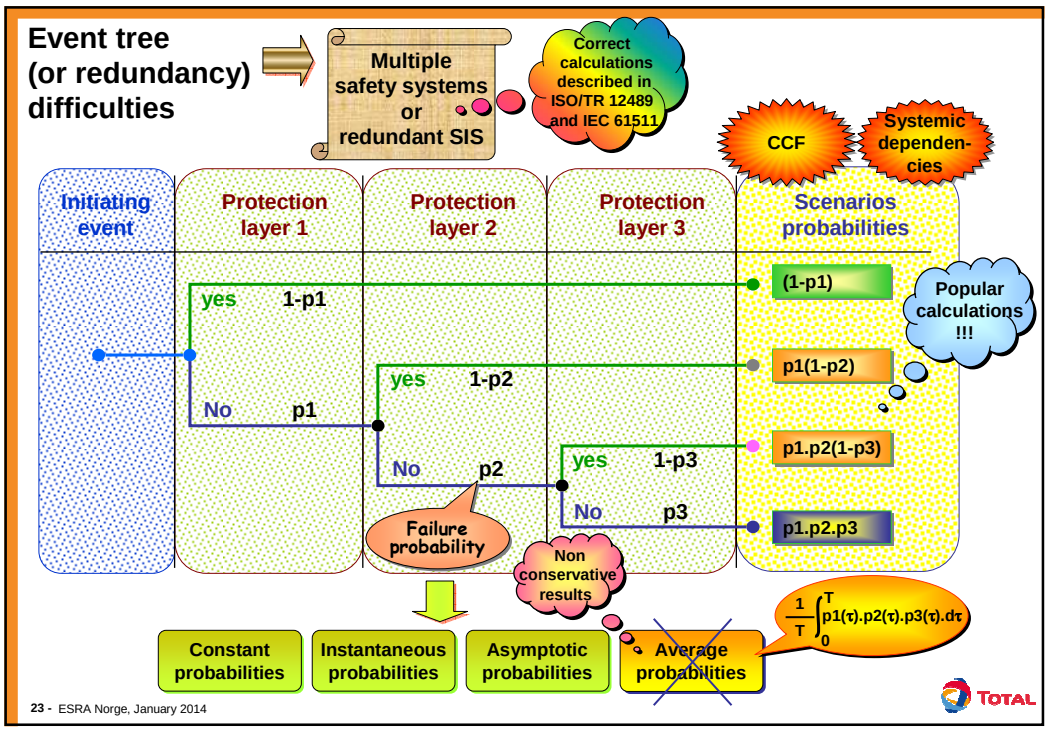
Not adapted for a complex system

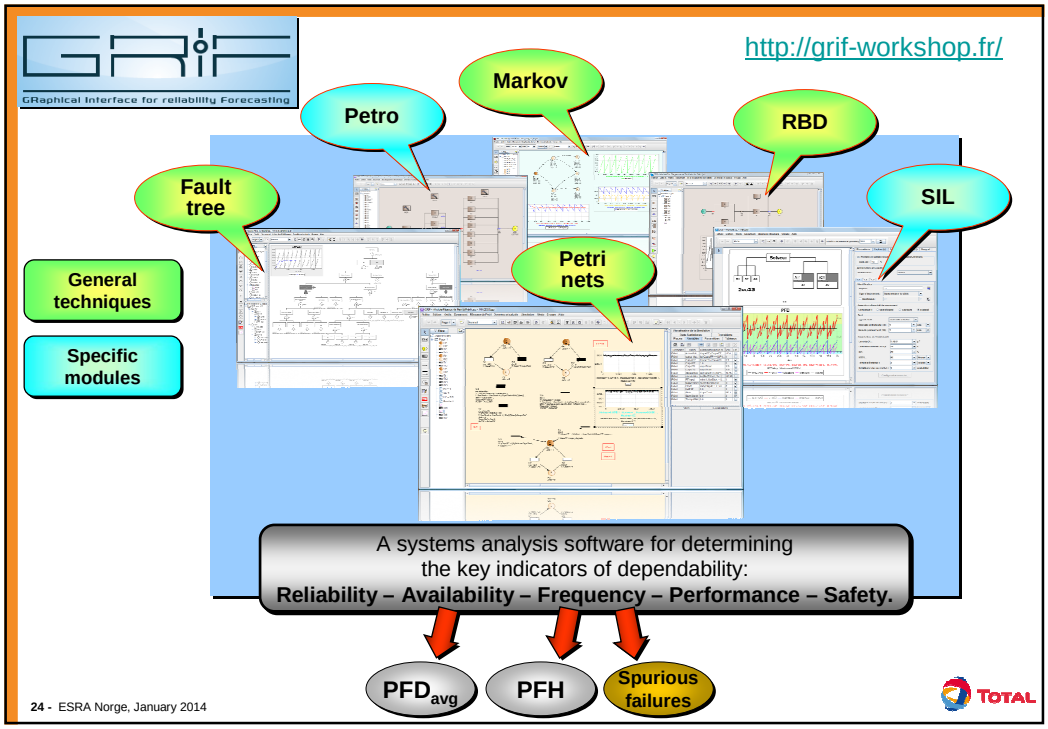
Boolean models

State transition models

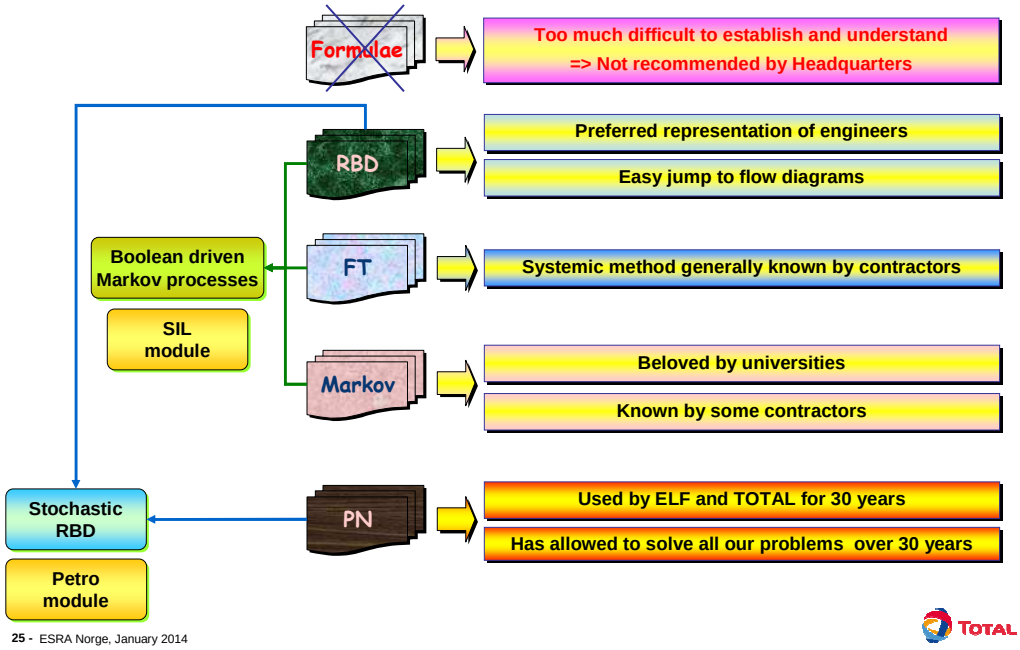
Go back to conventional calculation models

TOTAL


Event tree (or redundancy) difficulties
Multiple safety systems or redundant SIS
Correct calculations described in ISO/TR 12489 and IEC 61511
CCF
Systemic dependen-cies
Initiating event
Protection layer 1
Protection layer 2
Protection layer 3
Scenarios probabilities
yes
1-p1
No
p1
yes
1-p2
No
p2
yes
1-p3
No
p3
(1-p1)
p1(1-p2)
p1.p2(1-p3)
p1.p2.p3
Popular calculations !!!
Failure probability
Non conservative results
Constant probabilities
Instantaneous probabilities
Asymptotic probabilities
Average probabilities
$\frac{1}{T}\int_0^T p1(\tau).p2(\tau).p3(\tau).d\tau$
23 - ESRA Norge, January 2014
TOTAL

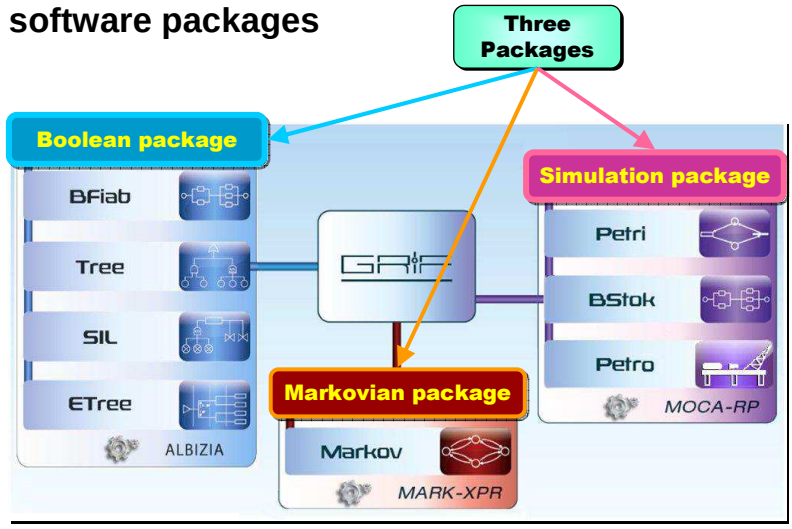

GRaphical Interface for reliability Forecasting
http://grif-workshop.fr/
Petro
Markov
RBD
Fault tree
SIL
Petri nets
General techniques
Specific modules
A systems analysis software for determining the key indicators of dependability:
Reliability – Availability – Frequency – Performance – Safety.
PFDavg
PFH
Spurious failures
24 - ESRA Norge, January 2014
TOTAL

Why those techniques have been chosen?



TOTAL

GRIF software packages

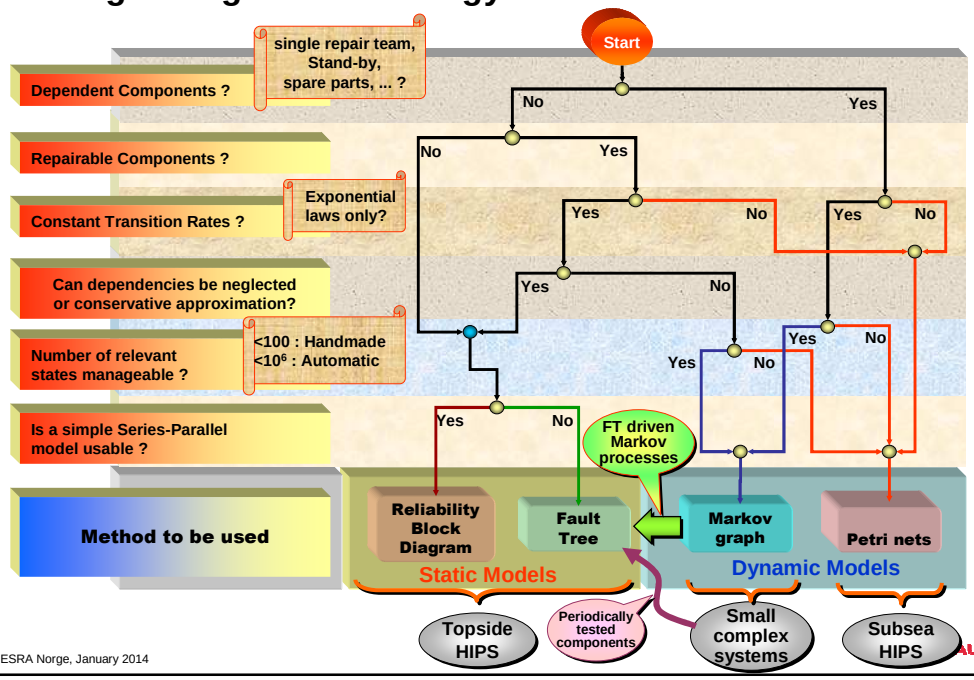


Enables to choose the most suitable modelling technique.

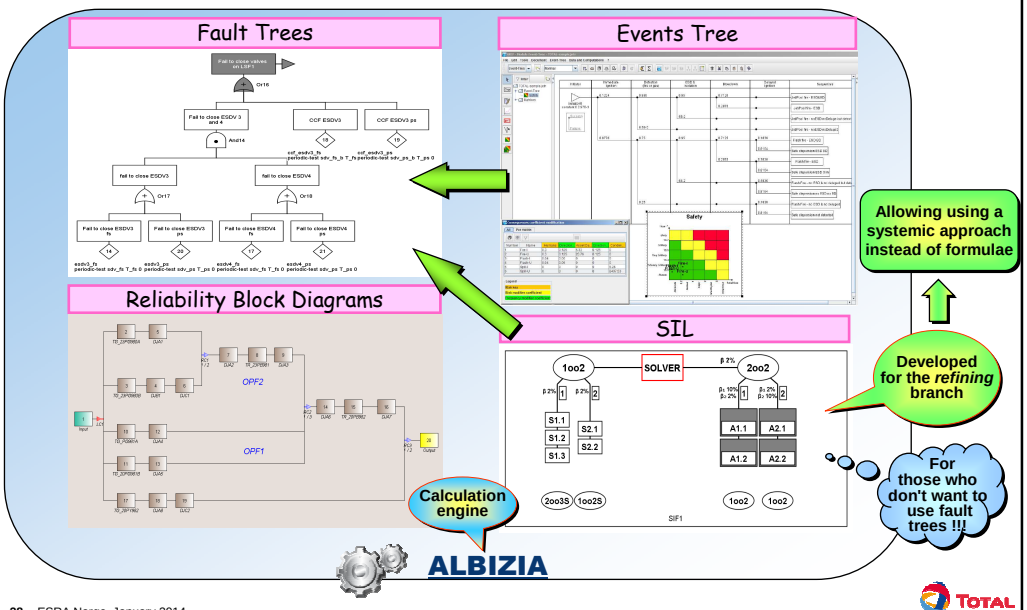
Includes pre-configured architectures, making modelling all the easier.

TOTAL

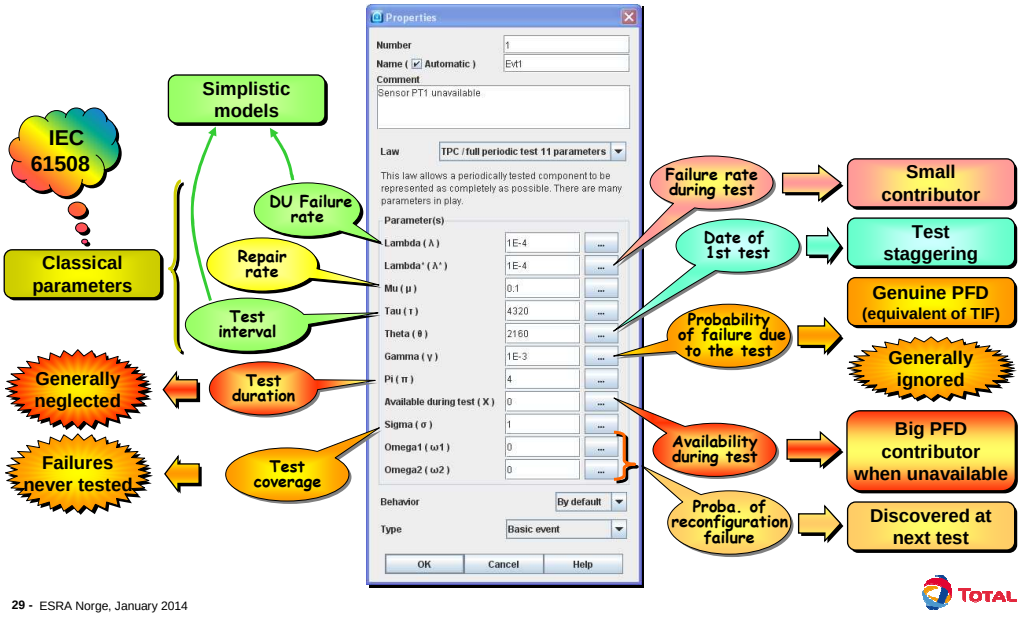
Choosing the right methodology



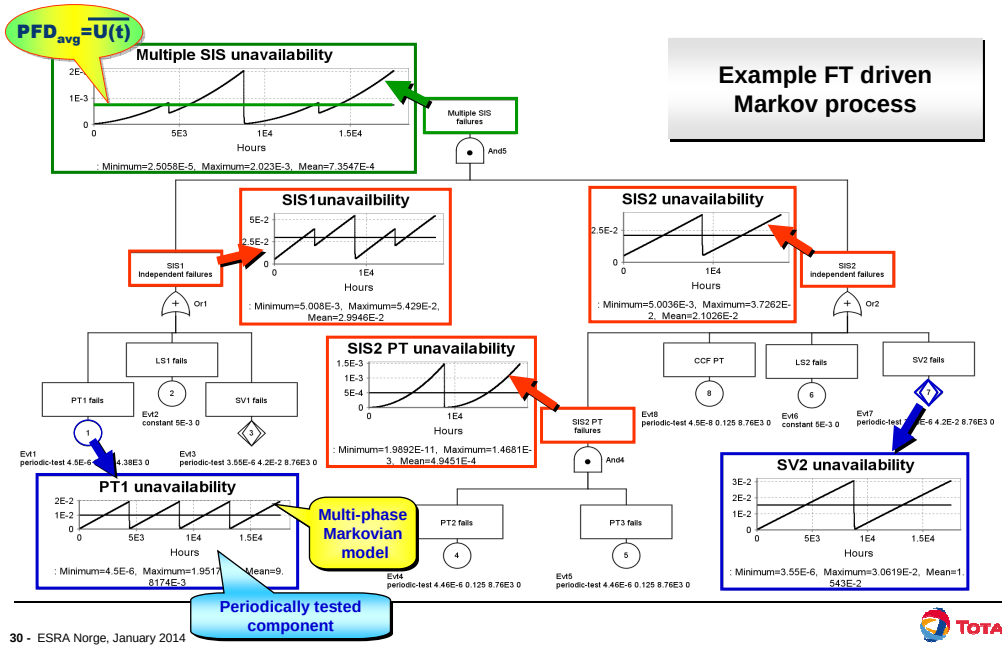
Boolean package

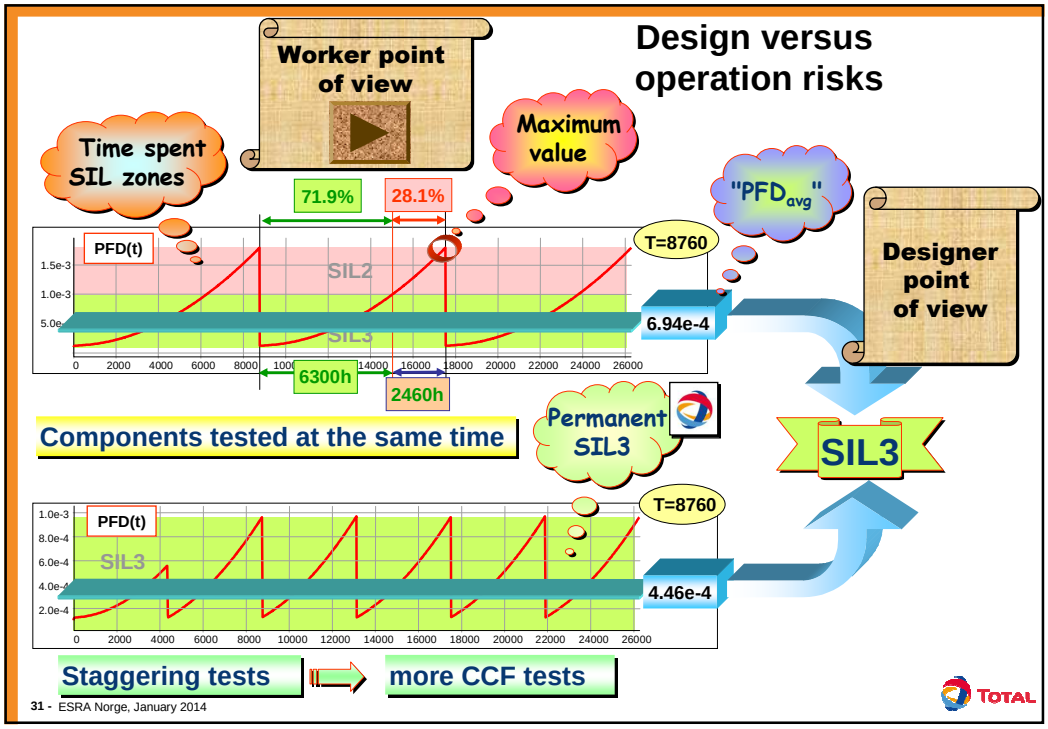


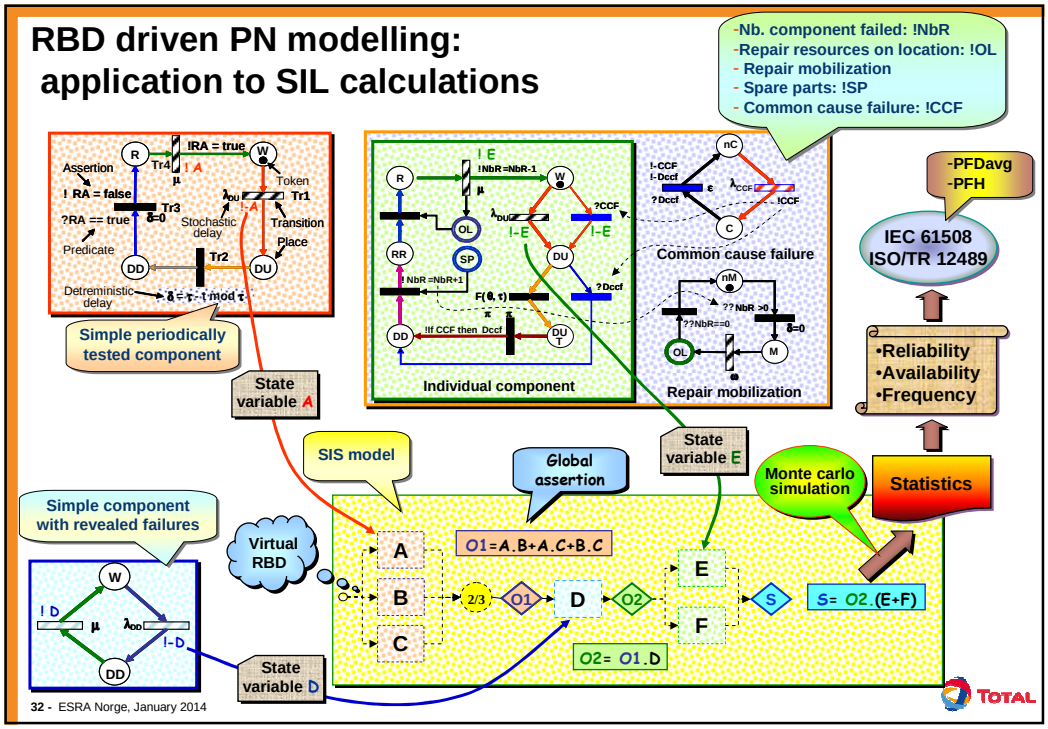
Parameters of a periodically tested component (dangerous undetected failures)



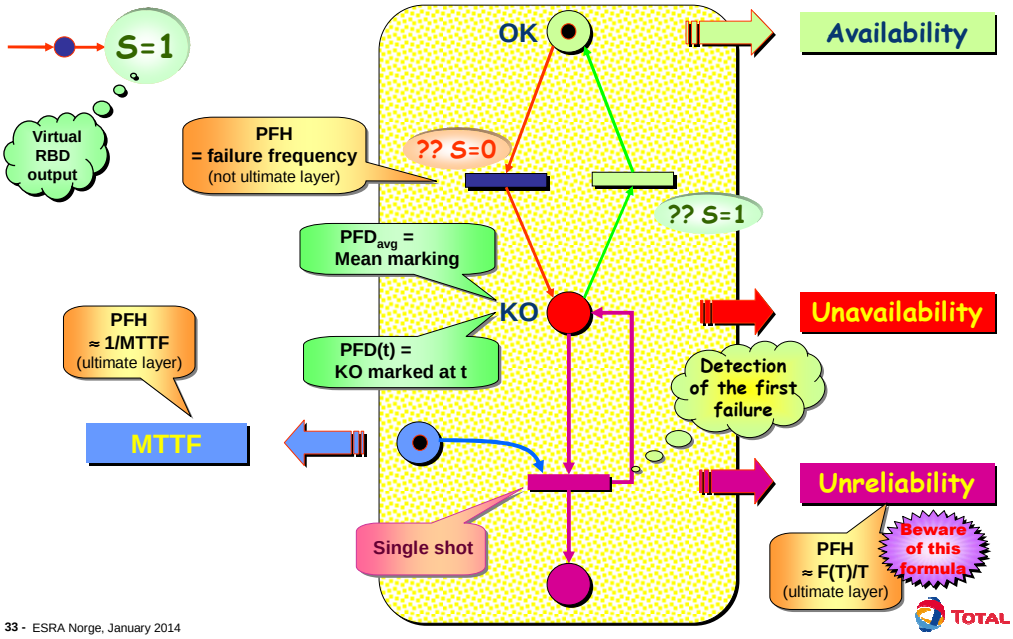
PFD_{avg} (Average unavailability) calculated by fault tree:




Design versus operation risks
Worker point of view
Time spent SIL zones
Maximum value
71.9%
28.1%
"PFDavg"
Designer point of view
PFD(t)
SIL2
SIL3
T=8760
6.94e-4
6300h
2460h
Components tested at the same time
Permanent SIL3
SIL3
PFD(t)
SIL3
T=8760
4.46e-4
Staggering tests
more CCF tests
31 - ESRA Norge, January 2014
TOTAL

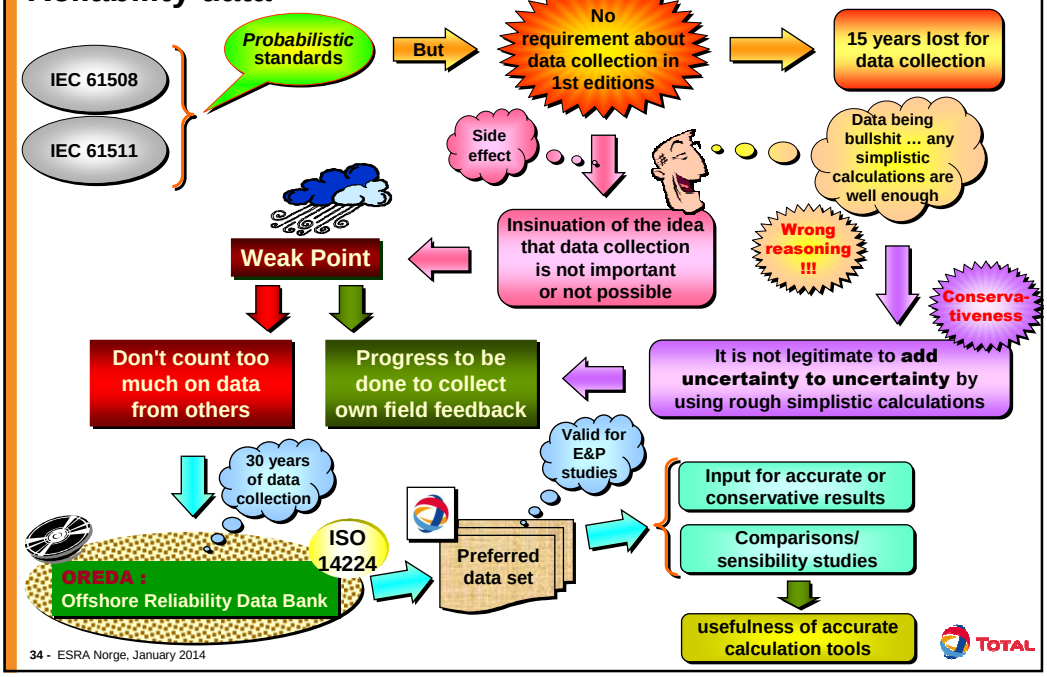

RBD driven PN modelling:
application to SIL calculations
-Nb. component failed: !NbR
-Repair resources on location: !OL
- Repair mobilization
- Spare parts: !SP
- Common cause failure: !CCF
-PFDavg
-PFH
IEC 61508
ISO/TR 12489
•Reliability
•Availability
•Frequency
Simple periodically tested component
State variable A
Individual component
Common cause failure
Repair mobilization
SIS model
Global assertion
State variable E
Monte carlo simulation
Statistics
Simple component with revealed failures
Virtual RBD
O1=A.B+A.C+B.C
O2= O1.D
S= O2.(E+F)
State variable D
32 - ESRA Norge, January 2014
TOTAL

Parameter calculations: The *magic* sub PN!

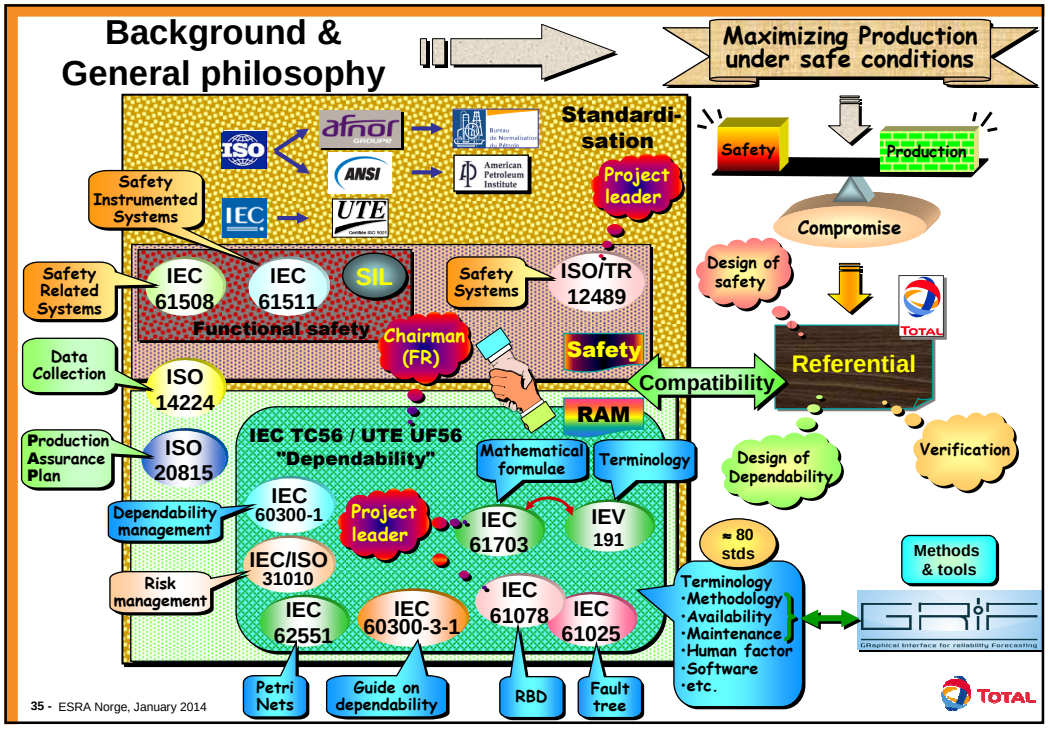


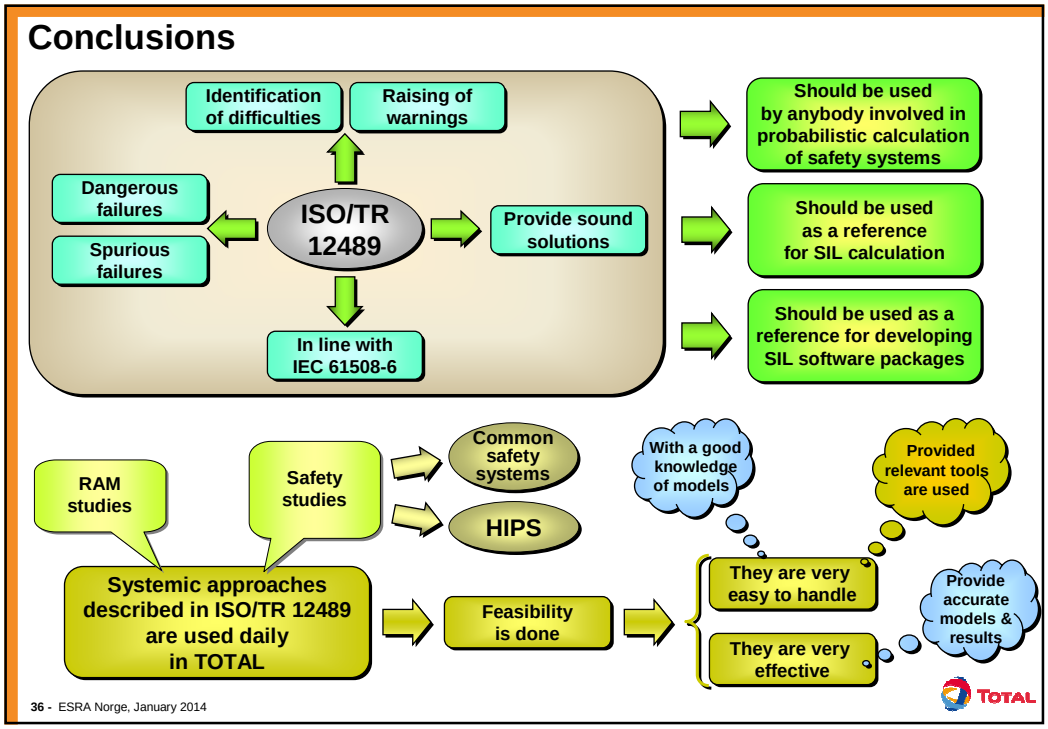
TOTAL

Reliability data



TOTAL


Background & General philosophy
Maximizing Production under safe conditions
Standardi-sation
Safety
Production
Compromise
Safety Instrumented Systems
Safety Related Systems
IEC 61508
IEC 61511
SIL
Functional safety
Safety Systems
ISO/TR 12489
Project leader
Chairman (FR)
Safety
Design of safety
Referential
Compatibility
Data Collection
ISO 14224
RAM
Production Assurance Plan
ISO 20815
IEC TC56 / UTE UF56 "Dependability"
Mathematical formulae
Terminology
Design of Dependability
Verification
Dependability management
IEC 60300-1
Project leader
IEC 61703
IEV 191
≈ 80 stds
Methods & tools
Risk management
IEC/ISO 31010
IEC 62551
IEC 60300-3-1
IEC 61078
IEC 61025
Terminology
·Methodology
·Availability
·Maintenance
·Human factor
·Software
·etc.
Petri Nets
Guide on dependability
RBD
Fault tree
35 - ESRA Norge, January 2014

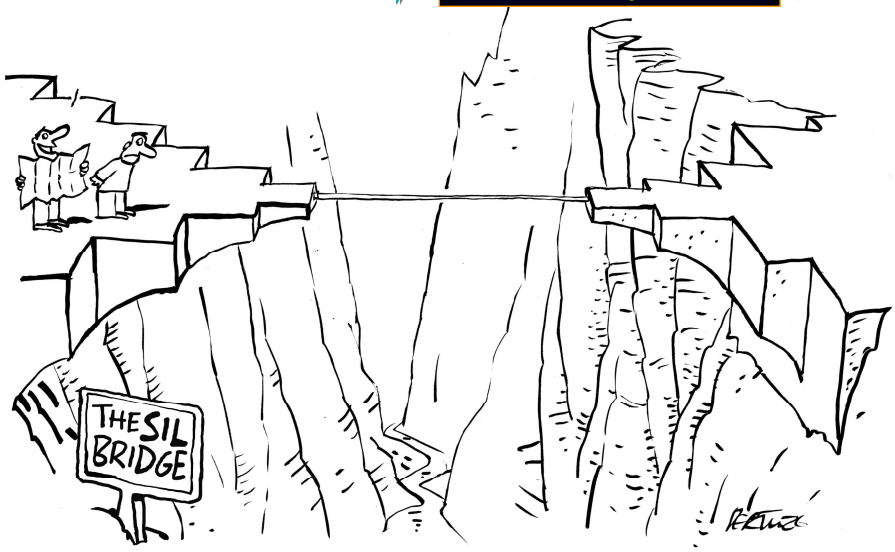

Conclusions
Identification of difficulties
Raising of warnings
Dangerous failures
Spurious failures
ISO/TR 12489
Provide sound solutions
In line with IEC 61508-6
Should be used by anybody involved in probabilistic calculation of safety systems
Should be used as a reference for SIL calculation
Should be used as a reference for developing SIL software packages
RAM studies
Safety studies
Common safety systems
HIPS
Systemic approaches described in ISO/TR 12489 are used daily in TOTAL
Feasibility is done
With a good knowledge of models
Provided relevant tools are used
They are very easy to handle
They are very effective
Provide accurate models & results
36 - ESRA Norge, January 2014

Any questions ?...

TOTAL

SIL Bridge !

PFDavg is not a good indicator for worker in operation



TOTAL