Design of complex safety-related systems in accordance with IEC 61508

F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier
French National Institute for Industrial Environment and Risk
& Troyes University of Technology

ESREL 2009 Annual Conference
7-10 September 2009, Prague, Czech Republic

utt université de technologie Troyes

INERIS

Overview

I. Introduction & IEC 61508

- safety systems & IEC 61508 framework
- introduction to design & development of complex systems

II. Design of complex systems

- reliability issues for complex systems
- fault tree based approach to deal with complex systems

III. Application

- case study on infrared gas transmitter
- reliability and uncertainty analyses

IV. Discussion & conclusion

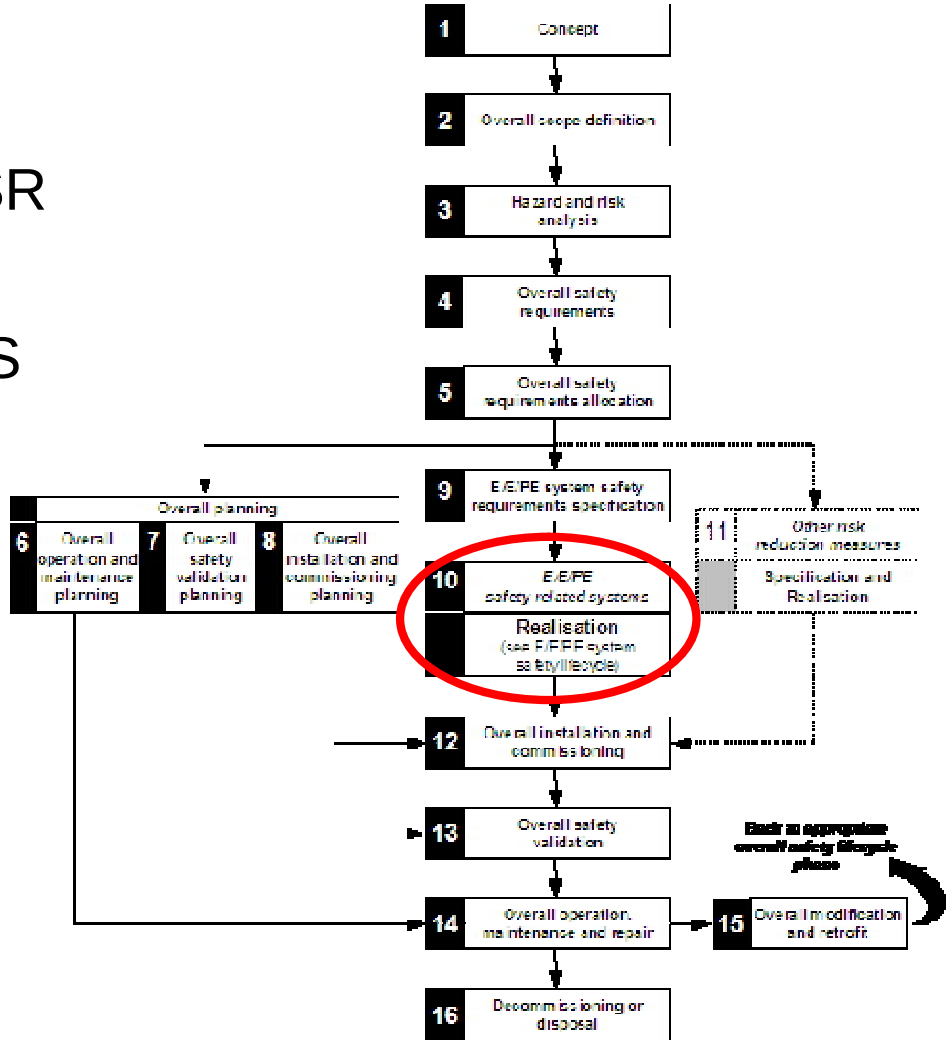
I. Introduction & IEC 61508 1/3

- **Safety instrumented systems (SIS)**
  - play a major part in industrial risk management
- **IEC 61508**
  - generic functional safety standard for SIS design
  - considers the overall system and software life cycle
  - introduces safety requirements (SR)
    - ***safety function***: to achieve a safe state of equipment under control
    - ***safety integrity***: probability of a SIS performing the safety function
  - ***safety integrity level*** (SIL)

SIL	Average probability of SIS failure to perform its safety function on demand (PFD_{avg})
SIL 4	$10^{-5} \leq PFD_{avg} < 10^{-4}$
SIL 3	$10^{-4} \leq PFD_{avg} < 10^{-3}$
SIL 2	$10^{-3} \leq PFD_{avg} < 10^{-2}$
SIL 1	$10^{-2} \leq PFD_{avg} < 10^{-1}$

I. Introduction & IEC 61508 2/3

- **IEC 61508 framework**
  - development of the overall SR
  - SR allocation to the SIS
  - SR specification for each SIS
  - ***SIS design & development***
  - installation, validation
  - operation, maintenance
- **Other requirements**
  - documentation
  - management
  - verification
- **Informative guidelines**



I. Introduction & IEC 61508 3/3

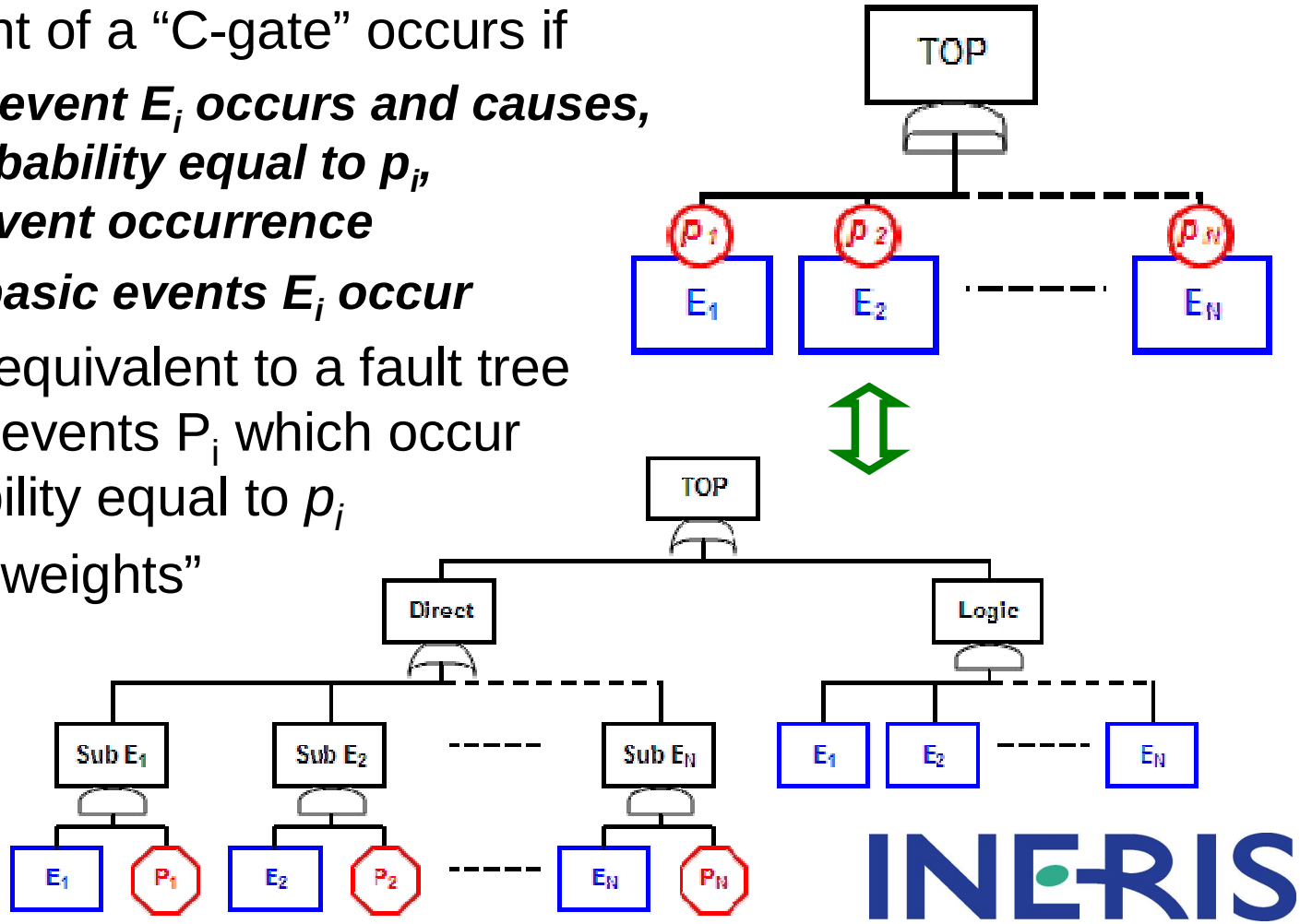
- **Requirements for SIS design & development**
  - hardware fault tolerance (HFT)
  - safe failure fraction (SFF)
  - ***average probability of SIS failure on demand (PFD_{avg})***
  - avoidance of the systematic faults, proven in use
  - some other specific requirements
- **Complex system (IEC 61508)**
  - ***not well defined failure mode*** for at least one component
  - or ***undetermined system behaviour under faulty conditions***
- **"Type B" system (IEC 61508)**
  - insufficient data to support claims for failure rates
  - or complex system

II. Design of complex systems 1/3

- **Reliability issues for “type B” systems**
  - many references deal with uncertainty on failure rates
    - e.g. comparison of data sources, Monte Carlo, fuzzy sets, etc.
  - fewer analyses regarding ***uncertainty into system behaviour***
- **Limitations of reliability models**
  - system responses to events have to be strictly defined…
  - …according to architectural constraints of discrete nature
    - e.g. fault tree gates, Markov graph states and transitions
  - random changes in models could yield unrealistic configurations
- **Proposal**
  - ***system behaviour should be parameterised so that the system part architectures can be continuously graduated***

II. Design of complex systems 2/3

- **Continuous gate for fault tree based approach**
  - the TOP-event of a “C-gate” occurs if
    - ***any basic event E_i occurs and causes, with a probability equal to p_i, the TOP-event occurrence***
    - or ***all the basic events E_i occur***
  - a “C-gate” is equivalent to a fault tree with fictitious events P_i which occur with a probability equal to p_i
  - p_i are called “weights”

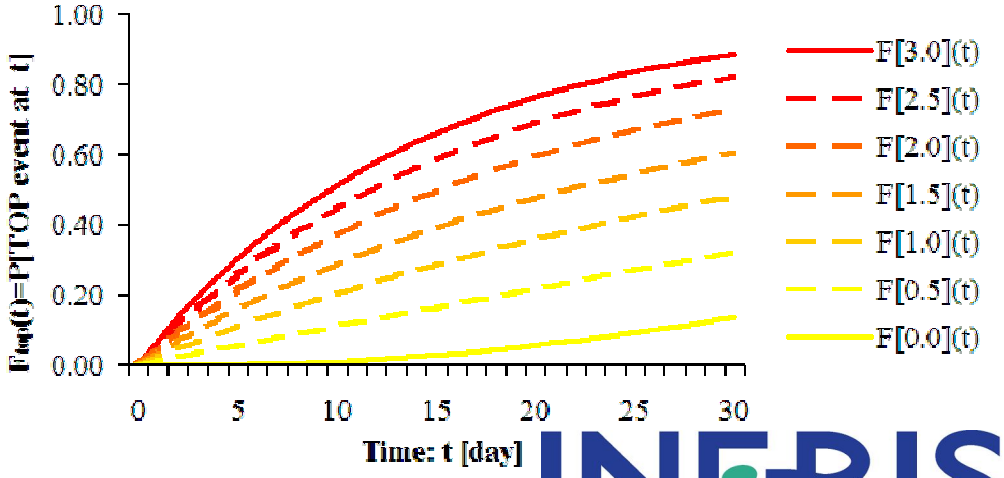


II. Design of complex systems 3/3

- **Continuous gate properties**
  - $F_i(t)$ probability of occurrence of basic event E_i at time *t*
  - p_i constant probability of occurrence of fictitious event P_i
  - $F_{top}(t)$ probability of occurrence of C-gate TOP-event at time *t*

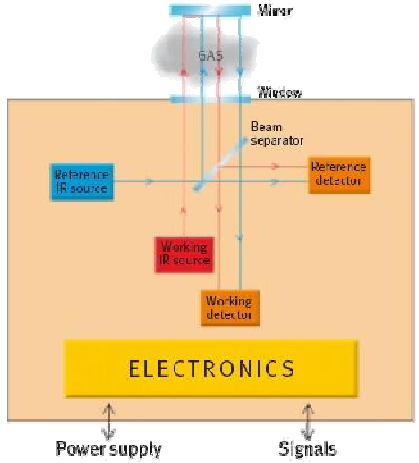
$$F_{top}(t) = 1 - \prod_{i=1}^{N} \left(1 - p_i \cdot F_i(t)\right) + \prod_{i=1}^{N} \left((1 - p_i) \cdot F_i(t)\right)$$

Weight			Unreliability function
p_1	p_2	p_3	
0	*0*	*0*	F[0.0](t) / parallel structure
0.5	*0*	*0*	F[0.5](t)
0.5	*0.5*	*0*	F[1.0](t)
0.5	*0.5*	*0.5*	F[1.5](t)
1	*0.5*	*0.5*	F[2.0](t)
1	*1*	*0.5*	F[2.5](t)
1	*1*	*1*	F[3.0](t) / series structure

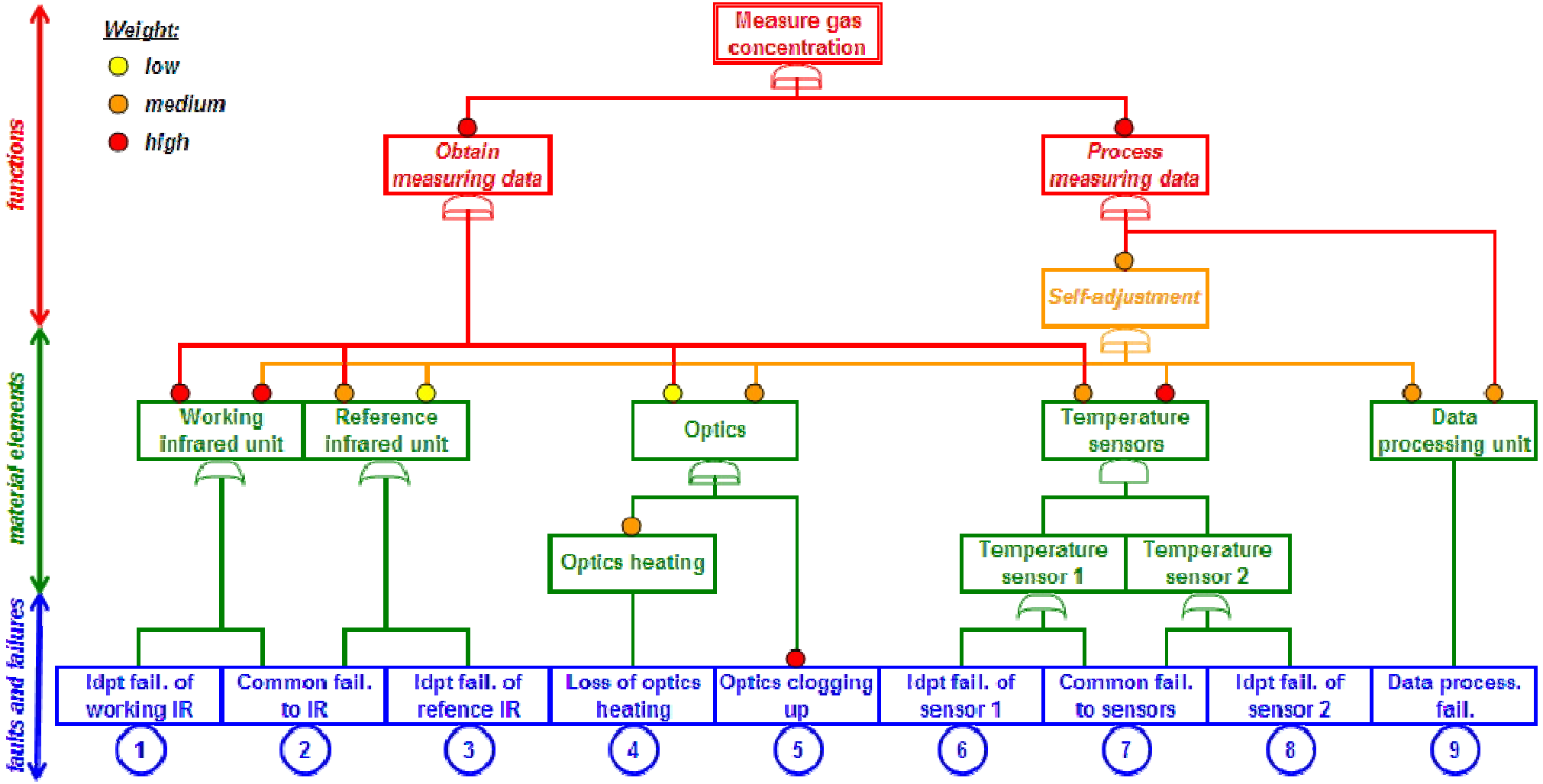


III. Application 1/5

- **Case study on infrared gas transmitter**
  - to measure gas concentration by infrared absorption
  - the use of a working and a reference infrared units allows corrections of the optics clogging up and power fluctuations
  - heating elements aim to prevent steam from building up on optics
  - redundant temperature sensors are used for digital compensation
  - a data processing unit carries out all processing and calculations
  - off-set and gain drift parameters are defined by self-adjustments



III. Application

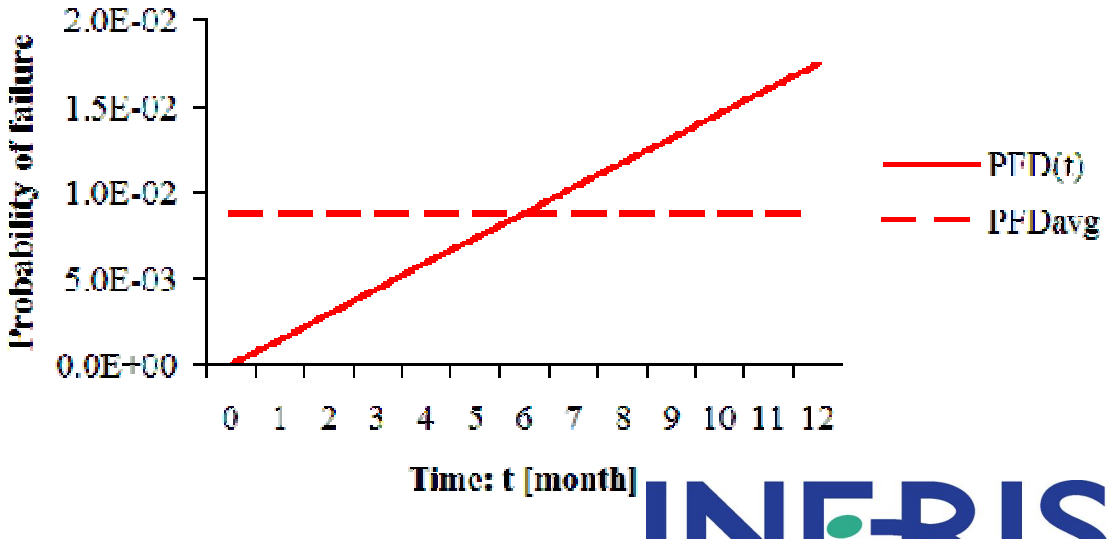


III. Application

- **Fault tree analyses**
  - input data:
    - $\{p_L, p_M, p_H\}$ weigh value according to type
    - $F_i(t) = exp(-\lambda_i \cdot t)$ probability of fault or failure occurrence *i* at time *t*
  - analyses are performed using equivalent fault trees and SimTree from Aralia WorkShop software tool

Type	Name	Base value
low	p_L	*0.10*
medium	p_M	*0.50*
high	p_H	*0.90*

Name	Base value [hour^{-1}]
λ_1	$4.0 \cdot 10^{-7}$
λ_2	$1.0 \cdot 10^{-7}$
λ_3	$4.0 \cdot 10^{-7}$
λ_4	$1.0 \cdot 10^{-6}$
λ_5	$3.0 \cdot 10^{-6}$
λ_6	$5.0 \cdot 10^{-7}$
λ_7	$1.5 \cdot 10^{-7}$
λ_8	$5.0 \cdot 10^{-7}$
λ_9	$5.0 \cdot 10^{-7}$



III. Application 4/5

- **Uncertainty analyses: input data**
  - failure rate uncertainties are represented by lognormal distributions with error factors equal to *5*
  - system behaviour uncertainties are translated into weight value uncertainties and are represented by uniform distributions
  - ***variances are greater for weight values than for failure rates***

Name	Uncertainty analysis		
	law	mean	variance
λ_1	log-Normal	$4.0 \cdot 10^{-7}$	$3.2 \cdot 10^{-14}$
λ_2	log-Normal	$1.0 \cdot 10^{-7}$	$2.0 \cdot 10^{-15}$
λ_3	log-Normal	$4.0 \cdot 10^{-7}$	$3.2 \cdot 10^{-14}$
λ_4	log-Normal	$1.0 \cdot 10^{-6}$	$2.0 \cdot 10^{-13}$
λ_5	log-Normal	$3.0 \cdot 10^{-6}$	$1.8 \cdot 10^{-12}$
λ_6	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$
λ_7	log-Normal	$1.5 \cdot 10^{-7}$	$4.5 \cdot 10^{-15}$
λ_8	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$
λ_9	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$

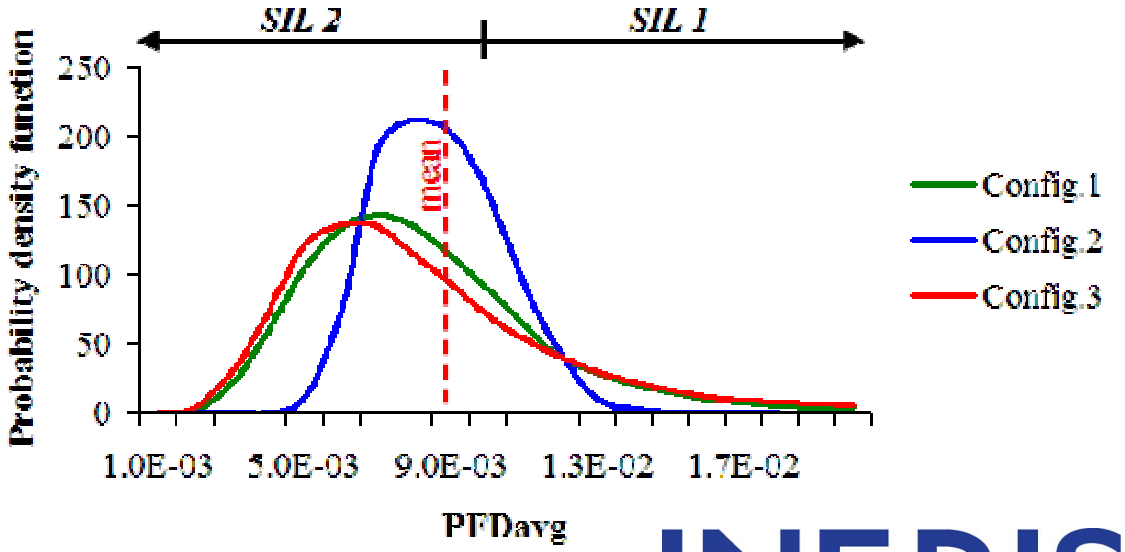
Type	Name	Uncertainty analysis		
		law	mean	variance
low	p_L	U[*0.0*, *0.2*]	*0.10*	$3.3 \cdot 10^{-3}$
medium	p_M	U[*0.2*, *0.8*]	*0.50*	$3.0 \cdot 10^{-2}$
high	p_H	U[*0.8*, *1.0*]	*0.90*	$3.3 \cdot 10^{-3}$

III. Application 5/5

- **Uncertainty analyses: results**
  - three configurations are compared
  - each analysis is performed by 1,000,000 Monte Carlo simulations
  - ***variances are much lower for results than for any input***
  - ***uncertainties into system behaviour are not significant***

Configuration	Uncertainty analysis on
Config.1	Failure rates only
Config.2	System behaviour (i.e. weight values) only
Config.3	Failure rates and system behaviour

Configuration	Mean	Variance	P[SIL2]	P[SIL1]
Config.1	$8.69 \cdot 10^{-3}$	$1.5 \cdot 10^{-5}$	0.74	0.26
Config.2	$8.73 \cdot 10^{-3}$	$2.9 \cdot 10^{-6}$	0.78	0.22
Config.3	$8.68 \cdot 10^{-3}$	$2.0 \cdot 10^{-5}$	0.74	0.26



IV. Discussion & conclusion 1/1

- **Uncertainties into system behaviour**
  - can be taken into account by continuous fault tree gates
  - can be translated into equivalent fault trees using fictitious events
- **Discussion of results**
  - taking the system behaviour uncertainties into account leads to PFD_{avg} evaluation with a relatively small variance
  - uncertainties into inputs, especially for weight values, are partially mitigated through the proposed model
  - assuming uncertainties into failure rates, the addition of system behaviour uncertainties does not have a significant effect
- **the lack of knowledge in system behaviour can be accounted for and partially compensated for by the proposed approach to evaluate PFD_{avg}**

Thanks for your attention

Questions & Comments are Welcome

florent.brissaud@ineris.fr

ESREL 2009 Annual Conference
7-10 September 2009, Prague, Czech Republic

utt université de technologie Troyes

INERIS