An *a posteriori* estimation of the performance level for a safety function using *NF EN ISO 13849-1:2008*

Sabrina JOCELYN, ing. jr., M.Sc.A.
Mechanical and Physical Risk Prevention

With the collaboration of
James Baudoin, INRS
Philippe Charpentier, INRS
Yuvin Chinniah, Polytechnique

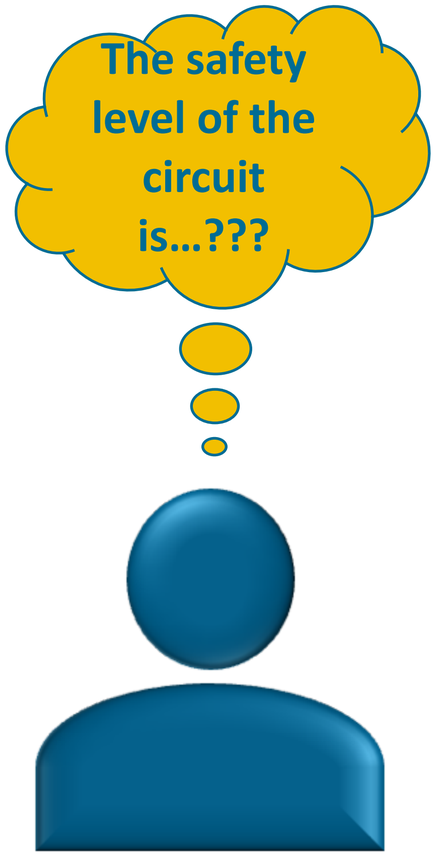
With the collaboration of

- James BAUDOIN

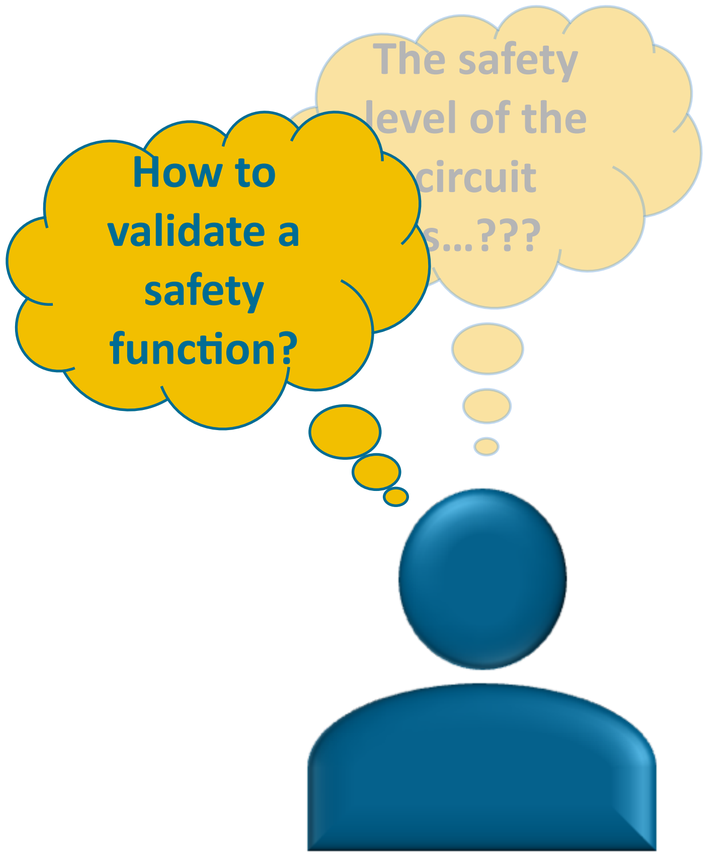
- Philippe CHARPENTIER

- Yuvin CHINNIAH

Issue & aim



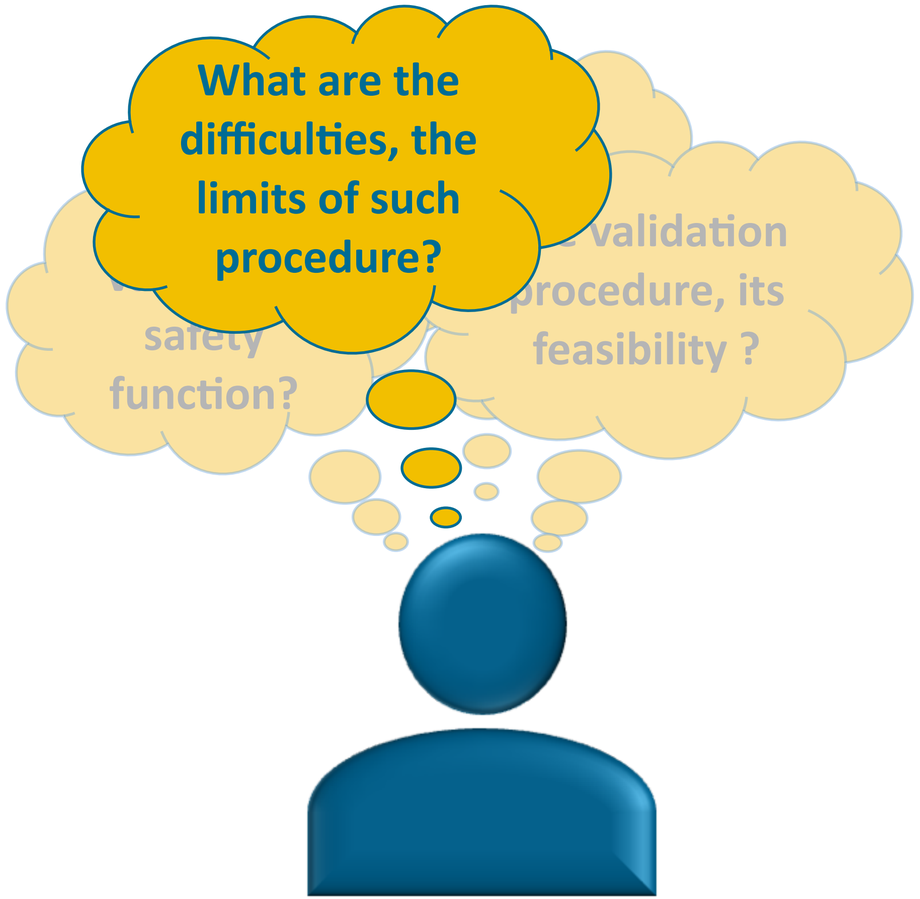
Issue & aim


The safety level of the circuit s…???
How to validate a safety function?

Issue & aim


The safety level of the
How to validate a safety function?
The validation procedure, its feasibility ?

Issue & aim


What are the difficulties, the limits of such procedure?
validation procedure, its feasibility ?
safety function?

Plan

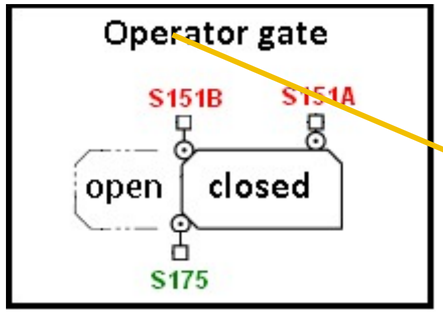
- A brief presentation of the validation procedure:
  - Preliminary steps
  - Subsequent steps
- Results of the validation procedure
- Assumptions made and impacts

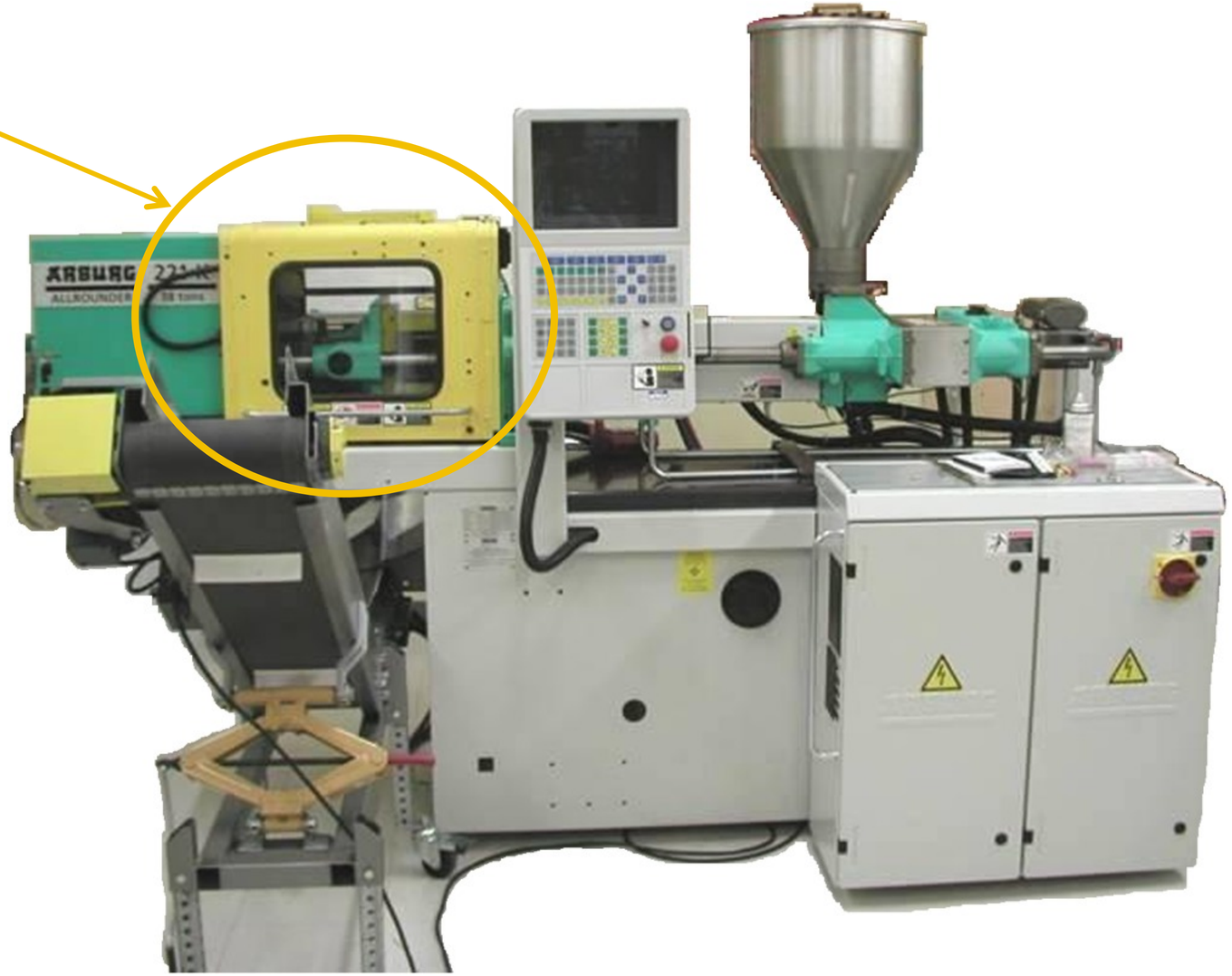
The validation procedure

Preliminary steps

- The safety function: Identification and specification
- Choice of the standard
- The required safety level?

The safety function





*"**Stopping** the **closing movement of** the movable **platen when opening** the operator **gate**"*

Choice of the standard

Hydraulic
and
electrical
safety function

2 types of energy

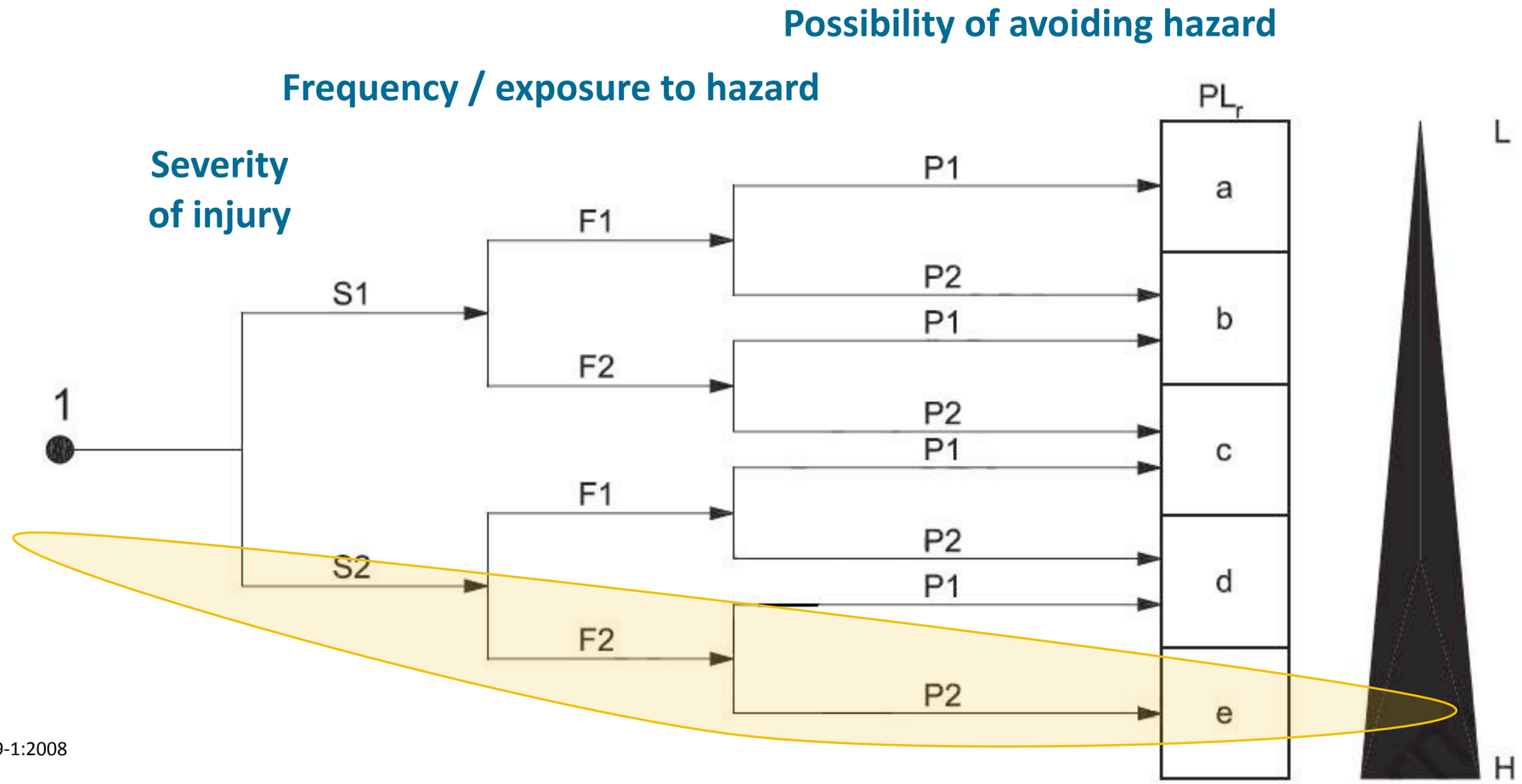
Validation with:

NF EN ISO 13849-1:2008

instead of

IEC 62061

The required safety level



Source : NF EN ISO 13849-1:2008

PL	a	b	c	d	e
PFH_d	$[10^{-5}; 10^{-4}[$	$[3\times10^{-6}; 10^{-5}[$	$[10^{-6}; 3\times10^{-6}[$	$[10^{-7}; 10^{-6}[$	$[10^{-8}; 10^{-7}[$

The validation procedure

Subsequent steps

- Designated architecture
- $MTTF_d$ (mean time to dangerous failure)
- DC_{avg} (average diagnostic coverage)
- CCF (common cause failures)
- Safety-related software
- Systematic failures
- Ability to perform the safety function under expected environmental conditions
- $PL \geq PL_r$?

The validation results

"Laboratory" context: 2 h/day during 5 days/year

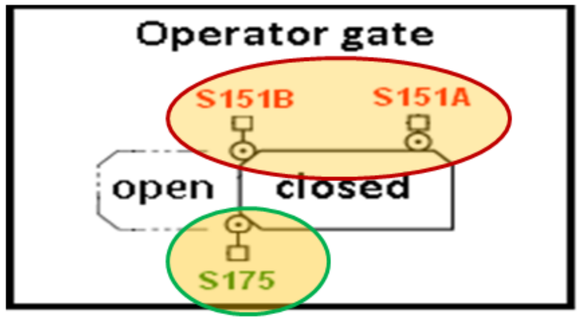
Parameters	Value	
Category	None of the 4 possible categories is satisfied	**PL undetermined → PL_r not satisfied**
Score to counter CCF	65 → minimum required score satisfied	
Resulting $MTTF_d$	100 years → High $MTTF_d$	
DC_{avg}	19,64 % → DC_{avg} zero	

"Industrial" context: 20 h/day during 350 days/year

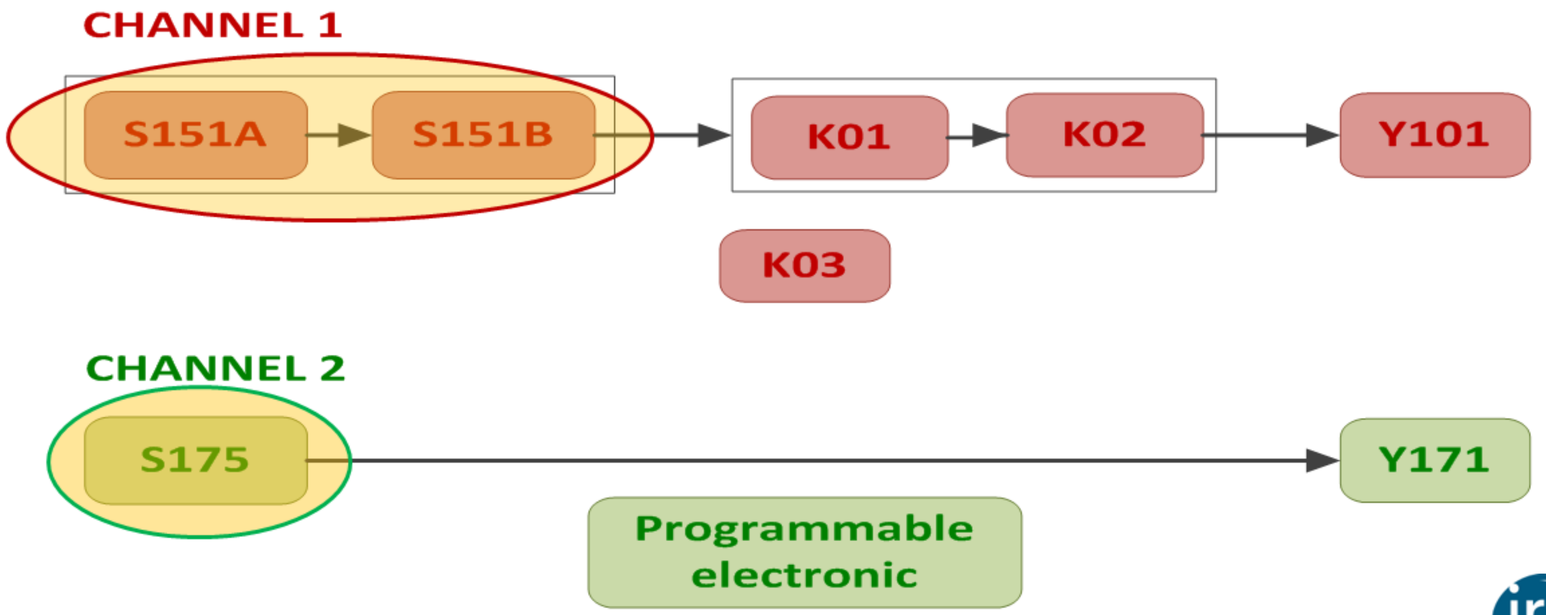
Parameters	Value	
Category	3	**PL = e = PL_r**
Score to counter CCF	65 → minimum required score satisfied	
Resulting $MTTF_d$	66,67 years → High $MTTF_d$	
DC_{avg}	98,43 % → Medium DC_{avg}	

The designated architecture: **assumptions made & impacts**

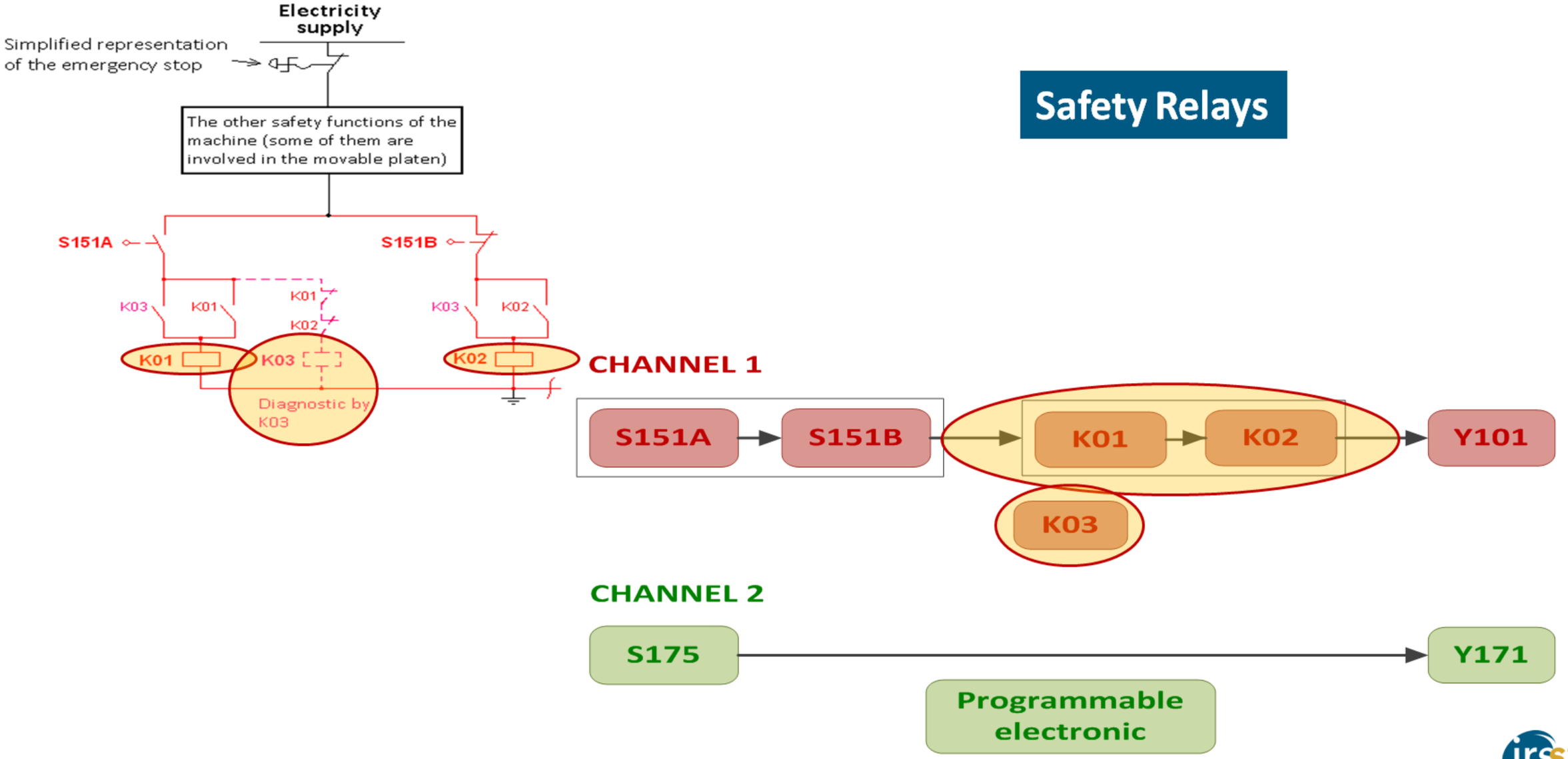
The designated architecture



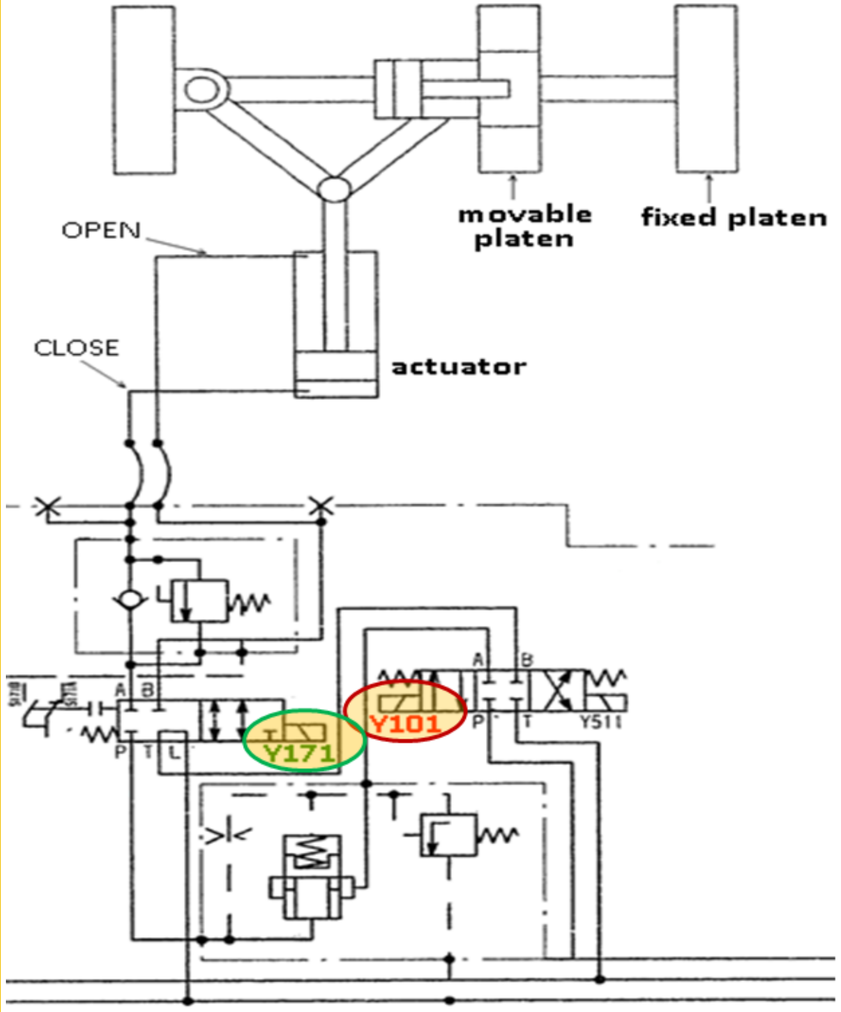
Switches



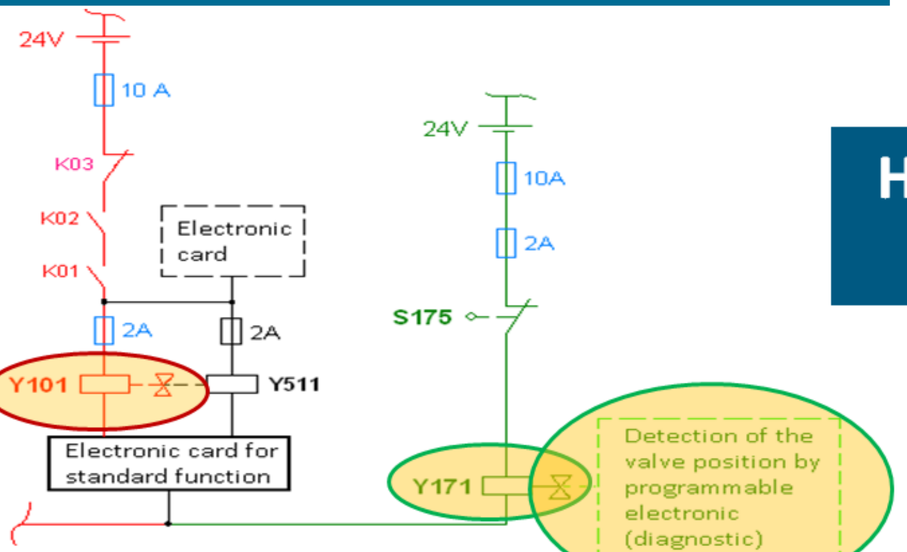
The designated architecture



The designated architecture



Source: ARBURG



Hydraulic valves

CHANNEL 1

S151A → S151B → K01 → K02 → Y101

K03

CHANNEL 2

S175 → Y171

Programmable electronic

Calculation of $MTTF_d$ and DC_{avg}: **assumptions made & impacts**

Calculation of $MTTF_d$ and DC_{avg} (1/2)

$$MTTF_d = \frac{2}{3}\left(MTTF_{d\ CHANNEL\ 1} + MTTF_{d\ CHANNEL\ 2} - \frac{1}{\frac{1}{MTTF_{d\ CHANNEL\ 1}} + \frac{1}{MTTF_{d\ CHANNEL\ 2}}} \right)$$

$$DC_{avg} = \frac{\frac{DC_{S151A}}{MTTF_{d\ S151A}} + \frac{DC_{K01}}{MTTF_{d\ K01}} + \frac{DC_{K02}}{MTTF_{d\ K02}} + \frac{DC_{Y101}}{MTTF_{d\ Y101}} + \frac{DC_{Y171}}{MTTF_{d\ Y171}}}{\frac{1}{MTTF_{d\ S151A}} + \frac{1}{MTTF_{d\ K01}} + \frac{1}{MTTF_{d\ K02}} + \frac{1}{MTTF_{d\ Y101}} + \frac{1}{MTTF_{d\ Y171}}}$$

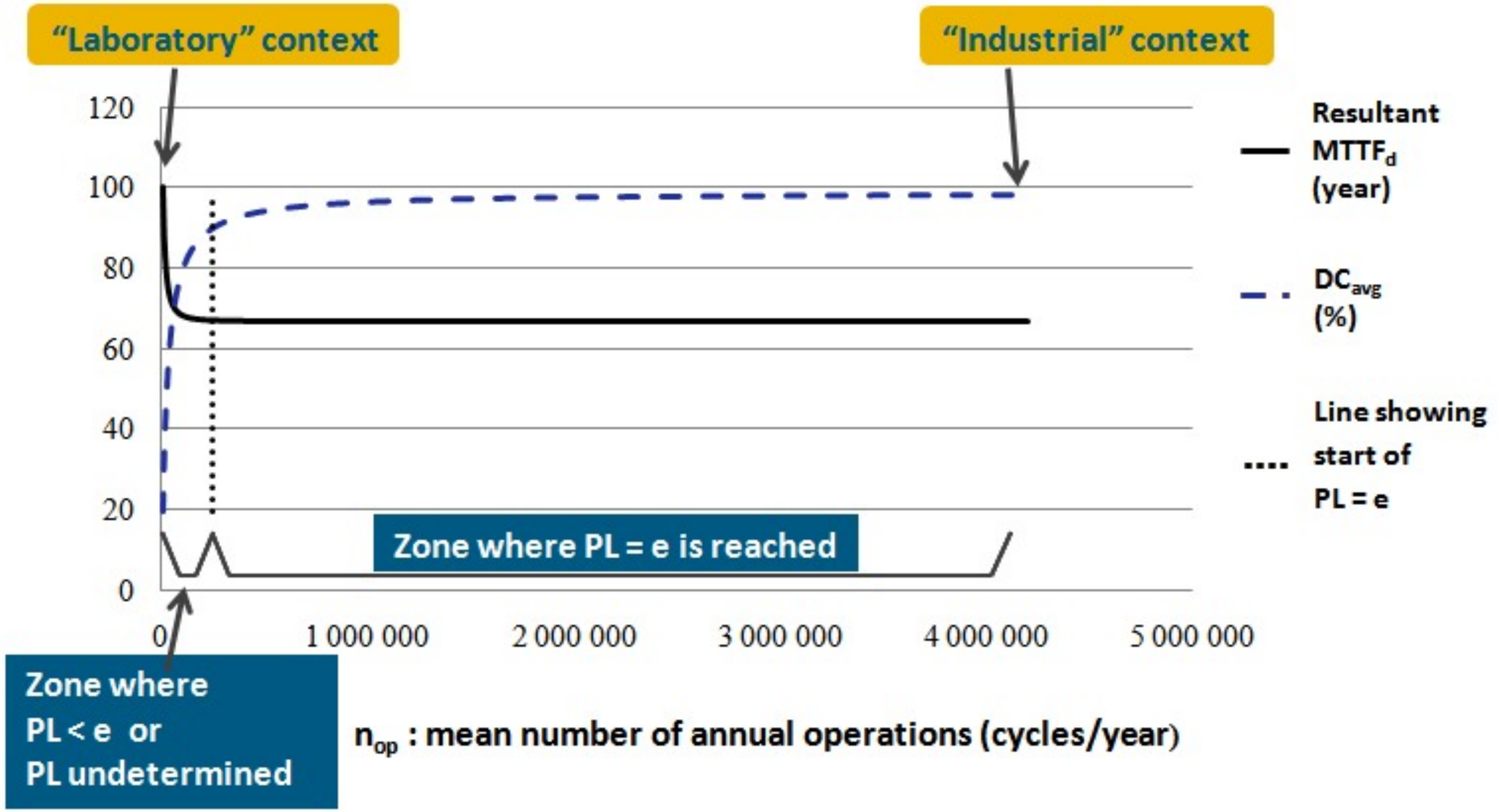
$MTTF_d$ for components:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

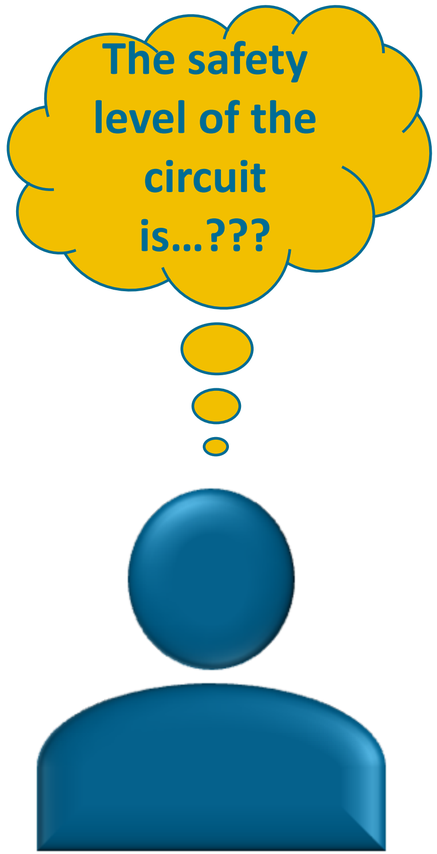
B_{10d}: number of cycles until 10 % of the components fail dangerously

n_{op}: mean number of annual operations

Calculation of $MTTF_d$ and DC_{avg} (2/2)



Conclusion



IEC 62061 → Safety level is “SIL”

ISO 13849-1 → Safety level is “PL”

“Laboratory” context

- PL undetermined

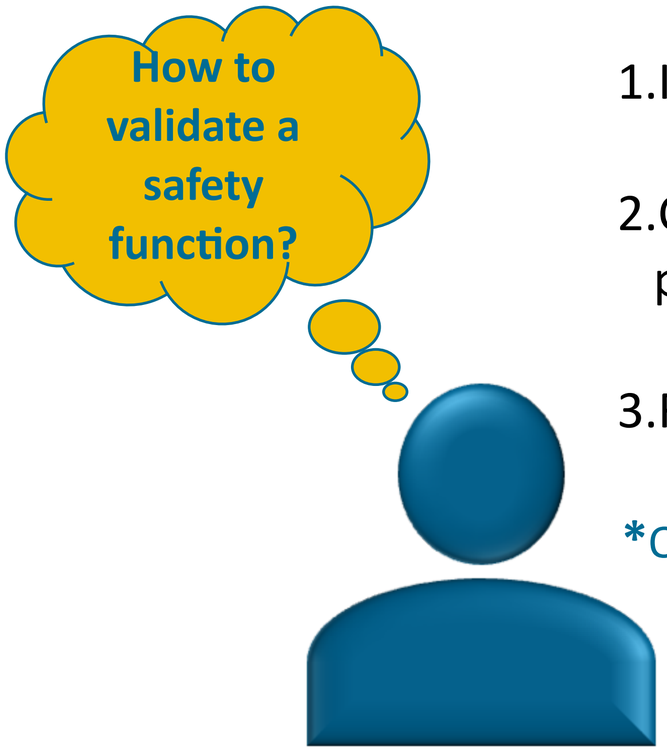
→ PL_r not satisfied

“Industrial” context

- PL = e

→ PL_r satisfied

Conclusion



If applying a standard, follow these steps:

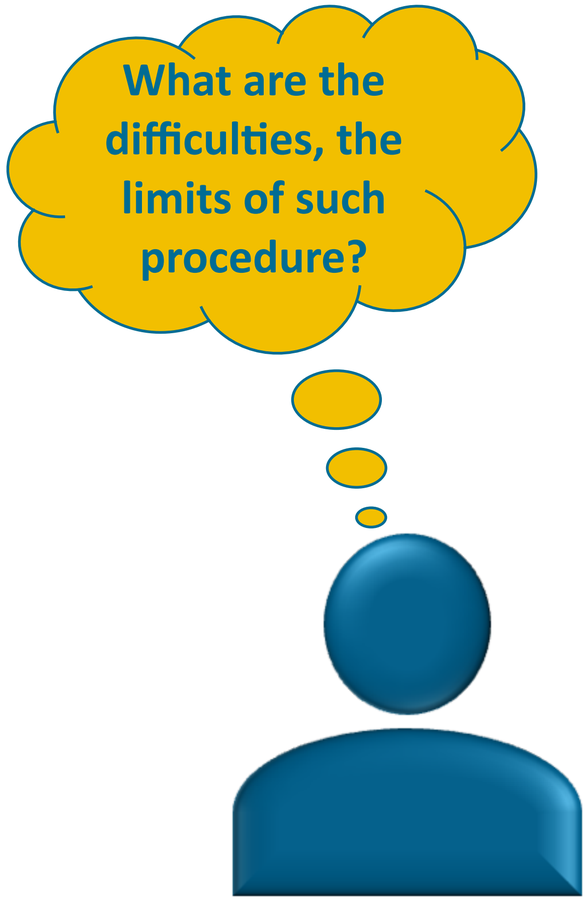
1. Identify and specify the safety function

2. Choose the appropriate standard depending on the technology performing the safety function*

3. Follow the steps suggested in the chosen standard*

*Or, follow a calculation method other than the one in the standard.

Conclusion



The *a posteriori* estimation procedure is difficult to achieve due to :

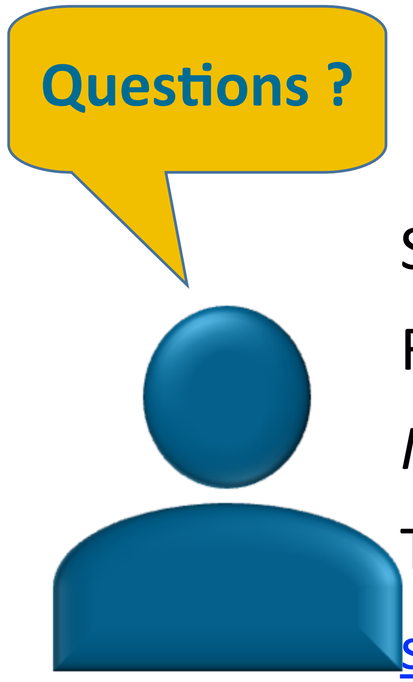
- The **many assumptions** made (e.g.: role of the components, number of demands (impact on the results: “Laboratory” vs. “Industrial”))
- The **lack of information** that could be available if the designer/ manufacturer were involved
- This lack creates **uncertainties in the results**
- The results of such exercise **depend on the people** who achieved the *a posteriori* estimation

Conclusion

Carrying out an *a posteriori* estimation of the PL for a safety function is possible, but:

- The results should be carefully considered

- The accuracy of the results can only be optimized by **surrounding oneself with experts** in safety-related control system design or, ideally, by **involving the designer**



Sabrina JOCELYN, ing. jr., M.Sc.A.

Research assistant

IRSST, Mechanical and Physical Risk Prevention

Tel : 514 288-1551, ext. 407

sabjoc@irsst.qc.ca