SOURCES OF MISTAKES IN *PFD* CALCULATIONS FOR SAFETY-RELATED LOOP TYPICALS

Daniel Düpont
University of Kaiserslautern
P.O. Box 3049
67653 Kaiserslautern
Germany

Lothar Litz
University of Kaiserslautern
P.O. Box 3049
67653 Kaiserslautern
Germany

Pirmin Netter
Infraserv Höchst
Industriepark Höchst C769
65926 Frankfurt/ Main
Germany

Abstract - In order to prevent any harm for human beings and environment, IEC 61511 imposes strict requirements on safety instrumented functions (SIFs) in chemical and pharmaceutical production plants. As measure of quality a safety integrity level (SIL) of 1, 2, 3 or 4 is postulated for the SIF. In this context for every SIF realization, i.e. safety-related loop, a SIL-specific probability of failure on demand (*PFD*) must be proven. Usually, the *PFD* calculation is performed based on the failure rates of each loop component aided by commercial software tools. But this bottom-up approach suffers from many uncertainties. Especially a lack of reliable failure rate data causes many problems. Reference data for different environmental conditions are available to solve this situation. However, this pragmatism leads to a *PFD* bandwidth, not to a single *PFD* value as desired. In order to make a decision for a numerical value appropriate for plant applications in chemical industry, a data ascertainment has been initiated by the European NAMUR within its member companies. Combined with statistical methods their results display large deficiencies for the bottom-up approach. As one main source of mistakes the distribution of the loop *PFD* has been identified. The well known percentages for sensor, logic solver and final element part often cited in literature could not be confirmed.

Index Terms — IEC 61511, SIL, SIF, SIS, *PFD*, Failure rates, Confidence intervals.

I. INTRODUCTION

To guarantee a homogenously high plant safety standard around the world, a global directive was created by IEC 61511 [1]. The implementation of this guideline imposes strict requirements to plant operators. One central term is given by the safety instrumented system (SIS) which implements one or more safety instrumented functions (SIFs). If the process tends to enter a dangerous range, the SIS has to interfere and bring the plant to a safe state. For example, a SIF avoiding the hazard case "burst of a vessel hull due to overpressure" could be realized by a loop in the SIS consisting of two pressure transmitters connected by a 1oo2 PLC (1 out of 2 programmable logic controller, for further abbreviations see chapter VIII) to two relief valves operating in parallel.

IEC 61511 prescribes the performance of a SIL assessment for every new-installed SIF. In general this process consists of two parts, see Fig. 1.

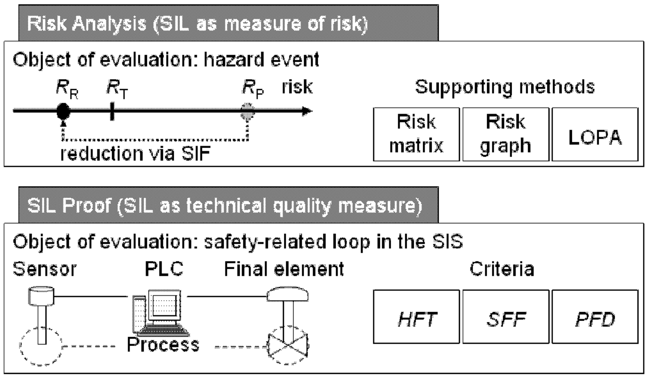
Risk Analysis (SIL as measure of risk)
Object of evaluation: hazard event
R_R
R_T
R_P
risk
reduction via SIF
Supporting methods
Risk matrix
Risk graph
LOPA
SIL Proof (SIL as technical quality measure)
Object of evaluation: safety-related loop in the SIS
Sensor
PLC
Final element
Criteria
Process
HFT
SFF
PFD

Fig. 1: SIL assessment

To determine the process risk R_P for a certain hazard case – defined as the risk without the SIF needed – a risk analysis must be performed. If R_P lies above the tolerable risk R_T all supporting methods result in one of the four safety integrity levels (SIL 1 to 4) as risk measure. For any dangerous scenario with a SIL classification a SIF must be identified and installed in the SIS. Thereby, a risk reduction to a residual risk below the tolerable one should be created.

The hardware realization of a SIF is given by a safety-related loop in the SIS which has to fulfill SIL-specific criteria. During the SIL proof the aimed SIL has to be verified under consideration of several, predominantly quantitative constraints imposed by [1]. These criteria describe the structural and technical loop quality, see Fig. 1. The most critical criterion impacting on a SIL is given by the average probability of failure on demand (*PFD*), see Table I.

TABLE I
SIL: *PFD* VALUES

SIL	*PFD* target value
4	$10^{-5} \leq PFD < 10^{-4}$
3	$10^{-4} \leq PFD < 10^{-3}$
2	$10^{-3} \leq PFD < 10^{-2}$
1	$10^{-2} \leq PFD < 10^{-1}$

From the technical point of view this quantity denotes the safety-related unavailability of the SIF. It can be calculated in two different ways:

Bottom-up methods are appropriate to determine the availability of any system consisting of components with known data (failure rates, availability), see [2]. Usually, they are used for the SIL proof.

In order to check the transferability of bottom-up *PFD*s onto the real failure behavior of loops in production plants, top-down methods are applied. They originate from real loops and are based on their statistics, see [3].

The ideal case would be represented by similar results for the outcomes of both, the bottom-up and the top-down approach. Applying both methods and comparing their results mirrors large discrepancies whose sources must be located. For the scope of this paper all examinations are focused on single-channel loops.

II. BOTTOM-UP APPROACH

In order to get representative results, special SIF realizations have to be defined which can serve as a kind of benchmark. Afterwards, reliability data are collected for each loop component. Finally, for these so-called typicals the *PFD* calculation is performed aided by commercial software tools.

A. Typical Compilation

Fixing representative single-channel SIF realizations requires two properties of the typicals. On the one hand their origin should be one of the leading chemical companies. On the other hand they are to be qualified as standard solutions if a pressure-, temperature- or level-based SIF is realized.

TABLE II
SINGLE-CHANNEL TYPICALS

		1oo1 Typical		
Observed process quantity		Pressure	Temp.	Level
Denotation		PIRZ+A+	TIRZ+A+	LIRZ+A+
Behavior of final element on demand		close	open	close
Sensor part	Sensing element	X	O	X
	Transmitter		O	
	Transmitter power supply	O	O	X
	PLC input	X	X	X
Logic solver part	PLC	X	X	X
Final element part	PLC output	X	X	X
	Solenoid driver	O	not used	not used
	Solenoid valve	O (pilot)	O (pilot)	O (direct)
	Actuator	O	O	O
	Ball valve	O	O	O

X Component with sufficient data.
O Component with no or insufficient data.

From the pool of single-channel typicals three loops are chosen: one typical for pressure, temperature and level control. Table II shows the types of the used components. Manufacturers and product names are not listed for keeping a neutral position. Moreover, an assignment of the modules to superior, more general layers is given, i.e. a classification in sensor, logic solver or final element part. For describing the functionality of each typical the monitored process quantities as well as the original denotations have been adopted. The behavior of the final element on demand plays an important role concerning the choice of the appropriate failure rates. The following information can be derived: All typicals are monitoring an upper limit value ("+"). On demand for "Pressure" and "Level" the valves are closed, whereas for "Temperature" the final element is opened.

B. Failure Rate Mining

In the next step failure rate data of each loop component is gathered. Normally, this process of data mining is intended to work by ordering so-called SIL conformity declarations from the component manufacturers. These documents should contain the relevant information for *PFD* calculations, i.e. at least the rate of dangerous, undetected failures λ_{DU}. In general three cases occur:

Case 1: A manufacturer declaration is available containing trustworthy failure rates ("X" in Table II).

Case 2: A manufacturer declaration is available containing either no failure rates or no trustworthy ones ("O" in Table II).

Case 3: No manufacturer declaration is available ("O" in Table II).

Unfortunately, many typical components feature insufficient data ("O" in Table II). Declarations assigned to case 2 mostly suffer from too conservative failure rates. For being on the safe side many manufacturers run their component analysis assuming worst case conditions (e.g. 60°C ambient air temperature). Often, the resulting failure rates are increased by a final addition of 10% or more. But also extremely good data are provided for marketing reasons. Case 3 mainly originates from a phenomenon induced by the component selection criteria of chemical companies. Before new developments are chosen for safety-critical applications, they must stand laboratory phases. Afterwards, a faultless one-year test period has to be passed in several applications of the BPCS. Hence, many of these proven-in-use components were developed in the early years of IEC 61511 or are even older. In combination with devices having direct contact with process fluid or working in aggressive atmospheres, they suffer from a lack of reliability data.

One admissible way out for case 2 and 3 components would be own failure rates derived by plant operators in addition to a proven-in-use declaration. But doing so requires an adequate statistical data base for the considered components. However, the data base volume of a single concern would be too small as consequence of the company size.

Consequently, reference values have to be mined for affected components ("O" in Table II).

TABLE III
REFERENCE DATA

Component type		Environment		
		Laboratory	Laboratory -Field	Field
		λ_{DU} [FIT]	λ_{DU} [FIT]	λ_{DU} [FIT]
RTD and transmitter		438	700	5670
Transmitter power supply		24	150	2835
Solenoid driver		0	100	not available
Solenoid valve	direct	62	585	1400
	pilot	213		
Actuator		19	670	in valve data
Ball valve		144	1350 close 960 open	19111 close 14553 open
				with actuator

Table III contains reference data collected under different environmental conditions. The major data sources are listed in [4] to [8]. To avoid any competition situation, the sources are not assigned to the values. Offshore rates taken from [5] have been filtered according to the usage conditions in chemical and pharmaceutical industry. Comparing the orders of magnitude graduated to different usage conditions in Table III, strong deviations are observable. The laboratory rates have strong theoretical character because they presume clean service usage. For realistic considerations the field influence is to be regarded. But without a highly sophisticated maintenance system the field usage ("Laboratory-Field" and "Field" in Table III) comes along with significantly worse component rates. If additionally offshore rates come into game ("Field" in Table III), high vibrations and corrosive effects lead to even worse reference rates. Summing up, the order of magnitude changes from column to column approximately one decimal power. Consequently, a strong sensitivity of the *PFD* outcome with respect to the choice of reference data is to be expected.

C. *PFD Determination*

Three commercial software tools are spread over Germany to support *PFD* calculations. Two of them make use of the *PFD* formulas given in IEC 61508 [9], whereas the third one takes Markov Models. As this paper exclusively deals with non-redundant structures, no significant deviations will be expected due to different tools. Therefore, the following calculations are done supported by one of them without mentioning its name and manufacturer.

As each typical suffers from missing or insufficient component failure rates, different reference rates have to be tested. Hence, the *PFD* calculation does not lead to a crisp value but to laboratory and field bandwidths. For each typical the *PFD* calculation is performed three times using different specifications:

PFD_{Lab} specification – reference data derived under **laboratory** conditions (given by manufacturers);

$PFD_{\text{Lab-Field}}$ specification – reference data derived under **laboratory** conditions modified by knowledge from small **field** studies (given by published data bases);

PFD_{Field} specification – reference data derived from **field** studies mostly from offshore applications (given by published data bases);

Because $PFD_{\text{Lab-Field}}$ denotes a limit value between laboratory and field environment it will serve as worst case for laboratory and best case for field application at the same time.

The proof test intervals have been adapted according to the NAMUR data in chapter III. Table IV contains the *PFD* outcome for the considered 1oo1 typicals.

TABLE IV
BOTTOM-UP *PFD* BANDWIDTHS

1oo1 Typical	*PFD* bandwidth [PFD_{Lab}; $PFD_{\text{Lab-Field}}$; PFD_{Field}]
Pressure (P)	[$2.09 \cdot 10^{-3}$; $1.20 \cdot 10^{-2}$; $9.48 \cdot 10^{-2}$]
Temperature (T)	[$3.38 \cdot 10^{-3}$; $1.23 \cdot 10^{-2}$; $9.84 \cdot 10^{-2}$]
Level (L)	[$3.21 \cdot 10^{-3}$; $1.28 \cdot 10^{-2}$; $8.48 \cdot 10^{-2}$]

According to the choice of the reference values the *PFD*s diverge more than one decimal power from each other. In comparison with Table I for laboratory environment a *PFD* of SIL 2 (best case laboratory) or SIL 1 (worst case laboratory) results for all typicals. As usually field application is of interest only a *PFD* of SIL 1 (best and worst case field) is verifiable. Moreover, no ranking according to the monitored process quantity is observable.

III. TOP-DOWN VALIDATION

A. *STATISTICAL DATA BASE*

In order to validate if the bottom-up approach has been able to map realistic *PFD*s for field conditions, the NAMUR [10] has motivated a data ascertainment within its member companies. In the year 2003 already 33 companies participated in this activity and from 2004 till 2005 the group of data suppliers increased to 37. Also the biggest chemical and pharmaceutical companies provided their data sets for the three years. The main advantage of this data base lies in its quality and quantity. As the material is gained in the field, it includes the observance of the process influence, i.e. the contact with process fluid. The data structure has become more and more complex over the years. For the initial year 2002 only a distinction between failures in single-channel and multi-channel loops was queried. For 2003 till 2005 a subdivision regarding the monitored process quantity raised the data complexity. Table V shows the single-channel data sets for the three years.

As not all data suppliers give the subdivision concerning the monitored process quantity, the elements of the "Total" groups do not meet the sum of the according subgroups. Moreover, groups like “Others”, “Manual” and “Quality” do exist. However, they are not considered here.

TABLE V
SINGLE-CHANNEL NAMUR DATA 2003 – 2005

Year	Group	Loops [absolute]	Dangerous, undetected failures [absolute]	T_I [years]
2003	Total	12,132	41	0.93
	Pressure (P)	1,479	11	0.93
	Temp. (T)	1,154	1	0.93
	Level (L)	1,020	2	0.95
2004	Total	16,172	43	0.93
	Pressure (P)	2,292	18	0.93
	Temp. (T)	1,936	5	0.93
	Level (L)	1,368	3	0.95
2005	Total	18,903	56	0.91
	Pressure (P)	2,098	17	0.89
	Temp. (T)	1,600	5	0.94
	Level (L)	1,911	5	0.90

In addition to the individuals of each group the numbers of dangerous, undetected failures are listed. This type of failure has the major influence on process safety. It does not only prevent the loop from proper functioning in the case of a demand in general. Additionally, it remains undetected until the regular proof test. The proof test intervals in practice have been interpolated from statements of data suppliers which have been providing this information since 2004. Hence, the intervals for 2004 are retrospectively assigned to the year 2003. For 2005 new proof test intervals are created by feedback of data suppliers.

In order to compare the results of the typicals with the values of the NAMUR data, it is not obligatory to examine the “Total” groups. But for getting an impression of the NAMUR data consistency a consideration of the whole 1oo1 data pool is very useful.

B. *PFD CONFIDENCE INTERVAL ESTIMATION*

Initially, the following assumptions are made:

1. Only dangerous, undetected failures are *PFD* relevant, dangerous, detected ones negligible.
2. Failure rates are constant over time.
3. *MTTR* << *MTTD*$_{DU}$, because normally *MTTR* ≈ 8h and *MTTD*$_{DU}$ > 0.5 y.
4. $\lambda_{DU} \cdot T_I << 1$.
5. The failure detection and repair during the proof test is perfect (*PTC* = 100%).
6. For the NAMUR data the following holds: Each safety-related loop can only suffer from at most one dangerous, undetected failure during the observation period of one year.

To derive *PFD* values from the given data pool, a *PFD* formula with adaptation to the NAMUR data is required. According to [3] the *PFD* of a 1oo1 loop can be determined by

$$PFD = \frac{F_{DU}}{L \cdot \Delta T} \cdot \frac{T_I}{2}, \qquad (1)$$

where F_{DU} and L denote the numbers of dangerous, undetected failures and loops in Table V. ΔT stands for the observation period, which is set to one year by the interrogation cycle of NAMUR.

But only using (1) for *PFD* calculations would not lead to trustworthy values as statistics always imply deficiencies. Therefore, IEC 61511 advises estimating confidence intervals to compensate for statistical inaccuracies. The first step to do so is finding an appropriate interval estimator. As for the NAMUR data structure a continuous model is not the best choice, the binomial distribution — as exactest discrete model — is used.

Assuming a binomial distribution, the interval boundaries for a given confidence level 1 – α are determined by

$$p_{low} = \max_{p} \sum_{x=F_{DU}}^{L} \binom{L}{x} (1-p)^{L-x} p^x \le \frac{\alpha}{2} \text{ for } 0 < F_{DU} < L \text{ and} \qquad (2)$$

$$p_{up} = \min_{p} \sum_{x=0}^{F_{DU}} \binom{L}{x} (1-p)^{L-x} p^x \le \frac{\alpha}{2} \text{ for } 0 < F_{DU} < L\,, \qquad (3)$$

see [10].

Solutions to (2) and (3) are found by iterative methods. The estimated quantity *p* corresponds to the ratio of F_{DU} and *L*:

$$p = \frac{F_{DU}}{L}. \qquad (4)$$

Hence, *p* can be interpreted as the failure probability related to ΔT. In a last step, the *p* confidence intervals must be transformed to *PFD* confidence intervals. Thus, the interval boundaries p_{low} and p_{up} are converted into PFD_{low} and PFD_{up} by combining (1) and (4):

$$PFD = p \cdot \frac{T_I}{2\Delta T}. \qquad (5)$$

Table VI shows the generated *PFD* confidence intervals for the NAMUR data. The confidence level has been chosen as 70% in accordance with IEC 61511 [1].

Analyzing the upper interval boundaries (worst case “field”), all *PFD* values are located in the *PFD* range of SIL 2. The set of lower interval boundaries (best case “field”) contains elements from SIL 2 to SIL 4. Furthermore, a ranking concerning the monitored process quantity is derivable: “Temperature” and “Level” show almost the same *PFD* quality, “Pressure” is worse.

Evaluating the bottom-up *PFD*s with the top-down intervals, there is a gap of almost two SILs. Hence, these large deviations between theory (bottom-up approach) and practice (top-down approach) must be examined.

TABLE VI
PFD CONFIDENCE INTERVALS

Year	Group	*PFD* confidence interval [PFD_{low}; PFD_{up}]
2003	Total	[$1.32 \cdot 10^{-3}$; $1.87 \cdot 10^{-3}$]
	Pressure (P)	[$2.40 \cdot 10^{-3}$; $4.89 \cdot 10^{-3}$]
	Temp. (T)	[$6.55 \cdot 10^{-5}$; $1.36 \cdot 10^{-3}$]
	Level (L)	[$3.18 \cdot 10^{-4}$; $2.20 \cdot 10^{-3}$]
2004	Total	[$1.04 \cdot 10^{-3}$; $1.46 \cdot 10^{-3}$]
	Pressure (P)	[$2.78 \cdot 10^{-3}$; $4.77 \cdot 10^{-3}$]
	Temp. (T)	[$6.69 \cdot 10^{-4}$; $2.04 \cdot 10^{-3}$]
	Level (L)	[$4.62 \cdot 10^{-4}$; $2.09 \cdot 10^{-3}$]
2005	Total	[$1.16 \cdot 10^{-3}$; $1.56 \cdot 10^{-3}$]
	Pressure (P)	[$2.72 \cdot 10^{-3}$; $4.74 \cdot 10^{-3}$]
	Temp. (T)	[$8.18 \cdot 10^{-4}$; $2.49 \cdot 10^{-3}$]
	Level (L)	[$6.56 \cdot 10^{-4}$; $2.00 \cdot 10^{-3}$]

IV. BACKTRACKING OF DEVIATIONS

Analyzing Table II it becomes obvious that final element parts seem to look similar for single-channel loops. They consist of a PLC output, connected with a solenoid valve which controls the actuator of a ball valve.

IEC 61508 says that 35% of the loop *PFD* is caused by the sensor, 15% by the logic solver and 50% by the final element part. In combination with the previous statement for typicals no ranking between the NAMUR groups "Pressure", "Temperature" and "Level" should be observable. However, a ranking does exist. Therefore, splitting the *PFD* on sensor, logic solver and final element part might be a promising approach for the isolation of mistake sources.

The necessary information for the typicals is immediately available as it is already content of the bottom-up calculation. For reasons of completeness a "Total" group is also generated as average of the typical PFD bandwidths.

For the NAMUR data more expense is required. Fortunately, in the years 2004 and 2005 a detailed failure splitting on sensor, logic solver and final element part does exist. All further calculations are based on a cumulative NAMUR data set 2004/ 2005, because a more detailed failure splitting causes a lower number of failures in the subgroups. Hence, an accumulation is reasonable for keeping the same level of statistical accuracy.

A. *DISTRIBUTION OF LOOP PFD*

Based on the NAMUR data set 2004/ 2005, for each group ("Total", "Pressure", "Temperature" and "Level") *PFD* confidence intervals can be estimated for sensor, logic solver and final element part separately. The relation of the PFD_{low} boundaries leads to a best case NAMUR distribution (field) for each group. Applying the same procedure to the PFD_{up} boundaries delivers the corresponding worst case NAMUR distributions (field), see Figs. 2 – 5 "NAMUR (field)".

By splitting the *PFD* outcomes of the typicals, the equivalent percentage distributions for the bottom-up approach are derivable. The following specifications are used for getting best and worst case typical distributions (field), see Figs. 2 – 5 "Typical (field)".

Typical (field):
best case → $PFD_{Lab\text{-}Field}$ distribution
worst case → PFD_{Field} distribution

For reasons of completeness the same pragmatism is also transferred to the typical bandwidths (laboratory). For this the just given specification is modified, see Figs. 2 – 5 "Typical (laboratory)".

Typical (laboratory):
best case → PFD_{Lab} distribution
worst case → $PFD_{Lab\text{-}Field}$ distribution

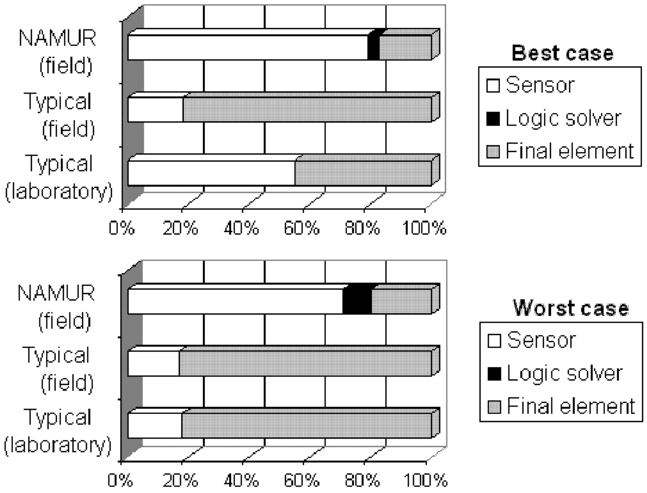

Fig. 2: *D*istribution of loop *PFD* for "Total"

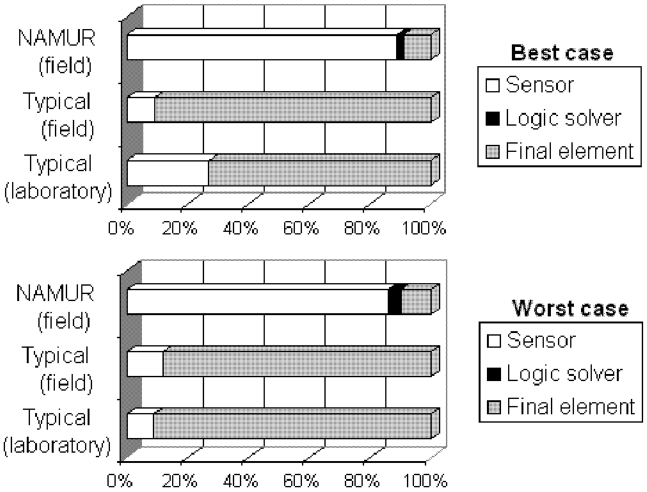

Fig. 3: *D*istribution of loop *PFD* for "Pressure"

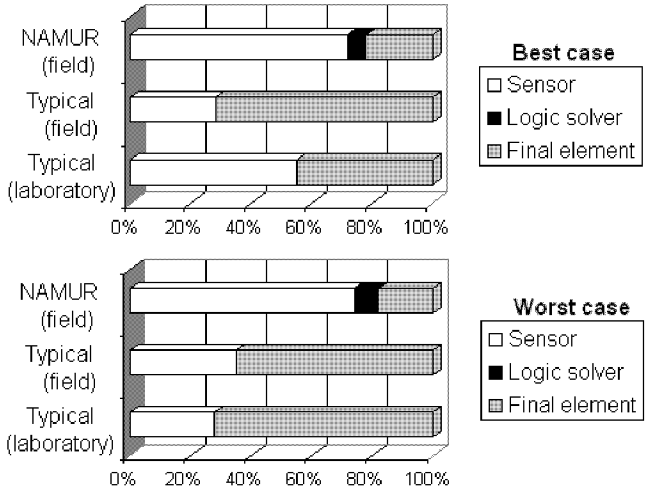

Fig. 4: *D*istribution of loop *PFD* for "Temperature"

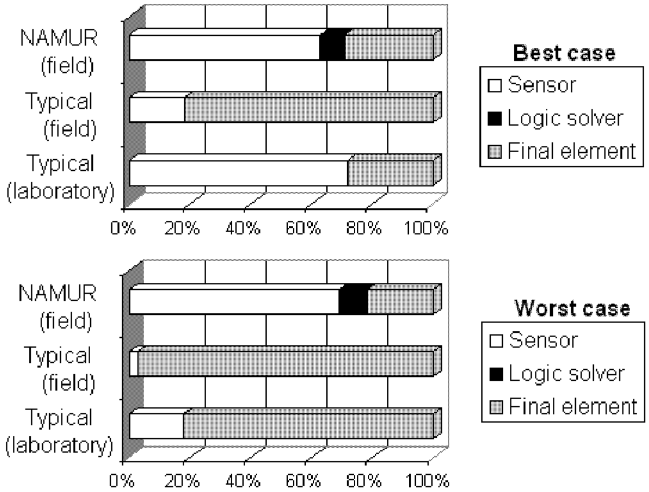

Fig. 5: *D*istribution of loop *PFD* for "Level"

B. AVERAGE PFD OF SENSOR- AND FINAL ELEMENT PART

For estimating the dimension of deviation between bottom-up and top-down a consideration of the absolute sensor, logic solver and final element *PFD*s is reasonable. A first analysis is performed for the "Total" groups.

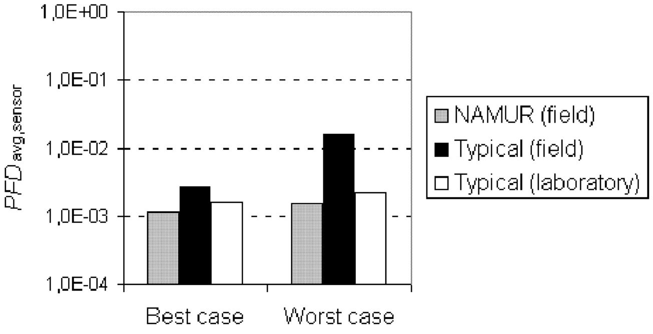

Fig. 6: *PFD*$_{\text{sensor}}$ "Total"

The logic solver part is not examined as it has no significant influence on the loop *PFD*. The *PFD* results of the sensor and final element parts are shown in Figs. 6 and 7. The observed specifications are chosen according to the *PFD* distributions in chapter IV A.

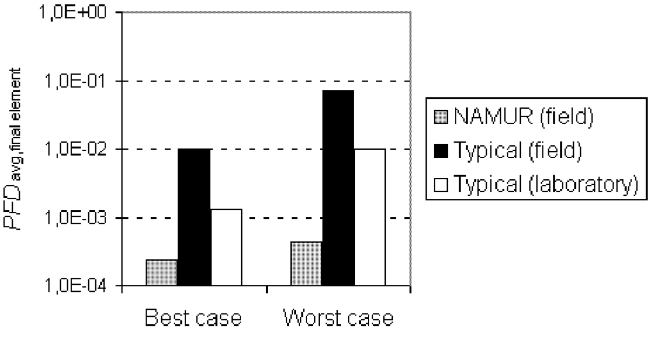

Fig. 7: *PFD*$_{\text{final element}}$ "Total"

V. CONCLUSIONS

The results of bottom-up (typicals) and top-down approach (NAMUR data) are presented by a graphical illustration.

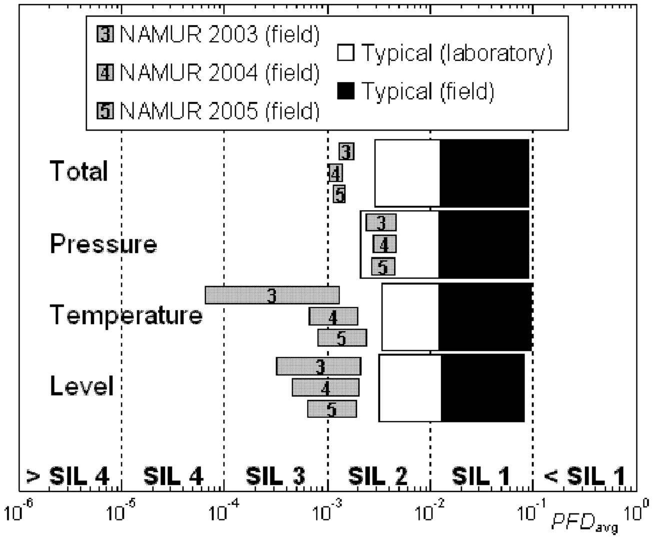

Fig. 8: Results – bottom-up versus top-down approach

Figure 8 shows the *PFD* confidence intervals 2003 to 2005 of the NAMUR data [10] as well as the *PFD* bandwidths of the typicals. As the difference between each consecutive SIL *PFD* range is one decimal power a logarithmic scaling is chosen. Based on Figure 8 several statements could be made:

1st statement: Analyzing the three single-channel subgroups of the NAMUR data, a kind of *PFD* ranking can be extracted: The best *PFD* spectrum is verified for the "Temperature" and "Level" loops. "Pressure" loops range significantly worse. This holds for all three years of the NAMUR data. In contrast to the top-down method no comparable effect can be derived for the bottom-up approach. The *PFD* spectra (Fig. 8 "Typical (field)") almost mirror congruency.

2nd statement: For the single-channel loops there is a large gap between the *PFD* confidence intervals and the *PFD* typical bandwidths, see Fig. 8 “NAMUR (field)” and “Typical (field)”. Although there is an intersection for “Pressure”, the results are not comparable in a strict sense. A correct comparison must proceed between “NAMUR (field)” and “Typical (field)” in Fig. 8. These field results do not only lie totally disjoint from each other, they even occupy completely different SIL *PFD* ranges. Being on the safe side for the *PFD* bandwidths as for the *PFD* confidence intervals only the worst case would be regarded as proven. Hence, for each single-channel typical only a *PFD* in the SIL 1 *PFD* range is verified. This is in contrast to the top-down reality comfortably fulfilling SIL 2.

Isolating the reasons for the large differences, the distribution of the loop *PFD* on sensor, logic solver and final element part delivers three important observations:

1st observation: The often cited *PFD* distribution in IEC 61508 [9] (35% sensor, 15% logic solver and 50% final element part) cannot be confirmed neither by the bottom-up typical bandwidths nor the top-down confidence intervals. Its incompatibility with the NAMUR data [10] indicates the incoherency of the classical distribution with conditions in European plants.

2nd observation: The top-down approach (NAMUR data) identifies the sensor part as main contributor of the loop *PFD*, the bottom-up method points at the final element part.

3rd observation: According to the bottom-up calculations the logic solver is no significant fraction of the loop *PFD.* However, the NAMUR data assign approximately 10% of the loop *PFD* to the logic solver part.

Comparing the absolute sensor and final element *PFD*s (Figs. 6 and 7) leads to an interesting phenomenon: The field sensor part *PFD*s of the typicals are 2 to 11 times worse than the NAMUR data ones. The ratio between the corresponding final element part *PFD*s is even 42 to 176 times worse.

From all observations a hint indicating too conservative assumptions can be derived caused by a lack of reliable failure rate information. Consequently, the bottom-up approach via commercial software tools has not been able to map realistic loop *PFD*s so far. The main source for the shown discrepancies is located in the final element part. Here, a deviation of more than two decimal powers from the NAMUR data could be demonstrated. One could doubt the reliability of the NAMUR data base. Thus, stability analyses were performed with respect to structure and behavior over time (2003 to 2005). The results confirm the NAMUR data as highly sophisticated information source. Hence, single-channel loops installed in European plants comfortably fulfill SIL 2 with respect to the *PFD.*

To close the gap between bottom-up and top-down approach there is cooperation between NAMUR and ZVEI. On the one hand standard failure rates for proven-in-use components are derived of the NAMUR data. On the other hand manufacturer rates are modified based on realistic environmental conditions.

VI. REFERENCES

[1] IEC 61511, parts 1-3, *Functional safety: Safety Instrumented Systems for Process Industry Sector*, 2002.

[2] L. Litz, “Safety and Availability of Components and Systems”, in IEEE PCIC Europe Conference Record, 2004, pp 16-21.

[3] L. Litz, D. Düpont and P. Netter, “SIL Validation of Safety Instrumented Loops in Use by Statistical Methods”, in IEEE PCIC Europe Conference Record, 2005, pp 69-76.

[4] Exida.com L.L.C., *Safety Equipment Reliability Handbook*, second edition, Sellerville (USA), 2005.

[5] SINTEF Industrial Management, *OREDA – Offshore Reliability Data*, Det Norsk Veritas, Hovik (Norway), 2002.

[6] S. Hauge, P. Hokstad, *Reliability Data for Safety Instrumented Systems – PDS Data Handbook*, SINTEF, Trondheim (Norway), 2004.

[7] MIL-HDBK 217F (Notice 2), *Reliability Prediction of Electronic Equipment*, Department of Defence, Washington DC (USA), 1995.

[8] ICI database GEG 3.2.

[9] IEC 61508, parts 1-7, *Functional safety of electrical/ electronic/ programmable electronic safety-related systems*, 2002.

[10] NAMUR, “Interessengemeinschaft Automatisierungstechnik der Prozessindustrie”, http://www.namur.de.

[11] ZVEI, „Zentralverband Elektrotechnik- und Elektronikindustrie e.V.“, http://www.zvei.de.

VII. VITAE

Daniel Düpont graduated from the University of Kaiserslautern in 2004 with a Dipl.-Math. oec. degree. From 2004 till today he is research assistant at the Institute of Automatic Control at the University of Kaiserslautern, Germany. His major fields of research are methods for SIL proof evaluation.

Lothar Litz graduated from the University of Karlsruhe in 1975 with a Dipl.-Ing degree. In 1979 and 1982, respectively, he got his doctor and the Dr.-habil. degree from the same university. He was a control engineer with the German Hoechst AG between 1982 and 1992. From 1992 till today he is professor at the University of Kaiserslautern, Germany, and head of the Institute of Automatic Control. Since 2005 he is also vice president of the University of Kaiserslautern. Major fields of research and education are Safety-related Automatic Control, Failure Detection and Diagnosis, Ambient Intelligence and Wireless Networked Control Systems.

Pirmin Netter graduated from the University of Heidelberg in 1975 with a Dipl.-Phys. degree. In 1979 he received his doctorate. He was a control engineer with the German Hoechst AG between 1981 and 1996. From 1996 till today he is member of the Infraserv Höchst and head of the department for work and plant safety. His major fields of work are work safety, radiation protection and plant safety, especially plant safety by devices of process control engineering.

VIII. NOMENCLATURE

SIS	Safety instrumented system.
SIF	Safety instrumented function.
SIL	Safety integrity level.
R_P	Process risk (money per time unit).
R_T	Tolerable risk (money per time unit).
R_R	Residual risk (money per time unit).
LOPA	Layers of protection analysis.
PLC	Programmable logic controller.
HFT	Hardware fault tolerance (absolute).

SFF	Safe failure fraction (%).
PFD	Average probability of failure on demand (absolute).
*M*oo*N*	*M* out of *N* voting (absolute).
λ_{DU}	Rate of dangerous, undetected failures (FIT).
FIT	Failures in time (1/ 10^9h)
BPCS	Basic process control system.
RTD	Resistance temperature detector.
PTC	Proof test coverage (%).
T_{I}	Proof test interval (years).
L	Number of loops (absolute).
F_{DU}	Number of dangerous, undetected failures (absolute).
ΔT	Observation period (years).
$1 - \alpha$	Confidence level (%).
MTTR	Mean time to repair (years).
$MTTD_{\mathrm{DU}}$	Mean time to detection of dangerous, undetected failures (years).
p	Failure probability related to ΔT (absolute).
p_{low}	Lower confidence interval boundary of *p* (absolute).
p_{lup}	Upper confidence interval boundary of *p* (absolute).
PFD_{low}	Lower confidence interval boundary of *PFD* (absolute).
PFD_{up}	Upper confidence interval boundary of *PFD* (absolute).