TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

FB Elektro- und Informationstechnik
Lehrstuhl für Automatisierungstechnik
Prof. Dr.-Ing. habil. Lothar Litz

Projekt:
Durchführung einer Studie und Erstellung einer Methode zum Nachweis des „Safety Integrity Level (SIL)“ für PLT-Schutzeinrichtungen auf Basis statistischer Daten realisierter PLT-Schutzeinrichtungen

-Bericht-

Daniel Düpont
Kaiserslautern, den 30.04.2005

Inhalt

NOMENKLATUR 3

1 TOP-DOWN: ERWEITERTE AUSWERTUNG DER NAMUR-STÖRDATEN 2003 4

1.1 STANDARDBEWERTUNG 4

1.2 HYPOTHESENTEST 6

1.2.1 SIL-äquivalente Ausfallwahrscheinlichkeit 6

1.2.2 Modell des Hypothesentests 9

1.2.3 Ergebnis 12

1.3 KONFIDENZINTERVALLE 15

1.3.1 Theorie 15

1.3.2 Ergebnis 16

2 BOTTOM-UP: PFD-BERECHNUNG MIT TRAC (ABB) 18

2.1 ANNAHMEN UND EIGENSCHAFTEN DER SOFTWARE 18

2.2 BEISPIELBERECHNUNG EINES TYPICALS 25

2.2.1 Struktur und verwendete Komponenten 25

2.2.2 *PFD*-Bandbreite (Sensibilitätsanalyse) 27

2.3 BEWERTUNG 29

QUELLEN 30

Nomenklatur

Einige Abkürzungen:

SIL	Safety integrity level
SIF	Safety instrumented function
SFF	Safe failure fraction
HFT	Hardwarefehlertoleranz
n	Anzahl erfasster sicherheitsgerichteter Schaltungen
k	Anzahl passiver Fehler
ΔT	Beobachtungszeitraum
T_I	Wartungsintervall
MTBF	mittlere Zeit zwischen zwei Fehlern
PFD	Ausfallwahrscheinlichkeit im Anforderungsfall
λ	Fehlerrate
λ_D	Fehlerrate gefährlicher Fehler
λ_{DU}	Fehlerrate gefährlicher, unentdeckter Fehler
λ_{DD}	Fehlerrate gefährlicher, entdeckter Fehler
λ_S	Fehlerrate sicherer Fehler
λ_{SU}	Fehlerrate sicherer, unentdeckter Fehler
λ_{SD}	Fehlerrate sicherer, entdeckter Fehler
$p(\Delta T)$	Fehlerwahrscheinlichkeit am Ende des Betrachtungszeitraumes ΔT
H_0	Nullhypothese
H_1	Alternative
R	Ablehnungsbereich von H_0
KI_{PFD}	Konfidenzintervall

1 Top-Down: erweiterte Auswertung der NAMUR-Stördaten 2003

Alle im Rahmen dieses Kapitels durchgeführten Berechnungen sind, bedingt durch die zugrunde liegende Datenstruktur, nicht geeignet, den Einzelkreis zu bewerten oder ein Risk Assessment zu ersetzen. Sie dienen lediglich dazu, die Richtigkeit der bisherigen Instrumentierungspraxis der Stördatenlieferanten zu verifizieren und in späteren Projektstadien den Bottom-Up-Ansatz zu optimieren.

1.1 Standardbewertung

Im Zuge der NAMUR-Stördatenerfassung 2003 wurden mehr als 10000 einkanalige sicherheitsgerichtete Schaltungen erfasst. Aufgrund dieser Fülle an Rohdaten wurde eine Unterteilung in diverse Untergruppierungen vorgenommen, die als Unterscheidungskriterium die Art der überwachten Größe heranziehen. Sowohl für die Gesamtheit aller Kreise, als auch für jede Gruppe wurde die Anzahl der aufgetretenen passiven Fehler während des Betrachtungszeitraumes gespeichert.
Mehrkanalige Safety Instrumented Functions (SIF) wurden ebenfalls überwacht. Allerdings soll im Rahmen dieses Berichts noch keine weitergehende Auswertung erfolgen, da bei Mehrkanaligkeit eine erheblich größere Strukturvielfalt vorliegt als bei einkanaligen Kreisen. Im Detail hat der Anlagenbetreiber die Möglichkeit, den Redundanzgrad zu variieren und dabei homogen redundant, diversitär redundant oder sogar nur teilredundant auszulegen. Eine derartige Fülle an Strukturunterschieden bietet somit keine gute Grundlage für statistische Analysen. Eine Betrachtung mehrkanaliger Kreise scheint somit erst dann sinnvoll, sobald nähere Informationen vorliegen. Diese werden im Zuge einer erweiterten Stördatenerfassung in naher Zukunft zur Verfügung stehen, und man wird erneut über die Sinnhaftigkeit einer Auswertung redundant ausgelegter Loops rekapitulieren müssen. Art und Umfang der bei mehrkanaligen Kreisen zukünftig zu erfassenden Daten wurden von uns mit der NAMUR (Dr. Netter) abgestimmt.
Grundlage der durchgeführten statistischen Auswertungen bildet das in Tabelle I dargestellte Datenmaterial.

TABELLE I
NAMUR-Daten 2003
(einkanalige SIFs)
n: Anzahl der überwachten Loops
k: Anzahl entdeckter passiver Fehler
ΔT: Betrachtungszeitraum
T_I : Wartungsintervall

GRUPPE	n [absolut]	k [absolut]	ΔT [Jahre]	T_I [Jahre]
Total	12132	41	1	1
Druck (**P**)	1479	11	1	1
Temperatur (**T**)	1154	1	1	1
Füllstand (**L**)	1020	2	1	1
Analyse (**Q**)	417	6	1	0.25
Hand (**M**)	537	0	1	1
Andere	1526	6	1	1

Bei näherer Betrachtung von Tabelle I wird augenscheinlich, dass die einzelnen Gruppen in Summe nicht der Anzahl der Kreise der Gesamtheit entsprechen. Dieses Phänomen ist dadurch bedingt, dass nicht alle Unternehmen, die an der Datenerhebung teilnehmen,

Informationen bezüglich der Verteilung ihrer Safety Loops auf die verschiedenen Gruppierungen zur Verfügung stellen.
Für das Wartungsintervall waren ebenfalls nur schwer genaue Werte zu erhalten, was zu der Entscheidung führte, generell T_I auf 1 Jahr festzulegen. Eine Ausnahme repräsentieren dabei die Analysemessungen, die fast monatlich geprüft werden. Deshalb erschien es sinnvoll, hier speziell, unter Berücksichtigung des Worst-Case, einen Wert von 0,25 Jahren zu wählen. Es wurde allerdings darauf verzichtet, die Gruppe „Analyse“ bei Festlegung des Wartungsintervalls für „Total“ zu berücksichtigen, da der prozentuale Anteil von „Analyse“ an „Total“ sehr gering ist. Folglich ist man auch für „Total“ bei $T_I = 1$ Jahr geblieben. Dadurch sind die berechneten PFD-Werte der Gruppe „Total“ geringfügig schlechter als die tatsächlichen dieser Kategorie.
Für alle noch folgenden Ausführungen sei a priori bemerkt, dass die *PFD* als alleiniges Kriterium zur *SIL*-Einstufung gesehen wird. De facto schreiben die Normen IEC 61508 und IEC 61511 noch weitere Prämissen vor, die in diesem Kontext zu berücksichtigen sind. Dazu zählen beispielsweise die *HFT* und eine Kategorisierung der in der sicherheitsgerichteten Schaltung verwendeten Geräte in Typ A oder B. Für alle weiteren Betrachtungen seien diese Faktoren jedoch ausgeklammert.
Um nun aus dem bereitgestellten Datenmaterial *PFD*-Werte abzuleiten, benötigt man die Formel [4]:

$$PFD = \frac{0,5 \cdot T_I}{MTBF + 0,5 \cdot T_I} \tag{1}$$

Die empirische MTBF ist durch

$$MTBF = \frac{n \cdot \Delta T}{k} \tag{2}$$

bestimmbar.
Hieraus ergeben sich für die PFD-Berechnung die in Tabelle II dargestellten Werte.

TABELLE II
Standard-*PFD*-Berechnung
NAMUR-Daten 2003
(einkanalige SIFs)

GRUPPE	*MTBF* [Jahre]	*PFD* [absolut]	*SIL* [absolut]
Total	296	$1,69 \cdot 10^{-3}$	2
Druck (**P**)	135	$3,71 \cdot 10^{-3}$	2
Temperatur (**T**)	1154	$4,33 \cdot 10^{-4}$	3
Füllstand (**L**)	510	$9,79 \cdot 10^{-4}$	3
Analyse (**Q**)	70	$1,80 \cdot 10^{-3}$	2

Wie aus Tabelle II ersichtlich ist, werden generell bei allen Kategorien *PFD*-Werte erreicht, die eine Einstufung in SIL 2 rechtfertigen. Die Gruppen „Temperatur“ und „Füllstand“ halten sogar den Anforderungen für SIL 3 stand. Für sicherheitsgerichtete Schaltungen mit manueller Eingriffsmöglichkeit, sowie die Gruppe „Andere“ erfolgt keine Auswertung. Die Gründe hierfür werden später erläutert.
Problematisch wirkt sich bei diesem Verfahren allerdings aus, dass keiner Maßzahl für das Vertrauen in eine derartige Rechnung gegeben wird. Denn im Gegensatz dazu legt die Norm

[1] nahe, numerische Nachweise mit einem Mindestvertrauen von 70% abzusichern. Dies hat zur Folge, dass erweiterte statistische Methoden benötigt werden, um den Wahrheitsgehalt der Ergebnisse zu untermauern.

1.2 Hypothesentest

Ziel eines Hypothesentests ist es, eine Hypothese mit einem festgelegten Vertrauensniveau anzunehmen oder abzulehnen. Das Verfahren arbeitet stets mit zwei Mengen, genannt Hypothese und Alternative, die disjunkt sein müssen. Bei dem hier vorliegenden Fall könnte als Hypothese "höchstens *SIL* 1 ist erfüllt" gegen die Alternative "mindestens *SIL* 2 ist erfüllt" getestet werden. Nähere Informationen über die Theorie von Hypothesentests können in [3], [5] und [6] nachgelesen werden. In dem hier vorliegenden Fall wird das Verfahren verwendet, um *PFD*-Werte auf Basis statistischer Daten anzunehmen oder abzulehnen, was gleichsam für die damit verknüpfte *SIL*-Einstufung gilt. Als Vertrauensniveau werden die laut Norm [1] postulierten 70% angestrebt.

1.2.1 *SIL*-äquivalente Ausfallwahrscheinlichkeit

Betrachtet man die Fehlerhäufigkeit eines Sicherheitskreises während seiner Lebensdauer, wird eine Exponentialverteilung unterstellt, d.h.

$$F_{\exp}(t) = 1 - e^{-\lambda t}. \tag{3}$$

Durch Ersetzen der herkömmlichen Exponentialfunktion durch ihre Reihendarstellung

$$e^{x} = \sum_{i=0}^{\infty} \frac{x^{i}}{i!} \tag{4}$$

erhält man

$$F_{\exp}(t) = 1 - \left(1 + (-\lambda t) + \frac{(-\lambda t)^{2}}{2!} + \frac{(-\lambda t)^{3}}{3!} + \ldots\right). \tag{5}$$

Vorausgesetzt, t nimmt nur sehr kleine Werte ΔT an, kann $F_{\exp}(t)$ durch eine lineare Approximation angenähert werden (siehe Fig. 1).

$$F_{\exp}(\Delta T) = 1 - \left(1 + (-\lambda \Delta T) + 0\right) = \lambda \Delta T \tag{6}$$

Zusammenfassend gilt also für einen Betrachtungszeitraum ΔT, der klein im Vergleich zu $1/\lambda$ ist:

$$F_{\exp}(t) \approx F_{\exp}(\Delta T) = \lambda \Delta T \text{ für } \Delta T \text{ klein} \tag{7}$$

Wie aus Fig. 1 ersichtlich wird, bedeutet die Quantifikation "klein" eine sehr gute Annäherung für Werte von ΔT bis zu 10 Jahren in Verbindung mit kleinen *MTBFs* von höchstens ca. 50 Jahren.
So beträgt die Fehlerwahrscheinlichkeit $p(\Delta T)$ am Ende des Betrachtungszeitraumes ΔT:

$$p(\Delta T) = F_{\exp}(\Delta T) = \lambda \Delta T \tag{8}$$

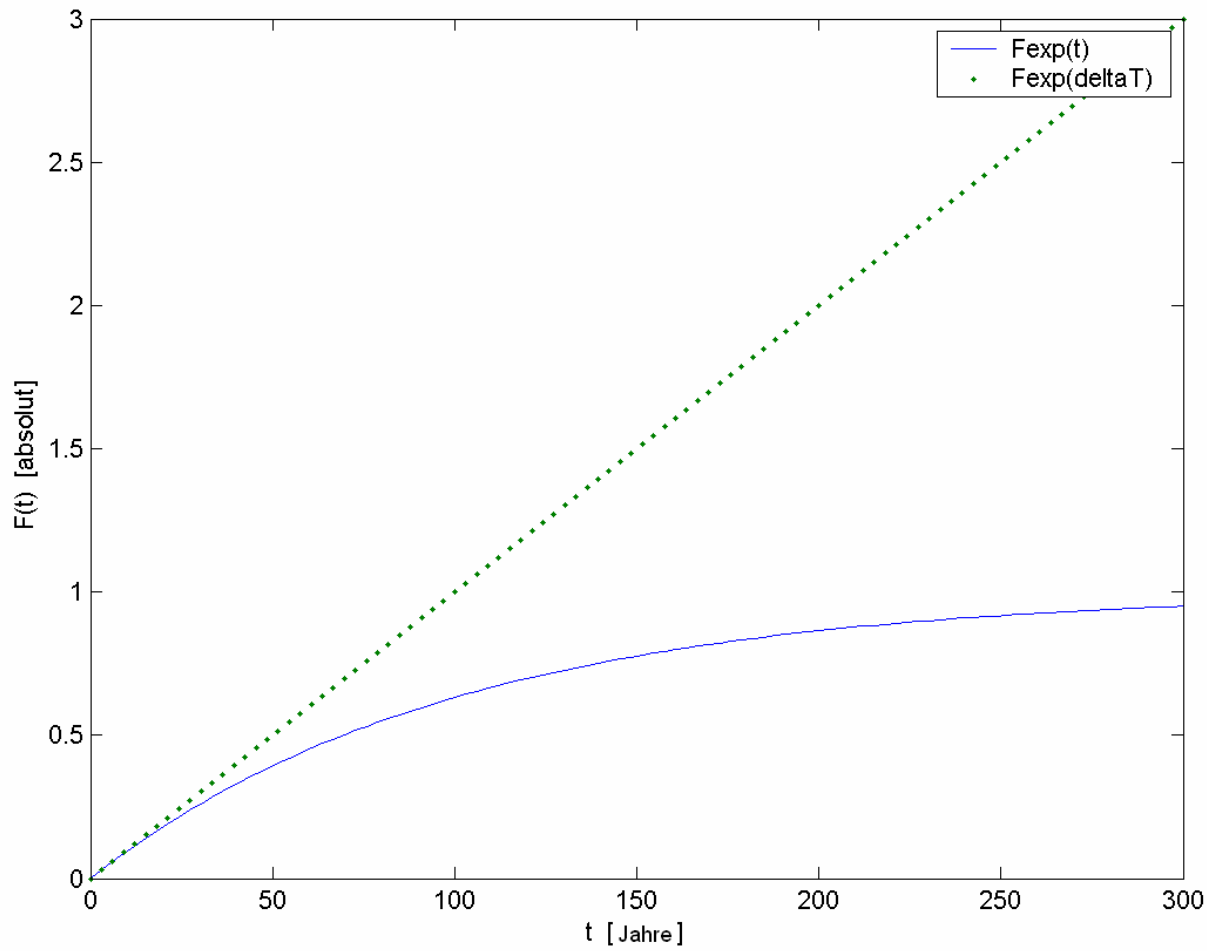

Fig. 1: Plot von $F_{\exp}(t)$ und $F_{\exp}(\Delta T)$ für $\lambda = 0,01$

Um eine hohe Verfügbarkeit des Sicherheitskreises zu gewährleisten, ist eine niedrige *PFD* zu postulieren. Diese Größe ist bei gegebener *MTBF* und bekanntem Wartungsintervall T_{I} bestimmbar durch

$$PFD = \frac{0,5 \cdot T_I}{MTBF + 0,5 \cdot T_I}. \tag{9}$$

[4]. Nach Umstellung dieser Formel erhält man:

$$MTBF = \frac{T_I \left(1 - PFD\right)}{2 \cdot PFD} \tag{10}$$

Da die Fehlerrate λ umgekehrt proportional zur *MTBF* ist, gilt:

$$\lambda = \frac{1}{MTBF} \tag{11}$$

Durch Ersetzung mit (11) in (8) erhält man eine Formel für die Fehlerwahrscheinlichkeit am Ende des Betrachtungszeitraumes.

$$p\left(\Delta T\right) = \frac{\Delta T}{MTBF} \tag{12}$$

Wird (10) zusätzlich berücksichtigt, erreicht man schließlich die angestrebte Form.

$$p(\Delta T) = \frac{2 \cdot PFD \cdot \Delta T}{T_I (1 - PFD)} \tag{13}$$

Unter Verwendung der *PFD*-Werte aus Tabelle III und einem Wartungsintervall von einem Jahr können die „Zielwahrscheinlichkeiten“ $p(\Delta T)$ für die einzelnen *SIL*s mit (13) bestimmt werden. Eine graphische Veranschaulichung dieser Abhängigkeit ist in Fig. 2 abgebildet. Ein Interpretationsversuch an dieser Formel führt zu einem scheinbaren Paradoxon, denn je kleiner das Wartungsintervall T_I, desto größer $p(\Delta T)$. Jedoch führt ein vermehrtes Prüfen des Sicherheitskreises de facto zu einer geringeren *PFD*. Folglich tritt das Phänomen auf, dass ohne Änderung der *PFD* des „Ziel-SILs“ die erlaubte „Zielwahrscheinlichkeit“ $p(\Delta T)$ mit schrumpfendem Wartungsintervall T_I wächst.

TABELLE III
SIL: *PFD*-Werte aus [1]

Niedrige Anforderungsrate		
SIL	Zielwert für die *PFD*	Zielwert für die Risikoreduktion
4	$10^{-5} \leq PFD < 10^{-4}$	> 10.000 to ≤ 100.000
3	$10^{-4} \leq PFD < 10^{-3}$	> 1.000 to ≤ 10.000
2	$10^{-3} \leq PFD < 10^{-2}$	> 100 to ≤ 1000
1	$10^{-2} \leq PFD < 10^{-1}$	> 10 to ≤ 100

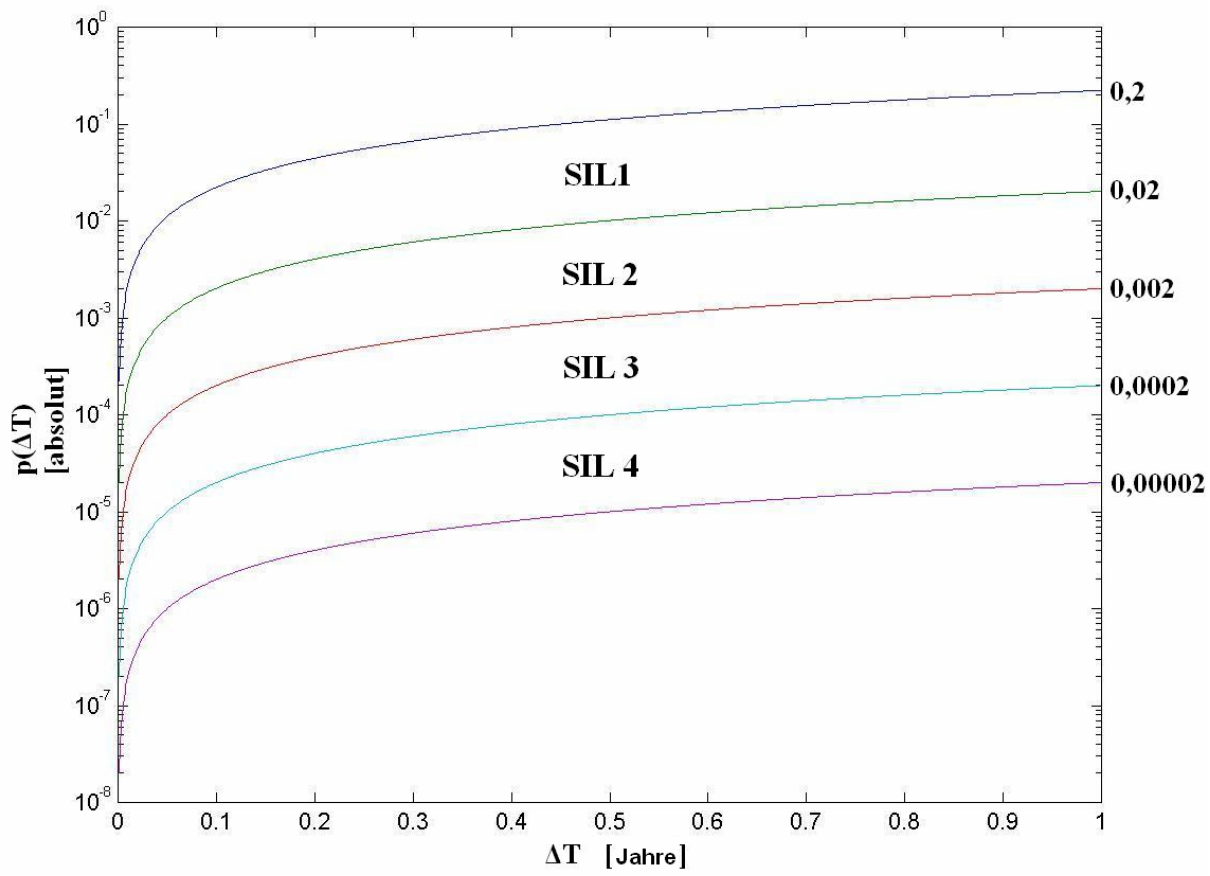

Fig. 2: Plot der „Zielwahrscheinlichkeiten“ $p(\Delta T)$ mit logarithmischer Skalierung

Dennoch steht weiterhin die Antwort auf eine wichtige Frage aus: Passen die “Zielwahrscheinlichkeiten” zu den gegebenen Größen *n* und *k* aus Tabelle I?

Um diese spezielle Eigenschaft nachzuweisen, sind die folgenden Transformationen notwendig. Unter Berücksichtigung, dass sich λ umgekehrt proportional zur MTBF verhält, gilt:

$$\lambda = \frac{k}{n \cdot \Delta T} \tag{14}$$

Ersetzt man nun λ in (8) durch (14), so ist das gewünschte Ergebnis erreicht.

$$p(\Delta T) = \lambda \cdot \Delta T = \frac{k}{n} \tag{15}$$

1.2.2 Modell des Hypothesentests

Bei Auswahl eines Testtyps erweist sich die Konstruktion eines Parametertests im Fall einer Nullhypothese als geeignet. Dem Begriff „Parametermenge“ kommt dabei eine Schlüsselrolle zu.

Definition 1: Die Menge aller Zahlen, die als mögliche Ausprägungen eines unbekannten Parameters ϑ einer Verteilungsfunktion in Frage kommen, heißt Parametermenge Θ.

Dabei bezeichnet ϑ die “Zielwahrscheinlichkeit” *p(ΔT)* aus (13).

$$\vartheta = p(\Delta T) \in [0,1] = \Theta \tag{16}$$

Bevor es möglich ist, de facto eine Nullhypothese zu wählen, sollte folgende Bemerkung beachtet werden.

Bemerkung: Wird eine Nullhypothese H_0 abgelehnt, kann man die Alternative H_1 mit Vertrauen $1-\alpha$ als wahr ansehen. Ist H_0 nicht ablehnbar, kann die damit verbundene Fehlerwahrscheinlichkeit sehr hoch sein. Vor diesem Hintergrund sollte der gewünschte Ausgang immer als Alternative H_1 gewählt werden.

Der Hypothesentest zielt also darauf ab, eine Entscheidung für ein Statement der Form “mindestens *SIL* z” zu treffen. Umgekehrt wird also eine Nullhypothese derart formuliert: „höchstens *SIL* z”. Da *p(ΔT)* mit steigendem *SIL* fällt, muss die Form von H_0 und H_1 eine bestimmte Eigenschaft erfüllen.

$$H_0 \in [g,1] \text{ und } H_1 \in [0,g[\text{ mit } 0 < g < 1 \tag{17}$$

Daher

$$H_0 : p(\Delta T) \geq g \text{ und } H_1 : p(\Delta T) < g \,. \tag{18}$$

Beispiel:

H_0: „höchstens *SIL* 1”
versus
H_1: „mindestens *SIL* 2”

Unter Verwendung von Tabelle III kann dies umformuliert werden zu

H_0: $PFD \geq 0{,}01$ versus. H_1: $PFD < 0{,}01$.

Mit Hilfe von (13) ergibt sich für $T_1 = 1$ Jahr und $g = 0{,}02$

H_0: $p(\Delta T) \geq 0{,}02$ vs. H_1: $p(\Delta T) < 0{,}02$ (siehe Fig. 3).

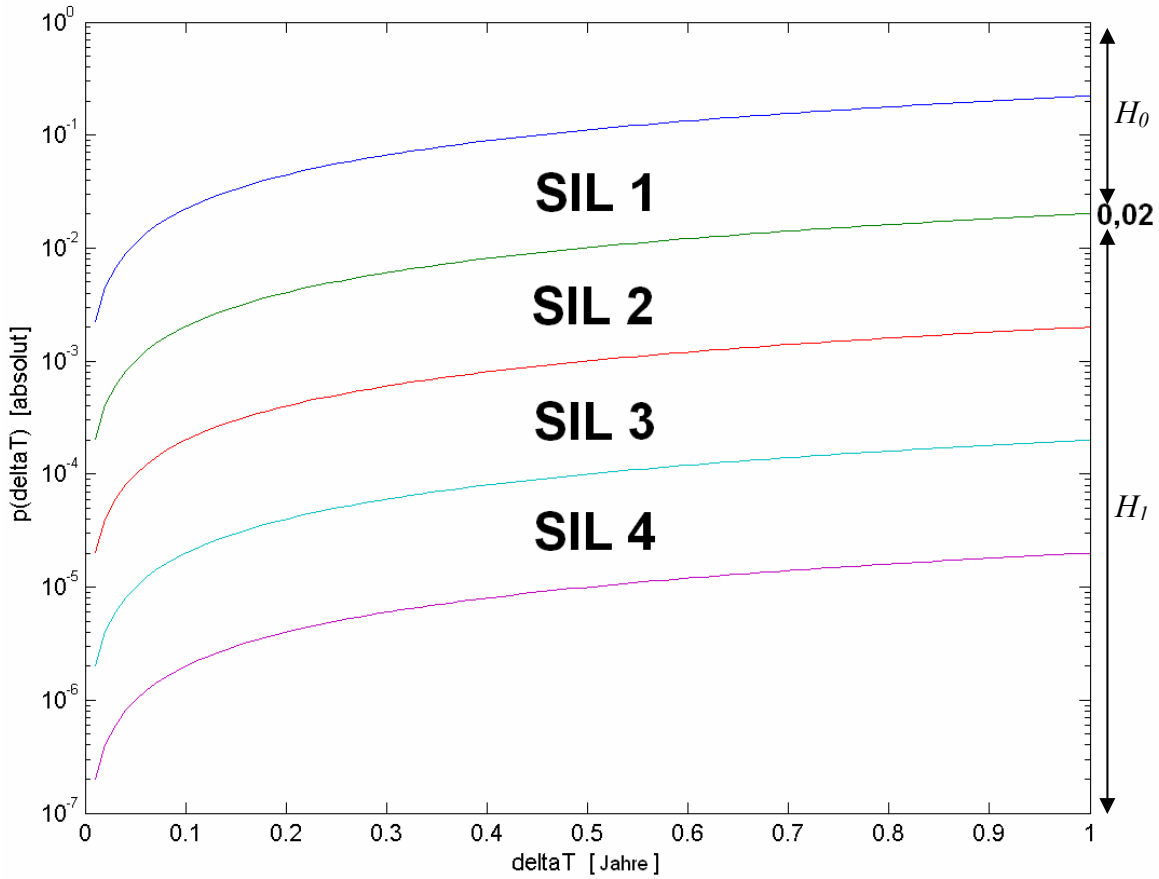

Fig. 3: Plot der H_0- und H_1-Gebiete mit logarithmischer Skalierung

Nun muss eine dem Test unterstellte Verteilung gewählt werden. Da keine Informationen bezüglich des zeitlichen Auftretens passiver Fehler innerhalb des Betrachtungszeitraumes zur Verfügung stehen, was auf die Fehlerdiagnostik, die nur während der Wartung stattfindet, zurückzuführen ist, scheint die Binomialverteilung eine geeignete Wahl. Um diese Lösung allerdings zulässig zu machen, ist eine Restriktion zu formulieren.

Annahme: Während des Beobachtungszeitraumes ΔT kann in einem Sicherheitskreis nur ein passiver Fehler auftreten, d.h. entweder weist ein Loop einen passiven Fehler auf, oder er ist intakt.

Darüber hinaus wird eine Zufallsvariable, welche die Anzahl auftretender passiver Fehler modelliert, benötigt.

Definition 2: Sei X eine diskrete Zufallsvariable mit Wertebereich $X = \{0, 1,..., n\}$, welche die Anzahl defekter Loops unter n Kreisen beschreibt.

Also entspricht die Wahrscheinlichkeit, unter n Kreisen x defekte zu haben, bei Fehlerwahrscheinlichkeit $p(\Delta T)$:

$$P_{p(\Delta T)}\left(X=x\right)=b_{n,p(\Delta T)}\left(x\right)=\binom{n}{x}p\left(\Delta T\right)^{x}\left(1-p\left(\Delta T\right)\right)^{n-x} \tag{19}$$

Da laut H_0 gefordert wird, dass $p(\Delta T) \geq g$ gilt, muss der Ablehnungsbereich R von H_0 alle Werte x von X enthalten, die kleiner oder gleich einer Untergrenze $t \in X$ sind, d.h.

$$\mathrm{R} = \{\mathrm{x} \in \mathrm{X}: \mathrm{x} \leq \mathrm{t}, \mathrm{t} \in \mathrm{X}\}. \tag{20}$$

Verbindet man die Erkenntnisse von (18) und (19) resultiert

$$\beta\left(p\left(\Delta T\right)|\,t,n\right)=P_{p(\Delta T)}\left(X\leq t\right)=\sum_{x=0}^{t}\binom{n}{x}p\left(\Delta T\right)^{x}\left(1-p\left(\Delta T\right)\right)^{n-x}. \tag{21}$$

Definition 3: Bei einem Hypothesentest liegt ein Fehler erster Ordnung vor, falls eine wahre Nullhypothese H_0 abgelehnt wird. Die Wahrscheinlichkeit, einen Fehler erster Ordnung zu begehen, wird mit α bezeichnet.
Entsprechend liegt ein Fehler zweiter Ordnung vor, wenn eine falsche Nullhypothese H_0 angenommen wird. Dabei wird die Wahrscheinlichkeit, einen Fehler zweiter Ordnung zu begehen, mit β deklariert.

Falls $p(\Delta T) \in H_0$ gilt, bezeichnet (21) die Wahrscheinlichkeit, einen Fehler erster Ordnung zu begehen. Daher folgt für gegebenes α:

$$\beta\left(p\left(\Delta T\right)|\,t,n\right)\leq\alpha \tag{22}$$

Falls $p(\Delta T) \in H_1$ ist, stellt (21) die sog. Macht des Tests dar. Nimmt die Macht des Tests einen Wert nahe bei 1 an, so ist die Wahrscheinlichkeit

$$\beta=1-\beta\left(p\left(\Delta T\right)|\,t,n\right), \tag{23}$$

einen Fehler zweiter Ordnung zu begehen, sehr klein.
Fig. 4 verdeutlicht den Zusammenhang zwischen α und β. Zu Demonstrationszwecken wird das Kriterium von Moivre-Laplace als erfüllt angenommen, also konvergiert die Binomial- gegen die Normalverteilung.

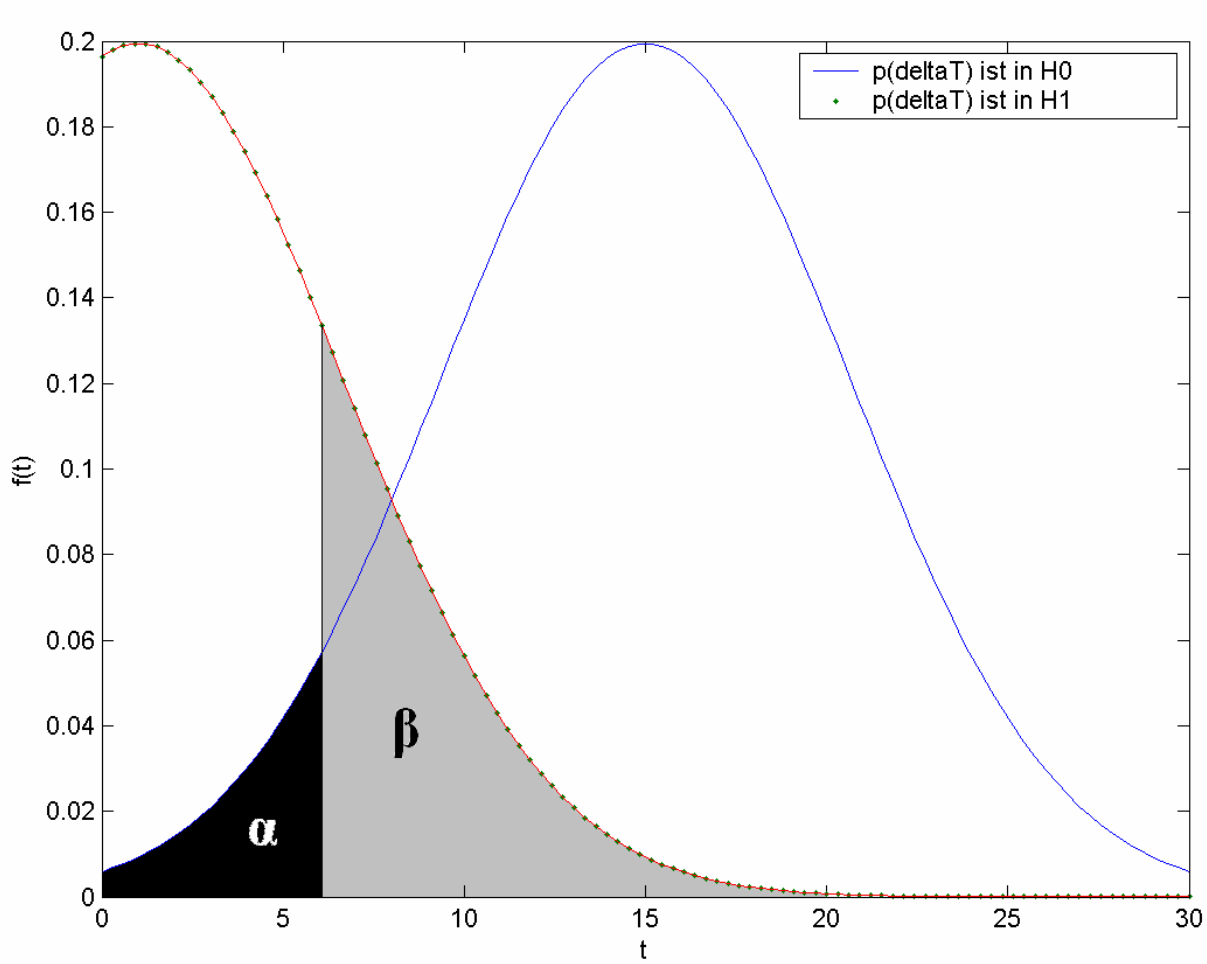

Fig. 4: Visualisierung von α und β

1.2.3 Ergebnis

Die mittels Durchführung von Hypothesentests auf Basis der NAMUR-Stördaten (siehe Tabelle I) gewonnenen Erkenntnisse sind in Tabelle IV bis VIII illustriert. Die Gruppen „Hand“ und „Andere“ werden bewusst ausgelassen. Die erste aufgrund der Tatsache, dass es eine manuelle Möglichkeit gibt, in das System einzugreifen, und die zweite, da hier eine Vielfalt unterschiedlicher, überwachter Größen vermischt wurde.
Zunächst wird die Hypothese „höchstens SIL 1“ gegen die Alternative „mindestens SIL 2“ untersucht, um SIL 2 nachzuweisen.
Anschließend führt man das entsprechende Verfahren mit “mindestens SIL 3” als Alternative zum Nachweis von SIL 3 durch. Zusätzlich sei nochmals angemerkt, dass bei allen Tests das laut [1] geforderte Mindestvertrauen von 70% angestrebt wird. Folglich muss die Wahrscheinlichkeit eines Fehlers erster Ordnung, α , kleiner oder gleich 0,3 sein.
Ziel ist es nun, H_0 abzulehnen und H_1 als wahr anzunehmen, was zur Folge hat, dass untersucht wird, wie α zu belegen ist, damit die Anzahl aufgetretener passiver Fehler k Element des Ablehnungsbereiches R von H_0 ist. Ist diese Eigenschaft erfüllt, bezeichnet $1-\alpha$ das Vertrauen in H_1. Wird die Analyse so praktiziert, muss die Wahrscheinlichkeit eines Fehlers zweiter Ordnung nicht betrachtet werden. Denn mitunter kann es sehr problematisch sein festzulegen, wie groß die Abweichung von der Hypothese sein darf, damit die Macht des Tests einen aussagekräftigen Wert annimmt. Um der Notwendigkeit einer solchen Diskussion vorzubeugen, wird das Verfahren in der erläuterten Struktur angewendet und so ein weiterer Unsicherheitsfaktor ausgeklammert.

TABELLE IV
Gruppe “Total”

H_0: höchstens *SIL* 1	H_1: mindestens *SIL* 2
$PFD \geq 0{,}01$	$PFD < 0{,}01$
$p(1) \geq 0{,}02$	$p(1) < 0{,}02$

Ergebnis	Vertrauen
H_1 gilt	99%

H_0: höchstens *SIL* 2	H_1: mindestens *SIL* 3
$PFD \geq 0{,}001$	$PFD < 0{,}001$
$p(1) \geq 0{,}002$	$p(1) < 0{,}002$

Ergebnis	Vertrauen
H_1 gilt	0,07%

TABELLE V
Gruppe “Druck”

H_0: höchstens *SIL* 1	H_1: mindestens *SIL* 2
$PFD \geq 0{,}01$	$PFD < 0{,}01$
$p(1) \geq 0{,}02$	$p(1) < 0{,}02$

Ergebnis	Vertrauen
H_1 gilt	99%

H_0: höchstens *SIL* 2	H_1: mindestens *SIL* 3
$PFD \geq 0{,}001$	$PFD < 0{,}001$
$p(1) \geq 0{,}002$	$p(1) < 0{,}002$

Ergebnis	Vertrauen
H_1 gilt	0,01%

TABELLE VI
Gruppe “Temperatur”

H_0: höchstens *SIL* 1	H_1: mindestens *SIL* 2
$PFD \geq 0{,}01$	$PFD < 0{,}01$
$p(1) \geq 0{,}02$	$p(1) < 0{,}02$

Ergebnis	Vertrauen
H_1 gilt	99%

H_0: höchstens *SIL* 2	H_1: mindestens *SIL* 3
$PFD \geq 0{,}001$	$PFD < 0{,}001$
$p(1) \geq 0{,}002$	$p(1) < 0{,}002$

Ergebnis	Vertrauen
H_1 gilt	67,13%

TABELLE VII
Gruppe “Füllstand”

H_0: höchstens *SIL* 1	H_1: mindestens *SIL* 2
$PFD \geq 0{,}01$	$PFD < 0{,}01$
$p(1) \geq 0{,}02$	$p(1) < 0{,}02$

Ergebnis	Vertrauen
H_1 gilt	99%

H_0: höchstens *SIL* 2	H_1: mindestens *SIL* 3
$PFD \geq 0{,}001$	$PFD < 0{,}001$
$p(1) \geq 0{,}002$	$p(1) < 0{,}002$

Ergebnis	Vertrauen
H_1 gilt	33,42%

TABELLE VIII
Gruppe “Analyse”

H_0: höchstens *SIL* 1	H_1: mindestens *SIL* 2
$PFD \geq 0{,}01$	$PFD < 0{,}01$
$p(0{,}25) \geq 0{,}081$	$p(0{,}25) < 0{,}081$

Ergebnis	Vertrauen
H_1 gilt	99%

H_0: höchstens *SIL* 2	H_1: mindestens *SIL* 3
$PFD \geq 0{,}001$	$PFD < 0{,}001$
$p(0{,}25) \geq 0{,}0081$	$p(0{,}25) < 0{,}0081$

Ergebnis	Vertrauen
H_1 gilt	5,27%

Die Auswertung des Hypothesentests liefert interessante Ergebnisse. Sowohl für die Gesamtheit aller einkanaligen sicherheitsgerichteten Schaltungen, als auch jede Einzelgruppierung kann *SIL* 2 nachgewiesen werden. Hinzu kommt, dass der Nachweis sogar mit einem Vertrauensniveau von $1-\alpha = 99\,\%$ durchführbar ist.

Hinsichtlich eines *SIL* 3-Nachweises spiegeln die Ergebnisse nicht das gewünschte Bild wider. Weder für die Summe aller Loops, noch die einzelnen Kategorien lässt sich ein *SIL* 3 mit dem Mindestvertrauen von 70% nachweisen. Zu bemerken ist allerdings, dass die Gruppe „Temperatur“ mit 67% Vertrauen sehr nahe am Zielwert anzusiedeln ist, im Gegensatz zu allen anderen Gruppen, die diesen weit verfehlen.

Vergleicht man die Resultate des Tests mit denen der Standardbewertung, so stimmen sie größtenteils überein. Die *SIL* 3-Tauglichkeit der Temperatur- und Füllstandsüberwachungen lässt sich beim Hypothesentest im Gegensatz zur Standardauswertung nicht manifestieren.

Eine Verbesserung der *PFD*-Werte wäre jedoch durchaus mittels einer Erhöhung der Anzahl erfasster Kreise möglich, sofern die Zahl auftretender passiver Fehler in gleichem Maße nicht überproportional steigen würde.

1.3 Konfidenzintervalle

1.3.1 Theorie

Die Theorie zur Bestimmung von Konfidenzintervallen ist sehr eng verwandt mit dem bereits erläuterten Hypothesentest. Dies betrifft sowohl den Inhalt, als auch die zugrunde liegende Methodik des Verfahrens. Dadurch bedingt, behalten die im vorigen Kapitel getätigten Annahmen und Einschränkungen auch weiterhin Gültigkeit.
Unter der Prämisse einer Binomialverteilung kann das Verfahren zur Bestimmung von Konfidenzintervallen aus [7] auf die aktuelle Problemstellung angepasst werden. Nach Transformation der Größe „Verfügbarkeit“ zu ihrem Komplement „Fehlerwahrscheinlichkeit” ergeben sich die angestrebten Formeln zur Bestimmung der Intervallgrenzen.
Für gegebenes Vertrauensniveau von $1-\alpha$ gilt:

$$p_{low}(\Delta T)=\begin{cases} 0 \qquad \textit{für } k=0 \\ \max\limits_{p(\Delta T)} \sum\limits_{x=k}^{n} \binom{n}{x} \left(1-p(\Delta T)\right)^{n-x} p(\Delta T)^{x} \le \alpha \quad \textit{für } k=n \\ \max\limits_{p(\Delta T)} \sum\limits_{x=k}^{n} \binom{n}{x} \left(1-p(\Delta T)\right)^{n-x} p(\Delta T)^{x} \le \frac{\alpha}{2} \quad \textit{sonst} \end{cases} \tag{24}$$

$$p_{up}(\Delta T)=\begin{cases} 1 \qquad \textit{für } k=n \\ \min\limits_{p(\Delta T)} \sum\limits_{x=0}^{k} \binom{n}{x} \left(1-p(\Delta T)\right)^{n-x} p(\Delta T)^{x} \le \alpha \quad \textit{für } k=0 \\ \min\limits_{p(\Delta T)} \sum\limits_{x=0}^{k} \binom{n}{x} \left(1-p(\Delta T)\right)^{n-x} p(\Delta T)^{x} \le \frac{\alpha}{2} \quad \textit{sonst} \end{cases} \tag{25}$$

Die korrespondierenden Lösungen von (24) und (25) können mittels iterativer Methoden bestimmt werden. Variablenbezeichnungen und sonstige Notationen wurden vom Hypothesentest übernommen.
Nachdem das Maximierungs-/Minimierungsproblem in (24)/(25) gelöst ist, ergibt sich eine andere Unwägbarkeit. Um einen Vergleich zwischen den *PFD*-Bandbreiten aus Tabelle III und den Konfidenzintervallen, die mittels obiger Formeln ermittelt werden, durchzuführen, ist es notwendig, die Ergebnisse auf die *PFD*-Ebene zu transformieren. Zu diesem Zweck muss eine Betrachtung der Faktoren „Wartungsintervall“ und „Betrachtungszeitraum“ in die Vertrauensgrenzen integriert werden. Eine solche Umformung ist möglich, indem man die bereits beschriebene Prozedur zur Bestimmung der *SIL*-äquivalenten Fehlerwahrscheinlichkeit in umgekehrter Richtung anwendet.
Unter Verwendung von $p(\Delta T)$ kann die *MTBF* geschrieben werden als

$$MTBF=\frac{\Delta T}{p(\Delta T)}. \tag{26}$$

Ersetzt man die *MTBF* in (9) durch (26), führt dies zu

$$PFD = \frac{T_I \cdot p(\Delta T)}{2 \cdot \Delta T + T_I \cdot p(\Delta T)}. \tag{27}$$

Mittels (27) können die Werte für $p_{\text{low}}(\Delta T)$ und $p_{\text{up}}(\Delta T)$ zu PFD_{low} und PFD_{up} transformiert werden. Schließlich ergibt sich das gesuchte Konfidenzintervall für die *PFD*.

$$KI_{PFD} = \left[PFD_{low}; PFD_{up} \right] \tag{28}$$

1.3.2 Ergebnis

Wertet man die NAMUR-Daten 2003 aus Tabelle I gemäß dieser Methode aus, ergeben sich zunächst Konfidenzintervalle für $p(\Delta T)$. Durch eine Transformation entsprechend (27) wird die Berücksichtigung des Wartungsintervalls und des Betrachtungszeitraums in die Resultate integriert.
Für jede Gruppierung der Rohdaten werden auf diese Weise *PFD*-Spannen ermittelt. Dabei wird als Vertrauensniveau die Untergrenze von 70% laut [1] fixiert.
Das Ergebnis ist in Tabelle IX dargestellt. Erneut wurden die Gruppen „Hand“ und „Andere“ aus den bereits erläuterten Gründen nicht ausgewertet.

TABELLE IX
PFD-Konfidenzintervalle
NAMUR-Daten 2003 (einkanalig)

GRUPPE	KI_{PFD} [PFD_{low}; PFD_{up}]
Total	[0,00142; 0,00201]
Druck (**P**)	[0,00258; 0,00523]
Temperatur(**T**)	[0,00008; 0,00146]
Füllstand (**L**)	[0,00034; 0,00231]
Analyse (**Q**)	[0,00107; 0,00289]

Als Erklärung für das KI_{PFD}-Verhalten ist zu erwähnen, dass je größer die Anzahl überwachter Kreise, desto kleiner die Intervallbreite. Besonders deutlich ist diese Eigenart bei einem Vergleich der Gruppen “Total” und “Analyse” erkennbar.
Um zu verdeutlichen, wie die errechneten *PFD*-Bandbreiten über die verschiedenen *SIL*-*PFD*-Spannen verteilt sind, bieten sich zwei Darstellungsmöglichkeiten an.
Einerseits kann eine graphische Illustration verwendet werden, indem man die einzelnen Konfidenzintervalle über einem *SIL*-*PFD*-Band plottet, das aus optischen Gründen logarithmisch skaliert ist (siehe Fig. 5).
Andererseits kann eine exakte numerische Verteilung als prozentuale Anteile des KI_{PFD} in Bezug auf die *SIL*-*PFD*-Spannen berechnet werden (siehe Tabelle X).
Beide Möglichkeiten liefern eine gute und verständliche Darstellung, aus der die essentiellen Aussagen der Ergebnisse ablesbar sind.

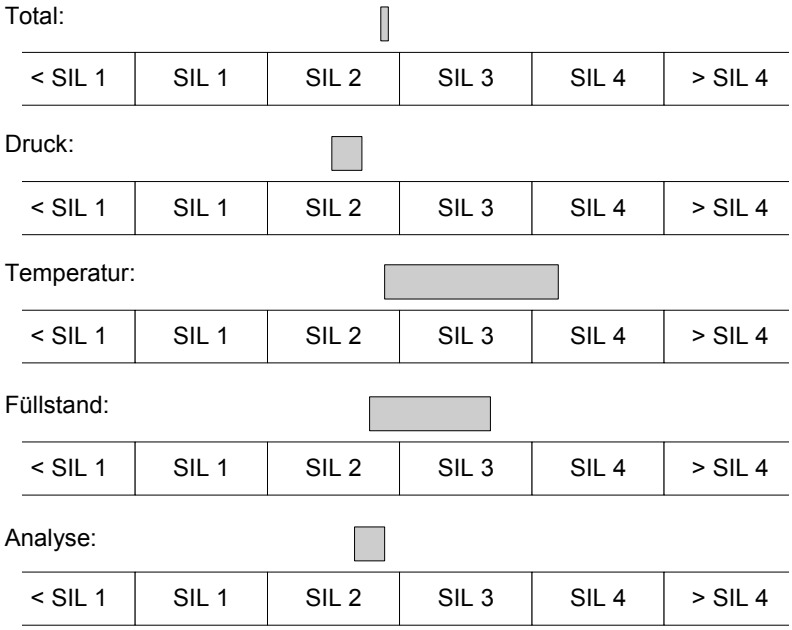

Fig. 5: Graphische KI_{PFD}-Klassifikation mit logarithmischer Skalierung

TABELLE X
Prozentuale Anteile der KI_{PFD}s

GRUPPE	< *SIL* 1 [%]	*SIL* 1 [%]	*SIL* 2 [%]	*SIL* 3 [%]	*SIL* 4 [%]	> *SIL* 4 [%]
Total	0	0	100	0	0	0
Druck (**P**)	0	0	100	0	0	0
Temperatur(**T**)	0	0	4	79	17	0
Füllstand (**L**)	0	0	17	83	0	0
Analyse (**Q**)	0	0	100	0	0	0

Im Kern decken sich die Aussagen der Konfidenzintervalle mit denen des Hypothesentests. Der *SIL* 2-Nachweis ist bei allen Intervallen unkritisch, wohingegen *SIL* 3 nicht konsolidierbar ist, was wiederum die Unzulänglichkeit der Standardbewertung unterstreicht. Obwohl 96% bei Temperaturüberwachung und 83% der Füllstandskontrolle im *SIL* 3-Bereich der *PFD* oder sogar besser liegen, kann dies nicht als Nachweis gelten. Die Begründung folgt aus der Tatsache heraus, dass die übrigen 4% bzw. 17% in das *SIL* 2-Spektrum reichen.
Zur Verbesserung des Ergebnisses kann sich der gleichen „Stellschrauben“ bedient werden, die bereits beim Hypothesentest erwähnt wurden. Vor diesem Hintergrund scheint eine Erweiterung des Dateneinzugskreises, sprich die Akquirierung neuer, zusätzlicher Stördatenlieferanten, sehr empfehlenswert.

2 Bottom-Up: PFD-Berechnung mit TRAC (ABB)

2.1 Annahmen und Eigenschaften der Software

Bevor auf Details der Software näher eingegangen wird, zunächst einige allgemeine Bemerkungen.
Das im Folgenden verwendete Tool des Herstellers „ABB“ zur Bewertung von sicherheitsgerichteten Schaltungen trägt den Namen „TRAC“. Als Basis wird die Version 2.2 (33) eingesetzt. Besonderes Augenmerk fällt dabei auf die Fähigkeit des Pakets, das gesamte Spektrum von Risikoanalyse, über Instrumentierung, bis zur *SIL*-Verifikation bearbeiten zu können. Zwangsläufig steigt ergo die Komplexität der Software, was mittels Integration finanzieller Aspekte noch zusätzlich forciert wird. Allerdings ist eine Vermischung von Kostenfaktoren und Sicherheitsaspekten nicht zulässig, wird bei TRAC jedoch praktiziert. Begründet ist diese Programmeigenschaft durch den geographischen Ursprung der Software, der in England zu finden ist. Dort steht man einer Verquickung von Sicherheits- und Finanzaspekten durchaus offen gegenüber.
Zunächst wird eine Einweisung in die wichtigen Grundzüge des Tools gegeben, wobei für die Zwecke des Projektes nur der numerische *SIL*-Nachweis relevant ist. Dieser Punkt wird während des Kapitels 2.2 nochmals explizit und detailliert kommentiert werden.
Nachdem eine neue Safety Function angelegt ist, sind einige grundlegende Informationen vom Benutzer einzugeben (siehe Fig. 6).

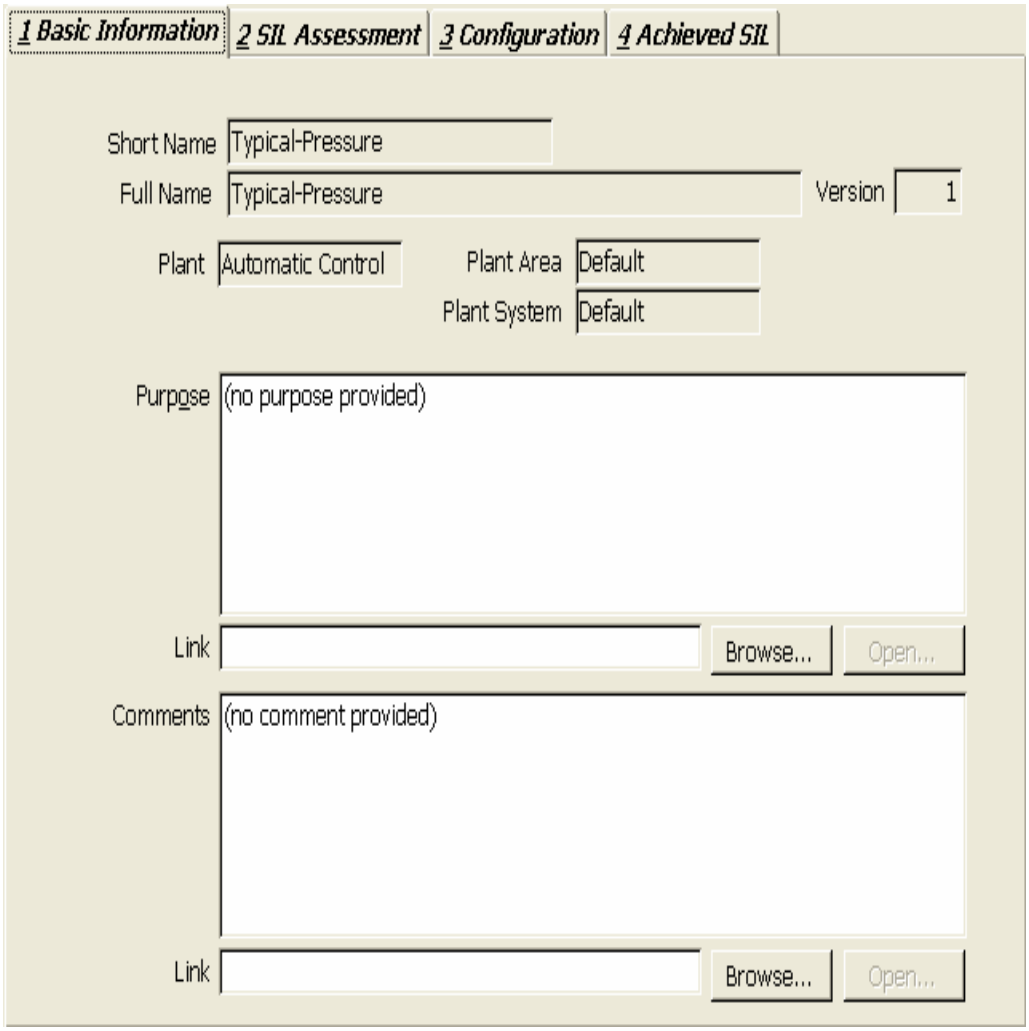

Fig. 6: Allgemeine Informationen zur SIF

Zusätzlich besteht die Möglichkeit, die Richtigkeit der Eingaben durch Hinterlegung von Quellen (Link) zu untermauern. Die Versionsnummer wird nicht näher kommentiert, da diese zur Thematik „Security“ zu rechnen ist.
Im Anschluss folgt das sog. „*SIL*-Assessment“ (siehe Fig. 7).

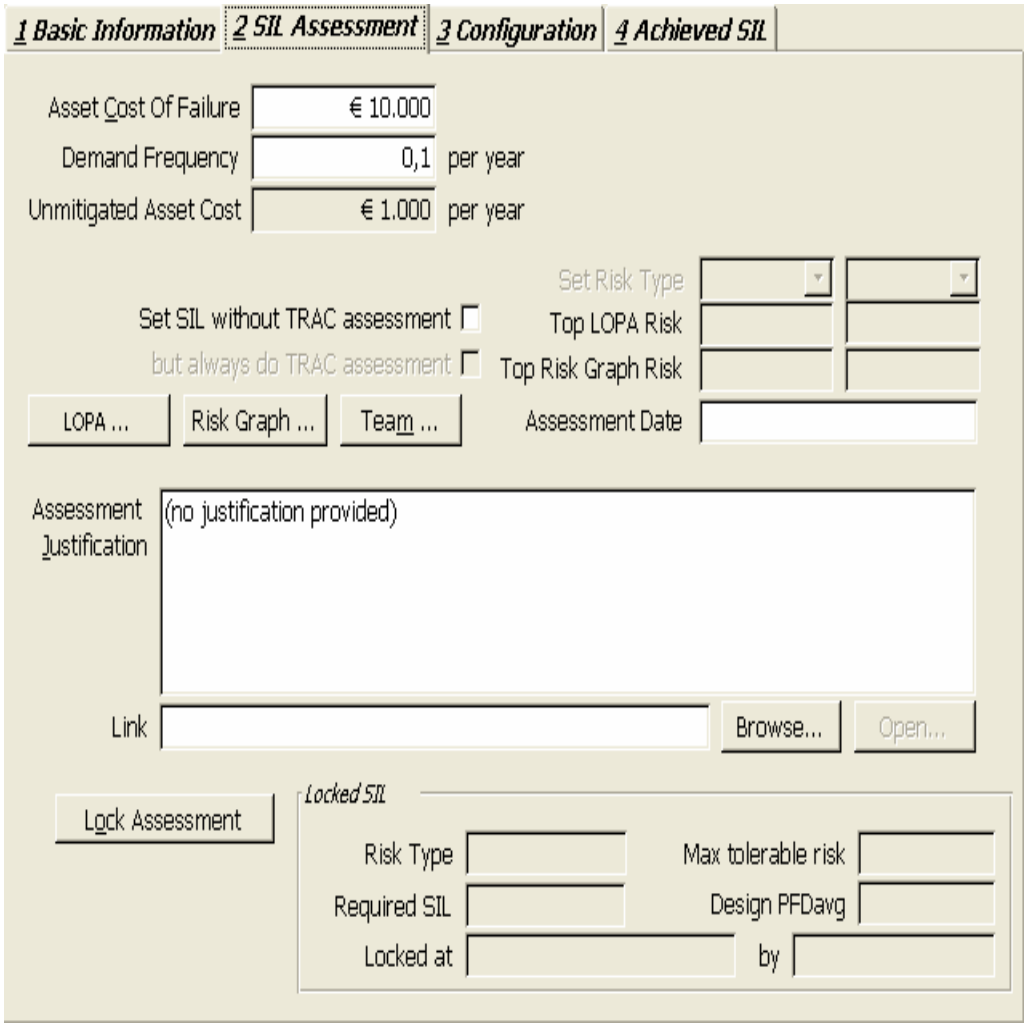

Fig. 7: SIL-Assessment der SIF

Als Instrumente zur Risikoanalyse hat der User die LOPA-Methode und den Risikographen zur Auswahl, wobei letzteres das in Deutschland bevorzugte Verfahren darstellt. Am Ende der Karteikarte erfolgt die Fixierung des *SIL*s, dem die SIF genügen muss. Auffällig wird zudem die bereits angesprochene Verknüpfung finanzieller und sicherheitsrelevanter Aspekte, denn nach Eingabe der Ausfallkosten (Asset Cost Of Failure) wird sofort die Anforderungsrate (Demand Frequency) quantifiziert. Diese Größe hat direkten Einfluss auf die Struktur des Risikographen (siehe Fig. 8), denn je nach dem dort festgelegten Wert wird eine bestimmte Eintrittswahrscheinlichkeit im Risikographen vorgeschrieben. Wählt der User nicht die mit einem Stern markierte Eintrittswahrscheinlichkeit W 1-3, so erscheint eine Fehlermeldung, die auf Inkonsistenz des Graphen hinweist. Jedoch ist die Anforderungsrate nicht mit der Schadenseintrittswahrscheinlichkeit identisch, da beispielsweise fest verbaute Schutzeinrichtungen ebenfalls eine Rolle spielen. Ferner wird durch den Einfluss einer quantitativen Größe (Demand Frequency) auf ein qualitatives Instrument (Risikograph) eine nicht zulässige Verknüpfung vorgenommen. Jedoch wurde von Seiten des Herstellers in diesem Punkt Nachbesserung zugesichert.

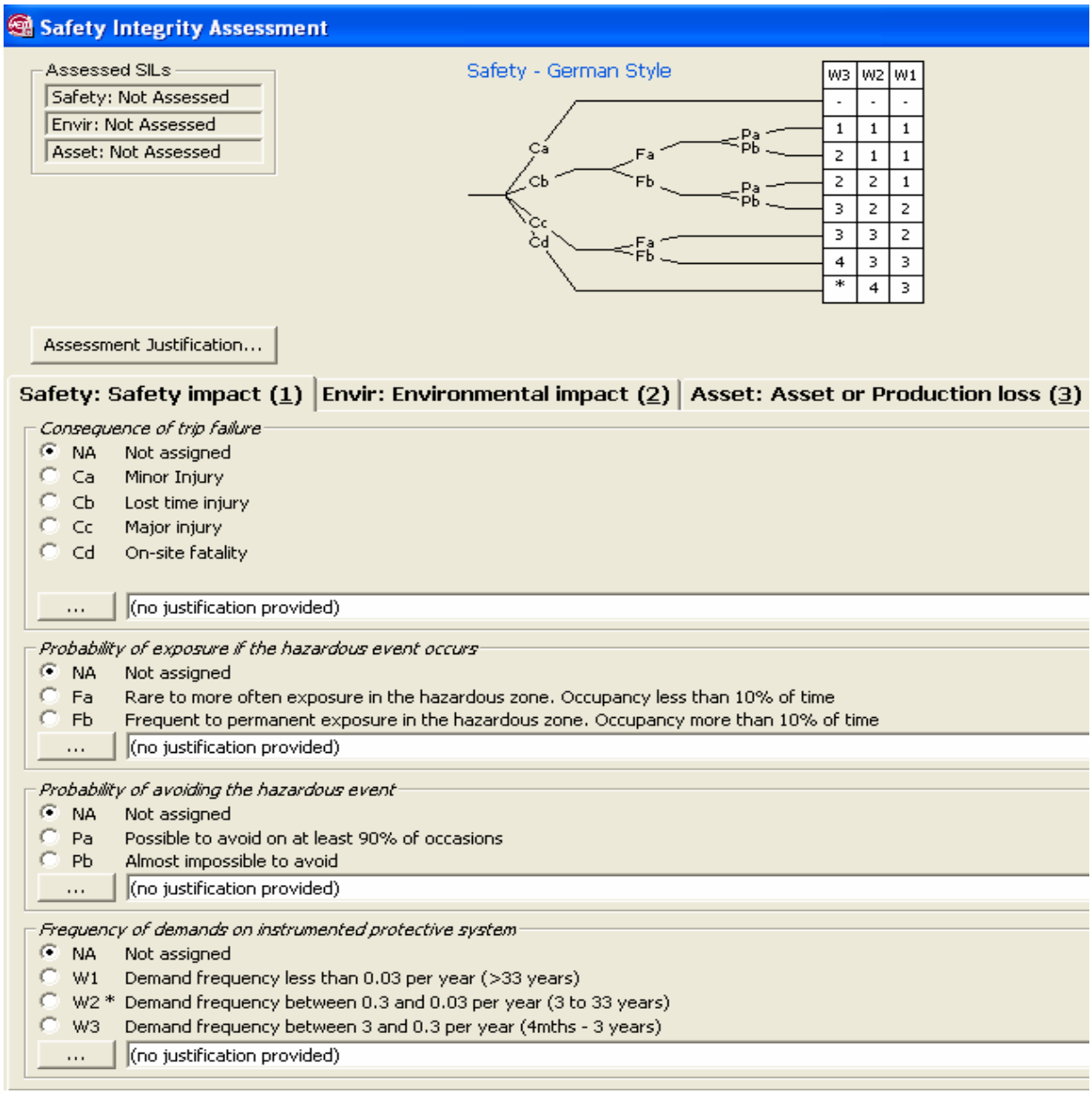

Fig. 8: Risikograph

Außerdem kann der Benutzer eine Risikobewertung mit bis zu drei Graphen gleichzeitig vornehmen, von denen einer erneut einen finanziellen Hintergrund aufweist (Asset Or Production Loss), wie anhand der Karteikarten in Fig. 8 ersichtlich ist. Vorteilhaft gereicht jedoch die flexible Strukturanpassung des Risikographen, der in Fig. 8 bereits auf die in Deutschland empfohlene Form umdefiniert ist (Safety-German Style).
Nach Abschluss der Risikoanalyse und somit der Festlegung eines „Soll-*SIL*s“ wird die Architektur und die Instrumentierung der SIF behandelt (siehe Fig. 9). Dies beinhaltet sowohl die Angabe der verbauten Komponenten/ Einzelgeräte als auch den Redundanzgrad für Eingabe-, Logik- und Aktorteil. Nebenbei sei hier bemerkt, dass unter TRAC nur homogene und keine diversitäre Redundanz möglich ist. Auch diesbezüglich hat ABB Nachbesserung angekündigt. Bei der Auswahl geeigneter Geräte kann der Benutzer entweder auf „hauseigene“ Daten zugreifen oder manuell Geräte einpflegen, wobei ABB jedoch dann jede Haftung ablehnt. Bei manueller Eingabe ist zu prüfen, ob der jeweilige Komponenten-hersteller bereits in der TRAC internen Liste aufgeführt ist, ansonsten muss er vom Benutzer hinzugefügt werden (siehe Fig. 10).

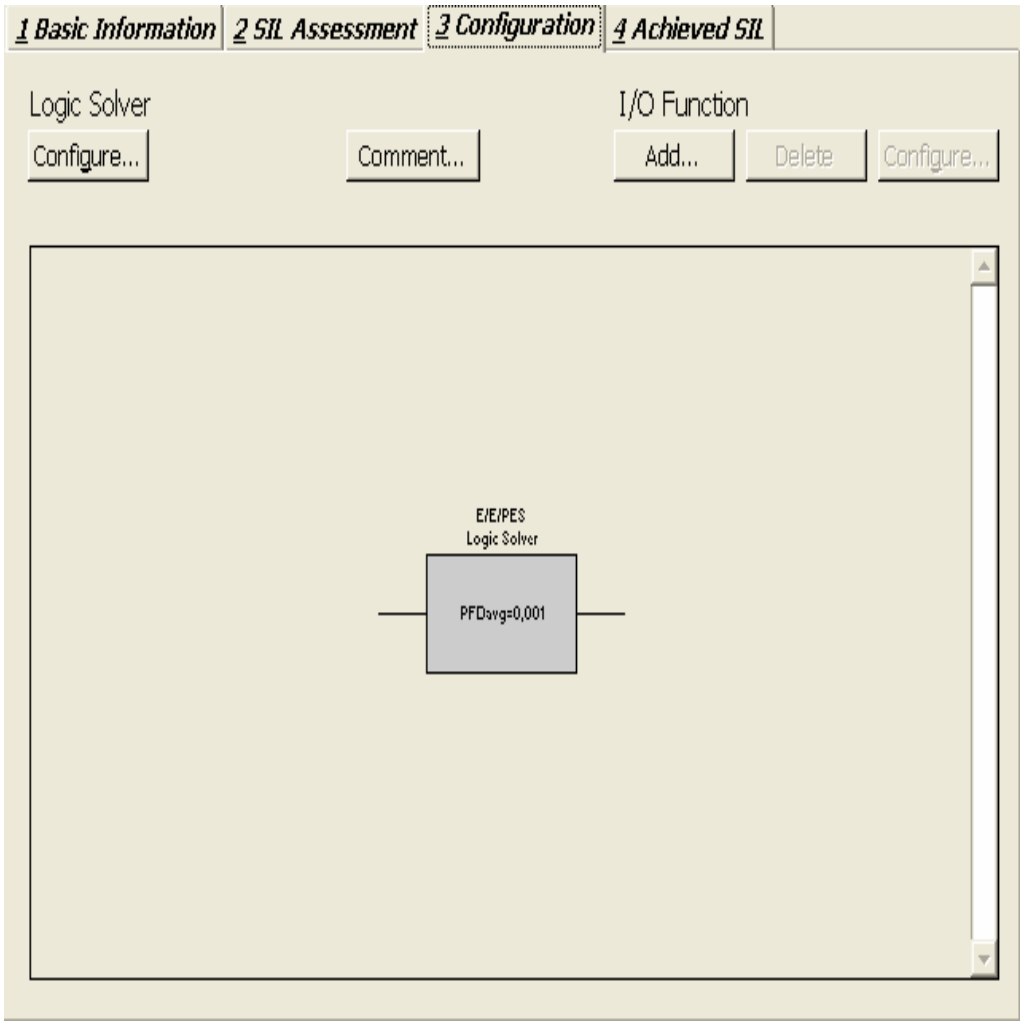

Fig. 9: Architektur und Instrumentierung der SIF

	Code	Name	Tag	IsPredefined
▶	ABB	ABB	ABB	True
	Bestobell Mobrey	Bestobell Mobrey	Bestobell Mobrey	True
	Controlotron	Controlotron	Controlotron	True
	Demo	Demo - for demonstration use only	Demo	True
	Endress & Hauser	Endress & Hauser	Endress & Hauser	True
	Fisher Rosemount	Fisher Rosemount	Fisher Rosemount	True
	Foxboro	Foxboro	Foxboro	True
	Generic	Generic	Generic	True
	Heinrichs	Heinrichs	Heinrichs	True
	HIMA	HIMA	HIMA	False
	Honeywell	Honeywell	Honeywell	True
	Krohne	Krohne	Krohne	True

Fig. 10: Herstellerliste

Der gleiche Mechanismus gilt für die Definition neuer Gerätetypen (siehe Fig. 11).

	Code	Name	Tag	IsWetted	IsPredefined
▶	AI-Card	Analog-Input-Card	AIC	False	False
	Analyser	Analyser	ANA	True	True
	Annunciator	Alarm Annunciator	ALMANN	False	True
	Ball Valve	Ball Valve	BV	False	False
	Barrier	Barrier	BR	False	True
	Contact	Contact on receiving instrument	CON	False	True
	Contactor	Contactor (MCC)	CONT	False	True
	Controller	Electronic Controller	EC	False	True
	Default (non-wetted)	Default Instrument, non-wetted	DEFAULTN	False	True
	Default (wetted)	Default Instrument, wetted	DEFAULTW	True	True
	Detector	Detector	DETECT	False	True
	DO-Card	Digital-Output-Card	DOC	False	False
	DP Transmitter	D P Transmitter	DP	True	True
	DP Transmitter Elec	D P Transmitter Electronic	DPE	True	True
	DP Transmitter Pneu	D P Transmitter Pneumatic	DPP	True	True
	Flame Failure	Flame Failure Device	FFD	True	True
	Flow - Coriolis	Flow Transmitter Coriolis	FTC	True	True
	Flow - E/M	Flow Transmitter Electromagnetic	FTE	True	True
	Flow - Turbine	Flow Transmitter Turbine	FTT	True	True
	Flow - Vortex	Flow Transmitter Vortex	FTV	True	True
	Flow Switch	Flow Switch	FSW	True	True
	Flow Transmitter	Flow Transmitter	FTX	True	True
	Gas Detector	Gas Detector	GDET	True	True
	Hand Switch	Hand Switch	HSW	False	True
	Key Switch	Key Switch	KSW	False	True

Fig. 11: Gerätetypeneditor

Zusätzlich wird die Option gegeben, Medienberührung a priori zu fixieren (IsWetted).
Sind diese beiden Menupunkte vom Benutzer (bei Bedarf) bearbeitet, können die neuen Baugruppen eingepflegt werden. Als Werkzeug dazu dient eine Eingabemaske, die gleichzeitig sowohl als Suchmaschine für Einzelgeräte, als auch zum Erzeugen neuer Komponenten verwendbar ist. Erstere Funktion kann im oberen Teil des Fensters in Fig. 12 realisiert werden. Die Gerätedaten werden dann im unteren Windowbereich angezeigt, der aber auch als manuelle Dateneingabe zur Generierung neuer Einzelgeräte fungiert. So ist beispielsweise die Geräteart (Inst Type), der Hersteller (Manufacturer) und die genaue Bezeichnung (Model) abfragbar. Das Fixieren von Ausfalldaten im Anschluss ist recht benutzerfreundlich gehalten, denn es wird lediglich λ_D postuliert, dies jedoch in der etwas ungewöhnlichen Einheit „Ausfallwahrscheinlichkeit pro Jahr“. Normalerweise tritt an diese Stelle die Einheit „Ausfallwahrscheinlichkeit pro Stunde“, wobei aber auch die Bezeichnung „FIT“ (Ausfallwahrscheinlichkeit pro Billion Stunden) immer häufiger anzutreffen ist. Empfehlenswert wäre hier, die Einheit neben der jeweiligen Größe zu vermerken, damit der User eine Vorstellung davon hat, in welcher Maßeinheit dort zu rechnen ist. Die Tatsache, dass TRAC nur mit λ_D statt λ_{DU} arbeitet, impliziert bereits eine Worst-Case-Annahme, denn nur für rein mechanische Bauteile sind diese beiden Größen identisch. Die übrigen λ-Werte

sind nicht von Interesse, was die These stützt, dass zur Berechnung der *PFD* lediglich die gängige, vereinfachte Formel

$$PFD = \frac{T_I}{2} \cdot \lambda_{DU} \text{, bei TRAC } PFD = \frac{T_I}{2} \cdot \lambda_D \tag{29}$$

verwendet wird.

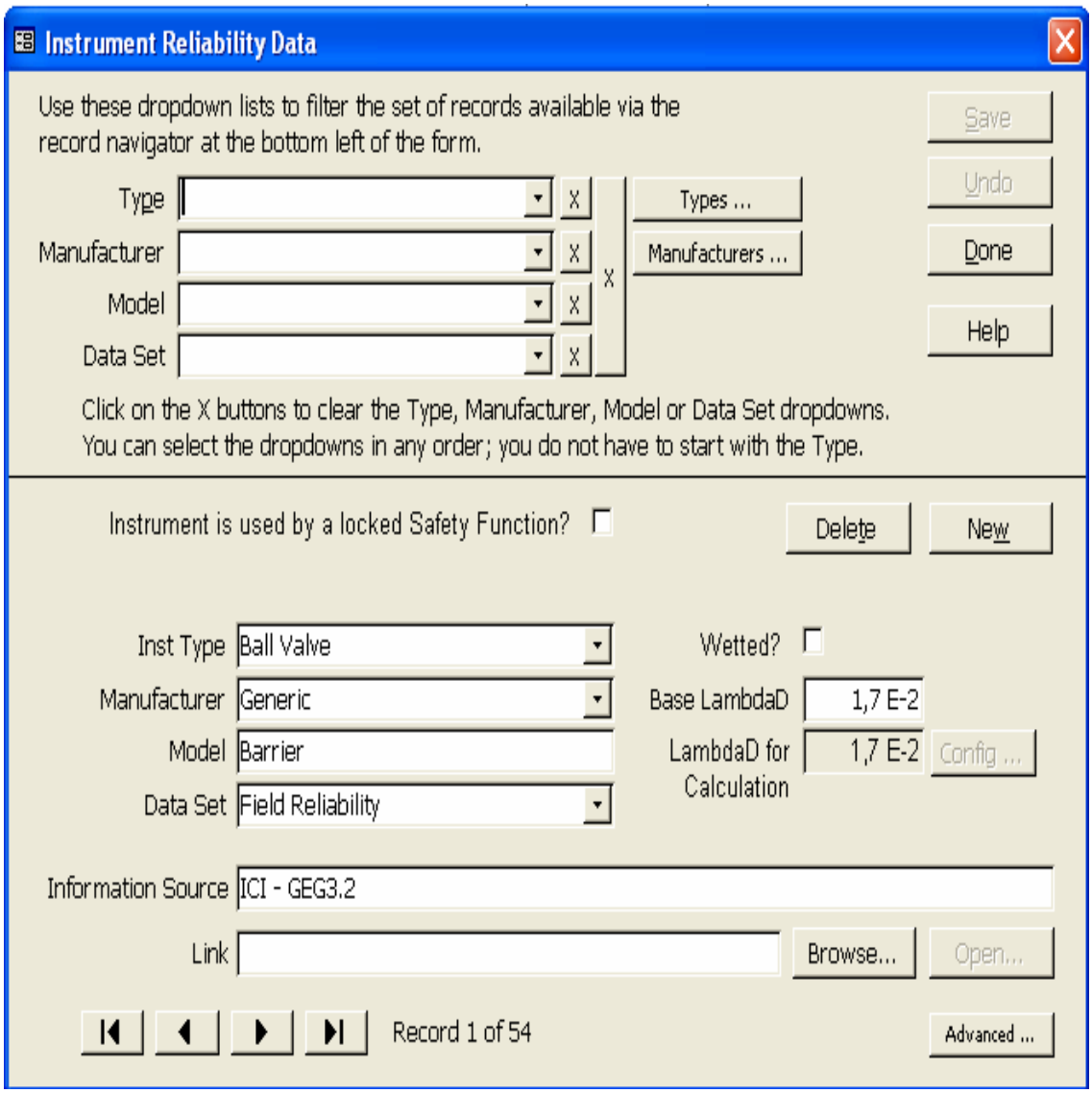

Fig. 12: Baugruppeneditor

Der Einfluss von Medienberührung der Komponenten ist ebenfalls in TRAC modellierbar, allerdings nur, wenn als Datenmenge (Data Set) die Kategorie „Herstellerdaten“ (Manufacturers Predicted Reliability) eingestellt wird. Dann ist offeriert, mittels des Buttons „Config…“ (siehe Fig. 12) einen sog. „Schmutzfaktor“ auszuwählen, mit dem λ_D bei der Berechnung multipliziert wird. Der User kann sich zwischen Faktor 1, 2, 5 und 10 entscheiden, es sind jedoch auch beliebige, andere Werte bei entsprechender Konfiguration einpflegbar. Deklariert der Benutzer jedoch als „Felddaten“ (Field Reliability), wird impliziert, dass die Medienberührung schon berücksichtigt ist, und die Option entfällt. Dies ist durchaus korrekt, da im Falle von Felddaten, denn nichts anderes sind auch die NAMUR-Störddaten, der Kontakt der Komponenten mit Prozessflüssigkeit mit enthalten ist.

Die Angabe der Gerätespezifikationen bei der Logikverarbeitung erfolgt nach einem anderen Schema, dazu jedoch in Kapitel 2.2.1 Näheres.
Auch werden stets wieder Warnungen angezeigt, falls die gewählte Architektur laut [1] bezüglich der *HFT* nicht für den angestrebten „Soll-*SIL*“ zulässig ist. Dies ist jedoch im Rahmen des Berichts nicht von Interesse, da, wie bereits mehrmals angemerkt, die *PFD* hier als alleiniges Kriterium zur *SIL*-Festlegung betrachtet wird.
Ist der Menüpunkt in Fig. 9 abgeschlossen, kann zur *PFD*-Berechnung und damit der Verifikation des SILs übergegangen werden (siehe Fig. 13).

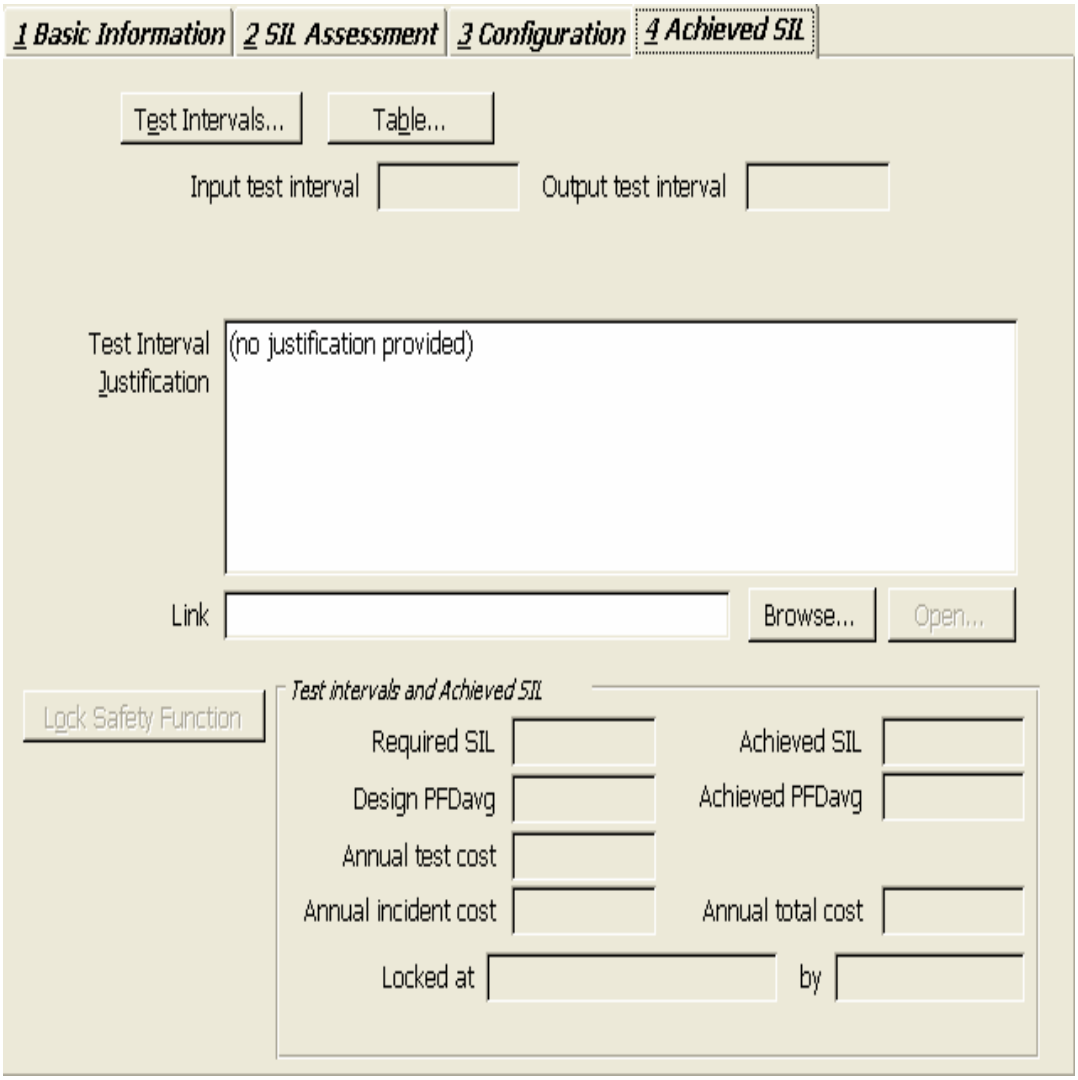

Fig. 13: *PFD*-Verifikation

Dazu sei nur angemerkt, dass an dieser Stelle noch die Wartungsintervalle für Sensorteil (Input test interval) und Aktorteil (Output test interval) fixiert werden, bevor die *PFD* anzeigt wird, und so der rein rechnerisch erreichte *SIL* ersichtlich ist.
Das Wartungsintervall der Logikverarbeitung geht bereits früher ein, doch dazu im weiteren Verlauf mehr.
Auch auf dieser abschließenden Karteikarte fällt erneut die Vermischung sicherheitstechnischer und finanzieller Gesichtspunkte auf.

2.2 Beispielberechnung eines Typicals

2.2.1 Struktur und verwendete Komponenten

Nachdem die Basis zum Verständnis der Funktionsweise der Software „TRAC“ gelegt ist, wird nun ein Typical für eine einkanalige Drucküberwachung Bottom-Up mittels TRAC analysiert. Es handelt sich dabei um eine typische sicherheitsgerichtete Schaltung, wie sie sich auch bereits vielfach in der chemischen und pharmazeutischen Industrie im Einsatz befindet. Komponenten- und Strukturdaten stammen von dem Dienstleister „InfraServ“, der die Informationen zwecks numerischen SIL-Nachweises zur Verfügung gestellt hat. Fig. 14 gibt einen Überblick über die wesentlichen Daten.

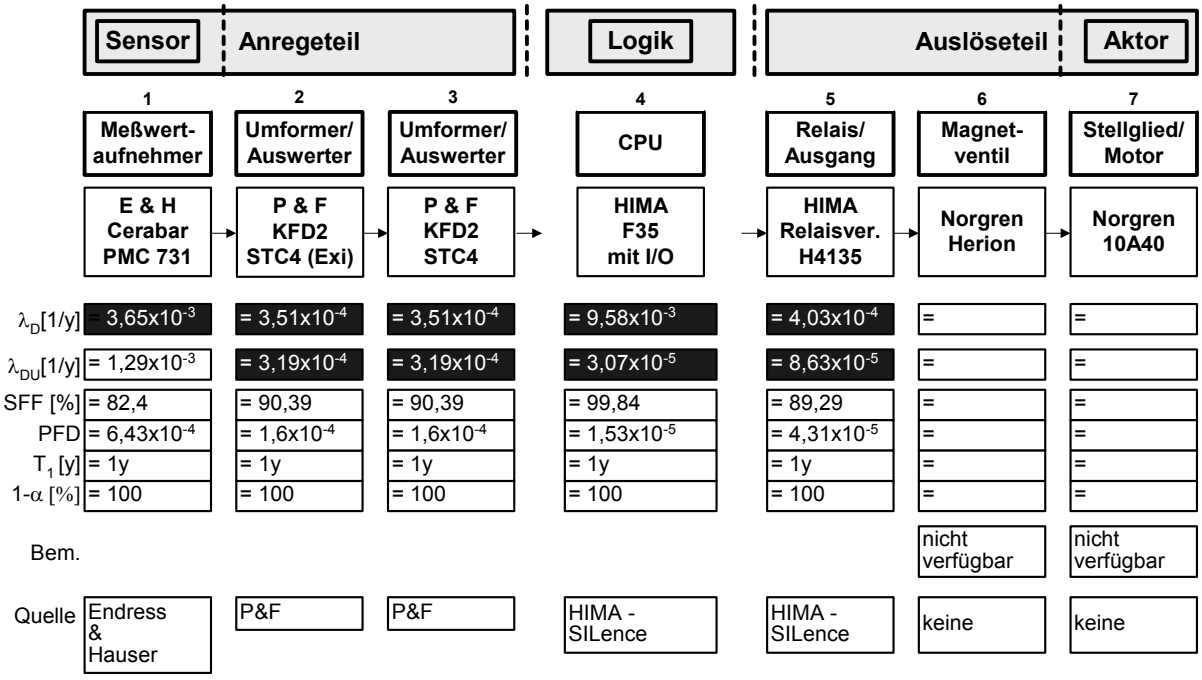

Fig. 14: Basisdaten des Typicals „Drucküberwachung“

Die benötigten Ausfalldaten wurden auf Anfrage oder direkt online vom jeweiligen Hersteller zur Verfügung gestellt.
Allerdings sind die Inhalte der schwarz hinterlegten Felder unter Verwendung von Annahmen und Formeln der Normen [1] und [10] aus den Angaben der Hersteller abgeleitet, darunter auch die von TRAC benötigten λ_D-Werte. In der „hauseigenen“ Datenbank von TRAC war keines der Geräte abgelegt, so dass alle Komponenten eingepflegt werden mussten. Der in der Software enthaltene Informationsfundus beschränkt sich überwiegend auf ICI-Datenbanken, die λ_D-Werte mit sehr hohen Sicherheitsaufschlägen verwenden.

Wie die Herstellerangaben in TRAC eingespeist werden, wird exemplarisch durch Fig. 15 und 16 illustriert. Speziell Fig. 16 beinhaltet den Prozess für die Logikverarbeitung, der, wie bereits angesprochen, von der üblichen Eingabe für Komponenten des Sensor- und Aktorteils differiert. Für die Signalverarbeitung ist direkt die Eingabe der *PFD* erforderlich, welche das Wartungsintervall implizit beinhaltet. Ferner sind hier Angaben über *HFT* und Programmierbarkeit zu tätigen.
Über das Magnetventil und den Kugelhahn waren keinerlei verlässliche Ausfalldaten zu erhalten.

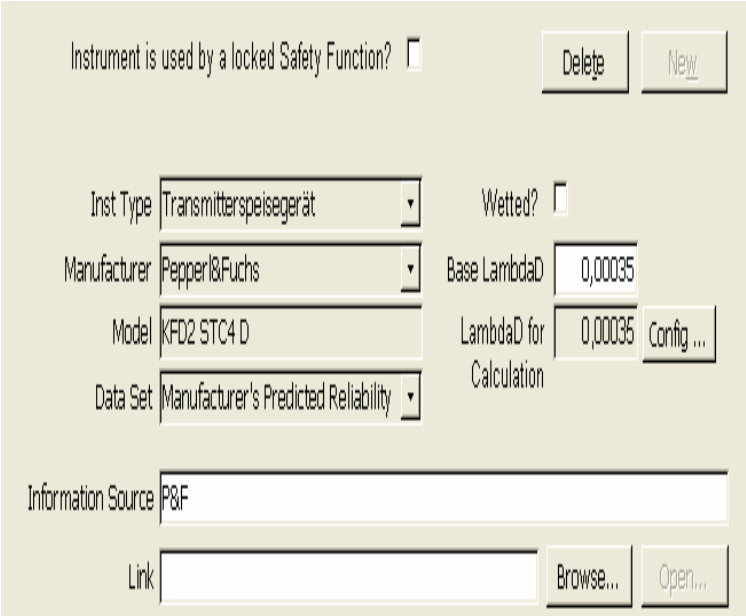

Fig. 15: Datenblatt des Transmitterspeisegeräts

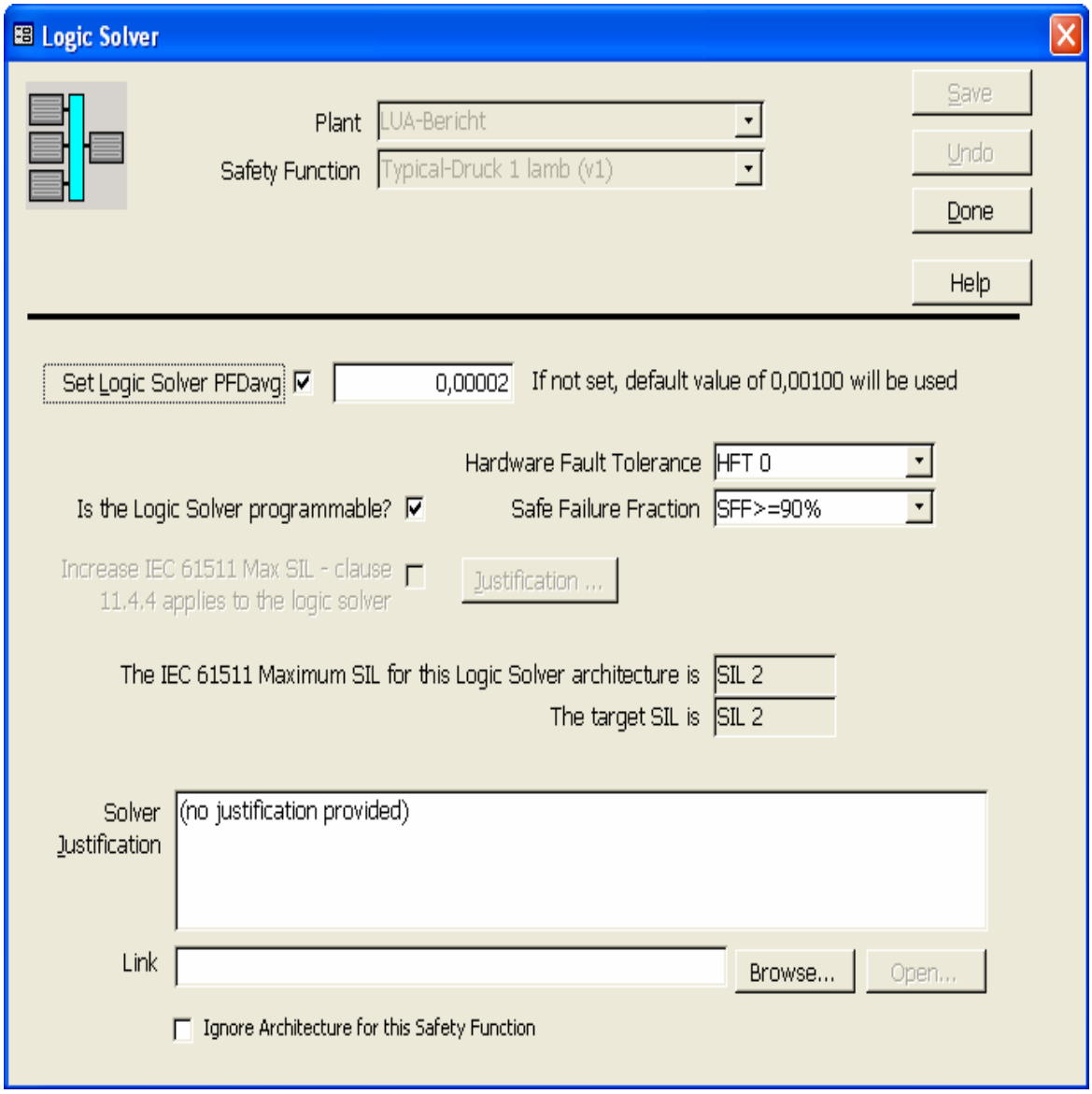

Fig. 16: Datenblatt der Logikverarbeitung

2.2.2 *PFD*-Bandbreite (Sensibilitätsanalyse)

Bedingt durch das Fehlen verlässlicher Daten für Magnetventil und Kugelhahn, sind Referenzwerte für diese Komponenten zu wählen. Entsprechende Größen sind in Tabelle XI und XII gelistet.

TABELLE XI
Referenzwerte Magnetventil Herion

Größe	**Generic 3-Wege (Exida)**	**Magnetventil (OLF-Handbuch)**
SFF [%]	60	---
λ [1/y]	0,05256	---
λ_D [1/y]	0,021024	0,012264
λ_{DU} [1/y]	0,021024	0,012264
λ_{DD} [1/y]	0	---
λ_S [1/y]	0,031536	---
λ_{SU} [1/y]	0,031536	---
λ_{SD} [1/y]	0	---

TABELLE XII
Referenzwerte Kugelhahn 10A40

Größe	**BEL Gatevalve pneu. (Exida)**	**Generic Air Operated (Exida)**
SFF [%]	75,72	67,3
λ [1/y]	0,01333272	0,02142696
λ_D [1/y]	0,0032412	0,007008
λ_{DU} [1/y]	0,0032412	0,007008
λ_{DD} [1/y]	0,00671892 (mit λ_{SD})	0
λ_S [1/y]	0,01009152	0,014454
λ_{SU} [1/y]	0,0033726	0,014454
λ_{SD} [1/y]	0,00671892 (mit λ_{DD})	0

Die schwarz hinterlegten Werte wurden mit Standardformeln in [1] und [10] aus den anderen Ausfalldaten errechnet. Es wird weiterhin unterstellt, dass es sich sowohl beim Magnetventil, als auch beim Kugelhahn um ein rein mechanisches Bauteil handelt und somit keine Eigendiagnostik vorhanden ist, also $\lambda_D = \lambda_{DU}$ gilt.

Ein weiteres Problem stellt die Mediumberührung dar. Sollte man mit oder ohne einen Wetted-Faktor von 5 rechnen (=Mittelwert bei TRAC).

Optionell ist darüber zu rekapitulieren, ob der Benutzer, wie bei TRAC postuliert, mit λ_D-Werten kalkuliert oder die exakteren λ_{DU}-Werte stattdessen berücksichtigt.

Aus diesen Unsicherheiten erwächst die Notwendigkeit einer Bestimmung von *PFD*-Bandbreiten. Dazu bietet es sich an, jeweils ein *PFD*-Band für λ_D und λ_{DU} zu ermitteln, wobei die Referenzen aus Tabelle XI und XII, sowie die Belegung des Wetted-Faktors zur *PFD*-Variation benutzt werden (siehe Fig. 17 und 18).

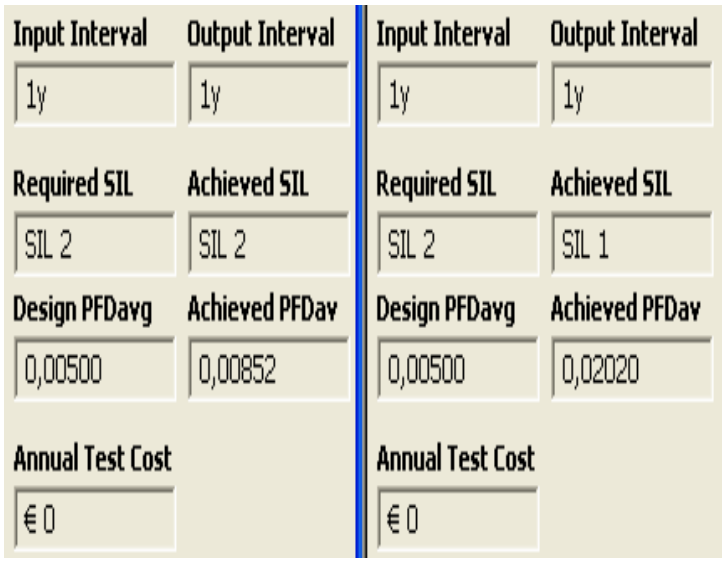

Fig. 17: *PFD*-Band für die λ_D-Werte des Typicals

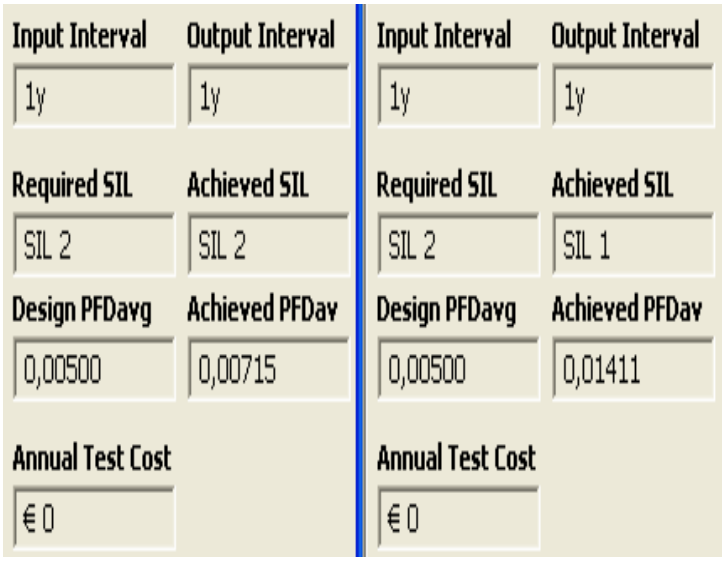

Fig. 18: *PFD*-Band für die λ_{DU}-Werte des Typicals

Augenscheinlich reicht das *PFD*-Spektrum für beide Bänder vom *SIL* 1- bis in den *SIL* 2-Bereich. Ergo entscheidet die Wahl der Referenzwerte, vor allem in Bezug auf die Parameter des Magnetventils, über die Zugehörigkeit zu verschiedenen *SIL*s.
Zur Berechnung der fehlenden Ausfalldaten in Tabelle XI und XII, sowie in Fig. 14 wurden die folgenden Formeln verwendet:

$$\lambda_S + \lambda_{DD} = \frac{SFF \cdot \lambda_{DU}}{(1 - SFF)} \tag{30}$$

$$\lambda_D = \frac{1}{2}\lambda \text{ (außer für die Referenz des Magnetventils und des Kugelhahns)} \tag{31}$$

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda} \tag{32}$$

2.3 Bewertung

In seiner Gesamtheit stellt das Softwarepaket „TRAC“ des Herstellers „ABB“ ein gelungenes, benutzerfreundliches Instrument zur umfassenden Bewertung sicherheitsgerichteter Schaltungen dar. Den Nachteilen einer Involvierung finanzieller Aspekte und der Notwendigkeit einer ausgereifteren Weiterentwicklung steht ein hohes Maß an Flexibilität gegenüber. Auf diese Weise birgt das Tool ein enormes Entwicklungspotential.
Ein wesentlich größerer Mangel wird bei der Zertifizierung von Baugruppen offenkundig. Oftmals geben Hersteller keine oder ungenügende Ausfalldaten für ihre Produkte heraus.
Ferner mangelt es bisweilen an der Kompatibilität der Variablen mit Deklarationen in [1] und [10]. So kommt es nicht nur vor, dass völlig andere Bezeichnungen verwendet werden, sondern standardisierte Variablen mit anderen Inhalten belegt werden.
Fraglich scheinen auch diverse Prüfverfahren, die in der angewendeten Weise nicht geeignet sind, Einzelgeräte zuverlässig zu beurteilen. Beispielsweise erfolgt zum Teil nur die Angabe einer *PFD* ohne das zugehörige Wartungsintervall, was die Information des *SIL*-Zertifikats im gleichen Zuge unbrauchbar macht.
Welche Erkenntnisse bringt jedoch ein Vergleich des Konfidenzintervalls für einkanalige Drucküberwachungen aus Kapitel 1 mit den *PFD*-Bändern des Typicals der gleichen Kategorie? Dazu ist am besten eine ähnliche Graphik wie in Fig. 5 geeignet (siehe Fig. 19).

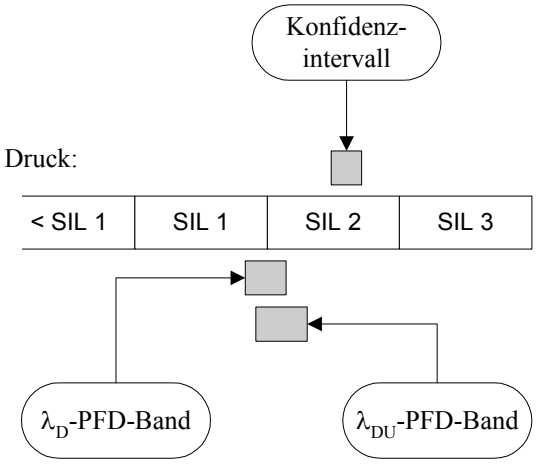

Fig. 19: Konfidenzintervall versus *PFD*-Bänder

Im Ergebnis deutet einiges darauf hin, dass die *PFD*-Werte de facto (Top-Down mittels der NAMUR-Stördaten) günstiger sind, als Bottom-Up berechnet wurde. Denn das Konfidenzintervall liegt nicht nur in einem geringeren *PFD*-Bereich, es weist sogar keinerlei Überschneidung mit den *PFD*-Bändern des Bottom-Up-Nachweises auf, trotz Berücksichtigung systematischer Fehler und Berührung mit Prozessflüssigkeit. Folglich liegt der Schluss nahe, dass die im Einsatz befindliche Technik in Wirklichkeit zuverlässiger ist, als bei theoretischer Berechnung ausgewiesen. Es sind allerdings noch weitere Analysen notwendig, um diese Vermutung zu untermauern.
Zusammenfassend sind viele interessante Einsichten entstanden, denen unbedingt weiter nachgegangen werden sollte.

Quellen

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

[2] L. Litz, „Grundlagen der sicherheitsgerichteten Automatisierungstechnik*"*, *Automatisierungstechnik: Theoretische Grundlagen, Methoden, Anwendungen*, Heft 2, pp. 56-68, 46. Jahrgang 1998.

[3] L. Litz, *Wahrscheinlichkeitstheorie für Ingenieure: Grundlagen, Anwendungen, Übungen*, Heidelberg, Hüthig Verlag, 2001.

[4] L. Litz, „Safety and Availability of Components and Systems*"*, in *PCIC Europe Conference Documentation*, May 27-28, 2004 Basle, Switzerland, pp 16-21.

[5] U. Krengel, *Einführung in die Wahrscheinlichkeitstheorie und Statistik*, Braunschweig/ Wiesbaden, Vieweg Verlag, 2002.

[6] K. Bosch, *Elementare Einführung in die angewandte Statistik*, Braunschweig/ Wiesbaden, Vieweg Verlag, 2000.

[7] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, New York, IEEE Press, 1996.

[8] NAMUR, *Interessengemeinschaft Prozessleittechnik der chemischen und pharmazeutischen Industrie,*
http://www.namur.de

[9] P. Netter, P. Brusa, „Erste Anwendungserfahrungen mit probabilistischen Methoden in der Anlagensicherung", Technische Überwachung 05/ 2004 , Seite 22.

[10] IEC 61508, Teil 1-7, *Functional safety: Safety Instrumented Systems for Process Industry Sector*, 2002.