KLINISCHE MEDIZINTECHNIK

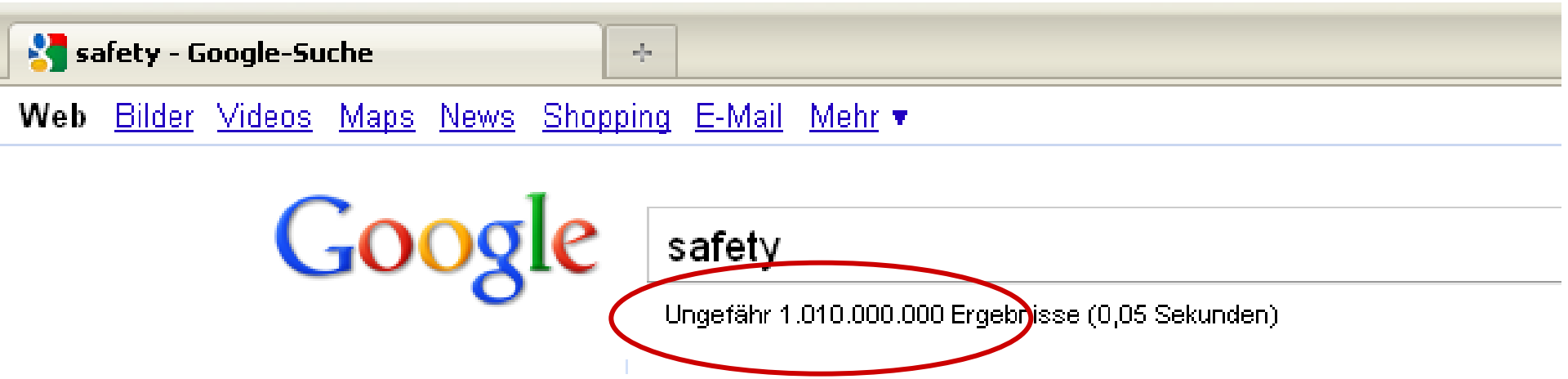
universitätbonn

Sicherheit in der Medizintechnik

1. Was ist Sicherheit

- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- Standards

- **Was ist Sicherheit**
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- Standards



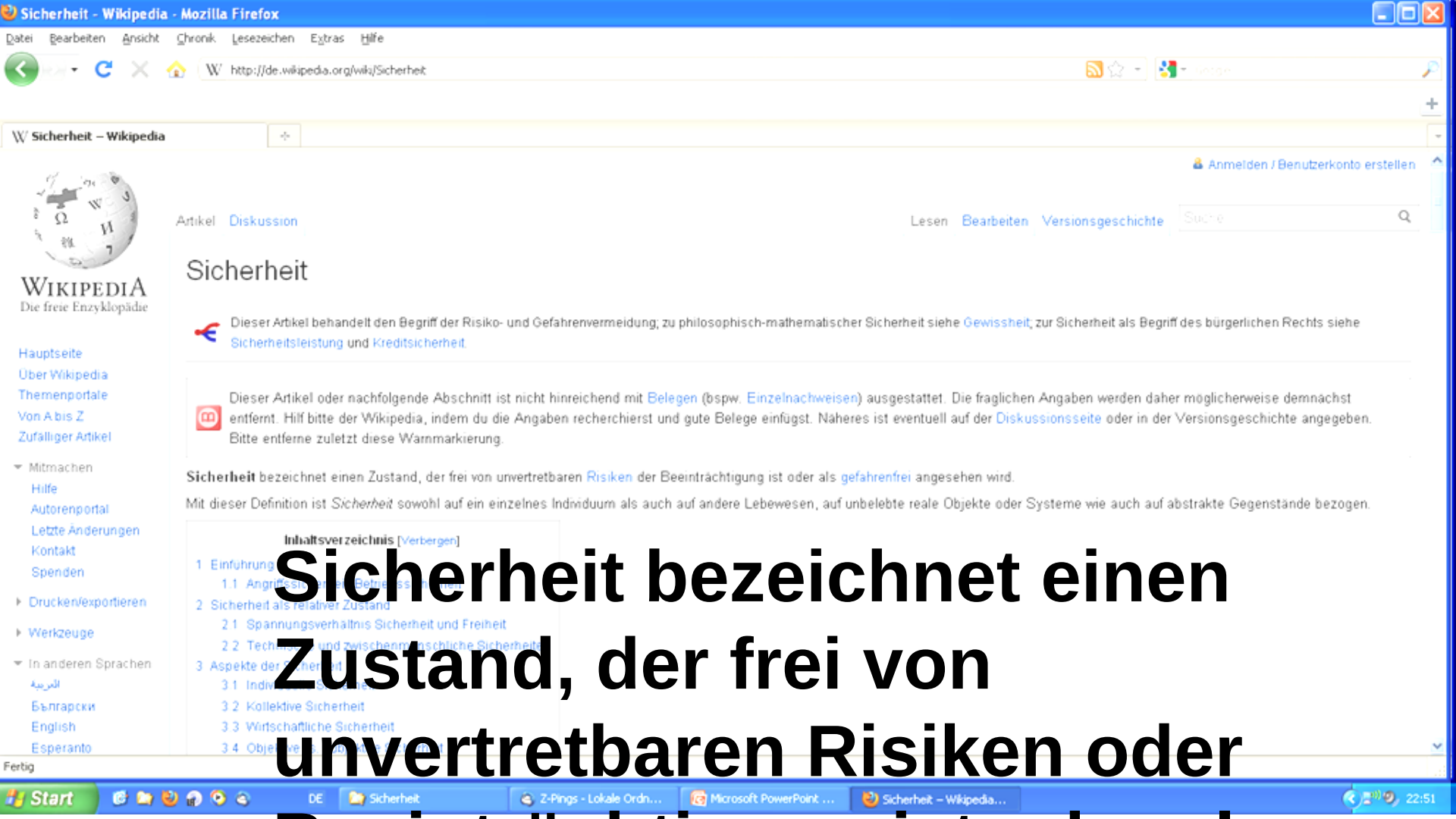
Scheinbar ein wichtiges Thema

Definieren Sie mal Sicherheit


A350
A350 AIRBUS
© AIRBUS S.A.S. 2006 - COMPUTER RENDERING BY FIXION - HCSGM


TU
RKISH

Was also ist Sicherheit ?



Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken oder Beeinträchtigung ist oder als gefahrenfrei angesehen wird.

Es gibt keine absolute Sicherheit, sondern nur einen Kompromiss zwischen Nutzen und Risiken.

- Was ist Sicherheit
  - **Der sichere Zustand**
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- Standards

Der sichere Zustand ist abhängig von

- **der Anwendung / Applikation**
- **den Risiken bei Fehler**
- **den Risiken bei Ausfall**

Die Ganzheit aller Sicherheitsaspekte in

- **Software**
- **Hardware**
- **Erst-Fehler-Sicherheit**
- **Redundanzen**
- **Tests**

DER SICHERE ZUSTAND

- Was ist Sicherheit
  - Der sichere Zustand
  - **FUSI**
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- Standards

Sicherheitsaspekte

- Elektrische Sicherheit
- Brandschutz
- Infektionssicherheit
- Biocompatibilität
- Pharmacocompatibilität
- Mechanische Sicherheit
- usw…..

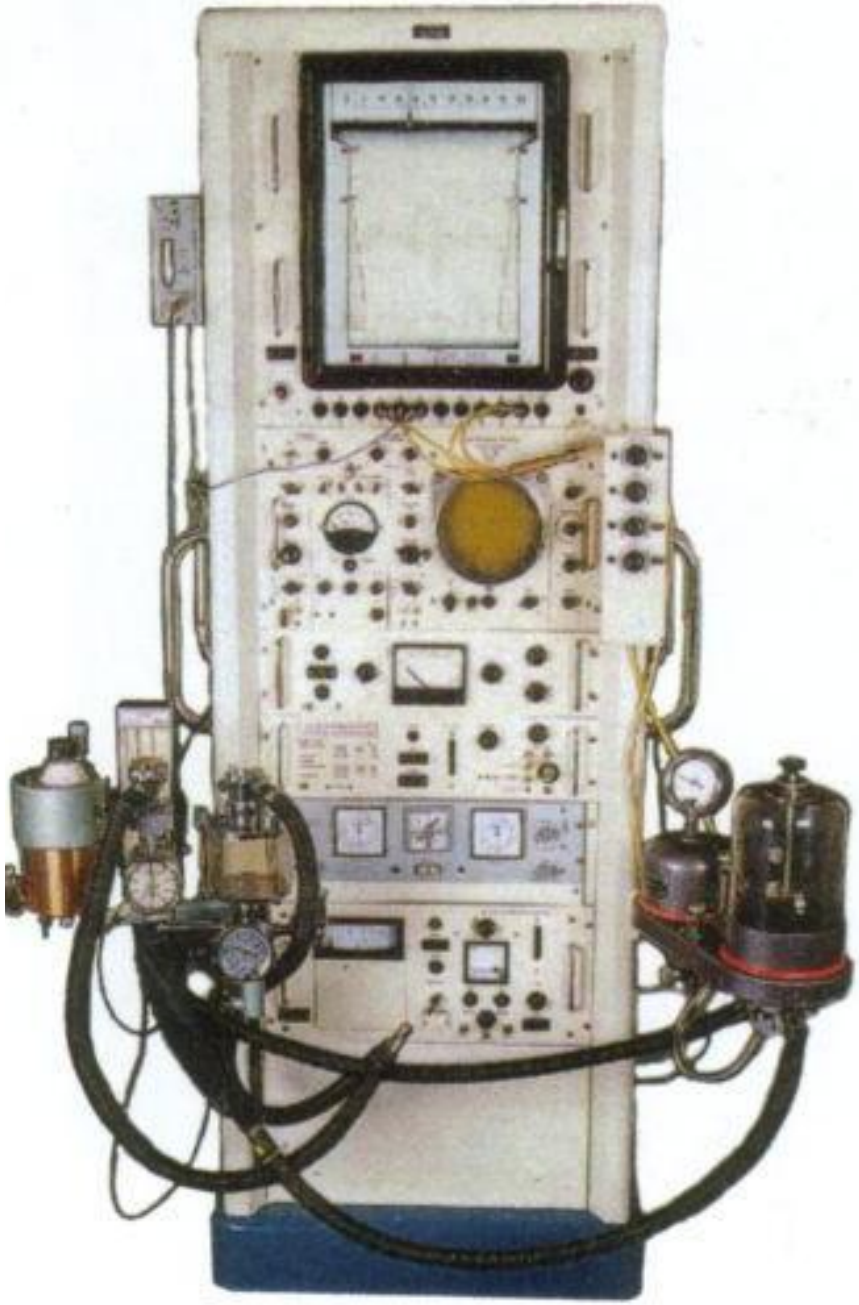
Aber, was leisten diese Sicherheiten ?

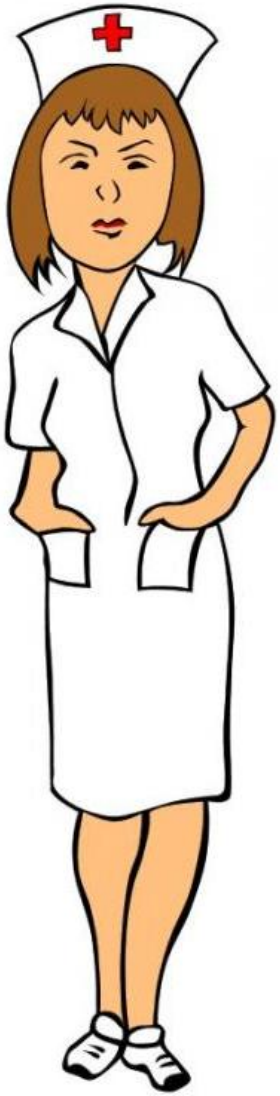
FuSi

Funktionale Sicherheit ist der aktive Teil der Sicherheit und betrifft:

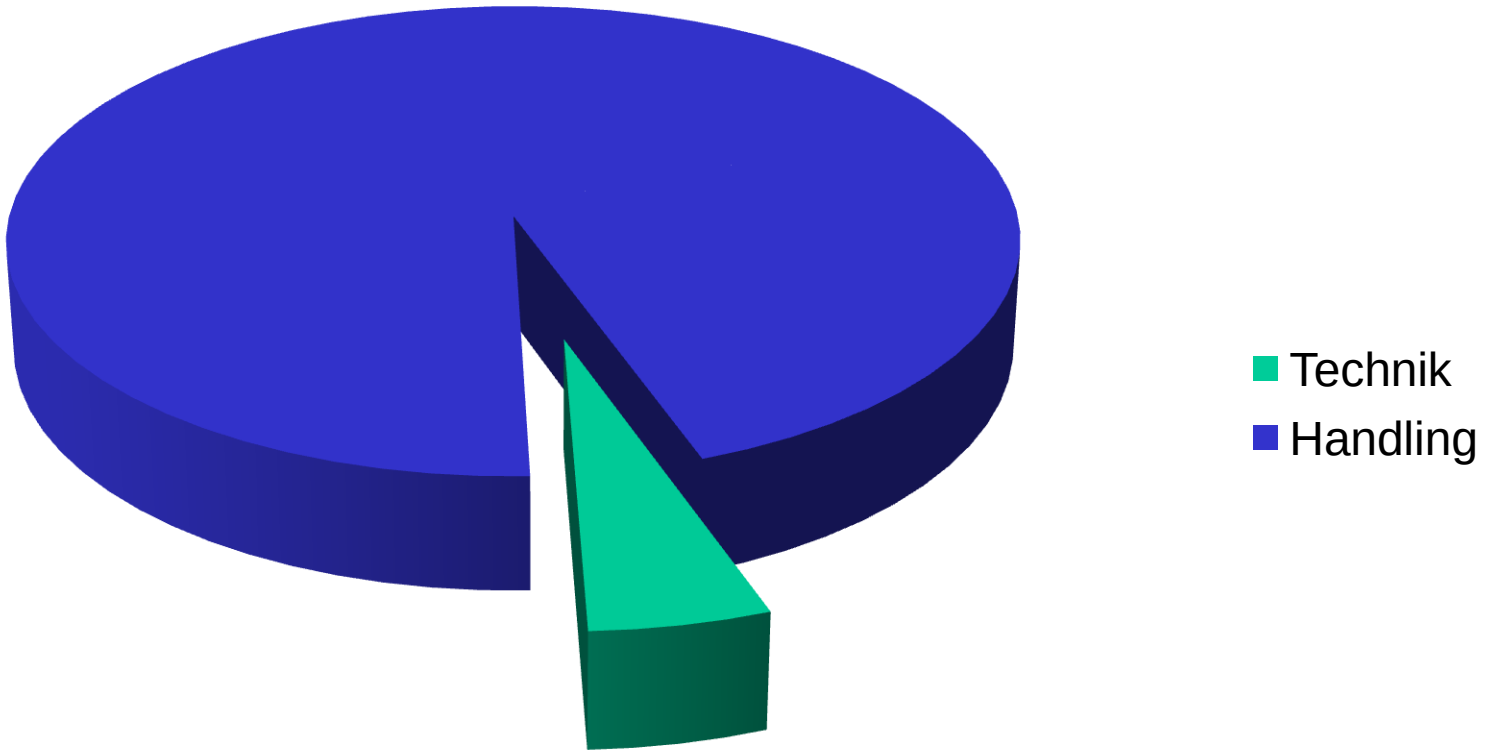
- **korrekte Funktion des Systems**
- **korrekte Funktion der Sicherheitssysteme**
- **schließt den “Sicheren Zustand“ ein.**

- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- **Mensch- Machinen System**
  - **Usability**
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- Standards

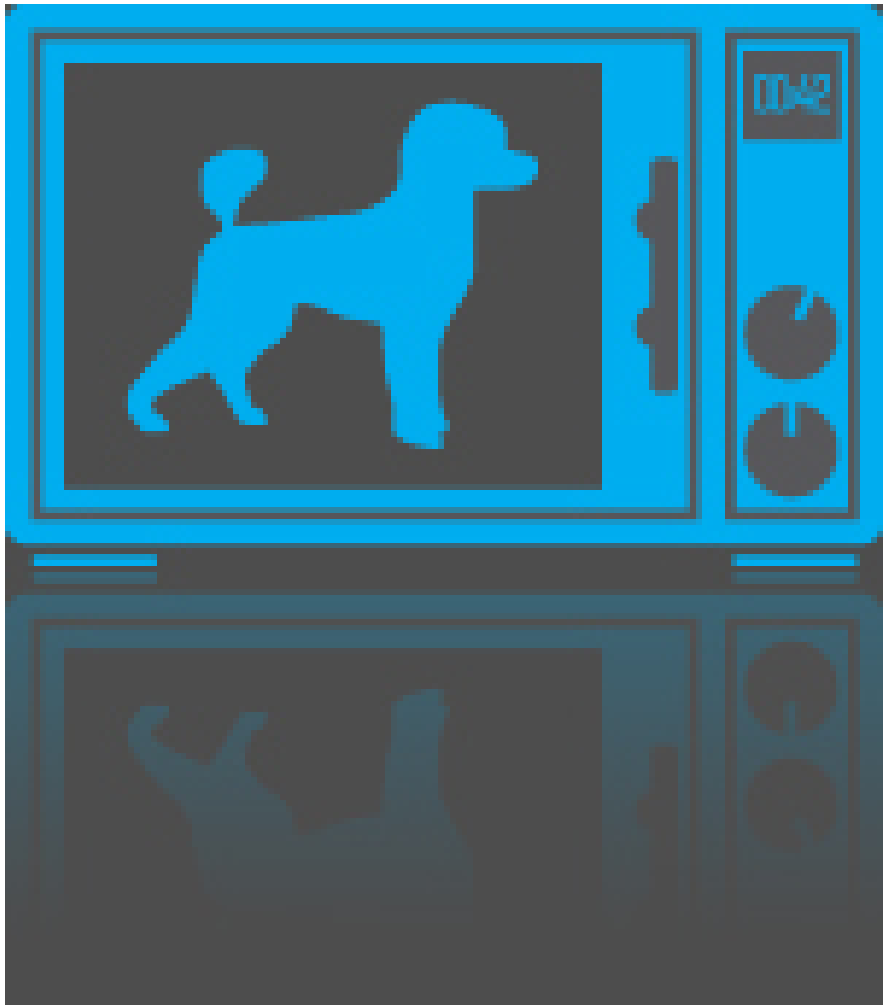




Zwischenfälle mit MT Geräten



- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - **Foreseeable misuse**
  - Automodi
- Risikoanalyse
- FMEA
- Standards



Forseeable und Unforeseeable Misuse

- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- **Risikoanalyse**
- FMEA
- Standards


Bar
Smirnoff

Risiko

Wahrscheinlichkeit

Gefahr

Auftretenswahrscheinlich keit (Occurrence)		Schweregrad (Severity)		
	IV – Vernachlässigbar (Negligible)	III – Gering (Marginal)	II – Kritisch (Critical)	I – Katastrophal (Catastrophic)
1 – Oft (Frequent)	B	A	A	A
2 – Gelegentlich (Occasional)	B	B	A	A
3 – Einigermaßen selten (Reasonably Remote)	B	B	A	A
4 – Selten (Remote)	C	B	B	A
5 – Sehr selten (Extremely Remote)	C	C	B	B
6 – Vernachlässigbar (Negligible Possibility)	C	C	C	B

Schweregrad (Severity)

Klassifi-zierung	Benennung	Beschreibung
I	Katastrophal	- Todesfall möglich
II	Kritisch	- schwerwiegende Verschlechterung des Gesundheitszustandes möglich
III	Gering	- Verschlechterung des Gesundheits-zustandes möglich
IV	Vernachlässigbar	- Geringfügige Verschlechterung des Gesundheitszustandes möglich

Auftretenswahrscheinlichkeit (Occurance)

Klassifi-zierung	Beschreibung	AW	Rational
1	Oft	15%	- kommt häufig vor
2	Gelegentlich	10%	- tritt einige Male während der Lebensdauer des Systems auf
3	Einigermaßen selten	5%	- tritt manchmal während der Lebensdauer des Systems auf
4	Selten	2,50%	- Unwahrscheinliches Auftreten bei einem System, aber möglich über die Lebensdauer des Produkts.
5	Sehr selten	1,00%	- Unwahrscheinliches Auftreten über die Lebensdauer des Produkts
6	Vernachlässig-bar	0,50%	- Auftreten unwahrscheinlich.

Hazard ID	Hazard	Harm	Generic cause	Cause ID	Specific Cause	Severity (Pre)	Occurence (Pre)	Risk (Pre)	Measure ID	Measures	Category	Decision	Where Addressed	Verification Test ID	Validation Test ID	Status	Sev. Post	Occ.post	Risk post	Comments
1	Overpressure in breathing circuit	Barotrauma	MC providing uncontrolled VA flow to the breathing system	1.1	Failed VA dosing valve	II	4	B	1.1.1	Limit maximum VA flow	design	implement	PRS.II.4.2.8; 6.8.1.2.8		MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 GUI T15 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
								B	1.1.2	Use only with ventilators according to current standards allowed (see list of standards)	advice	implement	URM MIRUS Section 2.		URM MIRUS M A-00, Chapter 2, Combination of ventilators and MIRUS system	Pass	II	5	B	Although noted in the URM, not every user may read the URM in detail. Therefore OCC post is reduced by one point only. The residual risk is a "C" only due to MID 1.1.1.
				1.2	Failed VA pressure control	II	4	B	1.2.1	Limit maximum VA pressure	design	implement	PRS.II.8.3.1; 6.8.7		MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
								B	1.1.2	Use only with ventilators according to current standards allowed (see list of standards)	advice	implement	URM MIRUS Sec 2		URM MIRUS M A-00, Chapter 2, Combination of ventilators and MIRUS system	Pass	II	5	B	Although noted in the URM, not every user may read the URM in detail. Therefore Occ. post is reduced by one point only. The total residual risk for this cause is a "C" due to MID 1.2.1.
				1.3	Software control failure	II	4	B	1.1.1	Limit maximum VA flow	design	implement	PRS.II.4.2.8; 6.8.1.2.8		MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 GUI T15 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
								B	1.3.1	Move system into fail safe mode	design	implement	PRS.II.4.2.8		MC Veri ZS SW R1.1 GUI T15	Pass	II	6	C	
				1.4	Electrical hardware failure	II	4	B	1.4.1	Test proper function with power up and system test prior to operation	design	implement	PRS.II.2.1; 2.2; 4.2.3; 4.2.4		MC Veri ZS SW R1.1 SysTest T09 MC Veri ZS SW R1.1 GUI T15	Pass	II	6	C	
2	Overpressure in breathing circuit	Barotrauma	MC providing uncontrolled purge flow to the breathing system	2.1	Failed purge valve	II	4	B	2.1.1	Limit maximum purge flow	design	implement	PRS II.9.2.2.2.1; 9.2.2.2.2		MC Veri ZS SW R1.1 eVAP T25 MC Veri ZS SW R1.1 PurgeFlow T32	Pass	II	6	C	MC purge flow system does not add external volume, but uses purge flow from breathing system
								B	1.1.2	Use only with ventilators according to current standards allowed (see list of standards)	advice	implement	URM MIRUS Section 2.		URM MIRUS M A-00, Chapter 2, Combination of ventilators and MIRUS system	Pass	II	5	B	Although noted in the URM, not every user may read the URM in detail. Therefore Occ. post is reduced by one point only. The total residual risk for this cause is a "C" due to MID 2.1.1.
				2.2	n/a	-	-	-			-	-	-							
				2.3	Software control failure	II	4	B	2.1.1	Limit maximum purge flow	design	implement	PRS II.9.2.2.2.1; 9.2.2.2.2		MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
								B	1.3.1	Move system into fail safe mode	design	implement	PRS.II.4.2.8		MC Veri ZS SW R1.1 GUI T15	Pass	II	6	C	
				2.4	Electrical hardware failure	II	4	B	1.4.1	Test proper function with power up and system test prior to operation	design	implement	PRS.II.2.1; 2.2; 4.2.3; 4.2.4		MC Veri ZS SW R1.1 Interface T26	Pass	II	6	C	
3	Negative pressure in breathing circuit	Barotrauma	MC sampling uncontrolled gas sample flow from breathing system	3.1	Failed internal gas monitor sampling pump control	II	4	B	3.1.1	Limit maximum sampling flow	design	implement	PRS II 9.2.2.2.2		MC Veri ZS SW R1.1 GasMon T24 MC Veri ZS SW R1.1 PurgeFlow T32	Pass	II	6	C	
				3.2	Failed external gas monitor sampling pump control (Basic only)	II	4	B	3.2.1	Use external gas monitor with limited maximum sampling flow	advice	implement	URM MIRUS Section 2.		Curently n/a					Basic Version is currently not applicable

Hazard ID	Hazard	Harm	Generic cause	Cause ID	Specific Cause	Severity (Pre)	Occurence (Pre)	Risk (Pre)
1	Overpressure in breathing circuit	Barotrauma	MC providing uncontrolled VA flow to the breathing system	1.1	Failed VA dosing valve	II	4	B
				1.2	Failed VA pressure control	II	4	B
				1.3	Software control failure	II	4	B
				1.4	Electrical hardware failure	II	4	B

Risiken

Risk (Pre)	Measure ID	Measures	Category	Decision	Where Addressed
B	1.1.1	Limit maximum VA flow	design	implement	PRS.II.4.2.8; 6.8.1.2.8
B	1.1.2	Use only with ventilators according to current standards allowed (see list of standards)	advice	implement	URM MIRUS Section 2.
B	1.2.1	Limit maximum VA pressure	design	implement	PRS.II.8.3.1; 6.8.7
B	1.1.2	Use only with ventilators according to current standards allowed (see list of standards)	advice	implement	URM MIRUS Sec 2
B	1.1.1	Limit maximum VA flow	design	implement	PRS.II.4.2.8; 6.8.1.2.8

Schutzmassnahme

Validation Test ID	Status	Sev. Post	Occ.post	Risk post	Comments
MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 GUI T15 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
URM MIRUS M A-00, Chapter 2, Combination of ventilators and MIRUS system	Pass	II	5	B	Although noted in the URM, not every user may read the URM in detail. Therefore OCC post is reduced by one point only. The residual risk is a "C" only due to MID 1.1.1.
MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	
URM MIRUS M A-00, Chapter 2, Combination of ventilators and MIRUS system	Pass	II	5	B	Although noted in the URM, not every user may read the URM in detail. Therefore Occ. post is reduced by one point only. The total residual risk for this cause is a "C" due to MID 1.2.1.
MC Veri ZS SW R1.1 DosControl T12 MC Veri ZS SW R1.1 GUI T15 MC Veri ZS SW R1.1 eVAP T25	Pass	II	6	C	

Verifikation

Risiko vor Massnahme

Risiko Level / Risk level	Anzahl / Total amount	Interpretation/ interpretation
A	66	Nicht akzeptables Risiko / non acceptable risk
B	120	Akzeptables Risiko / acceptable risk
C	134	Vernachlässigbares Risiko /negligible risk

Risiko nach Massnahme

Risiko Level / Risk level	Anzahl / Total amount	Interpretation/ interpretation
A	0	Nicht akzeptables Risiko / non acceptable risk
B	158	Akzeptables Risiko / acceptable risk
C	202	Vernachlässigbares Risiko /negligible risk

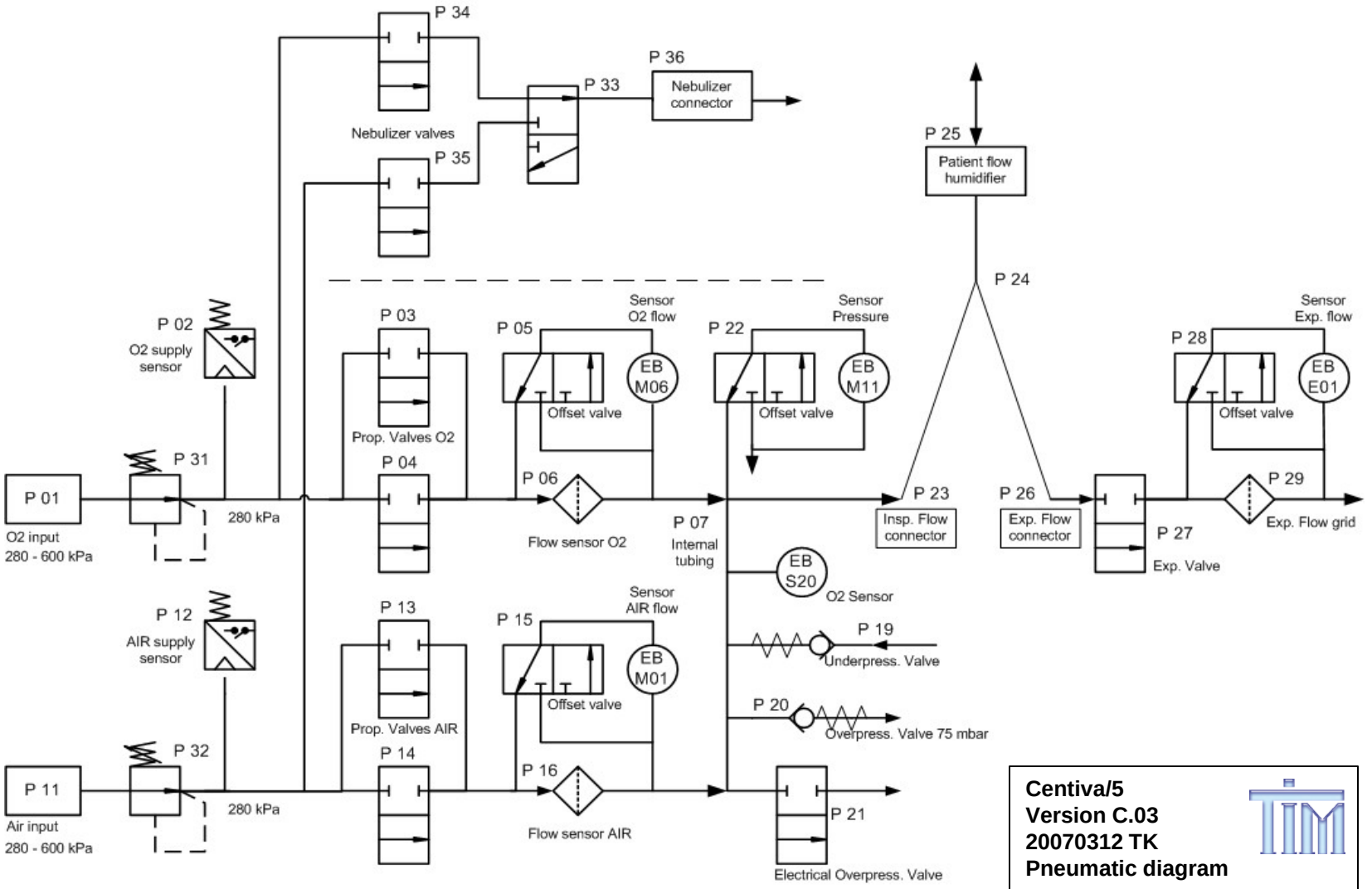
- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- **FMEA**
- Standards

Fehler

Möglichkeiten

Einfluss

Analyse



Centiva/5
Version C.03
20070312 TK
Pneumatic diagram

FMEA ID		Component	PRS ID	Cause ID	Specific cause	Generic cause	Harm	Severity (Pre)	Occurence (Pre)	Risk (Pre)	Measure ID	Measures	Category	Decision	Where addressed	Verification Test ID	Status	Validation Test ID	Status	Sev. Post	Occ. Post	Risk, Post	Comments
FMEA.I	1.1.1	Upper and lower Housing	na	1.1	Sharp edge	injection molding incorrect	user injury	III	4	B	1.1.1	Surfaces, corners and edges according to IEC 60601-1	design	implement	PRS				Pass	III	6	C	
FMEA.I	1.1.2			1.2	Craking	instable material	user injury	III	4	B	1.1.2	Use stable material	design	implement	PRS				Pass	III	6	C	
FMEA.I	1.2.1	P01 (Python park bay)	PRS II 6.1.4	2.1	spring defective	Leaks when Python is inserted	none, system will not pass system test	IV	6	C	2.1	n/a							Pass			C	
FMEA.I	1.2.2			2.2	Seal missing																		
FMEA.I	1.2.3			2.3	Seal defective																		
FMEA.I	1.3.1	E02 (Python park bay switch)	PRS II 6.1.5	3.1	electrical disconnection	Does not start system test	none, system will not pass system test	IV	6	C	3.1								Pass			C	
FMEA.I	1.3.2			3.2	switch defective																		
FMEA.I	1.4.1	E08 (Agent fillport detection)	PRS II 6.1.32	10.1	fillport detection electrically disconnected	Reservoir can not be refilled	None, system may be replaced	IV	6	C												C	
FMEA.I	1.4.2			10.2	fillport detection mechnically defective																	C	
FMEA.I	1.5.1	E09 (Agent fillport lock)	PRS II 6.1.33	11.1	fillport lock electrically disconnected	Reservoir can not be refilled	None, system may be replaced	IV	6	C												C	
FMEA.I	1.5.2			11.2	fillport lock mechnically defective																	C	

SA-B

ID		Component	PRS ID	Cause ID	Specific cause	Generic cause	Harm	Severity (Pre)	Occurence (Pre)	Risk (Pre)	Measure ID	Measures	Category	Decision	Where addressed	Verification Test ID	Status	Validation Test ID	Status	Sev. Post	Occ. Post	Risk, Post	Comments
FMEA.II	2.1.1	EP01 (Line inlet 90-264 V AC)	PRS II 6.1.7	1.1	AC too low	Device does not turn on	none	IV	6	C													
FMEA.II	2.1.2			1.2	AC too high	Device does not turn on	none	IV	6	C													
FMEA.II	2.2.1	EP02 (AC Power Supply)	PRS II 6.2.2	2.1	Power supply defective	Device does not turn on	none	IV	6	C										IV			
FMEA.II	2.2.2			2.2		Operating device is no longer powered by AC	Interruption of operation	II	5	B	2.2.1	Care for UPS supply to maintain operation for a minium of 10 min.	design	implement									
FMEA.II	2.3.1	EP03 (Charger for UPS Battery)	na	3.1	Charger defective	UPS battery does not charge	none	IV	6	C										II			

FMEA ID		Component	PRS ID	Cause ID	Specific cause	Generic cause	Harm	Severity (Pre)	Occurence (Pre)	Risk (Pre)
FMEA.I	1.1.1	Upper and lower Housing	na	1.1	Sharp edge	injection molding incorrect	user injury	III	4	**B**
FMEA.I	1.1.2			1.2	Craking	instable material	user injury	III	4	**B**
FMEA.I	1.2.1	P01 (Python park bay)	PRS II 6.1.4	2.1	spring defective	Leaks when Python is inserted	none, system will not pass system test	IV	6	**C**
FMEA.I	1.2.2			2.2	Seal missing					
FMEA.I	1.2.3			2.3	Seal defective					
FMEA.I	1.3.1	E02 (Python park bay switch)	PRS II 6.1.5	3.1	electrical disconnection	Does not start system test	none, system will not pass system test	IV	6	**C**
FMEA.I	1.3.2			3.2	switch defective					
FMEA.I	1.4.1	E08 (Agent fillport detection)	PRS II 6.1.32	10.1	fillport detection electrically disconnected	Reservoir can not be refilled	None, system may be replaced	IV	6	**C**
FMEA.I	1.4.2			10.2	fillport detection mechnically defective					
FMEA.I	1.5.1	E09 (Agent fillport lock)	PRS II 6.1.33	11.1	fillport lock electrically disconnected	Reservoir can not be refilled	None, system may be replaced	IV	6	**C**
FMEA.I	1.5.2			11.2	fillport lock mechnically defective					

Fehler

Measure ID	Measures	Category	Decision	Where addressed	Verification Test ID	Status
2.2.1	Care for UPS supply to maintain operation for a minium of 10 min.	design	implement			
2.2.1	For that case create a panic alarm that still allopws alarming the loss of both supply	design	implement			
8.1.1	System test to verify correct function of controller	design	implement	DSS test sequence		

Schutzmassnahme

Validation Test ID	Status	Sev. Post	Occ. Post	Risk, Post	Comments
	Pass	III	6	C	
	Pass	III	6	C	
	Pass			C	
	Pass			C	
				C	
				C	
				C	

Verifikation

Risiko vor Massnahme

Risiko Level / Risk level	Anzahl / Total amount	Interpretation/ interpretation
A	66	Nicht akzeptables Risiko / non acceptable risk
B	120	Akzeptables Risiko / acceptable risk
C	134	Vernachlässigbares Risiko /negligible risk

Risiko nach Massnahme

Risiko Level / Risk level	Anzahl / Total amount	Interpretation/ interpretation
A	0	Nicht akzeptables Risiko / non acceptable risk
B	158	Akzeptables Risiko / acceptable risk
C	202	Vernachlässigbares Risiko /negligible risk

- Was ist Sicherheit
  - Der sichere Zustand
  - FUSI
- Mensch- Machinen System
  - Usability
  - Foreseeable misuse
  - Automodi
- Risikoanalyse
- FMEA
- **Standards**

- **Wozu Normen**
  - **Stand der Technik**
  - **Haftungsbasis**

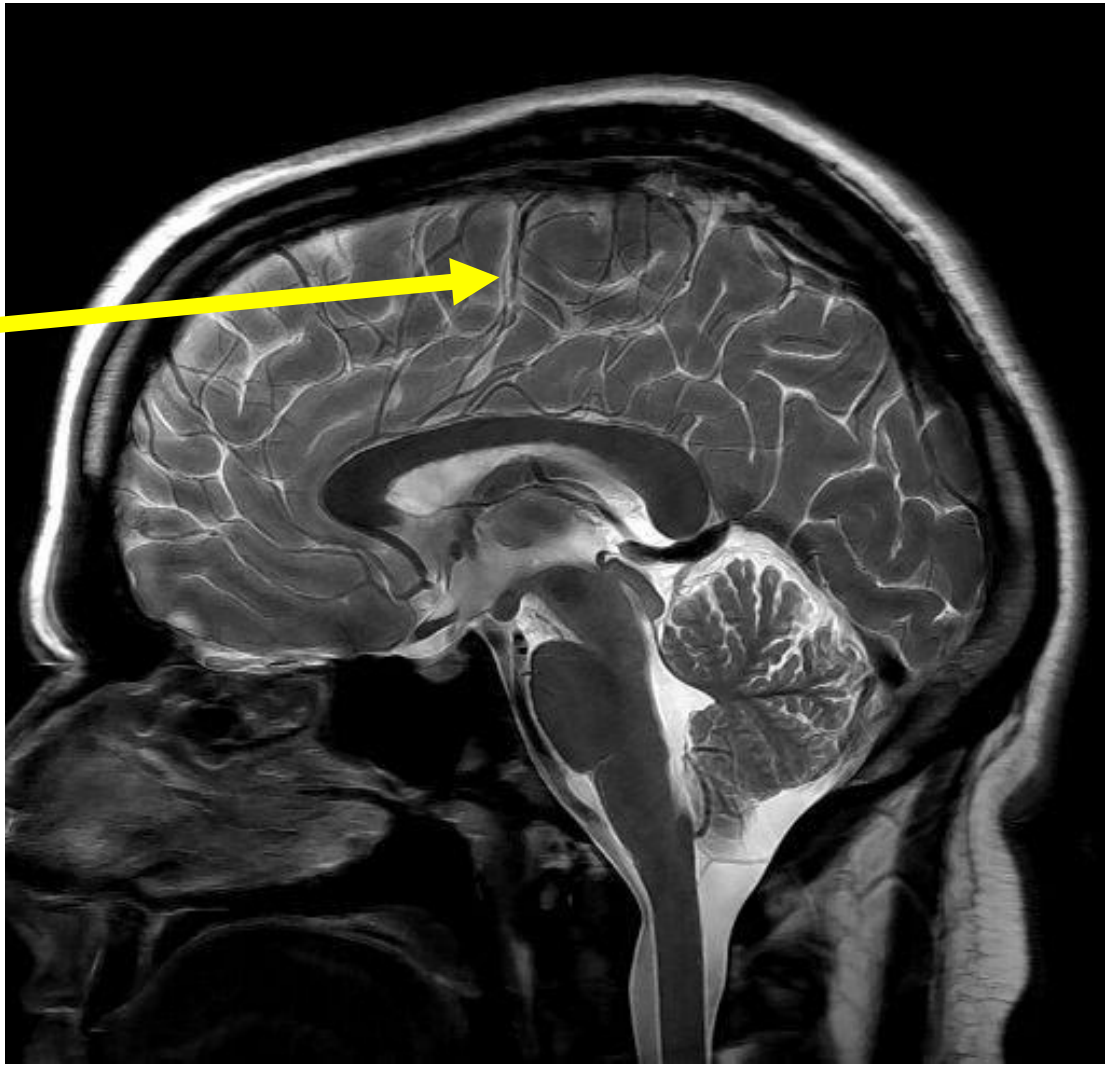
- **Wer erstellt eine Norm**
  - **Industrie Norm**
    - **Vertreter der Industrie**
    - **Vertreter der Anwender**
    - **Gesetzliche Vertreter**

- Elektrische Standards
  - IEC
  - VDE (alt)
- Technische Standards
  - ISO
  - DIN
- EN als Kennzeichen der EU

- Ausserhalb EU
  - ASTM
  - CSA
  - etc.

Speichern Sie bitte

HIER.



Danke für Ihre Aufmerksamkeit.