

Risikoanalyse - reloaded

Nadine Langguth

Matthias Hölzer-Klүpfel



WITTENSTEIN

intens



Über WITTENSTEIN intens

Tochter der WITTENSTEIN SE mit 28 Mitarbeitern



Über WITTENSTEIN intens

- ▶ Entwicklung, Vertrieb, Montage (inkl. Sterilisation)
- ▶ Markteinführung des FITBONE® im Jahre 1997
- ▶ 2.000ste FITBONE® OP im Jahr 2012



Über den FITBONE®

FITBONE® Steuerungsset
mit Verlängerungsmarknagel



FITBONE® Instrumentarium
und Verriegelungsschrauben

Aufgabenstellung



Was bisher geschah...

- ▶ Produkt wurde 1997 erstmals in Verkehr gebracht
- ▶ Regelmäßige Weiterentwicklung mit Delta-Risikoanalysen



... und was daraus werden sollte

- ▶ Zusammenführung der Risikoanalysen
- ▶ Bessere Integration in die technische Dokumentation
- ▶ Zulassung weiterer Varianten
- ▶ Basis für zukünftige Varianten und neue Produkte schaffen

Was ist eigentlich die Gefährdung?



Die Bananenschale?



Verwechslung von Ursache und Gefährdung

- ▶ Gefährdung: potentielle Schadensquelle
- ▶ Vorsicht, wenn etwas Schadensquelle und Ursache sein kann, z.B.
 - ▶ Vibration
 - ▶ hohe Temperatur
 - ▶ ...



Lösungsansatz: root cause

- ▶ Gefährdungssituationen werden mit dem ursprünglichen Auslöser gekennzeichnet
- ▶ Beispiele:
 - ▶ Vibration
 - ▶ Transportschaden
 - ▶ Benutzungsfehler

Manufacturing Fault	▼
n/a	
Use Error	
Transport Damage	
Neglected Maintenance	
Vibration	
ESD	
Wear	
Manufacturing Fault	
Cleaning	
Disinfection	
Overheating	
Fall / External Force	
MRT	
Improper Packaging	
Defibrillation	
Incomplete Sterilization	
Reuse	
Forseeable Misuse	
Design Fault	
Bio-Compatibility	
Reset to Default	

Was ist die Maßnahme?



Offensichtliche Maßnahmen

- ▶ Manche Risikobeherrschungsmaßnahmen sind offensichtlich:
 - ▶ Stromkabel werden isoliert
 - ▶ Implantate werden sterilisiert
 - ▶ Dialysegeräte werden redundant und diversitär konzipiert

Lösungsansatz: State of the Art

- ▶ Wenn der durchschnittliche Konstrukteur “von der Straße” es so macht, ist es Design und keine Maßnahme!
- ▶ Aber:
 - ▶ Wenn die Maßnahme besonders verifiziert und nachverfolgt werden muss: aufnehmen!
 - ▶ Beispiel: Sterilisation

Eintrittswahrscheinlichkeit

- ▶ Eigentliches Problem: wie (und warum) schätzt man die Eintrittswahrscheinlichkeit **vor** Risikobeherrschungsmaßnahmen?

Wie formuliere ich die Maßnahme?



Typisches Beispiel

- ▶ Gefährdungssituation:
 - ▶ Patient verlängert zu viel, weil er die Bewegung des Motors nicht wahrnimmt
- ▶ Bisherige Maßnahmen:
 - ▶ Motor macht ein Laufgeräusch
 - ▶ Dem Gerät wird ein Stethoskop beigelegt
 - ▶ Steuergerät blinkt während der Distraction
 - ▶ Patient muss das Laufgeräusch mit dem Stethoskop überwachen und das Blinken beobachten

Mitigation auf Systemebene

- ▶ Gefährdungssituation:
 - ▶ Patient verlängert zu viel, weil er die Bewegung des Motors nicht wahrnimmt
- ▶ Neue Maßnahme auf Systemebene:
 - ▶ System muss Distraction optisch und akustisch erkennbar machen
- ▶ Details der Umsetzung dann auf einer tieferen Ebene des Designs

Unterschied zw. FMEA und Risikoanalyse?



Failure Mode & Effects Analysis (FMEA)

- ▶ Findet unbekannte Auswirkungen möglicher Fehler
- ▶ bottom-up Ansatz
- ▶ Anwendbar nach Festlegung der Systemarchitektur
- ▶ Elemente der FMEA
 - ▶ Komponenten des Systems
 - ▶ möglich Fehlerereignisse
 - ▶ Auswirkungen

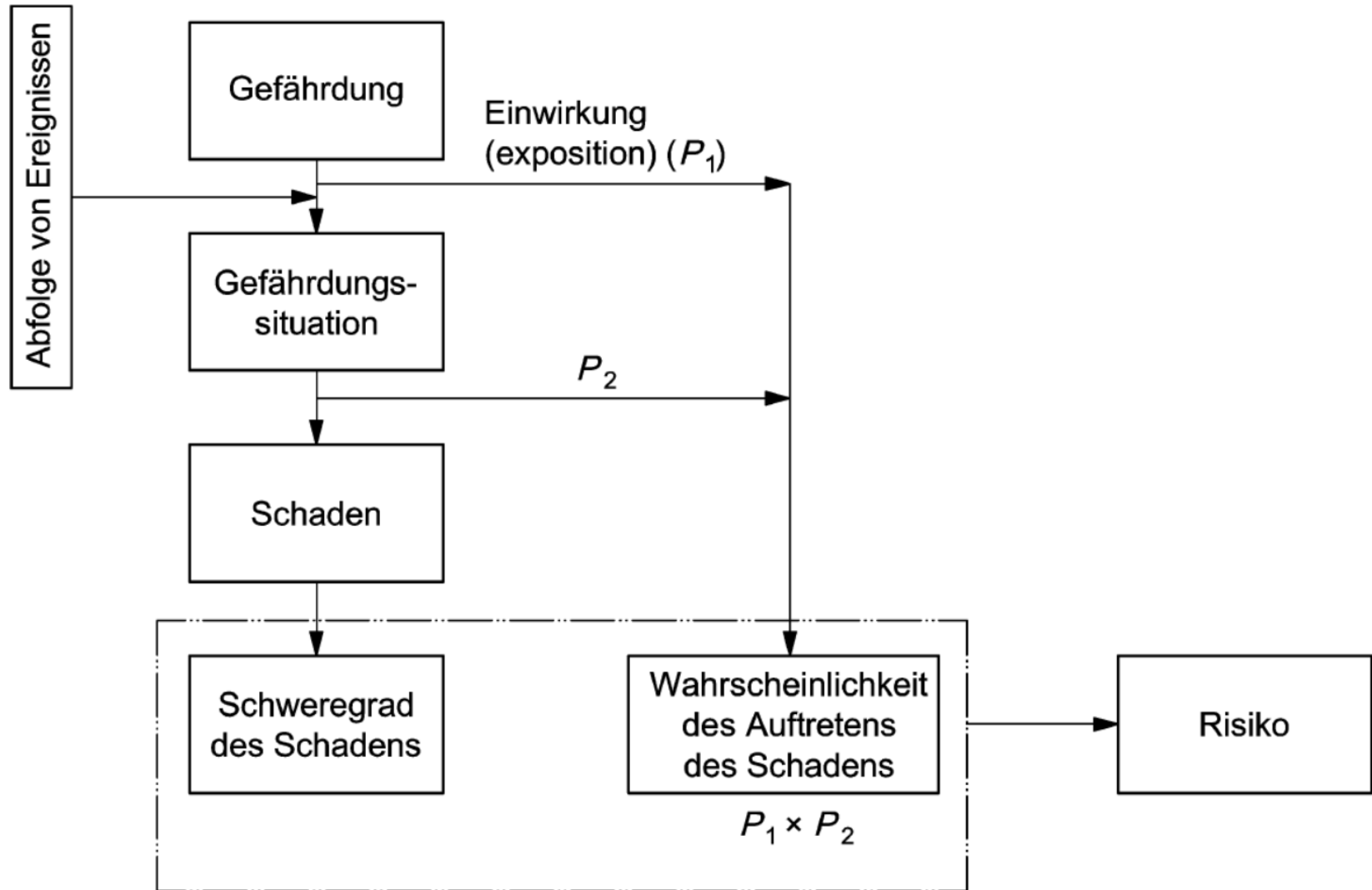
Das ist aber noch nicht alles

- ▶ FMEA bewertet Fehlfunktionen, aber Risiken entstehen auch bei korrekter Funktion aller Systembestandteile
- ▶ FMEA ist erst spät im Entwicklungsprozess möglich
- ▶ Beschränkung auf eine (bottom-up) Methode liefert keine Plausibilitätsprüfung auf Vollständigkeit

Was ist P1 und P2?



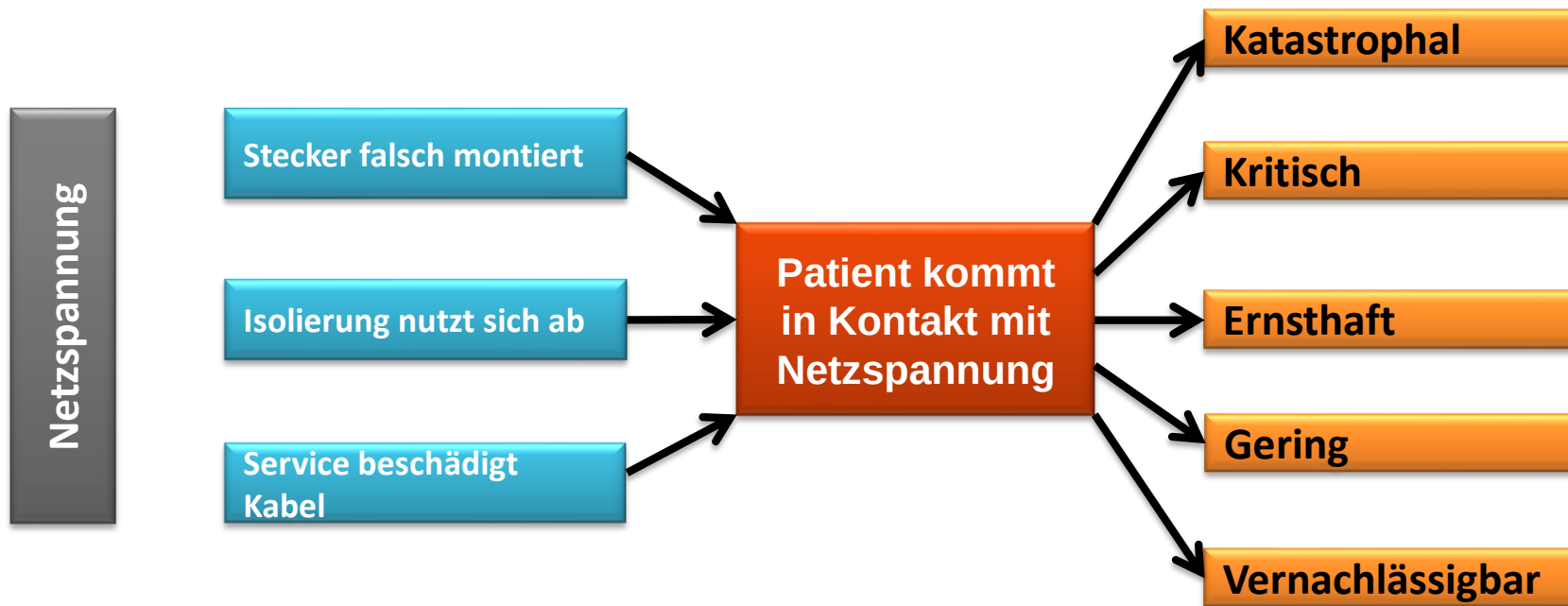
Schätzung der Eintrittswahrscheinlichkeit



P_1 ist die Wahrscheinlichkeit des Auftretens einer Gefährdungssituation.

P_2 ist die Wahrscheinlichkeit einer Gefährdungssituation, die zu Schaden führt.

Von der Gefährdung zum Schaden



Gefährdung Abfolge von Ereignissen P1 Gefährdungssituation P2 Schweregrad des Schadens

“Der Tod ist immer eine Option”

- ▶ Früher hätte man den worst-case angenommen:
 - ▶ P2 für Tod des Patienten = 100%
 - ▶ Fälle, in denen der Patient einen Stromschlag überlebt, fallen unter den Tisch
- ▶ Besser ist es, alle möglichen Endpunkte zu betrachten:
 - ▶ P2 für Tod: ca. 4%
 - ▶ P2 für schwere Verletzung: ca. 40%
 - ▶ ...

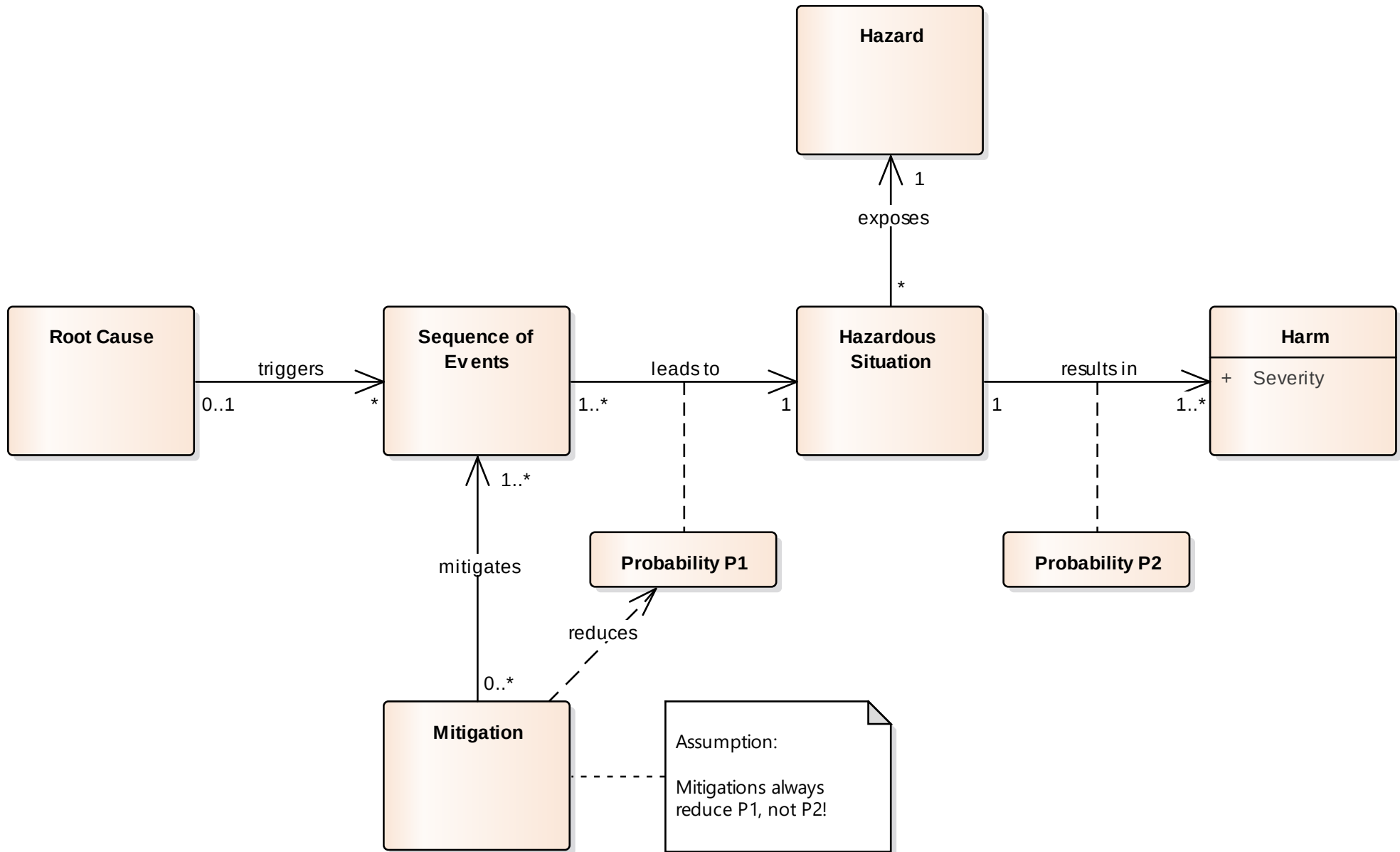
Kompetenztrennung

- ▶ P1 ist die Domäne der Technik(er):
 - ▶ was kann alles schiefgehen?
 - ▶ wie wahrscheinlich ist das?
- ▶ P2 ist die Domäne der Medizin(er):
 - ▶ wie oft komm es vor, dass ...?
 - ▶ wie schlimm ist es, wenn ...?

Wie integrieren wir die RA in DOORS?



Informationsmodell



Schweregrade

Common term	Description	Example
Catastrophic	Results in death of one or multiple persons	
Critical	Results in permanent impairment or life-threatening injury	amputation of the limbs affected ventricular fibrillation
Serious	Results in injury or non-permanent impairment requiring professional medical intervention	revision surgery required to, for example, exchange or at least remove the implant premature termination of treatment the patient has to take antibiotics
Minor	Results in temporary injury or impairment not requiring professional medical intervention	the patient has a skin rash or feels sick
Negligible	No consequence or temporary discomfort	replacement of control set

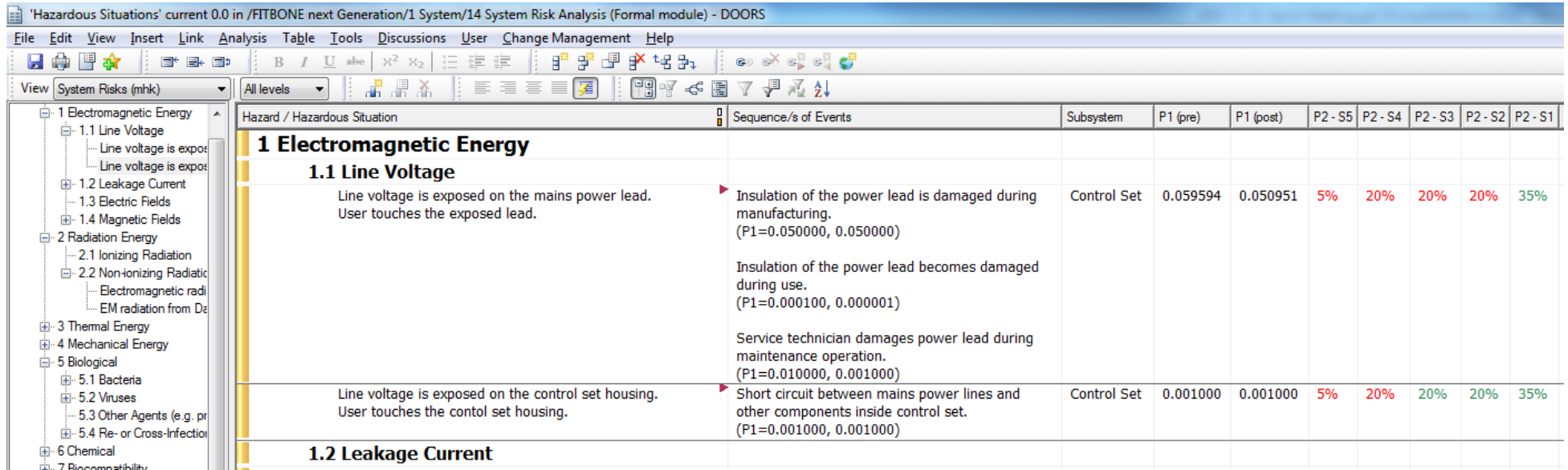
Eintrittswahrscheinlichkeiten

Common terms	Probability range
incredible	$< 10^{-6}$
improbable	$< 10^{-5} \geq 10^{-6}$
remote	$< 10^{-4} \geq 10^{-5}$
occasional	$< 10^{-3} \geq 10^{-4}$
probable	$< 10^{-2} \geq 10^{-3}$
frequent	$> 10^{-2}$

Based on one implanted system!

- P1 Eintrittswahrscheinlichkeit einer Gefährdungssituation
- P2 Wahrscheinlichkeit, dass daraus ein bestimmter Schaden entsteht (**in %**)
- P = P1 * P2 Gesamtwahrscheinlichkeit für einen bestimmten Schaden

Abbildung in DOORS



The screenshot displays the DOORS software interface for a risk analysis. The left sidebar shows a hierarchical tree of system risks, with '1 Electromagnetic Energy' selected. The main table, titled 'Hazard / Hazardous Situation', lists various hazards and their associated sequences of events, subsystems, and probabilities. The table columns include: Hazard / Hazardous Situation, Sequence/s of Events, Subsystem, P1 (pre), P1 (post), P2 - S5, P2 - S4, P2 - S3, P2 - S2, and P2 - S1.

Hazard / Hazardous Situation	Sequence/s of Events	Subsystem	P1 (pre)	P1 (post)	P2 - S5	P2 - S4	P2 - S3	P2 - S2	P2 - S1
1 Electromagnetic Energy									
1.1 Line Voltage									
Line voltage is exposed on the mains power lead. User touches the exposed lead.	Insulation of the power lead is damaged during manufacturing. (P1=0.050000, 0.050000)	Control Set	0.059594	0.050951	5%	20%	20%	20%	35%
	Insulation of the power lead becomes damaged during use. (P1=0.000100, 0.000001)								
	Service technician damages power lead during maintenance operation. (P1=0.010000, 0.001000)								
Line voltage is exposed on the control set housing. User touches the control set housing.	Short circuit between mains power lines and other components inside control set. (P1=0.001000, 0.001000)	Control Set	0.001000	0.001000	5%	20%	20%	20%	35%
1.2 Leakage Current									

- ▶ Eigene Module für „Hazardous Situations“, „Sequences of Events“ und „Mitigations“
- ▶ Für jede Gefährdungssituation werden alle denkbaren Schäden bewertet
- ▶ Eintrittswahrscheinlichkeiten werden automatisch kumuliert
- ▶ Der Risikograph wird automatisch berechnet

Risikograph

'Risk Graph' current 0.0 in /FITBONE next Generation/1 System/14 System Risk Analysis (Formal module) - DOORS

File Edit View Insert Link Analysis Table Tools Discussions User Change Management Help

View Standard view

All levels

Risk Graph

- 1 Risks Before Mitigations
 - 1.0-1
 - 1.0-2
 - 1.0-3
 - 1.0-4
 - 1.0-5
 - 1.0-6
- 2 Risks After Mitigations
 - 2.0-1
 - 2.0-2
 - 2.0-3
 - 2.0-4
 - 2.0-5
 - 2.0-6

ID	Probability	Neg	Min	Ser	Cri	Cat
1	1 Risks Before Mitigations					
3	Frequent					
4	Probable					
5	Occasional					
6	Remote				1	
7	Improbable					
8	Incredible		3		2	
2	2 Risks After Mitigations					
9	Frequent					
10	Probable					
11	Occasional					
12	Remote					
13	Improbable				1	
14	Incredible		3		2	

Wie bewertet man den fehlerfreien Fall?



“Pseudorisiko” für normale Therapie

'Hazardous Situations' current 3.0 in /FITBONE TAA variants/1 System/14 System Risk Analysis (Formal module) - DOORS										
File Edit View Insert Link Analysis Table Tools Discussions User INTENS Change Management Help										
View System Risk Analysis PLM										
All levels										
Hazardous Situations 1 Electromagnetic Energy 1.1 Voltages Electrical shock with line Electrical shock with tra Static discharge Voltage from the IPLD. 1.2 Leakage Current 1.3 Electric Fields 1.4 Magnetic Fields 1.5 Electromagnetic Fields 2 Radiation Energy 3 Thermal Energy 4 Mechanical Energy 5 Biological 6 Chemical 7 Biocompatibility 8 Function 8.1 Incorrect or Inappropriat 8.2 Incorrect Measurement 8.3 Loss or Deterioration of f 8.4 Correct Function 9 Use Error 10 Labeling 11 Operating Instructions 12 Warnings 13 No Hazard										
ID	Hazard	Sequence/s of Events / Hazardous Situation	Harm(s)	Affected U	Mitigations	P2 - S5	P2 - S4	P2 - S3	P2 - S2	P2 - S1
	8.4 Correct Function									
R-01c561-000517	No hazard for the user.	The patient performs a normal distraction therapy without any complications. (P1=1.000000, 0.000001)	Severe pain (S3) Light pain / discomfort (S2) Restricted range of movement (S2) Prickle (S1) No harm (S1)	Patient	The system shall clearly state the contraindication that patients with insufficient femoral head containment (hip dysplasia) for femoral lengthenings are not suited for treatment. The system shall disclose the normal, expectable side-effects of the treatment to the patient. The system shall clearly state the contraindication that patients with a lack of stability in adjacent joints are not suited for treatment.	0%	0%	60%	30%	10%

“Pseudorisiko” für normale Therapie

Ham(s)	P2 - S5	P2 - S4	P2 - S3	P2 - S2	P2 - S1
Severe pain (S3)	0%	0%	60%	30%	10%
Light pain / discomfort (S2)					
Restricted range of movement (S2)					
Prickle (S1)					
No harm (S1)					

Ergebnis



Die neue Risikoanalyse

- ▶ Ein Risikofile, komplett in DOORS
- ▶ Verknüpfung ins Anforderungsmanagement und zu den Nachweisen = Redundanzarme Darstellung und Verwaltung
- ▶ Gemeinsames Verständnis im Team
- ▶ Basis für zukünftige Produkte

A photograph of a campfire at night. The fire is burning brightly in a dark, rocky fire pit. A book is placed on the fire, its cover visible. The cover has the text 'Norm ISO 24971 anschauen' written on it. Several other books are visible in the background, some with labels like 'LN' and 'HKM'. The scene is illuminated by the warm light of the fire, contrasting with the dark night.

Norm
ISO 24971
anschauen

HKM

LN

LN

LN

Norm
ISO 24971
anschauen

Kontakt



MATTHIAS HÖLZER-KLÜPFEL DIPLOM-PHYSIKER, M.SC.

- ▶ **post** Zweite Felsengasse 5
 97082 Würzburg
 Germany
- ▶ **tel** +49 931 32072-821
 fax +49 931 32072-819
 mobil +49 176 6085 7994
- ▶ **mail** matthias@hoelzer-kluepfel.de
 web www.hoelzer-kluepfel.de