

# Computer-Safety

Draft

27. Juli 2011



---

## Inhaltsverzeichnis

---

1	Ein Beispiel für eine alltägliche technische Risikoanalyse	11
1.1	Technische Risikoanalyse . . . . .	11
1.2	Telefone auf Tankstellenhöfen: Kausale Analyse . . . . .	13
1.3	Telefone auf Vorhöfen: Safety Politik . . . . .	18
1.4	Einige Prinzipien . . . . .	22
2	Grundlagen der Systemanalyse	29
2.1	Einleitung: Über die Bedeutsamkeit des Schlussfolgerns . . . . .	29
2.1.1	Der Vorrang des Schlussfolgerns bei Vorhersagen . . . . .	29
2.2	Formale kausale Systemanalyse . . . . .	33
2.3	Was ist ein System? . . . . .	34
2.4	Objekte und Fluents . . . . .	37
2.5	Zustände, Ereignisse und Verhalten . . . . .	38
2.6	Vergleichen von Zuständen . . . . .	40
2.7	Objekte, Teile und das Schließen auf Fehler . . . . .	46
3	Unfall-Analyse	53
3.1	Why Investigate Accidents? . . . . .	53
3.2	What-If Reasoning . . . . .	54
3.3	Where Does This Get Us? . . . . .	59
3.4	The Warsaw Lufthansa A320 Accident [73] . . . . .	60
3.5	The 1988 Habsheim Accident [16] . . . . .	68
3.6	Conclusions . . . . .	71
4	Beispiel einer Why-Because-Analyse	73
4.1	Anfangsbericht . . . . .	73

4.2	Identifizierte Faktoren . . . . .	73
4.2.1	Die folgenden Fakten wurden in der Erzählung als potentielle Faktoren identifiziert . . . . .	73
4.2.2	Die folgenden Aussagen des Anfangsberichts wurden aus den folgenden Gründen aus der Faktorliste ausgelassen . . . . .	76
4.3	Schaden . . . . .	77
4.4	Unfallereignisse . . . . .	77
4.5	Direkte Folgen der Unfallereignisse . . . . .	77
4.6	Potentielle umgebungsbedingte Faktoren . . . . .	77
4.7	Initialer Why-Because Graph dieser Faktoren . . . . .	78
4.8	Der finale Why-Because Graph . . . . .	79
4.9	Zusatzfaktoren . . . . .	84
4.10	Verifizierung des finalen Why-Because Graph . . . . .	84
4.11	Erläuterung des Zwischenfalles . . . . .	87
4.12	Grapheditierung . . . . .	87
4.12.1	Diese Ursachen lassen sich wie folgt gruppieren . . . . .	87
4.12.2	Editierter Why-Because Graph . . . . .	89
4.13	Vergleich mit der Analyse von Gruppe Ladkin . . . . .	94
4.13.1	Die folgenden Gruppenknoten wurden in beiden Analysen als gemeinschaftlich identifiziert . . . . .	94
4.13.2	Die folgenden Faktoren traten in unserem WBG, aber nicht in dem WBG der Gruppe Ladkin auf . . . . .	96
4.13.3	Die folgenden Faktoren traten in dem WBG der Gruppe Ladkin, aber nicht in unserem WBG auf . . . . .	96
4.13.4	Die folgenden kausalen Faktoren wurden von uns und Gruppe Ladkin unterschiedliche bewertet . . . . .	97
4.13.5	Die Gründe für diese unterschiedliche Bewertung erscheinen uns als die Folgenden . . . . .	97
4.14	Auflösung der Analyse mit der der Gruppe Ladkin . . . . .	98
4.14.1	Resultierender Why-Because-Graph . . . . .	98
5	Probleme mit der Verwendung des Begriffs <i>Hazard</i> zur Risikoberechnung	105
5.1	Fünf Konzepte für Hazards . . . . .	105
5.1.1	Auffassungen in System Safety und verwandte Ansichten . . .	105
5.1.2	Die MIL-STD-882 Definition: Hazard-5 . . . . .	107

---

5.2	Definition des Systems S . . . . .	108
5.3	Hazard-4 und Hazard-1 Zustände berechnen . . . . .	111
5.3.1	Hazard-4 Zustände identifizieren . . . . .	112
5.3.2	Hazard-1 Zustände identifizieren . . . . .	113
5.3.3	Ein Unfall ohne vorhergehenden Hazard . . . . .	113
5.4	Berechnen der Wahrscheinlichkeiten . . . . .	113
5.5	Berechnen von Hazard-3 und Hazard-5 Zuständen . . . . .	118
5.5.1	Bestimmen der Hazard-5 Zustände . . . . .	118
5.5.2	Bestimmen der Hazard-3 Zustände . . . . .	120
5.6	Die Berechnung des Risikos anhand von Hazards . . . . .	121
5.7	Das Problem . . . . .	122
5.7.1	Ein Risiko: Mehrfaches Erfassen . . . . .	122
5.7.2	Nicht allen Unfällen geht ein Hazard voraus . . . . .	123
5.7.3	Zusammenfassung . . . . .	123
5.8	Ein Versuch das Problem zu lösen . . . . .	123
5.9	Motivationen für das Konzept des Hazard . . . . .	125
5.9.1	Abschwächen der Unvermeidbarkeitsforderung . . . . .	126
5.9.2	Vermeidung problematischer Auffassungen . . . . .	128
5.9.3	Klassifizierung von Risiko über Statistiken . . . . .	129
5.10	Zusammenfassung . . . . .	134
6	Definitionen und Terminologie . . . . .	135
7	Einführung in die Gefährdungs-Analyse . . . . .	145
7.1	Einführung . . . . .	145
7.2	Das Beispielsystem . . . . .	146
7.3	Die HazOp des Beispiel-Systems . . . . .	147
7.3.1	Ein erstes Beispiel . . . . .	148
7.4	Failure Mode, Effects and Criticality Analysis (FMECA) . . . . .	149
7.5	Fault Tree Analysis (FTA) / Fehlerbaumanalyse . . . . .	150
7.6	Vergleichende Analysen . . . . .	150
8	Ontological Hazard Analysis — Überblick . . . . .	153
8.1	Introduction . . . . .	153
8.2	A Case Study: OHA for an Automotive Communications Bus System . . . . .	158
8.2.1	Initial System Description . . . . .	158

8.2.2	Ontology of the initial system description . . . . .	158
8.2.3	Guide-Word based Approach for Identification of Hazards . .	158
8.2.4	Formalisation of Deviations by Usage of Ontology . . . . .	162
8.2.5	Extended Partial Why-Because Graphs . . . . .	162
8.2.6	Statistics of the Analysis . . . . .	163
8.2.7	Transformation of epWBGs into Fault Trees . . . . .	164
8.2.8	Filtering of epWBGs . . . . .	165
8.2.9	Algorithm used for clustering epWBGs . . . . .	167
8.2.10	Conversion of clustered epWBGs into partial Fault Trees . . .	167
8.2.11	Combining partial Fault Trees into one overall Fault Tree . . .	167
9	OHA-Beispiel — Automobil-Kommunikationsbus	171
9.1	Introduction . . . . .	171
9.2	Ontological Hazard Analysis . . . . .	172
9.2.1	A Generic Digital-Communication Bus . . . . .	174
9.3	Level 0 . . . . .	177
9.3.1	Objects . . . . .	178
9.3.2	Properties . . . . .	179
9.3.3	Relations . . . . .	180
9.3.4	Meaning Postulates . . . . .	180
9.3.5	Using HAZOP . . . . .	182
9.3.6	Hazardous Happenstance: Summary and Discussion . . . . .	186
9.3.7	Hazardous Happenstance: Final Determination and Extended Vocabulary . . . . .	189
9.3.8	Hazardous Factor Mitigation and Avoidance . . . . .	192
9.4	Level 1: The First Refinement Level . . . . .	192
9.4.1	Moving to Level 1: Structuring Messages and Message-Passing	193
9.4.2	Level 1 General Definitions and General Meaning Postulates .	194
9.4.3	Level 1 Hazard Analysis for Lost(msg) . . . . .	196
9.4.4	Level 1 Rearrangement of HazHapps . . . . .	199
9.4.5	Level 1 HazHapp Avoidance and Mitigation . . . . .	199
9.4.6	Summary of Level 1 Results . . . . .	200
9.5	Level 2 Refinement . . . . .	203
9.6	Deciding on Level 3 . . . . .	204
9.7	Overall Summary . . . . .	205

---

9.8 Conclusion . . . . .	208
10 OHA-Beispiel — Zugleitbetrieb nach FV-NE	211
10.1 Einführung . . . . .	211
10.1.1 Sortenlogik ( <i>Many-Sorted Logic</i> ) . . . . .	211
10.2 Ebene 0 („UrSpec“) . . . . .	212
10.2.1 Sorten ( <i>sorts</i> ) . . . . .	212
10.2.2 Relationen . . . . .	212
10.2.3 Sicherheitsaxiome . . . . .	213
10.2.4 Ein Zug . . . . .	213
10.2.5 Zwei Züge . . . . .	214
10.2.6 Verfeinerung ( <i>Refinement</i> ) . . . . .	214
10.3 Ebene 1 — erste Verfeinerung ( <i>Refinement</i> ) . . . . .	215
10.3.1 Sorten . . . . .	215
10.3.2 Sicherheitsaxiome . . . . .	217
10.4 Ebene 2 . . . . .	218
10.4.1 Sorten . . . . .	218
10.4.2 Relationen . . . . .	218
10.4.3 Beschreibung einer Zugfahrt im Zugleitbetrieb . . . . .	219
10.4.4 Sicherheitsaxiome . . . . .	224
10.4.5 Beweis der Verfeinerung . . . . .	224
10.4.6 Hazards . . . . .	226
10.5 Ebene 3 . . . . .	227
10.5.1 Unvollständigkeit der FV-NE . . . . .	227
10.5.2 Zustandsautomaten mit Kommunikation . . . . .	228
10.5.3 Message-Flow-Graph . . . . .	228
10.6 Implementation in SPARK . . . . .	229
10.6.1 SPARK . . . . .	229
10.6.2 Spezifikation der Funktionen . . . . .	230
10.6.3 Zugführer . . . . .	231
10.7 Model-Checking mit SPIN . . . . .	232
10.7.1 Der SPIN-Model-Checker . . . . .	232
10.7.2 Implementation in PROMELA . . . . .	233
10.7.3 Assertions . . . . .	236
10.7.4 Lineare Strecke . . . . .	237

10.7.5 Zustandsmaschinen . . . . .	237
10.7.6 Verifikation . . . . .	239
10.7.7 Meaning Postulates . . . . .	244
10.7.8 Implementation der MFG . . . . .	248
10.7.9 MFG, Promela und SPARK . . . . .	251
<b>11 Probabilistische Risiko-Analyse</b>	<b>255</b>
<b>12 An Overview of IEC 61508 on E/E/PE Functional Safety</b>	<b>259</b>
12.1 What IEC 61508 is about, how it is standardised, how used . . . . .	259
12.2 Definitions of Basic Concepts . . . . .	260
12.3 The Major Concepts of IEC 61508 . . . . .	265
12.4 The System Life-Cycle . . . . .	266
12.4.1 The E/E/PE and Software Safety Lifecycles . . . . .	269
12.4.2 Common Software Lifecycle Stages and the IEC 61508 Lifecycle	269
12.5 Functional Safety . . . . .	277
12.5.1 Assuring Functional Safety and Safety Functions . . . . .	278
12.6 Risk and Risk Reduction . . . . .	279
12.6.1 Determination of Risk Reduction: Balancing the Options . . . . .	281
12.6.2 Risk Reduction and ALARP . . . . .	284
12.7 Subsystem Types . . . . .	286
12.8 Safety Integrity and Safety Integrity Levels (SILs) . . . . .	287
12.8.1 Lowest Recognised Risk Reduction . . . . .	291
12.8.2 Relationship between SILs and ALARP . . . . .	292
12.9 Appropriate and Inappropriate Applications of the IEC 61508 Approach	292
12.9.1 Safety Functions . . . . .	293
12.9.2 Safety Integrity Levels . . . . .	297
12.9.3 Difficulties with Applying ALARP . . . . .	298
<b>13 Kontextfreie SILs</b>	<b>301</b>
13.1 Zusammenfassung . . . . .	301
13.2 Einleitung . . . . .	301
13.3 Kontextfreie Bestimmung von Sicherheitslabels (SL) . . . . .	303
13.4 Das Gegenargument . . . . .	303
13.5 Bedeutung für die Integration . . . . .	304
13.6 Schlussfolgerung . . . . .	305

---

14 Software-Richtlinien für IEC 61508	307
14.1 Comments on Part 3, Annexes A and B . . . . .	307
14.2 A Proposal for Revised Requirements and Guidance on SW in Part 3 .	309
14.3 How the Proposals Will Achieve Higher SW Quality . . . . .	311
14.4 Software SILs . . . . .	312
14.5 Applicable Techniques and Recommendations (Annex A) . . . . .	314
15 Securing the Interface: Safety-Critical Interaction between Humans and Mo- bile Robots	317
15.1 Introduction . . . . .	317
15.2 Some Abstract Technical Preliminaries . . . . .	317
15.3 Engineered Multiagent Cooperative Functions . . . . .	318
15.4 Safety of EMC Function . . . . .	319
15.5 Humanoid Robots: Due Diligence and Beyond . . . . .	320
15.6 Principles of Design for Safety: the RCMC . . . . .	320
15.6.1 Principle: The Bounded-Rationality Criterion . . . . .	322
15.6.2 Principle: the Mutual Cognisance of Relevant Parameters . . .	323
15.6.3 Principle: Procedural Completeness Criterion (PCC) . . . . .	325
15.7 Too Strong? . . . . .	327
16 Herleitung einer Berechnung von Littlewood und Strigini	329
16.1 Bayessche Wahrscheinlichkeitsrechnung . . . . .	329
16.2 Homogene Anpassung . . . . .	330
16.3 Vorurteilsfreie $\lambda$ -Verteilung . . . . .	332
16.4 Fazit . . . . .	333
Abbildungsverzeichnis	336
Tabellenverzeichnis	339

