



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Besondere Betrachtung der Kaskadeneffekte in Bezug
auf das Risikomanagement von kritischen
Infrastrukturen am Beispiel eines Krankenhauses“

verfasst von / submitted by

Dipl.-Ing. (FH); Dipl.-WirtschIng. (FH) Charles FRAUENBERG

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Science (MSc)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

UA 992 242

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Risikoprävention und Katastrophenmanagement

Betreut von / Supervisor:

Dipl.-Ing.; Dr. Stefan SCHAUER

Danksagung

Für die Betreuung der Master Thesis möchte ich mich bei Dipl.-Ing.; Dr Stefan Schauer ganz herzlich bedanken. Wir haben uns regelmäßig ausgetauscht, sei es in geplanten Besprechungen oder auch kurzfristig per Telefon oder Emailverkehr. Danke für diese Verfügbarkeit. Dies war für mich eine große Stütze und ich habe dadurch den Fokus auf die wichtigen Themen behalten. Auch konnte ich die SAURON Propagation Engine vom Austrian Institute of Technology kostenlos nutzen.

Ganz besonders möchte ich meiner Familie danken. Ohne die Unterstützung, das Verständnis und die Motivation meiner Frau Marise sowie meiner beiden Söhnen Felix und Lex hätte ich den Weg durch das gesamte Studium nicht geschafft. Bedingt durch Beruf und Studium hatte ich in den letzten beiden Jahren wenig Zeit für sie, aber ich konnte immer auf sie zählen und dafür bin ich außerordentlich Dankbar. Auch hat meine Mutter Nanny die Familie in der Zeit tatkräftig unterstützt.

Für das Korrekturlesen der vorliegenden Arbeit, die kritischen Diskussionen und die Motivation während dem Schreiben, möchte ich mich bei Isabelle und Guy bedanken.

Die Software bcNAVIGATOR wurde mir kostenlos zur Verfügung gestellt, dafür ein Dankeschön an Gerald und Gerhard.

Meinem Arbeitgeber gebührt ein großes Dankeschön für die großartige Unterstützung während des gesamten Studiums und ganz besonders im Sommer 2021 während dem Schreiben dieser Arbeit. Insbesondere Herrn Georges Bassing (Verwaltungsdirektor), meinen Mitarbeiter*Innen (Carlo, Fränk, Jasmine, Marc, Michael und Nadine) der Abteilung „Protection et Prévention“ sowie den Mitgliedern des Krisen- und Koordinierungsstabes möchte ich Danken.

Für die Datensammlung war ich auf das Fachwissen der Expert*Innen aus den Fachabteilungen angewiesen und möchte mich bei Andy, Antonio, Cliff, Gerry, Guy, Patrick, Sandra und Sylvia ganz herzlich für die Unterstützung bedanken.

I. Inhaltsverzeichnis

Danksagung	III
I. Inhaltsverzeichnis.....	V
II. Abbildungsverzeichnis	IX
III. Tabellenverzeichnis	XIII
IV. Abkürzungsverzeichnis	XV
1 Domino-Effekte und Resilienz Förderung in kritischen Infrastrukturen	1
1.1 Gefährdungen	1
1.2 Problemstellung	3
1.3 Zielsetzung der Arbeit	4
1.4 Hypothesen und Forschungsfragen	4
1.4.1 Hypothese 1	4
1.4.2 Unterforschungsfrage 1	5
1.4.3 Unterforschungsfrage 2	5
1.4.4 Hypothese 2	5
1.4.5 Unterforschungsfrage 3	5
1.4.6 Unterforschungsfrage 4	5
2 Begriffsdefinitionen.....	2
3 Methodik.....	8
3.1 Literatur Recherche	8
3.1.1 Suchsysteme	8
3.1.2 Literatúrauswahl	9
3.1.3 Literaturverwaltung	10
3.2 Systemmodellierung	11
3.3 Informationsbeschaffung.....	13
3.4 Risikoanalyse	18
3.5 bcNAVIGATOR – bcIMPACT	20
3.6 SAURON Propagation Engine	24
4 Kritische Infrastrukturen und deren Abhängigkeiten	28
4.1 Kritische Infrastrukturen in der Gesellschaft	28
4.1.1 Sektoren	30
4.1.2 Kritische Infrastruktur Krankenhaus.....	31

4.2	Abhängigkeiten von kritischen Infrastrukturen	32
4.2.1	Interdependenzen	34
4.2.2	Umfeld	35
4.2.3	Verbindungen und Reaktionsverhalten.....	35
4.2.4	Charakteristik der Infrastruktur	35
4.2.5	Betriebszustand	35
4.2.6	Störungen	36
4.3	Kaskadeneffekte	36
4.3.1	CERBERUS-System.....	37
4.3.2	SAURON-Rahmenwerk	40
5	Digitalisierung und Cyber-physische Systeme.....	42
5.1	Vierte industrielle Revolution, Cyber-physische Systeme und Gesellschaft 4.0	42
5.2	Digitalisierung in kritischen Infrastrukturen – Krankenhaus 4.0	46
6	Verwundbarkeiten und deren Auswirkungen	50
6.1	Gefährdungen für kritische Infrastrukturen	50
6.2	Verwundbarkeit von kritischen Infrastrukturen.....	51
6.3	Abhängigkeiten	52
6.4	Auswirkungen von Zwischenfällen auf kritische Infrastrukturen	53
6.4.1	Fallbeispiel: Cyberangriff auf das Lukaskrankenhaus Neuss (D)	55
6.4.2	Fallbeispiel: Brand im BG Universitätskrankenhaus Bergmannsheil Bochum (D)	56
6.4.3	Fallbeispiel: Stromausfall am Bundeswehr-Krankenhaus Hamburg.....	57
7	Risikomanagement und Business Continuity Management.....	58
7.1	Risikomanagement	58
7.1.1	Risikoidentifikation, -analyse und -bewertung	61
7.1.2	Risikobewältigung	64
7.2	Business Continuity Management	66
7.3	Business Impact Analyse	69
7.4	Risikomanagement und Business Continuity Management in kritischen Infrastrukturen.....	72
8	Fallstudie am Bsp. der zentralen Aufbereitungseinheit für Medizinprodukte	76
8.1	Beschreibung des fiktiven Krankenhauses und der AEMP.....	76
8.1.1	Die Gebäudestruktur.....	76

8.1.2	Die Aufbereitungseinheit für Medizinprodukte	77
8.1.3	Digitalisierung im Krankenhaus und insbesondere in der AEMP	79
8.1.4	Prozesslandkarte	80
8.2	Datensammlung zu den wesentlichen Prozessen	81
8.2.1	Erstellung des Fragebogens	85
8.2.2	Erstellung der BIA-Matrix	88
8.3	Szenarien für die dynamischen Risikoanalysen	93
8.3.1	Szenario 1: Überschwemmung UG 2	93
8.3.2	Szenario 2: Cyberangriff	94
8.4	Statische Risikoanalyse	94
8.5	Dynamische Risikoanalyse	95
8.6	Auswertung der Ergebnisse	97
9	Diskussion der Ergebnisse	100
9.1	Unterforschungsfrage 1	100
9.2	Unterforschungsfrage 2	101
9.3	Unterforschungsfrage 3	101
9.4	Unterforschungsfrage 4	102
10	Zusammenfassung	104
11	Perspektive – Ausblick	110
12	Kurzzusammenfassung - Abstract	114
13	Literaturverzeichnis	116
14	Anhang	126
14.1	Prozessabhängigkeiten der AEMP	126
14.2	BIA-Datensammlung - Deckblatt	127
14.3	BIA-Datensammlung - Allgemeine Informationen	128
14.4	BIA-Datensammlung – Prozessbeschreibung	131
14.5	BIA-Matrix – Abhängigkeiten	134
14.6	BIA-Matrix – Prozess- und Ressourcenbeschreibung, Beschreibung der Robustheit	139
14.7	BIA-Matrix – Schadensklassen	142
14.8	BIA-Matrix – RPO, RTO, MTPD	145
14.9	Relationales Datenmodell der Versorgungssystem im fiktiven Krankenhaus	148
14.10	Parametrierung bcIMPACT	150

14.11	Parametrierung SAURON Propagation Engine.....	161
14.12	SAURON Übergangstabelle.....	167
14.13	Ergebnisse der Risikoanalysen	172
14.13.1	Statische Risikoanalyse - Kritische Prozesse	172
14.13.2	Statische Risikoanalyse - Kritische Ressourcen	178
14.13.3	Dynamische Risikoanalyse – Überschwemmung UG 2 > 1m.....	185
14.13.4	Dynamische Risikoanalyse - Cyberangriff	189
14.14	Mindmap der Literaturrecherche	193

II. Abbildungsverzeichnis

Abbildung 1: Beziehung zwischen Gefahr, Vulnerabilität, Risiko und angehörigen Konzepten (Quelle: ALEXANDER D. E. 2002: 29)	6
Abbildung 2: Risikomanagement-Prozess aus ONR 49000:2008 (Quelle: AUSTRIAN-STANDARDS 2008a: 17)	7
Abbildung 3: Auszug Mindmap zur Literaturrecherche am Bsp. der Kaskadeneffekte.....	10
Abbildung 4: Schematische Darstellung der CERBERUS Systemarchitektur (Quelle: SCHAUER S. et al. 2018: 316)	11
Abbildung 5: Allgemeine Bestandteile einer Prozessanalyse (Quelle: ANDLER N. 2015: 344)	17
Abbildung 6: Struktur zur Durchführung einer BIA (Quelle: TAARUP-ESBENSEN J. 2020)	20
Abbildung 7: Vorgehensweise für die Datensammlung zur Business Impact Analyse.....	20
Abbildung 8: bcNAVIGATOR (Quelle: BC-Consulting 2021a)	21
Abbildung 9: Menüfenster bcIMPACT	22
Abbildung 10: SAURON – Netzwerkeingabe, Bsp.: Netzwerk der Interdependenzen zur Aufbereitungseinheit von Medizinprodukten des fiktiven Krankenhauses	25
Abbildung 11: SAURON: Netzwerkknoten: Parametrierung der Übergänge	26
Abbildung 12: SAURON – Beispiel-Simulationseingabe.....	26
Abbildung 13: SAURON – Beispiel-Ergebnis einer Simulation	27
Abbildung 14: Sektoren und Branchen KRITIS (Quelle: BBK und BSI 2021b)	30
Abbildung 15: Die vier Ebenen der Gesundheitsversorgung als "Kritische Infrastruktur" (Quelle: BBK 2008: 8)	32
Abbildung 16: Anzahl der Zitierungen und Forschungsinteresse des Dokumentes (RINALDI S. M. et al. 2001) (Quelle: RESEARCHGATE 2021).....	33
Abbildung 17: Sechs Dimensionen zur Beschreibung der Interdependenzen von Infrastrukturen (Quelle: RINALDI S. M. et al. 2001: 12).....	34
Abbildung 18: Interdependenzen kritischer Infrastrukturen (Quelle: Ehlen M. und Vargas V. 2013: 6)	36
Abbildung 19: Schematische Darstellung des CERBERUS Modell (Quelle: SCHAUER S. et al. 2018: 318).....	38
Abbildung 20: SAURON Rahmenwerk mit der Propagation Engine (Markierung) (SCHAUER S. et al. 2019).....	41
Abbildung 21: Industrial revolution (Quelle Shutterstock)	42

Abbildung 22: Transition process from Mechatronics to CPS to Internet of Things (Quelle: HEHENBERGER P. et al. 2016: 274)	43
Abbildung 23: Cyber-Physical System (Quelle: EROARKE 2014)	43
Abbildung 24: Smart Mobility (Quelle Shutterstock).....	44
Abbildung 25: Smart Grid (Quelle: Shutterstock)	45
Abbildung 26: Smart City (Quelle Shutterstock).....	46
Abbildung 27: Smart Hospital (Quelle Shutterstock)	47
Abbildung 28: Kompetenzen des selbstbestimmten, souveränen digitalen Krankenhauses (Quelle: BURMANN A. et al. 2019: 10).....	47
Abbildung 29: Beispiel für logisches Topologiemodell eines KIS (fiktive Produktamen) (Quelle: HAAS P. 2005: 63).....	49
Abbildung 30: Beispiel Prozesslandschaft Krankenhaus (Quelle: KUNTSCHE P. und BÖRCHERS K. 2017a: 108)	52
Abbildung 31: Infrastruktur-Abhängigkeiten: Auswahl kritischer Infrastrukturen und wichtiger Ressourcen (Quelle: Ehlen M. und VARGAS V. 2013: 7).....	54
Abbildung 32: Example of Business and Operational Risks and their Domino Effects (vgl. World Economic Forum 2012: 32).....	58
Abbildung 33: Grundsätze des Risikomanagement nach ISO 31000:2018 – eigene Darstellung (Quelle: ISO 2018: 3-4)	59
Abbildung 34: Risikomanagement-Kreislauf (Quelle: KRYSTEK U. und FIEGE S. 2013)	64
Abbildung 35: Grundsätzliche Strategien zur Risikosteuerung (Quelle: ROMEIKE F. 2018: 47)	65
Abbildung 36: Resilienz schaffen durch verschiedene Sicherheitsthemen (Quelle: BSI 2021: 7)	67
Abbildung 37: BCMS-Bestandteile (Quelle: BSI 2021: 13)	68
Abbildung 38: Struktur zur Durchführung einer BIA (Quellen: TAARUP-ESBENSEN J. 2020: 4)	70
Abbildung 39: Erläuterung der Kenngrößen MTPD (MTPOD), RTO, RPO (Quelle: GOH M. H. 2011).....	72
Abbildung 40: Der Resilienztrichter (Quelle: MEISSNER J. O. 2017: 53)	73
Abbildung 41: Aufbereitungskreislauf für Medizinprodukte (Quelle: KIRMSE G. und WILD R. 2020: 123)	77
Abbildung 42: Raumkonzept einer AEMP (Quelle: CARTER A. et al. 2015: 6).....	79
Abbildung 43: Prozesslandkarte fiktives Krankenhaus	80
Abbildung 44: vereinfachter Kreislauf der wiederverwendbaren Medizinprodukte.....	81
Abbildung 45: Auszug BIA-Matrix - Darstellung der Abhängigkeiten	89

Abbildung 46: Auszug BIA-Matrix - Beschreibung und Robustheit	90
Abbildung 47: Auszug BIA-Matrix - Schadensklassen	90
Abbildung 48: Auszug BIA-Matrix - RPO, RTO, MTPD	91
Abbildung 49: Versorgung der AMEP - Auszug aus dem Datenmodell der Versorgungssystem (siehe Anhang 14.9)	93
Abbildung 50: Abhängigkeits-Netzwerk der AMEP (graphische Darstellung in der SAURON Propagation Engine)	96
Abbildung 51: PDCA-Zyklus eines Managementsystems (Quelle: BSI 2021: 14) ...	110
Abbildung 52: Prozessabhängigkeiten AEMP	126
Abbildung 53: Menüfenster bcIMPACT	150
Abbildung 54: bcIMPACT - Prozesstypen	150
Abbildung 55: bcImpact – Prozesskritikalitäten	151
Abbildung 56: bcIMPACT – Prozesskritikalität Schadensklasse-Zeitbereiche	151
Abbildung 57: bcIMPACT – Prozesskritikalitäten Schadensklasse-Werte	151
Abbildung 58: bcIMPACT – Prozesskritikalität Verfügbarkeit-Zeitbereiche	152
Abbildung 59: bcIMPACT – Prozesskritikalität Verfügbarkeit-Werte	152
Abbildung 60: bcIMPACT - zusätzliche Prozessfelder	152
Abbildung 61: bcIMPACT - Prozesskritikalitätskategorien	153
Abbildung 62: bcIMPACT - Organisationen	153
Abbildung 63: bcIMPACT - Rollen	154
Abbildung 64: bcIMPACT – Rolle, Bsp.: AEMP Stammdatenadministrator	154
Abbildung 65: bcIMPACT - Standorte	155
Abbildung 66: bcIMPACT - Partner	155
Abbildung 67: bcIMPACT – Partner, Bsp.: Wartungsfirma RDG	156
Abbildung 68: bcIMPACT - konfigurierbare Ressourcen	156
Abbildung 69: bcIMPACT - konfigurierbare Ressourcen, Bsp.: Reinigungs & Desinfektionsgeräte (RDG)	157
Abbildung 70: bcIMPACT – Ressourcenbeziehungen, Bsp.: Reinigungs- & Desinfektionsgeräte (RDG)	157
Abbildung 71: bcIMPACT – Prozesshierarchie	158
Abbildung 72: bcIMPACT - Prozess anlegen	159
Abbildung 73: bcIMPACT - Menü Prozessabhängigkeiten	159
Abbildung 74: bcIMPACT – Prozessbeziehungen, Bsp.: Aufbereitungseinheit für Medizinprodukte	160

Abbildung 75: bcIMPACT – Ressourcenbeziehungen, Bsp: Prozess maschinelle Reinigung & Desinfektion MP	160
Abbildung 76: SAURON – Dateienverwaltung	161
Abbildung 77: SAURON – Netzwerkeingabe, Bsp.: Netzwerk der Interdependenzen zur Aufbereitungseinheit von Medizinprodukten des fiktiven Krankenhauses	162
Abbildung 78: SAURON - Mehrfacheingabe von neuen Netzwerkknoten	163
Abbildung 79: SAURON – Netzwerkparametrierung.....	163
Abbildung 80: SAURON - Netzwerkknoten: Allgemeine Informationen	164
Abbildung 81: SAURON: Netzwerkknoten: Parametrierung der Übergänge	165
Abbildung 82: SAURON - Netzwerkknoten: Parametrierung der Interdependenzen	165
Abbildung 83: SAURON – Simulationseingabe.....	166
Abbildung 84: SAURON - Ergebnisanzeige der Simulation	166
Abbildung 85: Mindmap der Literaturrecherche	193

III. Tabellenverzeichnis

Tabelle 1: Indikative Liste der kritischen Infrastrukturen (Quelle: EU 2005: 26)	29
Tabelle 2: Methoden der Risikoidentifikation, -analyse und -bewertung (Quelle: ROMEIKE F. 2018: 56).....	61
Tabelle 3: Übersicht der Methoden im Risikomanagement-Prozess (Quellen: AUSTRIAN-STANDARDS 2008b: 5)	63
Tabelle 4: PDCA-Zyklus im BCM-Prozess (vgl. BSI 2021: 145)	68
Tabelle 5: kritische Prozessschritte der AEMP	82
Tabelle 6: Ressourcen-Kategorie Internes Personal.....	82
Tabelle 7: Ressourcen-Kategorie Externe Partner.....	83
Tabelle 8: Ressourcen-Kategorie IT-Software & Prozessgeräte.....	83
Tabelle 9: Ressourcen-Kategorie IT-Software & Prozessgeräte.....	84
Tabelle 10: Ressourcen-Kategorie Versorgung / Anlagen	84
Tabelle 11: Ressourcen-Kategorie Sicherheitstechnik.....	85
Tabelle 12: Technische Versorgungssysteme der AEMP	91
Tabelle 13: Vorschlag einer EU-Richtlinie über die Resilienz kritischer Einrichtungen - Sektoren & Teilsektoren (vgl. EU 2020b: 74)	111
Tabelle 14: SAURON – Menüführung zur Netzwerkeingabe	162
Tabelle 15: SAURON - Menüführung zur Parametrierung der Knoten	163
Tabelle 16: SAURON - Parameter der Übergangsmatrix.....	164
Tabelle 17: Risikoanlage - Überblick der kritischen Prozesse	172
Tabelle 18: stat. Risikoanalyse - Übersicht der Abhängigkeiten pro Prozess	173
Tabelle 19: stat. Risikoanalyse - kritische Ressourcen	178

IV. Abkürzungsverzeichnis

AEMP	<i>Aufbereitungseinheit für Medizinprodukte, Aufbereitungseinheit für Medizinprodukte</i>
BCM	<i>Business Continuity Management</i>
BCMS	<i>Business Continuity Management System</i>
BGM	<i>betriebliche Gesundheitsmanagement</i>
BIA	<i>Business Impact Analyse</i>
BT	<i>Bauteil</i>
CBRN	<i>Chemisch, Biologisch, Radioaktiv, Nuklear</i>
CERBERUS	<i>Cross Sectoral Risk Management for Object Protection of Critical Infrastructures</i>
CPS	<i>Cyber-physische Systeme</i>
EDV	<i>Elektronische Datenverarbeitung</i>
EG	<i>Europäische Gemeinschaft</i>
EMRAM	<i>Electronic Medical Record Adoption Model</i>
EU	<i>Europäische Union</i>
HIMSS	<i>Healthcare Information an Management Systems Society</i>
ISMS	<i>IT-Sicherheitsmanagementsystem</i>
ISO	<i>International Organization for Standardization</i>
IT	<i>Informationstechnologie</i>
KIS	<i>Krankenhausinformationssystem</i>
LIS	<i>Laboratory Information System</i>
MANV	<i>Massenanfall von Verletzten</i>
MBCO	<i>o Minimum Business Continuity Objective</i>
MP	<i>Medizinprodukt</i>
MTPD	<i>Maximum Tolerable Period of Disruption</i>
ONR	<i>ON-Regel (österreichisches Pendant zu ISO)</i>
OP	<i>Operation</i>
PACS	<i>Picture Archiving and Communication System</i>
PDCA	<i>Plan-Do-Check-Act</i>
QM	<i>Qualitätsmanagement</i>
RDG	<i>Reinigungs & Desinfektionsgeräte</i>
RIS	<i>Radiologie Information System</i>
RPO	<i>Recovery Point Objective</i>
RTO	<i>Recovery Time Objective, Recovery Time Objective</i>
SAURON	<i>Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports</i>
SD	<i>Shutdown</i>
SVG	<i>Scalable Vector Graphics</i>
WLAN	<i>Wireless Local Aera Network</i>

1 Domino-Effekte und Resilienz Förderung in kritischen Infrastrukturen

In der modernen vernetzten Gesellschaft sind viele System miteinander verbunden und stehen in Abhängigkeit. Wichtige gesellschaftliche Systeme zum Wohlergehen der Bevölkerung, werden durch kritische Infrastrukturen abgedeckt (vgl. EU 2008: L 345/77). Werden kritische Infrastrukturen beeinträchtigt, führt dies unmissverständlich zu Einschränkungen der Lebensgrundlage der Bevölkerung (vgl. BABS 2018: 5). Auch kritische Infrastrukturen sind den Risiken aus Naturkatastrophen, technischem Gebrechen, menschlichem Fehlverhalten, intentionalen Gefahren (u.a. Terror, Amoklauf, Geiselnahmen) und Cyberkriminalität ausgesetzt (vgl. BBK 2011: 5). Dadurch steigt die Wichtigkeit des Schutzes kritischer Infrastrukturen (vgl. BKA und BM.I 2014: 4). In diesem Kontext dürfen die Abhängigkeiten zwischen den kritischen Infrastrukturen nicht vernachlässigt werden.

Krankenhäuser müssen die medizinische Grundversorgung sicherstellen und gehören somit zu den kritischen Infrastrukturen. Das Krankenhaus betreibt innerhalb der Infrastruktur unterschiedliche Prozesse zur Patientenversorgung. Management-, Kern- und unterstützende Prozesse sind eng verzahnt und abhängig voneinander, damit die medizinische Grundversorgung gewährleistet werden kann (siehe Abbildung 43). Diese Vernetzung zwischen den Prozessen zur Patientenversorgung innerhalb einer Infrastruktur kann ähnlich betrachtet werden wie die Vernetzung auf der Ebene der kritischen Infrastrukturen.

Gemäß Abbildung 15 ist der Sektor Gesundheitsversorgung in vier Ebenen aufgeteilt. Der Sektor „Gesundheitsversorgung“ besteht u.a. aus den Akteuren Rettungsdienst, Labore, Apotheken, niedergelassenen Ärzte und Krankenhaus. Im Akteur „Krankenhaus“ werden u.a. die Prozesse Notaufnahme, Technik, Verwaltung, Pflegestationen, Küche, Labor und Aufbereitungseinheit für Medizinprodukte betrieben. Die Prozessebene „Notaufnahme“ setzt sich aus unterschiedlichen Komponenten (Ressourcen) zusammen. Dazu gehören u.a. das Fachpersonal, die medizintechnischen Geräte, die Daten und Unterlagen in der Patientenversorgung. Eine Vielzahl von Gefahren wirken auf diese Prozesse ein. Entsteht aus Gefahren ein reales Ereignis, können daraus massive Auswirkungen auf die Gesundheitsversorgung erfolgen. Sobald jedoch mehrere Akteure, Prozesse sowie Ressourcen betroffen sind, besteht die Gefahr von Kaskadeneffekten da einzelne Systeme sich beeinflussen können. (vgl. BARTELS M. et al. 2014: 217)

1.1 Gefährdungen

Dass Krankenhäuser nicht gefeit sind gegen Naturgefahren, technische Defekte oder intentionale Gefahren, das zeigen die unterschiedlichsten Pressemitteilungen, wie z.B. bei einer(m)

- Überschwemmung:
 - St. Antonius Hospital in Eschweiler: 1. Und 2. UG komplett überflutet, totaler Stromausfall, Evakuierung von 17 Intensivpatienten mit

Hubschraubern, Evakuierung von 278 Patienten mit Krankentransportwagen nachdem das Wasser abgezogen war, ca. 50 Mio. € Schaden (vgl. WAGENBACH E. 2021)

- Brand:
 - Bundeswehr Krankenhaus in Hamburg: OP-Trakt vorübergehend unbenutzbar, Ursache in Pressemitteilung unbekannt (vgl. REDAKTION-MOPO 2020)
 - Bad Segeberger Klinik: 85 Menschen evakuiert, Brandursache war ein Kaffeeautomat (vgl. GAERTNER R. 2020)
 - Marienhospital in Düsseldorf: 19 Verletzte, 100 Betroffene, 1 Toter, Ursache in Pressemitteilung unbekannt (vgl. SCHUSTER C. 2019)
- Stromausfall:
 - Krankenhaus der Barmherzigen Brüder in Trier: Ausfall der Sicherheits-Stromversorgung (SV), dadurch konnte das Notstromaggregat nicht automatisiert zugeschaltet werden, keine Patientenschäden, Ursache war ein technischer Defekt in der SV-Stromversorgung (vgl. BRÜDERKRANKENHAUS 2017)
 - Krankenhaus in Apenrade: 15 minütiger großflächiger Stromausfall in Nordschleswig, Krankenhaus Notstromversorgung konnte den Ausfall kompensieren, keine Patientenschäden waren zu beklagen (vgl. PETERS J. 2020)
- Fernwärmeausfall:
 - Kraftwerksbrand in Nürnberg im Februar führte zu einem stark reduzierten Wärmeproduktion, ca. 15.000 Menschen beeinträchtigt, darunter auch die SANA Klinik betroffen ohne größere Konsequenzen, die Sicherung der Fernwärmeversorgung mit mobilen Wärmeversorgungen dauerte mehrere Tage (vgl. SZ 2021)
- Cyberangriff:
 - Universitätsklinikum Düsseldorf: 13 Tage Abmeldung von Notfallversorgung, Verschiebung von planbaren und ambulanten Behandlungen, telefonisch und elektronisch nur eingeschränkt erreichbar, nach einem Monat konnte der Normalbetrieb wieder aufgenommen werden (vgl. UKD 2020a); (vgl. UKD 2020b)
 - Universitätsklinik Brno (CZE): nahezu kompletter Krankenhausbetrieb lahmgelegt, Absage von Operationen, Wochen bis der normale Betrieb wieder gewährleistet werden konnte, alle Rechner wurden abgeschaltet, Patientenversorgung ohne EDV-Einsatz, Transfer von akuten Kranken (vgl. T3N 2020)
 - Krankenhaus in Dax (F): vier Monate nach dem Angriff funktionieren immer noch nicht alle IT-Systeme, mindestens 30.000 händisch geschriebenen Patientenakten müssen nachträglich digitalisiert werden (BOURDY L. 2021)

1.2 **Problemstellung**

Die unterschiedlichen Prozesse innerhalb eines Krankenhauses sind sehr stark voneinander abhängig. Wird z.B. eine schwerverletzte Person ins Krankenhaus eingeliefert, wird in der zentralen Notaufnahme der Schockraum mit der entsprechenden Gerätschaft genutzt. Die Gerätschaft können mobile medizintechnische Untersuchungsgeräte sein, aber auch sterile wiederverwendbare Instrumente. Zur Beurteilung der Verletzungen werden unterschiedliche Prozesse benötigt. Unter anderem müssen im Labor unterschiedliche Proben ausgewertet werden und von der bildgebende Abteilung müssen kommentierte Röntgenbilder geliefert werden. Die Notfallmediziner bekommen alle Daten elektronisch über das Krankenhausinformationssystem zur Verfügung gestellt und können eine Diagnose stellen sowie die weitere Therapie festlegen. Muss die Person operiert werden, richtet ein OP-Team einen OP-Saal her. In diesem werden sterile wiederverwendbare Instrumente (Medizinprodukte) benötigt. Nach der OP wird die Person hospitalisiert und die notwendige weiterführenden Therapie sowie Behandlung werden durchgeführt. In jedem dieser Kontexte werden wiederverwendbare sterile Instrumente eingesetzt.

Dieses vereinfachte Beispiel stellt die Vernetzung und Abhängigkeiten der unterschiedlichen Prozesse dar. Fällt ein Prozess innerhalb dieser Kette aus, muss das Krankenhaus trotzdem die Patientenversorgung, gemäß Grundauftrag, durchführen können. Entsprechend müssen die kritischen Prozesse im Krankenhaus identifiziert werden und es müssen Schutzmaßnahmen ergriffen werden, damit die Wahrscheinlichkeit eines Prozessausfalles maximal reduziert wird und die Auswirkungen auf die Patientenversorgung unwesentlich (managebar) werden.

Eine zentrale, unverzichtbare Dienstleistung ist die Versorgung der Pflegestationen, der verschiedenen Ambulanzen, der zentrale Notaufnahme sowie der OP-Bereiche mit wiederverwendbaren sterilen Medizinprodukten. Die zentrale Aufbereitungseinheit für Medizinprodukte bezieht in diesem Prozess eine wesentliche Rolle und bereitet wiederverwendbare Medizinprodukte zur sterilen Benutzung auf.

Ein Ausfall dieser zentralen Leistungseinheit in Verbindung mit den komplexen Behandlungsabläufen im Operationsbereich stellen für das Krankenhaus ein enormes Schadenspotential dar (vgl. MEILINGER S. 2012). Die kritische Infrastruktur „Krankenhaus“ als sensibles und sehr komplexes System ist anfällig für jegliche Art von Störungen und Risiken.

Entsprechend können Prozess-Ausfälle innerhalb einer kritischen Infrastruktur einen Domino-Effekt verursachen, der sich über die Grenzen der Infrastruktur in den Interdependenzen der kritischen Infrastrukturen weiter entwickelt. Diese möglichen Auswirkungen müssen weitestgehend verhindert werden, indem die Prozesse und Infrastrukturen resilienter werden.

Gemäß den Anforderungen eines Risiko- und Kontinuitätsmanagement müssen die zentralen Aufgaben der Patientenversorgung in „Normalen Zeiten“ wie auch in „Krisenzeiten“ von einer Krankenhauseinrichtung erbracht werden. (vgl. SPÖRRER S. 2014)

1.3 Zielsetzung der Arbeit

Damit Organisationen resilienter werden und Auswirkungen von möglichen Gefährdungen reduziert werden können, müssen die Organisationen die Risiken kennen sowie die Betriebskontinuität wesentlicher Prozesse gewährleisten. Zur Gewährung der Betriebskontinuität ist es von Bedeutung den Impact von möglichen Auswirkungen auf die wesentlichen Prozesse zu kennen. In einem komplex vernetzten Krankenhaus kann durch die Implementierung vom Risiko- und Business Continuity Management, möglichen Risiken präventiv entgegen gewirkt und die Betriebskontinuität vorangetrieben werden.

Ziel dieser Arbeit ist es den CERBERUS Forschungsansatz und dessen Systemarchitektur (siehe Abbildung 4) zur Identifikation und Analyse von kritischen Prozessen sowie kritischen Ressourcen innerhalb eines Krankenhauses an einem Fallbeispiel anzuwenden. Mit diesem Ansatz können auch Abhängigkeiten und Kaskadeneffekte berücksichtigt werden.

Die Aufbereitungseinheit für Medizinprodukte (AEMP) wurde in diesem konkreten Fall als zu untersuchendes Fallbeispiel in einem fiktiven Krankenhaus ausgewählt. Wie vorher beschrieben, ist die Aufbereitungseinheit für Medizinprodukte eine zentrale Einheit und ein wesentlicher Prozess innerhalb eines Krankenhauses. Zur praktischen Anwendung werden die gewonnenen realistische Daten von einer bestehenden Infrastruktur benutzt. Auch wird die Datensammlung in realen Interviews, Befragungen und Workshops durchgeführt. Alle erhaltenen Informationen wurden anonymisiert.

Die vorliegende Arbeit betrachtet zum einen die Datensammlung, Identifikation der kritischen Prozesse und Ressourcen, zum anderen die softwarebasierte Auswertungen der statischen und der dynamischen Risikoanalyse. Die Betrachtung und Analyse wird an einem Fallbeispiel auf Praxistauglichkeit geprüft.

Im folgenden Schritt des Risikomanagementprozesses steht die Risikobewältigung. Die Ergebnisse aus der ganzheitlichen Risikobeurteilung müssen anschließend in Bewältigungsstrategien umgelegt werden. Die Erstellung dieser ist nicht Bestandteil dieser Arbeit.

Mit Abschluss der Arbeit sollte ein hybrides Modell für die Betrachtung der Kaskadeneffekte in Bezug auf das Risikomanagement innerhalb einer kritischen Infrastruktur zur Verfügung stehen und analysiert werden können. Mit diesem Modell sollten die statischen Abhängigkeiten bewertet und auch die dynamischen Kaskadeneffekte simuliert werden können.

1.4 Hypothesen und Forschungsfragen

1.4.1 Hypothese 1

Die Funktionsfähigkeit der zentralen Aufbereitungseinheit für Medizinprodukte ist stark abhängig von der fehlerfreien Funktion wesentlicher Prozesse und deren Ressourcen.

1.4.2 Unterforschungsfrage 1

Welche kritischen Prozesse betreffend die Aufbereitung von Medizinprodukten werden identifiziert?

1.4.3 Unterforschungsfrage 2

Welche kritischen Ressourcen auf der digitalen (cyber), der physischen sowie der personenbezogenen Ebene werden zum Betreiben der kritischen Prozesse benötigt?

1.4.4 Hypothese 2

Fällt eine kritische Ressource im Zusammenhang mit der Aufbereitungseinheit für Medizinprodukte aus, wirken sich die resultierenden kaskadenartigen Konsequenzen auf die kritischen Prozesse der Aufbereitungseinheit für Medizinprodukte aus.

1.4.5 Unterforschungsfrage 3

Welche Abhängigkeiten bestehen zwischen den identifizierten kritischen Prozessen und Ressourcen?

1.4.6 Unterforschungsfrage 4

Wie können die Abhängigkeiten zwischen den kritischen Prozessen und Ressourcen analysiert werden um die Kaskadeneffekte darzustellen?

Die vorliegende Arbeit wurde in drei Bereiche eingeteilt.

Bereich 1 mit der Beschreibung der Domino-Effekten und der Resilienz Förderung in kritischen Infrastrukturen als Einleitung in Kapitel 1, den Begriffsbestimmungen in Kapitel 2 und der Methodik in Kapitel 3.

Bereich 2 beinhaltet den theoretischen Teil zu den kritischen Infrastrukturen in Kapitel 4, der Digitalisierung und den Cyber-Physische Systeme in Kapitel 5, den Verwundbarkeiten und deren Auswirkungen in Kapitel 6 sowie das Risikomanagement und Business Continuity Management in Kapitel 7.

Im Bereich 3 wird die Fallstudie der Aufbereitungseinheit für Medizinprodukte in Kapitel 8 beschrieben mit anschließender Diskussion der Ergebnisse im Kapitel 9, der Zusammenfassung in Kapitel 10 und einer Perspektive / Ausblick in Kapitel 11.

2 Begriffsdefinitionen

Die nachfolgend definierten Begriffe stehen im Zusammenhang mit den kritischen Infrastrukturen, dem Risikomanagement, dem Business Continuity Management, den Kaskadeneffekten sowie den cyber-physischen Systemen. Zur Verdeutlichung der eingesetzten Begriffe in dieser Arbeit wurde auf unterschiedliche Quellen zurückgegriffen.

Abhängigkeit: „Eine Verknüpfung oder Verbindung zwischen zwei Infrastrukturen, durch die der Zustand der einen Infrastruktur den Zustand der anderen beeinflusst oder mit ihr korreliert ist“ (RINALDI S. M. et al. 2001: 13).

Business Continuity Management: „Business Continuity: Die Fähigkeit eines Unternehmens, nach einem störenden Zwischenfall auf vorher festgelegter akzeptabler Stufe weiterhin Produkte oder Dienstleistungen auszuliefern beziehungsweise anzubieten. Hier steht nicht die Wiederherstellung der EDV-Dienste im Vordergrund, sondern die ganzheitliche Wiederherstellung der Geschäftsabläufe in Unternehmen“ (SPÖRRER S. 2014: 132).

Business Impact Analyse: „Die Business Impact Analyse kann am besten als ein Prozess beschrieben werden, der Geschäftsprozesse untersucht, kritische Prozesse identifiziert, eine Bestandsaufnahme aller internen oder externen Abhängigkeiten vornimmt, die Anforderungen der Stakeholder auflistet und Bereiche mit hohem Risiko identifiziert, indem Techniken der Datenerfassung und Datenanalyse eingesetzt werden, um die wahrscheinlichen Auswirkungen von natürlichen oder vom Menschen verursachten negativen Ereignissen auf den reibungslosen Ablauf des Unternehmens zu untersuchen.“ (PRITI S. 2017: 21)

Cyber-physische Systeme: „Der Begriff cyber-physische Systeme bezieht sich auf eine neue Generation von Systemen mit integrierten rechnerischen und physikalischen Fähigkeiten, die über viele neue Modalitäten mit dem Menschen interagieren können“ (Baheti R. und Gill H. 2011: 1).

„Cyber-physische Systeme (CPS) beschreiben Hardware-Software-Systeme, die die physische Welt und die virtuelle Welt eng miteinander koppeln. Sie entstehen aus vernetzten eingebetteten Systemen, die über Sensoren und Aktoren mit der Außenwelt verbunden sind und die Fähigkeit haben, zusammenzuarbeiten, sich anzupassen und weiterzuentwickeln“ (MEIKE R. et al. 2017: 9).

Zukünftig werden Alltagsgegenstände (z. B. Häuser, Büros, Autos, Städte und Kleidung) mehr und mehr intelligent, hierzu werden cyber-physische Systeme eingesetzt. Außerdem können cyber-physische Systeme eine Vielzahl von Bereichen vereinen und so finden sie unter anderem in hochrelevanten Bereichen der Gesellschaft wie in der intelligente Fertigung, der intelligente Energieversorgung, der intelligenter Mobilität, der intelligente Stadt und dem intelligenten Gesundheitswesen Anwendung. In diesem

Zusammenhang sind auch viele kritische Infrastrukturen betroffen. (vgl. MEIKE R. et al. 2017: 11; 28)

Digitalisierung: „Das digitale Krankenhaus erbringt ärztliche und pflegerische Leistungen mithilfe von digital unterstützten Prozessen und ist gekennzeichnet durch: [...] eine umfassende, bedarfsorientierte Unterstützung durch (IT)- technische Services; Unterstützung einer durchgängigen Dokumentation, Kommunikation sowie Logistik (Waren, Daten und Wissen) im Sinne aller Akteure eines Krankenhauses“ (BURMANN A. et al. 2019: 6).

Gefahr: „Zustand, Umstand oder Vorgang, durch dessen Einwirkung ein Schaden an einem Schutzgut entstehen kann“ (BBK 2021a);

Gefährdung: „Möglichkeit, dass an einem konkreten Ort aus einer Gefahr ein Ereignis mit einer bestimmten Intensität erwächst, das Schaden an einem Schutzgut verursachen kann.

Anmerkung: Die Definition erfolgt im Kontext der Risikoanalyse/Gefährdungsanalyse“ (BBK 2021b);

Interdependenz: „Eine bidirektionale Beziehung zwischen zwei Infrastrukturen, bei der der Zustand der einen Infrastruktur den Zustand der anderen beeinflusst oder mit ihr korreliert ist. Allgemeiner ausgedrückt, zwei Infrastrukturen sind interdependent, wenn jede von der anderen abhängig ist“ (RINALDI S. M. et al. 2001: 14).

Kaskadeneffekte: „Kaskadeneffekte sind die Dynamik bei Katastrophen, bei denen die Auswirkung eines physischen Ereignisses oder die Entwicklung eines anfänglichen technologischen oder menschlichen Versagens eine Folge von Ereignissen in menschlichen Subsystemen erzeugt, die zu physischen, sozialen oder wirtschaftlichen Störungen führen. Auf diese Weise kann eine anfängliche Auswirkung andere Phänomene auslösen, die zu Folgen mit erheblichen Größenordnungen führen. Kaskadeneffekte sind komplex und mehrdimensional und entwickeln sich im Laufe der Zeit ständig weiter. Sie sind eher mit dem Ausmaß der Verwundbarkeit als mit dem der Gefährdung verbunden. Niedrigschwellige Gefahren können weitreichende Kaskadeneffekte erzeugen, wenn Schwachstellen im System weit verbreitet sind oder in Teilsystemen nicht angemessen behandelt werden. Aus diesen Gründen ist es möglich, die Elemente der Kette zu isolieren und sie als eigenständige (Subsystem-)Katastrophen zu betrachten. Insbesondere können Kaskadeneffekte mit den sekundären oder immateriellen Auswirkungen von Katastrophen interagieren“ (PESCAROLI G. und ALEXANDER D. 2015).

Kritikalität: „Einen wichtigen Teil der BIA stellen Erhebungen, Einschätzungen und Bewertungen im Rahmen der Kritikalitätsanalyse dar. Das Wort kritisch meint zunächst zeitkritisch. Dazu gibt man sich zunächst eine Zeitachse vor bzw. teilt die Zeit in Perioden ein. Nun wird in einem Ausfallszenario der Schaden für die Organisation in aller Regel mit der Dauer des Ausfalls steigen, das

heißt je länger der Ausfall bestehen bleibt, desto höher ist der Schaden. Ähnlich wie bei den Risiken teilt man die möglichen Schadenshöhen in Klassen ein und spricht von Kausalitätsklassen oder – stufen (siehe auch Wiederanlaufklasse). Bei einem Ausfall werden also Geschäftsprozesse mit fortschreitender Zeit eine immer höhere Kritikalitätsstufe erhalten, solange bis der Ausfall behoben ist“ (SPÖRRER S. 2014: 135).

Kritische Infrastruktur: Die Europäische Kommission hat in der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, die „kritische Infrastruktur“ folgendermaßen definiert:

„**kritische Infrastruktur**‘ die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten“ (EU 2008: L 345/77).

Am 16. Dezember 2020 hat die Europäische Kommission einen Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen veröffentlicht. In diesem Vorschlag wird die Definition der „kritische Infrastruktur“ durch drei zusammenhängende Definition ersetzt:

„**kritische Einrichtung**‘: eine öffentliche oder private Einrichtung einer im Anhang genannten Art, die ein Mitgliedstaat in Anwendung des Artikels 5 als solche eingestuft hat;

„**Infrastruktur**‘ ein Objekt, ein System oder einen Teil davon, das bzw. der für die Erbringung eines wesentlichen Dienstes erforderlich ist;

„**wesentlicher Dienst**‘ einen Dienst, der für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten wesentlich ist“ (EU 2020b: 26).

Markov-Ketten: „Markov-Ketten sind zeitdiskrete stochastische Prozesse mit abzählbarem (d.h. endlichem oder abzählbar unendlichem) Zustandsraum. Sie zeichnen sich durch ihre ‚Gedächtnislosigkeit‘ aus. Diese zentrale Eigenschaft (Markov-Eigenschaft) besagt, dass die zukünftige Entwicklung des Prozesses nur von dem zuletzt beobachteten Zustand abhängt und von der sonstigen Vorgeschichte unabhängig ist“ (WALDMANN K.-H. und HELM W. E. 2016a: 219).

Maximum Acceptable Outage (MAO) or Maximum Tolerable Period of Disruption (MTPoD or MTPD): “Time it would take for adverse impacts, which might

arise as a result of not providing a product/service or performing an activity, to become unacceptable” (ISO/TS 2015: 17).

Notbetriebsniveau: „Das Notbetriebsniveau definiert, wie leistungsfähig der Notbetrieb sein soll, um einen sinnvollen Geschäftsbetrieb gewährleisten zu können. Das Notbetriebsniveau wird je Geschäftsprozess individuell festgelegt“ (BSI 2021: 194).

Outsourcing: „Vereinbarung mit einer externen Organisation zur vollständigen Abgabe von Funktionen und Prozessen“ (SPÖRRER S. 2014: 136).

Ransomware: „Bei Ransomware (auch «Erpressungstrojaner» oder «Verschlüsselungstrojaner» genannt) handelt es sich um eine bestimmte Familie von Schadsoftware (sogenannte «Malware»; Kofferwort aus «malicious» und «Software»). Diese verbreitet sich üblicherweise über schädliche E-Mail-Anhänge oder gehackte Webseiten. Einmal infiziert, verschlüsselt Ransomware Dateien auf dem Computer des Opfers sowie auf allfällig verbundenen Netzlaufwerken und Speichermedien (beispielsweise USB-Sticks). Die verschlüsselten Dateien werden dadurch für das Opfer unbrauchbar. Wurden die Dateien auf dem Computer erst einmal durch die Ransomware verschlüsselt, zeigt diese dem Opfer einen «Sperrbildschirm» an. Dieser fordert das Opfer auf, einen bestimmten Geldbetrag in Form einer anonymen Internetwährung (beispielsweise Bitcoins) an die Angreifer zu bezahlen (Erpressung), damit diese die verschlüsselten Dateien wieder freigeben und somit wiederverwendet werden können“ (PORTMANN A. und HIRSCHI O. 2017: 459-460).

Risiko: In der ONR 49000 wird das Risiko folgendermaßen definiert:

„Der Begriff Risiko umfasst folgende Gesichtspunkte:

- die Auswirkungen können positiv oder negativ sein,
- die Unsicherheit bzw. Ungewissheit wird mit Wahrscheinlichkeiten geschätzt bzw. ermittelt,
- die Ziele der Organisation oder des Systems umfassen strategische, operationelle oder finanzielle Ziele, die Sicherheit von Menschen, Sachen und der Umwelt („safety, security“) genauso wie andere Ziele und
- Risiko ist eine Folge von Ereignissen oder von Entwicklungen“ (AUSTRIAN-STANDARDS 2008a).

Auf Basis der Abbildung 1 beschreiben GLADE T. et al. (2005: 1-2) das Risiko bestehend aus zwei Komponenten:

- der Wahrscheinlichkeit, dass etwas Unerwünschtes eintritt und
- die daraus entstehenden Konsequenzen.

Die Schnittmenge zwischen Gefahr und Verletzlichkeit definieren die Höhe des Risikos, wobei die Risikoelemente entsprechend berücksichtigt werden müssen.

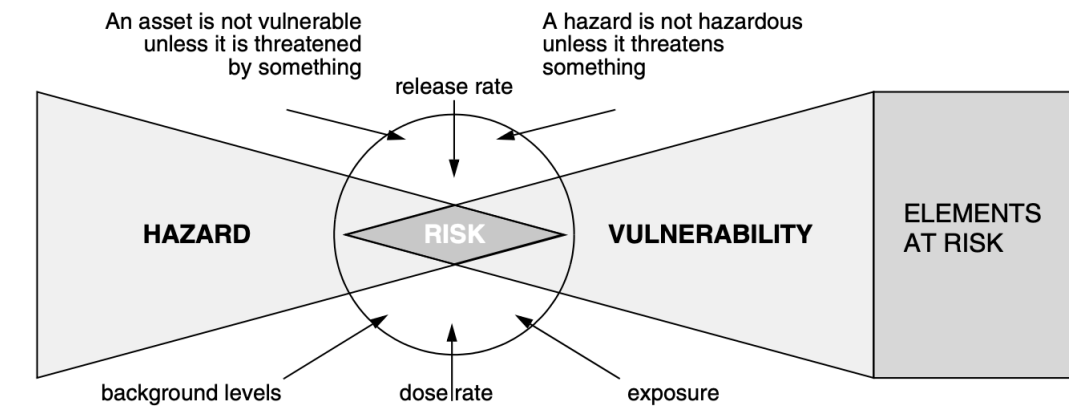


Abbildung 1: Beziehung zwischen Gefahr, Vulnerabilität, Risiko und angehörigen Konzepten (Quelle: ALEXANDER D. E. 2002: 29)

Risiko = f (Gefahr, Risikoelemente, Vulnerabilität)

„Risikoelemente: alle geschätzten Attribute, die durch die Gefahr bedroht sind; können Strukturen, Land, Ressourcen, soziale und physische Infrastruktur, produktive und nicht-produktive Aktivitäten, Umweltqualitäten, Leben und physisches und psychisches Wohlbefinden umfassen. Einige dieser Attribute sind quantifizierbar, einige können in wirtschaftlichen Begriffen ausgedrückt werden und andere entziehen sich einer einfachen Quantifizierung“ (GLADE T. et al. 2005: 33).

Recovery Time Objective (RTO): “Target time following an incident for: Product or service delivery resumption, or Activity resumption, or Resources recovery
NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable” (ISO/TS 2015: 17).

Recovery Point Objective (RPO) or Maximum Data Loss (MDL): “Point to which information used by an activity must be restored to enable the activity to operate on resumption” (ISO/TS 2015: 17).

Risikomanagement: „Der Risikomanagement-Prozess ist die systematische Anwendung von Grundsätzen, Verfahren und Tätigkeiten einer Organisation, um über Risiken zu kommunizieren, Informationen auszutauschen, Zusammenhänge zu erstellen, Risiken zu identifizieren, zu analysieren, zu bewerten, zu bewältigen sowie Risiken aufzuzeigen, zu verfolgen und zu überwachen“ (AUSTRIAN-STANDARDS 2008a).

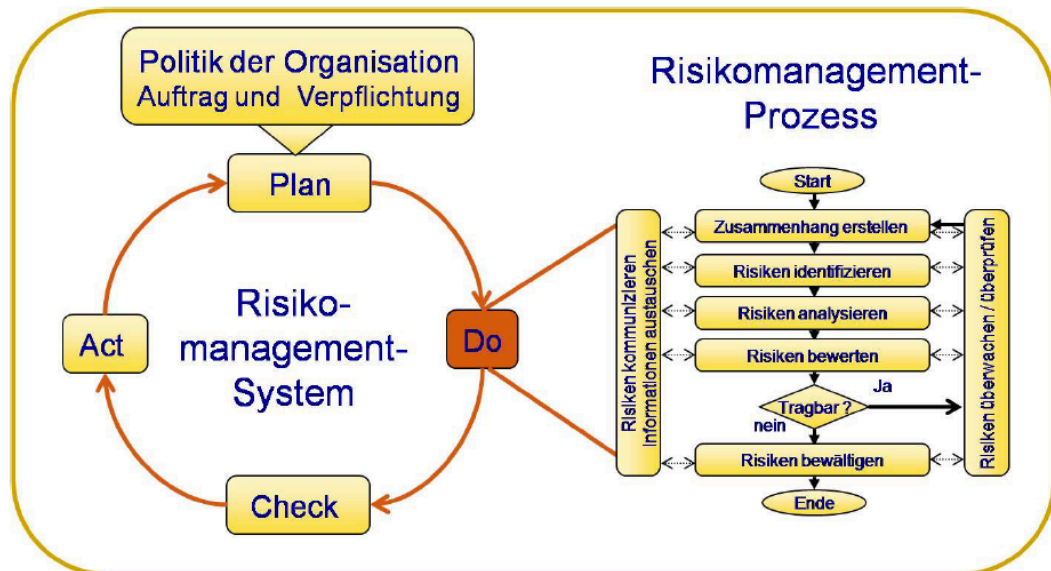


Abbildung 2: Risikomanagement-Prozess aus ONR 49000:2008 (Quelle: AUSTRIAN-STANDARDS 2008a: 17)

Resilienz: „Unternehmerische Resilienz ist die Eigenschaft eines Unternehmens, externe Schocks oder Verwerfungen der sozialen, wirtschaftlichen oder politischen Rahmenbedingungen auszuhalten und sich an die neuen Bedingungen anzupassen“ (GÜNTHER E. 2018).

Service Level Agreement (SLA): „Eine Dienstleistungs- oder Dienstgütevereinbarung, meist in verschiedene Stufen angeboten, welche zugesicherte Leistungseigenschaften beschreibt“ (SPÖRRER S. 2014: 137).

Simulation: „Die Simulation ist eine Technik, die den zeitlichen Ablauf in einem realen System imitiert, um so zu Erkenntnissen über interessierende Größen zu gelangen“ (WALDMANN K.-H. und HELM W. E. 2016a: 4).

stochastischen Prozess: „Folge von Zufallsvariablen $(X(t))_t$, die mit einem (z.B. zeitlichen) Index t aus einer Indexmenge (z.B. natürliche Zahlen oder $(0, \infty)$) versehen sind. Je nachdem, ob für jedes reelle t oder nur für einzelne, etwa ganzzahlige t eine Betrachtung erfolgt, unterscheidet man stochastische Prozesse mit stetiger oder diskreter Indexmenge (z.B. Zeit). Anhand der Verknüpfung zwischen den Verteilungen der Zufallsvariablen zu den verschiedenen Zeitpunkten bzw. den Abhängigkeiten zwischen Zufallsvariablen mit verschiedenen Indizes (z.B. Zeiten) werden verschiedene Typen von stochastischen Prozessen unterschieden“ (KAMPS U. 2018).

Vulnerabilität (auch: Verwundbarkeit oder Verletzlichkeit): „Maß für die anzunehmende Schadensanfälligkeit eines Schutzgutes in Bezug auf ein bestimmtes Ereignis.

Anmerkung: Die Definition erfolgt im Kontext der Risikoanalyse“ (BBK 2021c).

3 Methodik

3.1 Literatur Recherche

3.1.1 Suchsysteme

Bei der Literaturrecherche wurde auf fünf verschiedene Suchsysteme zurückgegriffen.

1. Schneeballsystem

Beim Schneeballsystem (vgl. LANGER C. o.J.: 34) wird von einem vorgegebenen Text ausgegangen und anhand der Literaturliste werden weitere Quellen ausfindig gemacht. Diese Vorgehensweise wird bei jedem neuen Text angewendet. Neue Quellen können so schnell identifiziert werden. Dadurch wächst die Anzahl der gefundenen Literatur. Allerdings gilt zu beachten, dass hier das Risiko besteht, immer wieder auf die gleichen Texte zu stoßen, entsprechend riskiert man einem Zitierkartell zu verfallen. Nicht zitierte Texte werden entsprechend nicht gefunden und es besteht die Gefahr einer lückenhaften Literaturauswahl. Mit dieser Methode kann fast nur auf ältere Literatur zurückgegriffen werden.

2. Systematische Suche

Auf einschlägigen Online-Portalen, Fachzeitschriften, Literaturdatenbanken oder spezifischen Web-Seiten wird systematisch nach Themen recherchiert. Dadurch kann relevante Literatur gefunden werden. Die Methode ist aufwendig, man verschafft sich einen breiten Überblick und erhält fachspezifische Literatur. Dadurch kann man einem Zitierkartell umgehen. (vgl. LANGER C. o.J.: 34)

3. Vorwärts gerichtete Suche

Ausgehend von einer Quelle, wird bei der vorwärts gerichteten Suche nach Autoren und Texten gesucht, die diese Quelle zitiert haben. Dieses System erlaubt es eine Suche nach vorne zu generieren, um so die aktuellen Titel zu finden. (vgl. LANGER C. o.J.: 35)

Für die vorwärts gerichtete Suche wurde auf das Web-Portal Google Scholar zurückgegriffen. (vgl. NORDHAUSEN T. und HIRT J. 2018: 226 ff.)

4. Handsuche

Diese Methode beruht auf der manuellen Suche nach relevanten Publikationen in Fachdatenbanken oder auf bekannten Webseiten. (vgl. NORDHAUSEN T. und HIRT J. 2018: 50)

5. Freie Websuche

Für die freie Websuche kann auf bekannte Suchmaschinen wie z.B. Google zurückgegriffen werden um im Internet nach weiteren Hinweisen, Quellen oder Dokumenten zu suchen. (vgl. NORDHAUSEN T. und HIRT J. 2018: 51)

3.1.2 Literaturauswahl

Mit der Anwendung dieser Such-Methoden konnten viele Quellen gefunden werden. Das Suchergebnis wurden anschließend nach relevanten und nicht relevanten Quellen getrennt. Die Quellen wurden gemäß folgendem Schema (vgl. LANGER C. o.J.: 36) ausgewählt:

1. Erscheinungsjahr – Filter gesetzt,
2. Titel, Untertitel – eventuell Suchtext verbessert und neue Suche ausgeführt,
3. Abstrakt – Recherche nach wesentlichen Informationen zum Thema,
4. Inhaltsverzeichnis – Suche nach Interessensschwerpunkten,
5. Grafiken und Tabellen – Suche nach relevanten Informationen,
6. Literaturverzeichnis – Suche nach zusätzlichen Quellen.

Für die Literaturrecherche wurde auf die Online-Angebote der Universitätsbibliothek Wien, der Nationalbibliothek in Luxemburg, dem Online Portal Research-Gate und auf Google Scholar zurückgegriffen. Wobei vor allem die Web-Portal Research-Gate und Google Scholar für die vorwärts gerichtete Recherche genutzt wurden. Es wurde auch auf Dokumente, Normen und Artikel aus der beruflichen Praxis, den Literaturangaben aus dem Studium und auf legislative Texte zurückgegriffen.

Vereinzelt wurde auf Bücher, Broschuren und Dokumente in Papierform zugegriffen.

Unter anderem, nachfolgende Schlagwörter wurden in den unterschiedlichen Datenbanken gesucht:

- Kritische Infrastruktur
- Critical infrastructure
- Cascading effects in critical infrastructure
- Resilienz
- Business Continuity Management
- Kaskadeneffekten
- Risikomanagement
- cascading disasters and cascading effects
- Expert*Innenbefragung Workshop
- Funktionsweise Markov-Ketten
- Digitalisierung Krankenhausinformationssysteme
- definition cascading effects
- definition cyber physical systems
- What is a Cyber-Physical System?
- Cyber-physical system in Smart Grids

- Cyber-physical system in Smart Mobility
- What is a Smart City
- Risikomanagement und Business Continuity Management in kritischen Infrastrukturen
- ...

3.1.3 Literaturverwaltung

LANGER C. (o.J.: 37) unterteilt die Literaturverwaltung in 4 verschiedene Punkte:

1. Literatur verwalten und auswerten

Die Verwaltung der Quellen wurden mit der Verwaltungssoftware EndNote X9 durchgeführt. Hier können die Quellen nach Gruppen und Untergruppen unterteilt archiviert werden. Die Annotation von Dokumenten kann direkt in dieser Software durchgeführt werden.

2. Ideen und Zitate notieren

Ausgewählte Zitate, Schlagwörter und Textpassage wurden nach den Quellen referenziert in einer Mindmap eingetragen. Dazu wurde die Software SimpleMind genutzt (

Abbildung 3; Anhang 14.14).

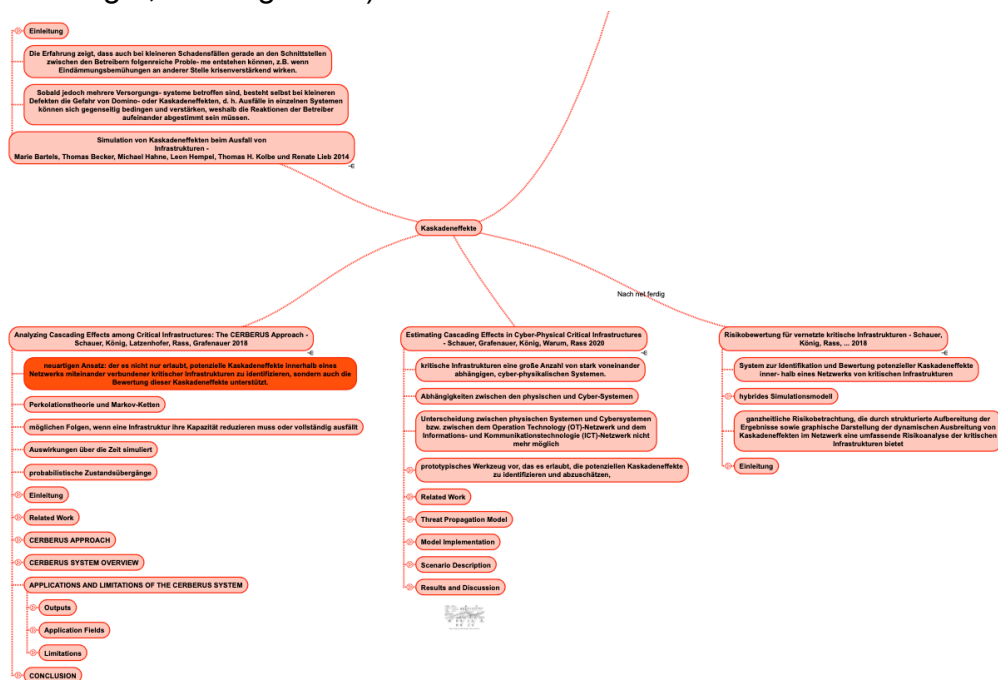


Abbildung 3: Auszug Mindmap zur Literaturrecherche am Bsp. der Kaskadeneffekte

Eine Mindmap eignet sich sehr gut für die Sammlung von zitierfähigen Textbausteinen. Aus den unterschiedlichen Quellen werden die einzelnen Textbausteine in die Mindmap übernommen, zu Gruppen zusammengefügt und gegeben falls untereinander verknüpft. Dadurch können Zusammenhänge dargestellt werden, es entsteht eine hierarchische Struktur und es können immer wieder Textbausteine hinzugefügt werden. (vgl. ANT M. 2018: 284-285)

3. Wissen organisieren und Texte strukturieren

Aus der Mindmap werden die zitierfähigen Textbausteine in das entsprechende Kapitel der Masterarbeit kopiert und daraus zusammenhängende strukturierte Texte geschrieben. Mittels einer Schnittstelle zwischen MS-Word und EndNote können die Textpassagen mit der entsprechenden Quelle zitiert werden.

4. Automatisches Erstellen und Formatieren des Literaturverzeichnisses

Anhand der Schnittstelle zwischen MS-Word und EndNote werden die zitierten Quellen automatisch in ein Literaturverzeichnis integriert. Die Formatierungen des Literaturverzeichnisses und der Zitierungen werden in EndNote gemäß dem „Zitierempfehlung des Institutes für Geographie und Regionalforschung der Universität Wien“ vorgenommen. (RUMPOLT P. A. und GLADE T. 2012)

3.2 Systemmodellierung

In der vorliegenden Arbeit wird die Anwendung des Systemmodells an einem fiktiven Krankenhaus durchgeführt. Das fiktive Krankenhaus basiert auf einer realen Organisation und auch die Informationserfassung wurde anhand von realen Daten und in realen Besprechungen gesammelt. Die Daten wurden zur Verwendung in der vorliegenden Arbeit anonymisiert.

Als Grundlage für die besonderen Betrachtungen der Kaskadeneffekte in Bezug auf das Risikomanagement in kritischen Infrastrukturen wird die CERBERUS Systemarchitektur angewendet.

Die Abkürzung „CERBERUS“ steht für „Cross Sectoral Risk Management for Object Protection of Critical Infrastructures“ und beschreibt eine strukturierte Aufbereitung von Objektschutzdaten von kritischen Infrastrukturen. Die gewonnenen Daten werden in einem Risikomodell zusammengeführt (Abbildung 4). In diesem Risikomodell werden Daten aus dynamischen Simulationen als auch statische Daten für die Analyse genutzt. Anhand dieser ganzheitlichen Sicht auf kritische Infrastrukturen können den Betreibern inhärente Abhängigkeiten dargestellt werden. Bei diesem Modellierungskonzept steht zwei Punkte im Vordergrund, zum einen müssen Abhängigkeiten erkannt werden und zum anderen die Zusammenhänge identifiziert werden. (vgl. BMLRT-FFG 2021)

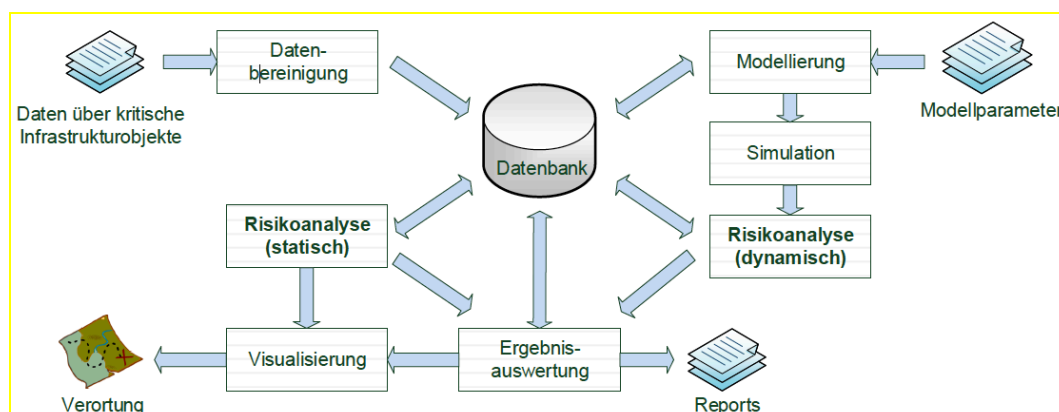


Abbildung 4: Schematische Darstellung der CERBERUS Systemarchitektur (Quelle: SCHAUER S. et al. 2018: 316)

Der CERBERUS Ansatz (vgl. SCHAUER S. et al. 2018) unterstützt die kritischen Infrastrukturen beim Risikomanagement, um Beeinträchtigungen oder einem

Totalausfall entgegenzuwirken. Der Ansatz kann sowohl im Netzwerk der kritischen Infrastrukturen auf Behördenebene eingesetzt werden als auch innerhalb einer kritischen Infrastruktur, um Zusammenhänge zwischen kritischen Prozessen und Ressourcen zu identifizieren. Dazu müssen interne Details zu diesen Prozessen und Ressourcen eingesetzt werden, dadurch ist der Ansatz stark datengetrieben und benötigt Expert*Innen aus den kritischen Infrastrukturen. Als Resultat liefert der Ansatz potenzielle Schwachstellen.

- **Datensammlung und Datenbereinigung**

Die Datensammlung zu den benötigten Prozessen in der Aufbereitungseinheit für Medizinprodukte (AEMP) erfolgt durch Befragung der einzelnen Abteilungsführungspersonen der betroffenen Abteilungen. Folgende Personen wurden befragt:

- Qualitätsbeauftragter der AEMP
- Abteilungsleiterin der AEMP
- Leiter Technische Abteilung
- Leiter IT-Abteilung
- IT-Prozessverantwortlicher der AEMP

Die Ergebnisse der Befragungen sind in eine eigens hierfür erstellte Excel-Datei eingeflossen. Nach dem Erhalt der Informationen zu kritischen Prozessen und Ressourcen wurde in Workshops eine Datenbereinigung durchgeführt. Im Kapitel 3.3 sind die einzelnen eingesetzten Werkzeuge zur Informationsbeschaffung beschrieben. Die Ergebnisse der Befragungen sowie der Datensammlung werden im Kapitel 8.1.4 beschrieben.

- **Modellparameter**

In den gleichen Workshops zur Datenbereinigung wurden die Modellparameter sowie die Abhängigkeiten zwischen den kritischen Prozessen und den benötigten Ressourcen festgelegt. Das Ergebnis wird in Kapitel 8.1.4 beschrieben.

- **Modellierung, Simulation und dynamische Risikoanalyse**

Die Modellierung, Simulation und dynamische Risikoanalyse der Abhängigkeitsmatrix von kritischen Prozessen und Ressourcen wird mittels der Software „SAURON Propagation Engine“ durchgeführt. Hierfür wird in der Software das Netzwerk mit allen Prozessen und Ressourcen sowie deren Abhängigkeiten parametrisiert. Für die Simulation werden die Abhängigkeiten in zufälliger Abfolge durchlaufen. Im Kapitel 3.6 wird der Einsatz der SAURON Propagation Engine beschrieben.

- **Statische Risikoanalyse**

Für die statische Risikoanalyse wird auf eine Business Impact Analyse zurückgegriffen (siehe hierzu Kapitel 3.4). Diese wird mit dem Software-Modul „bcIMPACT“ der Software „bcNAVIGATOR“ durchgeführt. Auch hier werden die

kritischen Prozessschritte und die Ressourcen sowie die Abhängigkeiten eingetragen. Die spezifischen Modellparameter für die statische Analyse werden für jeden Prozessschritt und für jeder Ressource eingetragen. Im Kapitel 3.5 wird die Verwendung der Software beschrieben. Im Kapitel 8.4 sind die einzelnen Schritte dargestellt.

- **Auswertung und Darstellung der Ergebnisse**

Die Ergebnisse können in den einzelnen Software Tools online visualisiert werden. Zusätzlich können die Ergebnisse in einem Bericht gespeichert und ausgedruckt werden. Dadurch, dass zwei unterschiedliche Ansätze genutzt werden, können die Ergebnisse für die statische Risikoanalyse getrennt von den Ergebnissen der dynamischen Risikoanalyse ausgewertet werden. Die beiden Analysen für das Fallbeispiel werden im Kapitel 8.6 ausgewertet.

Für die praktische Durchführung wird auf zwei unterschiedliche Softwares zurückgegriffen. Zum einen eine Business Impact Analyse Software für die statische Analyse und eine netzwerk-orientierte Analyse Software für die dynamische Analyse gemäß der CERBERUS-Systemarchitektur

3.3 Informationsbeschaffung

Für die analytische Arbeit und die Beschaffung von relevanten Fakten ist die Informationsbeschaffung eine wesentliche Grundlage und verhilft zu einer besseren Diagnose. (vgl. ANDLER N. 2015: 130)

Damit die Daten für das fiktive Krankenhaus auf Fakten basieren können, wurden die Daten von einem realen Krankenhaus übernommen und für die Verarbeitung des fiktiven Krankenhauses angepasst.

Durch den persönlichen Background als Elektrotechnik-Ingenieur und die persönliche Tätigkeit im Bereich der Arbeitssicherheit, des Brandschutzes und der Mitwirkung bei Infrastrukturprojekten kennt der Autor die Krankenhauslandschaft und deren technische Abläufe.

ANDLER N. (2015: 132-136) unterscheidet die Datenerfassung in 2 Kategorien. Die Primärdaten-Informationsbeschaffung zur Erhebung von neuen bisher noch nicht erfassten Daten kann unter anderem mit den Werkzeugen „Befragung“, „Gruppendiskussion“, „Workshops“, „Prozesskettenmodellierung“, „Interviews“ und „Fragebogen“ durchgeführt werden. Für die Sekundärquellen-Informationsbeschaffung kann auf interne oder externe Dokumente betreffend die Organisation zugegriffen werden. Dabei soll zwischen „notwendig“, „gut zu wissen“ und „unnötigem Wissen“ unterschieden werden und das Datenvolumen sollte auf das wesentliche reduziert werden. Die Art der Informationsbeschaffung kann zusätzlich in eine eigenständige und kollaborative Art unterschieden werden.

Für die ersten Informationsbeschaffungen wurden die Werkzeuge „Interview“ und „Schreibtisch-Forschung“ eingesetzt.

Das „Interview“ (vgl. ANDLER N. 2015: 144) eignet sich, um effizient Informationen im persönlichen Gespräch mit wenigen Einzelpersonen zu erhalten. Der Gesprächsführer

stellt mehrheitlich gezielte Fragen, um die benötigten Informationen zu erhalten. Hierfür kann er verschiedene Techniken anwenden. Im aktuellen Fall wurde beim ersten Interview ein freies Gespräch ohne jegliche Struktur mit der Verwendung offener Fragen und beim zweiten Interview ein freies Interview mit teil-direktiven Fragen eingesetzt.

Stehen unterschiedliche Wissensquellen wie Dokumente, Bibliotheken, Datenbanken, Bücher, Internet und andere zur Verfügung, ist die „Schreibtisch-Forschung“ (vgl. ANDLER N. 2015: 142-143) eine Lösung, um in einem persönlichen und unstrukturierten Ansatz die nötigen Informationen zu erhalten. Dies setzt voraus, dass auf die Wissensquellen zugegriffen werden kann.

Während der Erstellung des Exposés zur Masterthesis wurde, ein erstes „Interview“ (Okt. 2020) in einer freien Gesprächsform mit der Leiterin der AEMP, der QM-Beauftragten der AMEP und des Bereichsleiters der Pflegedirektion durchgeführt. Während diesem Gespräch wurden die Abläufe in der AEMP und erste Abhängigkeiten besprochen. Dem Autor wurden verschiedene interne Dokumente wie das QM-Handbuch, die Abteilungsbeschreibung und den Verweis auf die Internetseite der Deutschen Gesellschaft für Sterilgutversorgung e.V. übergeben.

Anschließend wurden in einer „Schreibtisch-Forschung“ die Dokumente gesichtet und ein erstes Prozessablaufdiagramm für das Exposé erstellt (siehe Abbildung 44). Ebenfalls wurde in einem unstrukturierten Ansatz auf Webseiten und in den Online-Bibliotheken nach erster Literatur gesucht. Die Ergebnisse der Recherche wurden zum Teil in das Exposé eingearbeitet.

Im Nachgang an die Einreichung des Exposé und der Anmeldung der Masterthesis wurde das Augenmerk der Informationsbeschaffung auf die Literaturrecherche, wie im Kapitel 3.1 beschrieben, gelegt. Die Ergebnisse der Literaturrecherche wurde, wie oben beschrieben, in eine Mindmap übertragen.

Für die nun folgende Informations- und Datenbeschaffung gab es keine Vorlage. Diese musste erst erstellt werden.

Die Vorgehensweise aus Abbildung 7 wurde für die Erstellung der Vorlagen verwendet. Ebenfalls wurde dieses Schema für die fortlaufende Orientierung der Informationsbeschaffung angewendete.

Ende Januar 2021 wurde mit der QM-Beauftragten der AEMP ein weiteres „Interview“ in einer freien Form durchgeführt, um ein besseres Verständnis über die AEMP zu erhalten und um den Prozess der Aufbereitung zu verstehen. Für die Gesprächsführung orientierte sich das Interview an den einzelnen Prozessschritten. Hierzu wurde im Vorfeld der gesamte Zyklus zur Aufbereitung von Medizinprodukten in die nachfolgenden einzelnen Schritte unterteilt:

- Benutzung (Kunde)
- Vorreinigung (Kunde)
- Demontage (Kunde)
- Transport (Logistik)

- Manuelle Vorreinigung (AEMP)
- Maschinelle Reinigung (AEMP)
- Desinfektion (AEMP)
- Prüfung (AEMP)
- Pflege (AEMP)
- Instandsetzung (AEMP)
- Verpackung (AEMP)
- Kennzeichnung (AEMP)
- Sterilisation (AEMP)
- Freigabe (AEMP)
- Transport (Logistik)
- Lagerung (Kunde)

Zuerst wurden die Schritte aufgeteilt in die Zugehörigkeit zur AEMP und zu den Kundenabteilungen (siehe obige Bezeichnungen in den Klammern).

Anschließend wurden für die einzelnen Prozessschritte der AEMP die nachfolgenden Themen in Frage gestellt:

- Personalstruktur
- Räumlichkeiten
- Spezifische technische Geräte und Einrichtungen
- Stromversorgung
- Druckluftversorgung
- VE-Wasser
- Zu- und Abluft
- Reindampfversorgung
- IT-Hardware
- IT-Software
- Sicherheitstechnik

Aus diesem Interview wurde eine erste Prozessbeschreibung und eine erste Business Impact Analyse Matrix (BIA-Matrix) in Form einer Abhängigkeitsmatrix erstellt (siehe Kapitel 8.2.2). Die fertige BIA-Matrix ist im Anhang 14.5, 14.6, 14.7 und 14.8 abgelegt.

Expert*Innenbefragungen (vgl. ANT M. 2018: 288) werden eingesetzt, um Daten und Informationen von besonders kundigen Fachleuten zu sammeln, um die eigene Analyse zu stärken und den Sachverhalt besser zu verstehen. Fachleute können so ihre Sachkenntnis aus der praktischen Erfahrung und aus dem täglichen Leben in die Analyse einbringen. Auch können sie die zukünftige Entwicklung sehr gut einschätzen.

Für die Expert*Innenbefragung muss der zu untersuchende Sachverhalt bestimmt und Fragen definiert werden.

Mit einem „Fragebogen“ (vgl. ANDLER N. 2015: 173-174) können quantitative und qualitative Daten erhoben werden. Die Fragen müssen sich sachlich auf das abzufragende Thema beziehen und idealerweise wird nur ein Aspekt pro Frage behandelt. Zusammengehörige Fragen werden in Gruppen zusammengefasst. Die Fragen müssen verständlich formuliert werden.

Für die Informationsbeschaffung zur Erstellung der Prozessbeschreibung und zur Datenerfassung der einzelnen Bereiche gemäß der Vorgehensweise wie in Abbildung 7 dargestellt, wurden die folgenden Fragen ausgearbeitet. Die Ausarbeitung des Fragebogens war ein kontinuierlicher Prozess. Die Fragen wurden in mehreren Expert*Innenbefragungen eingesetzt. Die direkten Rückmeldungen in den Expert*Innenbefragungen wurden umgehend eingearbeitet und die Fragen entsprechend angepasst. Die Fragen (siehe Kapitel 8.2.1) wurden so ausgewählt, dass die Antworten direkt in die BIA-Matrix eingearbeitet werden können. Der fertige Fragebogen befindet sich im Anhang 14.4.

Im Anschluss an die Erstellung des Fragebogens wurden in Expert*Innenbefragungen die BIA-Matrix befüllt und die Abhängigkeiten eingetragen.

In den Monaten Februar bis April 2021 wurden vier Befragungen durchgeführt. Jeweils eine separate Befragung in der angegebenen Reihenfolge fand mit den folgenden Expert*Innengruppen statt:

- 1) Leiterin und QM-Beauftragte der Aufbereitungseinheit für Medizinprodukte,
- 2) Leiter der Infrastrukturprojekte,
- 3) Leiter der IT-Abteilung und der IT-Experte zuständig für die AMEP,
- 4) Leiter der Technikabteilung.

In den jeweiligen Expert*Innenbefragungen wurden die kritischen Prozesse, Rollen, externe Partner, IT-Software, Versorgungssysteme aus deren Sicht festgelegt. Die Prozesse und Ressourcen sowie deren Robustheit wurden beschrieben. Auch wurden die Abhängigkeiten eingepflegt.

Die Prozessbeschreibungen wurden nicht in textlicher Form vorgenommen, sondern in graphisch-schematischer Darstellung ausgearbeitet.

Dafür wurde mit den Informationen und Daten eine Prozessanalyse durchgeführt.

In einer „Prozessanalyse“ (vgl. ANDLER N. 2015: 342-344) werden die gewonnenen Informationen in ein Flussdiagramm umgesetzt. Hier wird die Abfolge der Prozesse graphisch dargestellt und die Prozesse werden schematisch verknüpft. Mit dieser Methode kann ein guter Einblick in die operativen Verfahren einer Organisation dargestellt werden. Der Detaillierungsgrad kann, je nach Bedarf, abhängig von der gewünschten Informationsschärfe detaillierter oder übersichtlicher gestaltet werden. Für die Prozessmodellierung werden 2 Formen genutzt, zum einen ein schematischer Prozessablauf und zum anderen eine Beschreibung in tabellarischer Form zur Dokumentation der Details. Der Einsatz eines multidisziplinären Teams bringt

unterschiedliches Fachwissen und differenzierte Perspektiven für die Erstellung des schematischen Ablaufes mit. Die Bestandteile der Abbildung 5 sollten für jeden Prozessschritt überprüft werden.

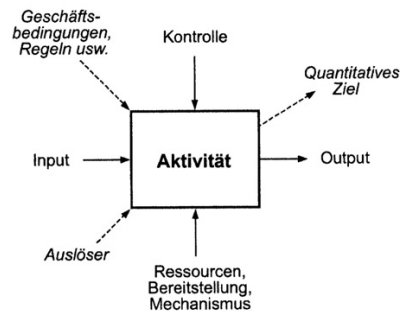


Abbildung 5: Allgemeine Bestandteile einer Prozessanalyse (Quelle: ANDLER N. 2015: 344)

Mit den gewonnenen Daten und Informationen aus den Interviews, der Schreibtisch-Forschung und den Expert*Innenbefragungen wurde ein Prozessflussdiagramm (siehe Anhang 14.1) für die Aufbereitungseinheit der Medizinprodukte erstellt. Anhand dieses Diagramms wurden die Abhängigkeiten der einzelnen Prozessschritte visualisiert und die BIA-Matrix konnte mit den nötigen Daten und Informationen vervollständigt werden.

Aus dem Prozessflussdiagramm gingen noch keine Abhängigkeiten der sehr komplexen versorgungstechnischen Ressourcen hervor. Ein Krankenhaus ist ein hoch komplexes versorgungstechnisches Konstrukt. Insbesondere wenn mehrere Gebäudeteile oder ein kompletter Campus versorgt werden müssen. Es konnte auf keine zusammenhängende Übersicht der versorgungstechnischen Systeme zurückgegriffen werden. Damit die einzelnen Abhängigkeiten von diesen Versorgungssystemen dargestellt werden können, wurde eine weitere Analyse durchgeführt. Zur Umsetzung dieser Analyse wurde auf ein relationales Datenmodell zurückgegriffen.

Ein „relationales Datenmodell“ (vgl. ANDLER N. 2015: 350) kann als grundlegendes Werkzeug für eine detaillierte technische Systemanalyse zur besseren Einschätzung angewendet werden. Innerhalb der Systemgrenzen werden alle technischen Systeme, Bereiche, Anlagen und Verknüpfungen im jeweiligen Kontext miteinander verbunden. Zur Darstellung der Datenflüsse und Abhängigkeiten können „Fließrichtungen“ mit Pfeilen angegeben werden. Mit der Angabe der Datenflüsse und den notwendigen Prozessen im Datenmodell, können die Zusammenhänge zwischen den technischen Systemen und den Prozessschritten dargestellt werden. Eine Überprüfung mit den Expert*Innen des relationale Datenmodells sollte vorgesehen werden.

Aus den Informationen der Prozessanalyse und der BIA-Matrix wurde ein relationales Datenmodell mit Bezug zur Aufbereitungseinheit für Medizinprodukte mit den relevanten technischen Versorgungssystemen erstellt. Es wurden insbesondere folgende Systeme analysiert und dargestellt:

- Allgemeine und Sicherheitsstromversorgung
- Kälteversorgung
- Wärmeversorgung

- Dampfversorgung
- Druckluftversorgung
- Trinkwasserversorgung und insbesondere die VE-Wasserversorgung
- Abwasserentsorgung
- Frischluftversorgung
- Telekomanbindung
- Internet-Anbindung
- IT-Netzwerk
- IT-Server
- Schwachstromsicherheitsanlagen

Das ausgearbeitete relationale Datenmodell befindet sich im Anhang 14.9. Zur Visualisierung und besseren Übersicht wird angeraten das relationale Datenmodell mindestens in DIN A1 Format auszudrucken.

Nachdem alle Daten gesammelt, die Prozessanalyse und das Datenmodell erstellt wurden, wurden im Mai 2021 in 2 Workshops die Bewertung der einzelnen Prozessschritte sowie der einzelnen Ressourcen zusammen mit den oben genannten Expert*Innen durchgeführt. Als Resultat der Bewertung wurden die Schadensklassen als auch Kenngrößen zur Business Impact Analyse definiert.

Die Beeinträchtigung der Schadensklassen „Operate“, „Legal“, „Finance“ und „Image“ wurden nach den 3 Kategorien „managebar“, „signifikant“ und „kritisch“ eingestuft.

Für die Kenngrößen der BIA wurden Festlegungen gemäß dem folgenden Schema definiert:

- 10 Minuten, 30 Minuten, 1 Stunde, 2 Stunden, 4 Stunden, 8 Stunden, 12 Stunden, 24 Stunden, 3 Tage und 7 Tage.

Die Herleitung der Kennwerte für die Bewertung im Workshop wird im Kapitel 7.3 beschrieben.

Den Abschluss der beiden Workshops bildet die BIA-Matrix wie in den Anhängen 14.5, 14.6, 14.7 und 14.8 beschrieben. Diese Bewertung wurde als Grundlage zur Parametrierung der beiden Software-Tools, wie in den Kapiteln 3.5 und 3.6 beschrieben, genutzt.

3.4 Risikoanalyse

So wie in der Abbildung 2 dargestellt, ist die Risikoanalyse ein Teilbereich des Risikomanagement Prozesses.

Je nach Verfügbarkeit der Informationen kann eine Risikoanalyse unterschiedlich komplex und detailliert ausgeführt werden. Bei einer Risikoanalyse können unterschiedliche Faktoren genutzt werden u.a. die Wahrscheinlichkeit der Ereignisse & deren Folgen, die Komplexität & die Verflechtung; die Empfindlichkeit & das Vertrauensniveau. Unterschiedliche Analysetechniken können genutzt werden, um

sowohl qualitative als auch quantitative Ergebnisse zu erhalten. Eine Risikoanalyse dient dazu Daten zur Bewertung des Risikos zu liefern. Diese Daten tragen zur Entscheidung bei, ob und wie ein Risiko behandelt werden kann. (vgl. ISO 2018: 12)

Im Kontext der besonderen Betrachtung der Kaskadeneffekte in Bezug auf das Risikomanagement von kritischen Infrastrukturen wird in dieser Arbeit der CEBERUS-Ansatz als Leitlinie genutzt. Damit die Interdependenzen analysiert werden können, werden detaillierte Informationen der unterschiedlichen Prozesse und Ressourcen benötigt. Auch müssen die kritischen Prozesse und Ressourcen identifiziert werden.

Zur Identifikation der kritischen Prozesse und Ressourcen sowie die Analyse der Interdependenzen wird in der vorliegenden Arbeit auf eine Business Impact Analyse zurückgegriffen.

In einer Business Impact Analyse einer Organisation werden zuerst die Produkte und Dienstleistungen priorisiert. Erst anschließend werden die Prozesse und Aktivitäten analysiert. (vgl. ISO/TS 2015: vi)

In der vorliegenden Arbeit werden ausschließlich die Prozesse der Aufbereitungseinheit für Medizinprodukte analysiert. Für ein Krankenhaus müsste diese Arbeit allumfänglich für alle Dienstleistungen durchgeführt werden.

Gemäß der ISO (2019: 13-14) wird die Durchführung eine Business Impact Analyse unter anderem folgendermaßen beschrieben:

- Bestimmung, welche Ressourcen zur Unterstützung der priorisierten Aktivitäten benötigt werden;
- Festlegung der Abhängigkeiten als auch der Interdependenzen, einschließlich der Partner und Zulieferer;
- Nutzung der Analyse zur Festlegung der kritischen Aktivitäten;
- Bestimmung des Zeitrahmens für die Wiederaufnahme der unterbrochenen Tätigkeit mit einer Mindestkapazität – „Recovery Time Objective (RTO)“;
- Bestimmung der Zeit, innerhalb derer die Auswirkungen der Nichtwiederaufnahme der Aktivität unannehmbar werden – Maximum Tolerable Period of Disruption (MTPD)“;

Werden informationsbasierte Aktivitäten analysiert, muss zusätzlich eine Zeit bestimmt werden, in derer ein möglicher Datenverlust für den Wiederanlauf akzeptiert werden kann – „Recovery Point Objective (RPO)“. (vgl. BSI 2021: 216)

TORABI S. A. et al. (2014: 311) haben in ihrem Rahmenwerk für die Durchführung einer Business Impact Analyse die nachfolgenden Schritte definiert:

- Identifizierung der Schlüsselprodukte der Organisation
- Zerlegung der Schlüsselprodukte in kleinste wesentliche Funktionen,
- Identifizierung der geschäftskritischen Funktionen,
- Ermittlung der Kontinuitätsparameter:
 - Maximum Tolerable Period of Disruption (MTPD) und
 - Minimum Business Continuity Objective (MBCO).

Nach PRITI S. (2017: 26) werden die nachfolgenden Informationen bei einer Datenerfassung zur Erstellung der Business Impact Analyse benötigt:

- die Geschäftsprozesse,
- die erforderlichen Ressourcen,
- Abhängigkeiten zwischen den Geschäftsprozessen,
- Die Auswirkung(en) eines ausgefallenen Geschäftsprozesses,
- Die Kritikalität der einzelnen Prozesse,
- Ein Recovery Time Objective (RTO) pro Prozess,
- Ein Recovery Point Objective (RPO) pro Prozess.

TAARUP-ESBENSEN J. (2020: 4) beschreibt in seine Struktur zur Durchführung einer Business Impact Analyse die Abfolge der Aktivitäten zur fundierten Analyse der Herausforderungen in Bezug auf das Business Continuity Management, mit dem eine Organisation konfrontiert ist.



Abbildung 6: Struktur zur Durchführung einer BIA (Quelle: TAARUP-ESBENSEN J. 2020)

„Der Erfolg einer Business Impact Analyse liegt in der Effektivität der Datenerfassung“ (PRITI S. 2017: 28).

Die einzelnen Quellen beschreiben zum Teil gleiche oder ähnliche Vorgehensweisen. Abgeleitet aus diesen Informationen wurde für die vorliegende Arbeit zur Besonderen Betrachtung der Kaskadeneffekte in Bezug auf das Risikomanagement von kritischen Infrastrukturen für die Datensammlung die Vorgehensweise gemäß Abbildung 7 festgelegt.

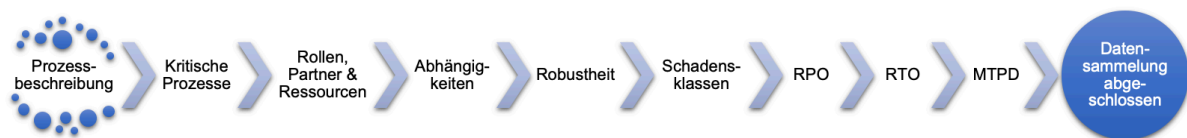


Abbildung 7: Vorgehensweise für die Datensammlung zur Business Impact Analyse

3.5 bcNAVIGATOR – bcIMPACT

Die Software bcNAVIGATOR kann, wie in Abbildung 8 dargestellt, in den vier klassischen Felder des Business Continuity Management eingesetzt werden.

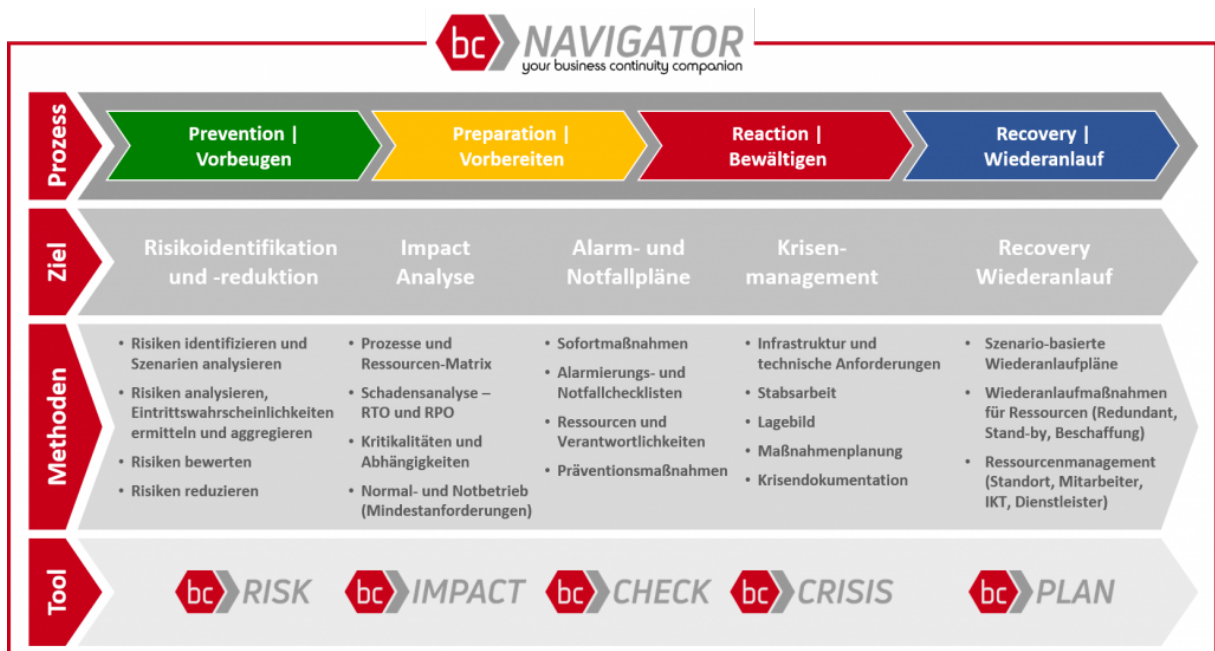


Abbildung 8: bcNAVIGATOR (Quelle: BC-Consulting 2021a)

In der besonderen Betrachtung der Kaskadeneffekte in Bezug auf das Risikomanagement werden die Abhängigkeiten von Prozessen und Ressourcen analysiert. Beim Einsetzen einer Business Impact Analyse zur Identifikation von wechselseitigen Abhängigkeiten zwischen Prozessen und Ressourcen können auch die Auswirkungen bei Ausfällen von Prozessen, die Kritikalität eines Prozesses sowie die Wiederanlaufzeiten aufgezeigt werden. (vgl. BC-CONSULTING 2021b)

Für diese Arbeit wird das Modul bcIMPACT genutzt. Zur Analyse des Ergebnisses muss im Vorfeld die Software parametrisiert und die Daten der Prozesse, Ressourcen und deren Abhängigkeiten eingetragen werden. Als Grundlage für die Eintragungen wurde eine BIA-Matrix auf Basis einer Tabellenkalkulationssoftware (siehe Kapitel 3.3) mit allen benötigten Informationen erstellt. Diese Matrix konnte durch das Importmenü in die Software importiert werden. Eine manuelle Eingabe ist ebenfalls möglich, allerdings zeitaufwendiger.

Die Prozesse basieren auf der Prozesslandkarte (siehe Abbildung 43) des fiktive Krankenhauses und die Ressource wurden durch die Abhängigkeiten abgeleitet.

Eine Schritt-für-Schritt Anleitung zur Parametrierung und manuellen Eingabe der Daten für die statische Risikoanalyse sind im Anhang 14.10 beschrieben. In Kapitel 8.4 wird die statische Risikoanalyse an einem Fallbeispiel beschrieben.

Für das Modul bcIMPACT sind im Startfenster (Abbildung 9) 4 Silos, die für die angewandte Business Impact Analyse genutzt wurden. Das Silo „Interview“ steht aktuell in der Software noch nicht zur Verfügung. Die Datenbeschaffung kann noch nicht im Werkzeug dokumentiert werden.

Einstellungen	Ressourcen	Prozesse	Interviews	Bericht BIA
Prozesstypen	Organisationen	Liste	Liste	Dashboard
Prozesskritikalitäten	Rollen	Hierarchie	Anlegen	Kritische Prozesse
Prozessfelder	Standorte	Anlegen		Kritische Ressourcen
Prozesskritikalitätskategorien	Personen			Bericht BIA
	Partner			Bericht Prozesse
	Konfigurierbare Ressourcen			

Abbildung 9: Menüfenster bclIMPACT

Im Folgenden werden die Parametrierung und die Dateneingabe in kurzer Form beschrieben.

- **Einstellungen**

Im Menü „Einstellungen“ wird die einmalige Basis-Parametrierung für die Business Impact Analyse vorgenommen.

- Prozesstypen

In der Maske „Prozesstypen“ werden die unterschiedlichen Prozessebenen gemäß der vorhandenen Prozesslandkarte parametriert.

- Prozesskritikalitäten

In der Maske „Prozesskritikalitäten“ werden die einzelnen Kritikalitäten parametriert. Zu den Kritikalitäten gehören die einzelnen Schadensklassen, RPO, RTO, und MTPD sowie zusätzliche Informationen. Die Kritikalitäts-Kategorien werden in der Maske „Prozesskritikalitätskategorien“ parametriert.

- Prozessfelder

Hier können zusätzliche Prozessfelder frei definiert werden. Für die Beschreibung der Robustheit, Informationen zum Outsourcing von Ressourcen und über den Analysestatus wurden zusätzlich Felder definiert.

- Prozesskritikalitätskategorien

Die drei Prozesskritikalitätskategorien Schadensklassen, Verfügbarkeit und Informationssicherheit wurden hier eingestellt.

- **Ressourcen**

Im Menü „Ressourcen“ wurden die einzelnen Ressourcen, die in Abhängigkeit zu den Prozessen stehen, hierarchisch-organisatorisch eingepflegt und beschrieben.

- Organisationen

In der Maske „Organisationen“ wurde eine fiktive hierarchische Organisationsstruktur (z.B. Verwaltungsorgan – Generaldirektion –

Administrative Direktion – Abteilungsleitung) für das Krankenhaus eingestellt.

- Rollen

In der Maske „Rollen“ wurden die wichtigsten fiktiven Rollen für die Funktionsfähigkeit der Aufbereitungseinheit für Medizinprodukte eingestellt, beschrieben und bewertet.

- Standorte

In der Maske „Standorte“ wurde eine fiktive architektonische hierarchische Struktur (z.B.: Hauptgebäude – BT 1.1. – Etage 2 – Etagenverteiler) der Infrastruktur parametrisiert.

- Personen

Wegen der Analyse in einem fiktiven Krankenhaus, wurden in der Maske „Personen“ keine Einträge eingegeben. Falls Personen hier eingepflegt werden, können diese Personen den Rollen zugewiesen werden. Ebenso können Prozess-Verantwortliche Personen festgelegt werden.

- Partner

In der Maske „Partner“ werden in diesem Fall die fiktiven externen Partner, welche zur Funktionsfähigkeit der Aufbereitungseinheit für Medizinprodukte benötigt werden, eingetragen und bewertet.

- Konfigurierbare Ressourcen

In der Maske „konfigurierbare Ressourcen“ wurden zusätzliche Ressourcen zu den bereits beschriebenen Ressourcen Organisation, Rollen und Standorte angelegt.

In der Menüleiste zur Bearbeitung von Ressourcen, kann eine weitere Maske „Ressourcenbeziehungen“ geöffnet werden. In dieser Maske können dann die Abhängigkeiten zwischen den unterschiedlichen Ressourcen parametrisiert werden.

- **Prozesse**

Das Menü „Prozesse“ wird genutzt, um neue Prozesse anzulegen und um die bereits angelegten Prozesse in Listen hierarchisch geordnet darzustellen.

- Liste / Hierarchie

In den Masken „Liste“ werden die Prozesse in alphabetischer Reihenfolge oder in der Maske „Hierarchie“ die Prozesse gemäß den Prozessebenen entsprechend aufgelistet.

- Anlegen

Die Maske „Anlegen“ dient dazu neue Prozesse in die Prozesslandschaft zu integrieren und den Prozess, gemäß der Parametrierung in den Einstellungen, anzulegen und zu bewerten. Die Prozesslandkarte vom

fiktiven Krankenhaus wurde als Grundlage für das Anlegen der Prozesse genutzt.

Ist der Prozess angelegt, müssen die Abhängigkeiten noch eingepflegt werden. Dazu gibt es zum einen die Prozessbeziehungen (Abhängigkeiten) und zum anderen die Ressourcenbeziehungen. Die Eintragungen erfolgen gemäß der BIA-Matrix.

- **Bericht BIA**

Das Menü „Bericht BIA“ dient der Auswertung der Business Impact Analyse. Alle vorherigen Parametrierungen und Eingaben werden hier zusammengefasst und bewertet. In der aktuellen Arbeit wird lediglich auf die nachfolgenden beiden Masken zurückgegriffen.

- Kritische Prozesse / kritische Ressourcen

In der Maske „kritische Prozesse“ werden die Prozesse in hierarchischer Form inkl. der Bewertung aufgelistet. Hier besteht die Möglichkeit die kritischen Prozesse in verschiedene Formate zu exportieren.

Das gleiche gilt für die Maske „kritische Ressourcen“.

3.6 SAURON Propagation Engine

Das SAURON Projekt wurde initiiert um den Betreibern der europäischen Häfen, als kritische Infrastruktur, Hilfestellung zu geben um gegen potenzielle physische-, Cyber- oder kombinierte Bedrohungen zu antizipieren und ihnen zu widerstehen. (SAURON 2020)

Das SAURON Rahmenwerk betrachtet und überwacht die beiden Bedrohungsarten separat voneinander, zusätzlich gibt es hier eine dritte Dimension der kombinierten Überwachung. Dadurch können kaskadierende Auswirkungen eines Vorfalls aus den beiden Bedrohungsarten (physisch und cyber) aufgezeigt werden. (vgl. SCHAUER S. et al. 2019)

Zur dynamischen Analyse von Kaskadeneffekten wird in dieser Arbeit auf die „Propagation Engine“ aus dem SAURON Rahmenwerk zurückgegriffen.

In der Propagation Engine wird die Infrastruktur und die Prozesslandschaft einer Organisation in einem graphisch Netzwerk aufgebaut. Die Knoten repräsentieren die einzelnen Ressourcen oder Prozesse (Asset) und die Kanten stellen die Abhängigkeiten zwischen den Vermögenswerten dar und beschreiben somit wie die einzelnen Knoten untereinander verbunden sind. Ist nun ein Asset durch einen physischen oder Cybervorfall betroffen und fällt aus bzw. muss die Aktivität reduziert werden, wird dieser Vorfall am betroffenen Knoten bewertet. Im Anschluss an diese Bewertung und in Abhängigkeit der Parametrierung der Knoten werden in der Propagation Engine die Kaskadeneffekte sowohl ausgewertet sowie auch dargestellt. Die Bewertung basiert auf dem mathematischen Modell der Markov-Ketten. Die Übergangsmatrix wird mit drei Zuständen beschrieben: „normaler“, „teilweise betroffener“ oder „vollständig betroffener“ Betrieb. Bedingt durch die parametrisierten Übergänge der Knoten und Kanten können die Nachbarknoten betroffen werden und

den Status ändern. Diese Bewertung erfolgt Schritt für Schritt und der ursprüngliche Vorfall kann sich kaskadenartig auf andere Assets ausbreiten. (vgl. SCHAUER S. et al. 2019)

Die Anwendung der Propagation Engine wird in den Kapiteln 8.5 beschrieben.

Eine Schritt-für-Schritt Anleitung der Parametrierung befindet sich im Anhang 14.11.

Nachfolgend werden für die Parametrierung sowie die Eingabe der Daten in die Propagation Engine kurz beschrieben. Die Beschreibung basiert auf den Angaben in der Hilfe Datei der SAURON Propagation Engine. (siehe WARUM M. et al. 2020)

- **Anlegen eines Netzwerkes**

In der Maske „Network“ wird das Netzwerk bestehend aus Prozessen und Ressourcen eingegeben und parametriert.



Abbildung 10: SAURON – Netzwerkeingabe, Bsp.: Netzwerk der Interdependenzen zur Aufbereitungseinheit von Medizinprodukten des fiktiven Krankenhauses

Jeder Knoten kann drei verschiedene Zustände annehmen:

1. Der Knoten ist funktionsfähig und unberührt vom Vorfall.
2. Der Knoten ist in seiner Funktion beeinträchtigt, kann aber noch funktionieren.
3. Der Knoten fällt aus und ist nicht mehr funktionsfähig.

Je Knoten können mehrere Übergänge beschrieben werden. Der Standard-Ausgangswert ist 1. Die Eingabe der Übergänge erfolgt gemäß folgendem Schema:

State space of **3 maschinelle Reinigung & Desinfektion MP**

Initial state: ✓ apply to group

Transition changes below are applied to all **7** other nodes in group **AEMP - kritische Prozessschritte !**

Trigger	From	Go To	Output	%
AV-SV Stromausfall	1	3	Ausfall AEMP	100%
eg. 'fire' ⚠	1 ✓	2 ✓	eg. 'fire' ⚠	50 % +

⚠

Abbildung 11: SAURON: Netzwerkknoten: Parametrierung der Übergänge

Die Abhängigkeit zwischen den Knoten wird vom Ausgangsknoten (A) zum nächsten Knoten (B) angegebenen und ist unidirektional. Um eine bidirektionale Verknüpfung herzustellen, muss ebenfalls die Abhängigkeit von Knoten B nach Knoten A eingestellt werden.

- **Simulation des Netzwerkes**

Sauron Web: 0.19.0 API: 1.2.1 Core: 1.3.1

Step 1: Select initially compromised asset(s)
Add initial trigger(s) for your network elements to the simulation. If no valid triggers for an element exist (i.e., the transition table does not have any transitions originating in the element's current state), it will be disabled in the list below.

Alert source: ✓

Trigger: ✓

add

Step 2: Configure simulation scenario
Here you can find your constructed scenario of triggers initially affecting corresponding assets. You can disable triggers in order not to simulate them or remove them from the scenario by using the corresponding action buttons.

Order	Asset Name	Trigger	Actions
1.	Schachtverteiler BT 2.0 Et.-2	Überschwemmung < 1m	✓ ⬆ ⬇ ⬇ ⬆ ✖
2.	Schachtverteiler BT 3.1 Et. -2	Überschwemmung < 1m	✓ ⬆ ⬇ ⬇ ⬆ ✖

Step 3: Set simulation parameters and simulate
Set how many simulation runs you want to execute and, if preferred, a time step limit. The latter restricts each simulation run to the given amount of logical time steps. In order to simulate, at least one trigger has to be enabled in the scenario!

Number of simulations: ✓ +100

Time step limit: ✓

simulate

Abbildung 12: SAURON – Beispiel-Simulationseingabe

Für die Simulation wird auf die zuvor eingestellten Knoten und Auslöser zurückgegriffen. An dieser Stelle wird das gewünschte Szenario mit der Beeinträchtigung oder dem Ausfall von Knoten (Alert source) eingestellt. Es können mehrere Knoten für den Start der Simulation ausgewählt werden. Auch können zu den unterschiedlichen Knoten, unterschiedliche Auslöser (Trigger) ausgewählt werden (sofern sie parametrisiert wurden). Sind alle Knoten und Auslöser ausgewählt und dem Szenario hinzugefügt muss nur noch die Anzahl der Simulationszyklen festgelegt werden. Je mehr Zyklen durchlaufen werden, um so präziser wird das Ergebnis. Hier hat sich eine Zahl zwischen 100 und 1.000 Simulationszyklen (vgl. WALDMANN K.-H. und HELM W. E. 2016b: 231) bewährt. Anschließend kann die Simulation gestartet werden.

Ist die Simulation durchgelaufen kann unter dem Reiter „Entity Analysis“ das Resultat visualisiert werden. Für jeden Knoten werden die möglichen Zustände farblich angezeigt und auch zahlenmäßig ausgedrückt. Dabei entspricht die Summe der Zahlen die Anzahl der Simulationszyklen.

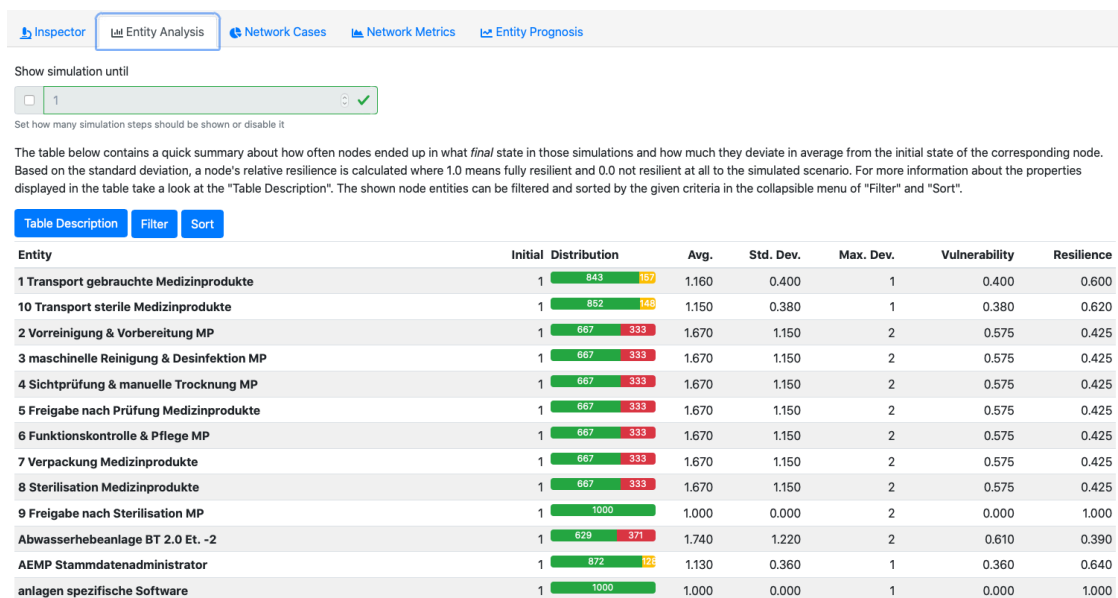


Abbildung 13: SAURON – Beispiel-Ergebnis einer Simulation

Das Ergebnis der Simulation für die Aufbereitungseinheit für Medizinprodukte für das fiktive Krankenhaus wird im Kapitel 8.6 ausgewertet.

4 Kritische Infrastrukturen und deren Abhängigkeiten

4.1 Kritische Infrastrukturen in der Gesellschaft

In der heutigen modernen, vernetzten Gesellschaft wird eine hochentwickelte Dienstleistungs- und Industriewirtschaft betrieben. Dies bedingt die Nutzung von unterschiedlichen leistungsfähigen Infrastrukturen wie z.B. Lebensmittelversorgung, Verkehrs-, Telekommunikation-, Energie-, Finanz-, Sozial- und Gesundheitsdienstleistungen. Diese Infrastrukturen genauso wie die gesamte Gesellschaft sind bedingt durch den Klimawandel vermehrt Naturkatastrophen ausgesetzt. Aber auch andere Gefahren wie z.B. technische Unfälle, menschliches Versagen, Cyberkriminalität und Terrorismus können die Funktionsfähigkeit beeinträchtigen. Im Extremfall kann eine Infrastruktur soweit betroffen werden, dass es zu einem Totalausfall kommt. (vgl. BKA und BM.I 2014: 4)

Werden diese „kritischen Infrastrukturen“ in ihrer Funktionsfähigkeit beeinträchtigt, steht die Frage im Vordergrund inwieweit die Bevölkerung in ihrer Lebensweise beeinträchtigt wird. Nach Angaben der Bundesamt für Bevölkerungsschutz aus der Schweiz können Ausfälle oder Zerstörungen von kritischen Infrastrukturen schwerwiegende Auswirkungen für die Bevölkerung und deren Lebensgrundlage haben. (vgl. BABS 2018: 5-6)

Die Europäische Kommission beschreibt in ihrem Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen im Jahr 2005, dass das Leben und Eigentum der EU-Bevölkerung mit dem Schutz kritischer Infrastrukturen zu schützen sei. Demzufolge sollten Störungen und Manipulationen in kritische Infrastrukturen nur ausnahmsweise, kurzzeitig und lokal begrenzt auftreten. Um den Schaden für alle Stakeholder so gering wie möglich zu halten, sollte die Funktionsfähigkeit relativ leicht wieder hergestellt werden können. (vgl. EU 2005: 2)

Welchen Auswirkungen die kritischen Infrastrukturen auf die Gesellschaft haben können, wird ersichtlich in der Indikativen Liste (Tabelle 1) zu den kritischen Infrastruktursektoren aus der Anlage 2 im Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen. In der Tabelle werden 11 unterschiedliche Sektoren mit insgesamt 37 Teilsektoren aufgelistet. Dies hohe Anzahl an Teilsektoren zeigt die enorme Komplexität der Thematik „Schutz kritischer Infrastrukturen“ auf. Dem entsprechend wurden Prioritäten gesetzt.

Auf der Grundlage des vorherigen zitierten Grünbuches, verabschiedete der Rat der Europäische Union eine erste EU-Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Bei der Umsetzung in nationale Gesetzgebungen durch die Mitgliedstaaten, sollte der Ansatz die kritischen Infrastrukturen vor Gefahren, wie von Menschen ausgehende technologische Bedrohungen, Naturkatastrophen und Terroranschläge zu schützen, berücksichtigt werden. Bedingt durch einen abgestuften Ansatz, konzentriert sich diese EU-Richtlinie lediglich auf die Sektoren Energie und Verkehr. Andere Sektoren wie z.B. der Informations- und Kommunikationssektor sollte

4 Kritische Infrastrukturen und deren Abhängigkeiten

tiefgehender untersucht werden und es wurde angeboten weitere Sektoren zu prüfen. (vgl. EU 2008: L 345/75 & 78)

Tabelle 1: Indikative Liste der kritischen Infrastrukturen (Quelle: EU 2005: 26)

Sector	Product or service
I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines
	2 Electricity generation
	3 Transmission of electricity, gas and oil
	4 Distribution of electricity, gas and oil
II Information, Communication Technologies, ICT	5 Information system and network protection
	6 Instrumentation automation and control systems (SCADA etc.)
	7 Internet
	8 Provision of fixed telecommunications
	9 Provision of mobile telecommunications
	10 Radio communication and navigation
	11 Satellite communication
	12 Broadcasting
III Water	13 Provision of drinking water
	14 Control of water quality
	15 Stemming and control of water quantity
IV Food	16 Provision of food and safeguarding food safety and security
V Health	17 Medical and hospital care
	18 Medicines, serums, vaccines and pharmaceuticals
	19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/payment structures (private)
	21 Government financial assignment
VII Public & Legal Order and Safety	22 Maintaining public & legal order, safety and security
	23 Administration of justice and detention
VIII Civil administration	24 Government functions
	25 Armed forces
	26 Civil administration services
	27 Emergency services
	28 Postal and courier services
IX Transport	29 Road transport
	30 Rail transport
	31 Air traffic
	32 Inland waterways transport
	33 Ocean and short-sea shipping
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances
	35 Pipelines of dangerous goods (chemical substances)
XI Space and Research	36 Space
	37 Research

Damit die Funktions- und Leistungsfähigkeit für die Gesellschaft gesichert werden kann, müssen die notwendigen Anpassungen von spezifischen Schutzmaßnahmen rechtzeitig getroffen werden. Für die Auswahl der bestmöglichen Maßnahmen müssen zahlreiche Faktoren beachtet werden. Insbesondere spezifische Eigenschaften und Charakteristika der einzelnen Sektoren müssen berücksichtigt sowie relevante Trends und Entwicklungen erkannt werden. (vgl. HABEGGER B. und KMIĘCIK S. 2010: 5)

4.1.1 Sektoren

Die Tabelle 1 veranschaulicht mögliche Sektoren und Teilsektoren zur Definition der kritischen Infrastrukturen welche von der EU-Kommission in deren Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen veröffentlicht wurde.

Da eine EU-Richtlinie nur Ziele vorgibt und nicht verbindlich für die Mitgliedsstaaten ist, können die Mitgliedsstaaten bei der Umsetzung der EU-Richtlinie in die nationale Gesetzgebung zusätzliche Sektoren integrieren. Dieser Ursache geschuldet, gibt es keine einheitliche Einteilung der Sektoren bzw. Teilsektoren für kritische Infrastrukturen.

Österreich hat hier den Ansatz „operator based approach“ gewählt und keine Sektoren definiert. Lediglich die Betreiber von strategischen Unternehmen werden als kritische Infrastruktur identifiziert. Österreich begründet dieses Vorgehensweise damit, dass in einer komplexen Wirtschaft die Interdependenzen nicht in Sektoren eingeteilt werden können. (BKA und BM.I 2014: 8)

Die Niederlande gehen einen ähnlichen Weg und definieren keine Sektoren, sondern kritische Prozesse und diese kritischen Prozesse zusammen bilden die kritische Infrastruktur der Niederlande. Der Nationaler Koordinator für Sicherheit und Terrorismusbekämpfung argumentiert diese Herangehensweise mit dem Argument, dass nicht alle Prozesse in einem Sektor kritisch sind. (vgl. NCTV 2018: 1)

Wie in der Abbildung 14 dargestellt sind in Deutschland die kritischen Infrastrukturen in zehn verschiedene Sektoren unterteilt. Zusätzlich erweitern sich diese Sektoren noch in 32 Teilsektoren. (vgl. BBK und BSI 2021a)



Abbildung 14: Sektoren und Branchen KRITIS (Quelle: BBK und BSI 2021b)

Luxemburg hat im Jahre 2018 für den Bereich der kritischen Infrastrukturen neun verschiedene Sektoren mit 31 Teilsektoren definiert (vgl. ME 2018a: A 152-1). Diese Einteilung kommt der Indikativen Liste der Tabelle 1 aus dem Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen sehr nahe.

Da es keine einheitliche Einteilung der Sektoren und Teilsektoren für alle Mitgliedstaaten gibt, muss jeder Betreiber einer kritischen Infrastruktur die national anzuwendende Gesetzgebung respektieren. Die vorliegende Arbeit orientiert sich an den beiden Modellen aus Deutschland und Luxemburg. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und das Bundesamt für die Sicherheit in der Informationstechnik haben in der aktuellen Einteilung (Juli 2021) der Sektoren und Branchen (Teilsektoren) für kritische Infrastrukturen die „medizinische Versorgung“ dem Sektor „Gesundheit“ zugeordnet (vgl. BBK und BSI 2021a). Das Hohe Kommissariat für nationale Sicherheit hat in seiner Einteilung der kritischen Infrastrukturen im Februar 2018 den Teilsektor „Krankenhausaktivität“ im Sektor „Gesundheit“ gesetzlich verankert (vgl. ME 2018a: A 152-1).

In Anlehnung an diese Einteilung gehören Krankenhäuser zu den kritischen Infrastrukturen. (vgl. RECHENBACH P. 2018: 23).

4.1.2 Kritische Infrastruktur Krankenhaus

Im Rahmen der Daseinsvorsorge wird die medizinische Grundversorgung durch Krankenhäusern sicher gestellt. Die Menschen stellen an die Gesundheitsversorgung die Erwartung, dass in jedem Krankenhaus geholfen werden kann um mindestens die Vitalfunktionen zu stabilisieren. Daraus folgt, dass in jedem Krankenhaus Vorbereitungen getroffen werden müssen um kurzfristig die Versorgungskapazität zu steigern. Krankenhäuser müssen auch funktionsfähig bleiben, wenn andere kritische Infrastrukturen wie z.B. die Energieversorgung oder die Abfallentsorgung ausfallen. Auf diese Situationen muss ein Krankenhaus vorbereitet sein. (vgl. RECHENBACH P. 2018: 23-25)

Bei einem Ereignisfall sind Krankenhäuser das letzte Glied in der Rettungskette und werden hier ganz besonders in die Verantwortung genommen. Würde das Krankenhaus ausfallen oder beeinträchtigt werden, würden umfassende Versorgungsengpässe entstehen und die öffentliche Sicherheit wäre gefährdet. Dies bedeutet, dass Krankenhäuser auch in einer Krise funktionsfähig bleiben müssen, zumindest für lebensnotwendige Bereiche. Damit sich Krankenhäuser als kritische Infrastruktur auf ihre Versorgungspflicht vorbereiten können, ist eine allumfassendes Risikomanagement einzusetzen. Ein wesentlicher Bestandteil davon ist die Risikoanalyse. (vgl. STOLZENBURG K. und KOWALZIK B. 2018: 72-75)

Im Sektor der Gesundheitsversorgung nehmen Krankenhäuser eine wesentliche Position ein. Das System Krankenhaus ist hoch sensibel und sehr komplex. Über verschiedene Ebenen hinweg ist das System Krankenhaus von einer Vielzahl interner und externer Kooperationspartnern, Funktionsbereichen und Komponenten abhängig. Die vier Ebenen aus Abbildung 15, zeigen schematisch die Interdependenzen am Beispiel der Notaufnahme.

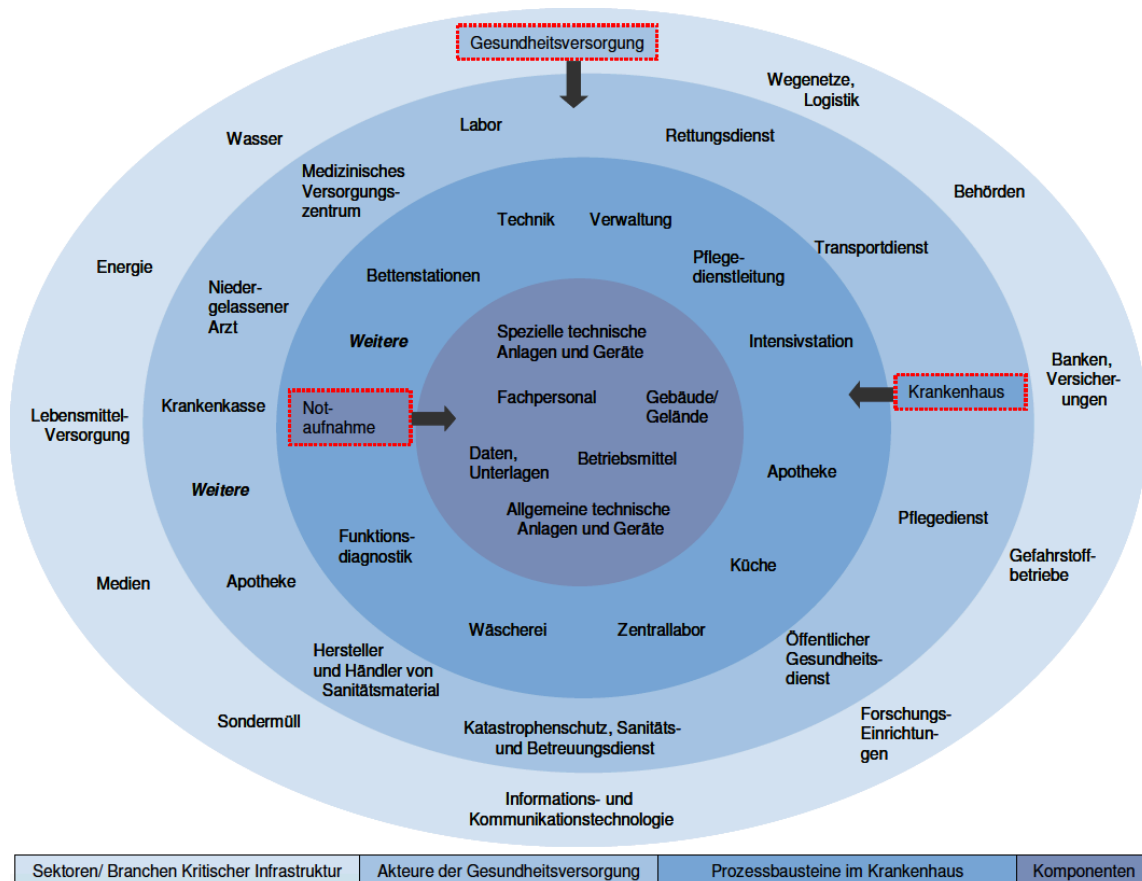


Abbildung 15: Die vier Ebenen der Gesundheitsversorgung als "Kritische Infrastruktur" (Quelle: BBK 2008: 8)

4.2 Abhängigkeiten von kritischen Infrastrukturen

In Deutschland wurden in den späten 1990er-Jahren die Betrachtungen zum Schutz von kritischen Infrastrukturen zum ersten Mal diskutiert. Dies geschah unter dem Impuls eines Abschlussberichtes aus dem Jahre 1997 einer Expert*Innenkommission in den USA. Im Jahr 2004 wurde die Europäische Kommission vom Europäischen Rat beauftragt eine Strategie zum Schutz von kritischen Infrastrukturen auszuarbeiten. Daraus entstand in 2005 ein „Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen“ (vgl. EU 2005: 2). Dieses Grünbuch war die Grundlage für die „Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008, über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern“ (EU 2008). In Österreich wurde 2008 ein erster Masterplan „Austrian Program for Critical Infrastructure Protection (APCIP)“ beschlossen (vgl. BKA und BM.I 2014: 4). In Deutschland wurde 2009 die erste „Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie)“ veröffentlicht (vgl. BBK 2020a: 9).

Im Dokument von RINALDI S. M. et al. (2001: 11) werden u.a. zwei große Stromausfälle und deren Auswirkungen in Kalifornien aus den Jahren 1998 und 2001 aufgeführt. Die Autoren beschreiben in diesem Dokument die Identifikation, das Verstehen und die Analyse von Abhängigkeiten zwischen den kritischen Infrastrukturen. Bei der Suche nach diesem Dokument auf den Online Plattformen wie Google Scholar oder ResearchGate können die Häufigkeit der Zitierung einer Publikation oder das

Interesse welches für das Dokument besteht, abgerufen werden. Für dieses Dokument gibt Google Scholar 2.921 (GOOGLE-SCHOLAR 2021) und ResearchGate gibt 2.044 Zitierungen an (RESEARCHGATE 2021). Damit kann dieses Dokument im Vergleich zu anderen Dokumenten als eines der Ursprungsdokumente zu diesem Thema gelten. In Abbildung 16 sind die Anzahl der Zitierungen und das Forschungsinteresse für dieses Dokument seit Beginn der Veröffentlichung dargestellt. Über die Jahre steigt die Anzahl der Zitierungen wohl, aber das Forschungsinteresse ändert sich über die ersten zwölf Jahre kaum. Ab 2013 steigt das Interesse sehr stark an. Berücksichtigt man die noch begrenzten Diskussionen zum Schutz von kritischen Infrastrukturen aus den späten 1990er-Jahren, könnte dies eine Erklärung für das geringer Interesse in den Anfangsjahren sein. Die Abhängigkeiten zwischen den kritischen Infrastrukturen war bis dahin noch wenig bis dahin thematisiert worden. Mit dem Anstieg des Forschungsinteresses ab 2013 kann man aber davon ausgehen, dass das Forschungsfeld zur Betrachtung der Abhängigkeiten von kritischen Infrastrukturen an Wichtigkeit gewinnt.

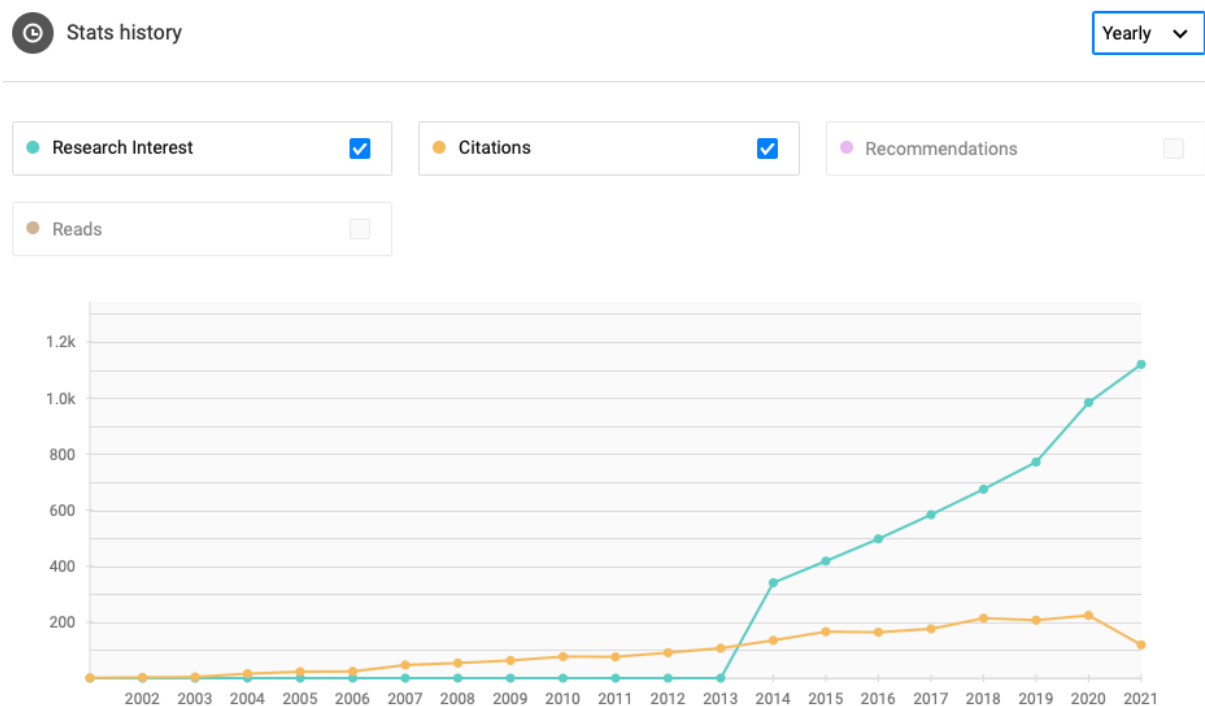


Abbildung 16: Anzahl der Zitierungen und Forschungsinteresse des Dokumentes (RINALDI S. M. et al. 2001) (Quelle: RESEARCHGATE 2021)

Für Nationen oder geografische Regionen sind kritische Infrastrukturen derart wichtig, dass deren Funktionsunfähigkeit oder Funktionsausfall zu größeren Beeinträchtigungen der regionalen, nationalen oder globalen Wirtschaft führen können. Die Planung sowie der Betrieb von kritischen Infrastrukturen werden meist unabhängig von anderen kritischen Infrastrukturen ausgeführt. (vgl. GUEYE A. et al. 2020) Allerdings hat die Vergangenheit gezeigt, dass durch Störungen einer Infrastruktur direkt oder indirekt andere Infrastrukturen betroffen werden. Diese Abhängigkeiten wirken oft kaskadenartig, so dass ein System ein anderes System beeinträchtigt. (vgl. RINALDI S. M. et al. 2001)

„Die Abhängigkeit von kritischen Infrastrukturen, die in hohem Maße miteinander vernetzt sind, ist eine der größten Schwachstellen der Gesellschaft“ (MACDERMOTT Á. et al. 2014: 1).

RINALDI S. M. et al. (2001: 12) beschreiben in ihrem sechs Dimensionen Modell (siehe Abbildung 17) zahlreiche Faktoren zu den Abhängigkeiten von kritischen Infrastrukturen. Dabei unterteilen sie die Faktoren in sechs Dimensionen „Interdependenzen“ (Types of Interdependencies), „Umfeld“ (Environment), „Verbindungen und Reaktionsverhalten“ (Coupling an Response Behavior), „Störungen“ (Type of Failure), „Charakteristik der Infrastruktur“ (Infrastructure Characteristics) und „Betriebszustand“ (State of Operation).

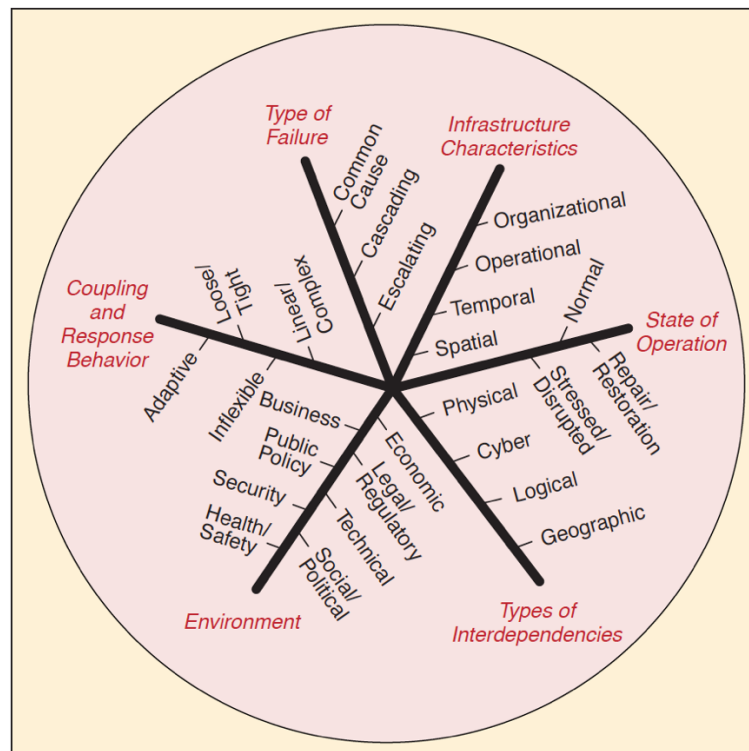


Abbildung 17: Sechs Dimensionen zur Beschreibung der Interdependenzen von Infrastrukturen (Quelle: RINALDI S. M. et al. 2001: 12)

4.2.1 Interdependenzen

Physische Interdependenzen zwischen zwei Infrastrukturen bestehen, wenn die eine Infrastruktur von einem physischen Produkt der anderen Infrastruktur abhängig ist und eine entsprechende Gegenleistung aufbringt. Ein elektronischer Datenaustausch zwischen zwei Infrastrukturen beschreibt die Cyber-Interdependenzen. Diese sind aus der Informatisierung und Automatisierung der Infrastrukturen entstanden. Werden Infrastrukturen in unmittelbarer räumlicher Nähe zueinander betrieben, können Ereignisse korrelierte Störungen hervorrufen und mehrere Infrastrukturen beeinträchtigen. Verbindungen zwischen Infrastrukturen, welche nicht physisch, cybertechnisch oder geografisch verknüpft sind, werden als logische Interdependenzen beschrieben. (vgl. RINALDI S. M. et al. 2001: 14-16)

4.2.2 Umfeld

Im Umfeld von einer Infrastruktur können eine Vielzahl von Verknüpfungen mit anderen auftreten. Abhängigkeiten können wirtschaftlicher oder geschäftlicher Natur sein. Die öffentliche Ordnung sowie rechtliche und regulatorische Belange können Interdependenzen hervorrufen. Aspekte der öffentlichen Gesundheit und Sicherheit, wie z.B. Schutz von Menschenleben sowie Eigentum gehören ebenfalls zu dieser Dimension. Staatliche Investitionsentscheidungen wäre ein weiterer wichtiger Faktor, der berücksichtigt werden muss. (vgl. RINALDI S. M. et al. 2001: 16-18)

4.2.3 Verbindungen und Reaktionsverhalten

Koppelungen von zeitabhängigen Prozessen zwischen Infrastrukturen werden als enge Verbindungen gekennzeichnet, entsprechend verbreiten sich Störungen schnell. Dem gegenüber werden lose Verbindungen nur schwache Beeinträchtigungen verursachen. Werden mehrere Infrastrukturen untereinander verbunden, dann besteht entweder eine direkte Verbindung von Infrastruktur A zur Infrastruktur B oder eine indirekte Verbindung von Infrastruktur A, über Infrastruktur B zur Infrastruktur C. Rückkopplungsschleifen n-ter Ordnung können entstehen, wenn die Kette der Infrastrukturen folgendermaßen verbunden ist: $A > B > C > \dots > A$. Erwartet und vertraute Verknüpfungen werden als lineare Interaktionen bezeichnet, wohingegen ungeplante, ungewohnte und unerwartete Abläufe als komplexe Interaktionen bezeichnet werden. Eigenschaften von Prozessen, aus denen sich Infrastrukturen zusammensetzen, werden im Falle von Belastungen oder Störungen bestimmen, ob die Infrastruktur anpassungsfähig oder unflexibel ist. (ebd.: 18-20)

4.2.4 Charakteristik der Infrastruktur

Räumliche Parameter können in Infrastrukturen sehr unterschiedlich sein. Innerhalb einer Infrastruktur werden die einzelnen Elemente Bauteil-Einheit-Teilsystem-System zum räumlichen Faktor gezählt. Im Umfeld von Infrastrukturen werden anschließend noch die Interdependenzen zu anderen Infrastrukturen berücksichtigt. Zeitliche Faktoren werden abhängig deren Beeinträchtigungsausmaß mit sehr kleinen Werten oder ganz großen Werten angegeben. Diese zeitlichen Faktoren werden abhängig von der Größenordnung bei Simulationen berücksichtigt oder sie sind möglicherweise nicht relevant. Betriebsverfahren, Sicherheitsrichtlinien, Backups und redundante Systeme, Notfallpläne, regelmäßige Überprüfungen, Aus- und Weiterbildung werden als betriebliche Faktoren bezeichnet. Unternehmenspolitik und -motivation werden in organisatorischen Erwägungen zusammengefasst. (ebd.: 21)

4.2.5 Betriebszustand

Zur Dimension Betriebszustand wird der normale Ablauf von Prozessen unter normalen Betriebsbedingungen verstanden. Aber auch die Störungen und extremen Belastungen sowie die Reparaturen und Instandsetzungen werden in diesem Faktor berücksichtigt. (ebd.: 22)

4.2.6 Störungen

In Infrastrukturen können Störungen unterschiedlicher Art auftreten. Diese verursachen Einschränkungen in der Funktionsfähigkeit. Bestehen zwei unabhängige Störungen in zwei unterschiedlichen Infrastrukturen und die bestehende Störung der einen Infrastruktur die unabhängige Störung der anderen Infrastruktur verschlimmert, dann wird das als eskalierender Ausfall bezeichnet. Werden zwei oder mehr Infrastrukturnetze gleichzeitig betroffen liegt eine Störung mit gemeinsamer Ursache vor. (vgl. RINALDI S. M. et al. 2001: 22)

Zusätzlich zu den anderen beiden Störungen wird noch die Kaskadenstörung zur Dimension Störungen gezählt.

„Ein Kaskadenstörung liegt vor, wenn eine Störung in einer Infrastruktur den Ausfall einer Komponente in einer zweiten Infrastruktur verursacht, was wiederum eine Störung in der zweiten Infrastruktur verursacht“ (RINALDI S. M. et al. 2001: 22).

4.3 Kaskadeneffekte

Gemäß der vorherigen Definition von RINALDI S. M. et al. (2001: 22) wird das Ausmaß der Infrastrukturinterdependenzen unter anderem als Menge der Verbindungen zwischen Infrastrukturen beschrieben. Auswirkungen einer Infrastruktur können dem entsprechend Auswirkungen auf mehrere Infrastrukturen verursachen und dabei weitreichende wirtschaftliche Störungen verursachen. Wie in Abbildung 18 dargestellt, werden Störungen sich über viele Infrastrukturen, über den geografischen Raum und über die Zeit hinaus ausbreiten und durch die Abhängigkeit der Infrastrukturen „Kaskaden“-artig entwickeln. (vgl. EHLEN M. und VARGAS V. 2013: 6)

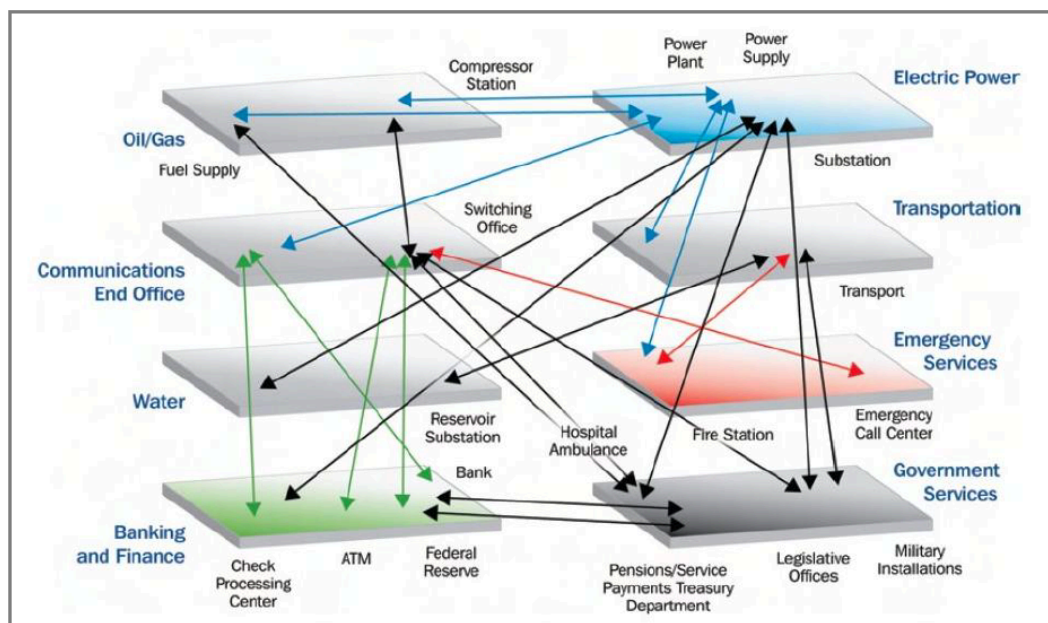


Abbildung 18: Interdependenzen kritischer Infrastrukturen (Quelle: Ehlen M. und Vargas V. 2013: 6)

Kaskadenartige Ausfälle werden durch ein oder mehrere Ereignisse ausgelöst. Die Ursache dafür liegt meistens im Ausfall von einzelnen Komponenten (Prozessen oder Ressourcen) in einer oder mehreren Infrastrukturen. Durch diese auslösenden Ereignisse werden die Infrastrukturnetze beeinträchtigt. (vgl. HINES P. et al. 2017: 2)

Abgeleitet aus diesen Quellen, müssen Kaskadeneffekte intern wie extern von Organisationen analysiert werden. Hierzu kann auf die Verfahren von Business Continuity Management und Risikomanagement zurückgegriffen werden. Auch wenn solche Systeme öfters in kritischen Infrastrukturen eingesetzt werden, betrachten sie aber meistens nur individuelle Bedrohungen und selten die Abhängigkeiten zu anderen Infrastrukturen oder internen Prozessen. Ein mögliches Modell zur Untersuchung der Kaskadeneffekte ist das CERBERUS-System, welches nachfolgend beschrieben wird. (vgl. SCHAUER S. et al. 2018: 314)

4.3.1 CERBERUS-System

Im CERBERUS-System (Abbildung 4) werden einerseits statische Daten und andererseits dynamische Daten innerhalb eines Infrastrukturnetzwerkes oder einer Infrastruktur identifiziert und in einem hybriden Simulationsmodell verarbeitet. Dadurch kann eine ganzheitliche Risikobetrachtung durchgeführt werden. Hierzu werden die Ergebnisse strukturiert ausgewertet und für die dynamische Aufbereitung graphisch in einem Netzwerkmodell dargestellt. (ebd.: 313)

Das CERBERUS-System wurde für 2 Hauptanwendungen entwickelt. Zum einen können Behörden das System nutzen um kritische Infrastruktur-Netzwerke zu analysieren und bei Vorfällen im Netzwerk können Ausfälle simuliert werden. Zum anderen können Betreiber kritischer Infrastrukturen das System nutzen, um Abhängigkeiten von verschiedenen Prozessen, Ressourcen, Bereichen, Standorten und externen Partner zu analysieren. In der vorliegenden Arbeit wird der Prozess „Aufbereitung von Medizinprodukten“ innerhalb der fiktiven kritischen Infrastruktur Krankenhaus analysiert. (ebd.: 320)

Zur Ausführung der CERBERUS Systemarchitektur werden von den nachfolgenden Komponenten Hauptaufgaben wahr genommen.

- **Datenbereinigung**

Damit Daten nutzbar werden, müssen sie im Vorfeld gesammelt werden. Hierzu wird Expert*Innenwissen benötigt und idealerweise werden die gesammelten Daten im Konsens definiert und beschrieben. Dafür wird im Anschluss an die Datenbeschaffung eine Datenbereinigung durchgeführt, um so die Unsicherheiten der Informationen zu verringern. (ebd.: 315)

- **Modellierung**

Je mehr Daten gesammelt werden, um so präziser wird die Modellierung ausgeführt. Die benötigten Modellparameter werden zusammen mit Expert*Innen abgeschätzt. (ebd.: 315)

- **Statische Risikoanalyse**

Für die Risikoanalyse von einzelnen Komponenten wird auf die grundlegenden Charakteristiken der Komponenten zurückgegriffen und auf der Basis von Expert*Innenwissen werden die Risikobewertungen durchgeführt.

In der aktuellen Arbeit, wird die CERBERUS Risikoanalyse (vgl. SCHAUER S. et al. 2018: 315-317) nicht in jedem Detail übernommen, sondern dient als

Orientierungshilfe. D.h. im Konkreten wurde keine GAP-Analyse zwischen Maßnahmen und Gefährdungen durchgeführt, sondern es wurde eine Business Impact Analyse (siehe Kapitel 7.3) angewendet um die gefährdeten Komponenten zu bestimmen und zu bewerten. Hierzu wurde jede kritische Komponente, ob Prozess oder Ressource, identifiziert und beschrieben. An Stelle des Reifegrades wurde hier die Robustheit beschrieben und je robuster die Komponente umso geringer die Ausfallmöglichkeit. Für die Bewertung der möglichen Schäden wurde ein Ansatz mit vier Schadensklassen (operative, finanziell, legale und imageschädigend) gewählt. Je Schadensklasse können die Komponenten auf drei Zustände (managebar-verwaltbar, signifikant, kritisch) bewertet werden. Für die zeitliche Bewertung wurde auf die klassische BIA-Parameter Recovery Point Objective (RPO), Recovery Time Objective (RTO) und die Maximum Tolerable Period of Disruption (MTPD) zurückgegriffen. Für die theoretische Beschreibung der Business Impact Analyse wird auf das Kapitel 7.3 und für die praktische Ausführung der Risikoanalyse auf Kapitel 3.4 verwiesen.

- **Dynamische Risikoanalyse inkl. Simulation**

Die Abhängigkeiten aus dem statischen Risikomodell können auch für das dynamischen Risikomodell genutzt werden. Bei der dynamischen Risikoanalyse wurde ein graphentheoretischer Ansatz gewählt, bei dem in der aktuellen Arbeit Komponenten als Knoten und die Abhängigkeiten als gerichtete Kanten dargestellt werden. Wobei jeder Knotenpunkt und jede Kante mit den gesammelten Informationen und Bewertungen parametrisiert werden müssen.

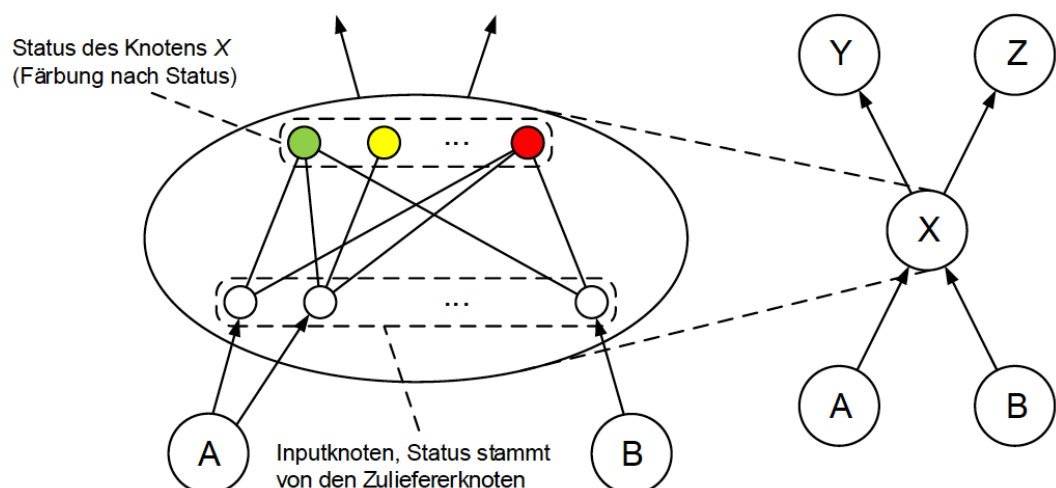


Abbildung 19: Schematische Darstellung des CERBERUS Modells (Quelle: SCHAUER S. et al. 2018: 318)

Das Besondere am CERBERUS-System ist die Darstellung und Bewertung von Knoten mit drei verschiedenen Beeinträchtigungsgraden. Bei der Simulation werden die Statusübergänge durch einen stochastischen Prozess ausgeführt.

Somit können die Auswirkungen eines Ausfalls von einer oder mehreren Komponente(n) auf die anderen Komponenten simuliert und ausgewertet werden. Besonderes Augenmerk wurde auf die Tatsache gelegt, die Balance zwischen Komplexität und Ausdrucksstärke zu gewähren ohne eine zu große

Anzahl an Parametern einstellen zu müssen. Im Modell werden zusätzlich stochastische und deterministische Abhängigkeiten beschrieben.

Abbildung 19 werden die verschiedenen Zustände der Knoten dargestellt. Die Knoten können Prozesse, Ressourcen, Teilbereiche, Abteilungen, Standorte oder eine ganze Infrastruktur simulieren. Die Auswirkung der Knoten kann in drei Zuständen „grün“ - managebar, „gelb“ – signifikant und „rot“ – kritisch gekennzeichnet werden. Die Inputknoten werden mit einem dieser drei Zuständen initiiert. Wird dabei ein Inputknoten in den „gelben“ oder „roten“ Zustand übergehen, so werden die Auswirkungen auf die nachfolgenden Knoten abhängig der Parametrierung den Zustand anpassen. Da die Folgen nur wahrscheinlich vorhergesagt werden können, werden sie durch Zufallsvariablen beschrieben. Zustandsänderungen in der Infrastruktur werden sich dann nur nach einer gewissen Wahrscheinlichkeit ändern. Dafür wird auf eine stochastische Simulation mit Markov-Ketten zurückgegriffen.

Markov-Ketten werden zu den Simulationsprozessen einer schwach ausgeprägten Abhängigkeitsstruktur gezählt und werden als ein wichtiges Analyseinstrument betrachtet. Dadurch werden sie in unterschiedlichen Bereichen zur Klärung von u.a. ökonomischen, technischen und naturwissenschaftlichen Fragestellungen eingesetzt. (vgl. ebd.: WALDMANN K.-H. und HELM W. E. 2016a: 219)

Sind Knoten abhängig von multiplen Kanten, können die Knoten verschieden Zustände annehmen. Auf Grund von mehreren Möglichkeiten, wird nur der schlimmste Zustand (worst case) an die folgenden Knoten weitergeleitet. In der vorliegenden Arbeit wird für die stochastische Simulation auf die identisch funktionierende SAURON Propagation Engine zurückgegriffen (siehe Kapitel 4.3.2). Die Simulation kann mit einem bestimmten Ereignis initiiert werden. Im konkreten Fall für diese Arbeit wird eine Überschwemmung vom 2. Kellergeschoss und ein Cyber-Angriff simuliert. (vgl. SCHAUER S. et al. 2018: 317-318)

- **Ergebnisauswertung und Visualisierung**

Bedingt durch die unterschiedlichen Ansätze, können die Ergebnisse der beiden Risikoanalysen nicht verglichen werden. Durch die Anwendung der Business Impact Analyse in der Software bclIMPACT, wird für die statische Risikoanalyse das Ergebnis in der Software in einer Tabellenform inkl. der BIA-Faktoren dargestellt (siehe Kapitel 8.4). Mit der Anwendung der SAURON Propagation Engine werden die Abhängigkeiten in der dynamischen Risikoanalyse in einer Netzwerkgraphik dargestellt. Als Resultat der Szenario basierten Simulation wird eine Tabelle mit den wahrscheinlichen Ausfällen oder Beeinträchtigungen von Ressourcen angegeben (siehe Kapitel 8.5).

4.3.2 SAURON-Rahmenwerk

In der Vergangenheit kam es immer wieder zu Bedrohungen von kritischen Infrastrukturen. Auch waren hier Gesundheitssysteme oder Krankenhäuser betroffen (siehe Kapitel 6.4). (vgl. SCHAUER S. et al. 2019: 191)

Aus den eigenen Erfahrungen des Autors werden in Krankenhäusern zunehmend Gefahrenmanagementsysteme eingesetzt um die physische Sicherheit der Krankenhausinfrastruktur zu sichern und zu überwachen. In diesen Gefahrenmanagementsystemen werden u.a. Brandmeldeanlagen, Zutrittskontrollsysteme, Einbruchmeldeanlagen, Videoüberwachungsanlagen, Fluchtwegemanagementsysteme, Gebäudeleittechnik (Überwachung und Steuerung der technischen Versorgungsanlagen), Alarmkommunikationsserver eingebunden und an einer zentralen Leitwarte überwacht. Das Gleiche gilt für die Informationstechnik (IT), hier werden Cyber-Überwachungssysteme mit Monitoring-Systemen zur Überwachung des Netzwerkverkehrs, der Netzwerk-Eindringung durch Fremde der Serverlandschaften mittels Logfile Analyse eingesetzt. Die Überwachung der physischen und wie auch der Cyber-Systemen wird jedoch meistens eigenständig ausgeführt, ohne dass die Überwachung in kombinierter Art und Weise erfolgt.

Das SAURON-Rahmenwerk (Abbildung 20) wurde für die kombinierte Überwachung von physischen wie auch Cyber-Angriffen in kritischen Infrastrukturen entwickelt. Im physischen Sicherheitssystem werden alle möglichen Daten aus verschiedenen Quellen (Videoüberwachung, Zutrittskontrolle, Brandmeldung, ...) der Gebäudesicherheit gesammelt, geo-lokalisiert und ausgewertet. Bei Anomalien werden durch die Mensch-Maschine Schnittstelle (HMI) Alarmmeldungen visualisiert. Diese werden von technischem Überwachungspersonal aufgenommen und anschließend werden die relevanten Stellen gewarnt. Ebenfalls werden diese Informationen an die hybride Sicherheitsplattform zur weiteren Untersuchung und Bewertung weitergeleitet. (vgl. SCHAUER S. et al. 2019: 194-195)

Im Cyber-Sicherheitssystem werden analog zum physischen Sicherheitssystem Daten aus den unterschiedlichsten Sensorquellen (Netzwerke, Servern, Datenspeicherungssystemen, ...) gewonnen. Diese Daten werden verarbeitet und analysiert bevor Warnmeldungen zu eventuellen Störungen/Ereignissen über die Mensch-Maschinen Schnittstelle an das IT-Überwachungspersonal übertragen. Auf Basis dieser Warnmeldungen werden weitere Schritte zur Eliminierung der Störung vorgenommen. Gleichzeitig werden die Informationen und Daten an die hybride Sicherheitsplattform zur weiteren Analyse gesendet. (vgl. SCHAUER S. et al. 2019: 195-196)

In der hybriden Sicherheitsplattform werden die Daten auf bestehenden Interdependenzen untersucht und bewertet. Als Hauptziel werden kaskadenartige Auswirkungen in beiden Sicherheitssystemen aufgezeigt. Mit dem SAURON Rahmenwerk können kombinierte Angriffe auf eine Infrastruktur erkannt werden. In der hybriden Sicherheitsplattform werden die Daten in einer „Event Correlation Engine“ analysiert und bewertet. Für die Identifizierung, Bewertung und Analyse der Kaskadeneffekte wird die „Threat Propagation Engine“ eingesetzt. Die Propagation Engine, welche im SAURON Rahmenwerk eingesetzt wird, basiert auf der

graphenorientierten, stochastischen Simulationskomponente mit Knoten und Kanten wie bereits im CERBERUS-System bereits beschrieben (siehe 4.3.1). Die Ergebnisse in Form einer Liste der betroffenen Komponenten mit den Angaben über die Wahrscheinlichkeiten von Auswirkungen werden dem Sicherheitspersonal über die Mensch-Maschine Schnittstelle übermittelt. Durch das Sicherheitspersonal werden anschließend Maßnahmen zur Schadensbegrenzung eingeleitet. (vgl. SCHAUER S. et al. 2019: 196-198)

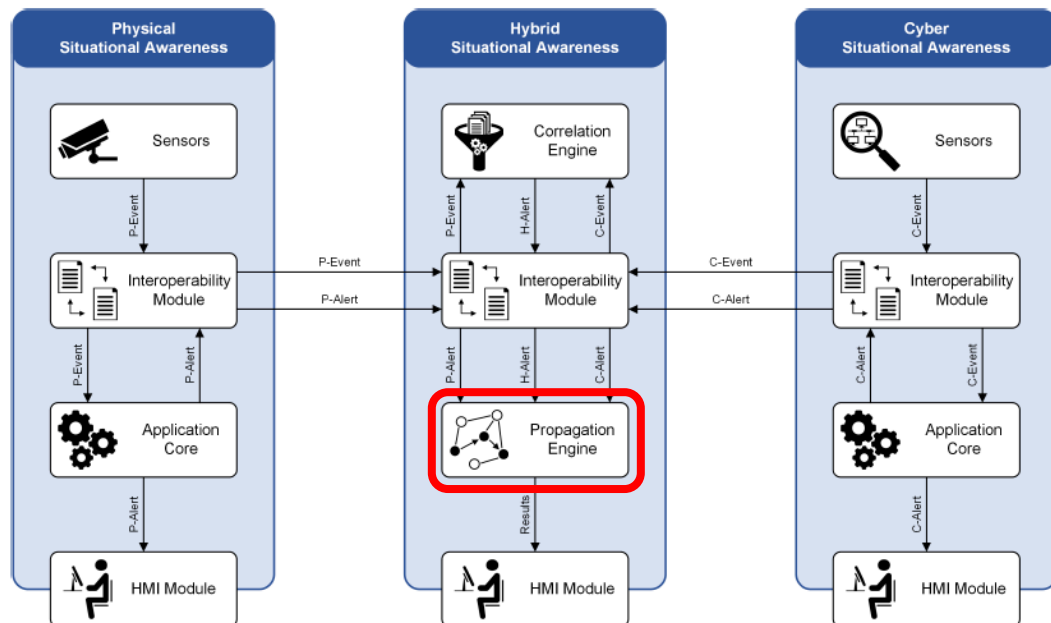


Abbildung 20: SAURON Rahmenwerk mit der Propagation Engine (Markierung) (SCHAUER S. et al. 2019)

Aus diesem Ansatz heraus und durch die vermehrte Anwendung von physischen, wie auch Cyber-Systemen in der kritischen Infrastruktur Krankenhaus, wurde in der vorliegenden Arbeit die SAURON Propagation Engine für die Simulation in der dynamischen Risikoanalyse aus der CERBERUS-Systemarchitektur eingesetzt.

Nach der Vorstellung der Methodik für die vorliegende Master Thesis werden in den anschließenden Kapitel 4 bis 7 die theoretischen Ansätze beschrieben.

5 Digitalisierung und Cyber-physische Systeme

5.1 Vierte industrielle Revolution, Cyber-physische Systeme und Gesellschaft 4.0

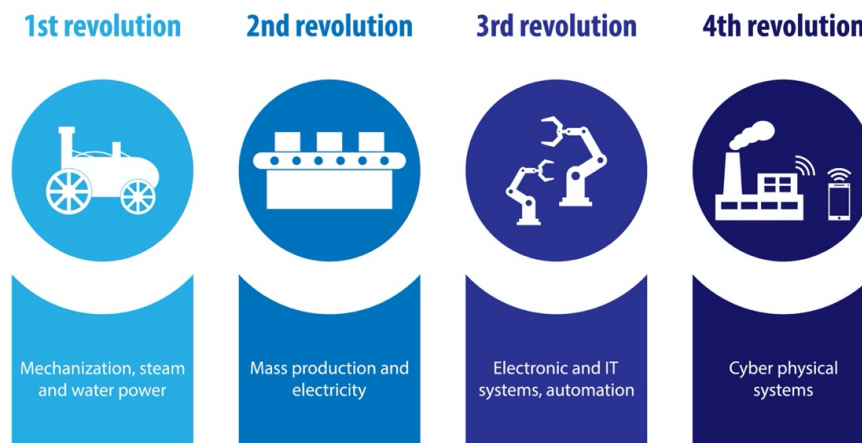


Abbildung 21: Industrial revolution (Quelle Shutterstock)

In westlichen Ländern gab es ab dem 18. Jahrhundert mehrere größere Veränderungen (Abbildung 21). Während der ersten Revolution wurden wasserkraft- oder dampfbetriebene Maschinen entwickelt. Diese wurden als Grundvoraussetzung für die Massenproduktion benötigt. Während der zweiten Revolution wurde für die Erweiterung der Massenproduktion, die elektrische Energie für die Nutzung der Maschinen weiterentwickelt. In der dritten Revolution wurde vorrangig die Informationstechnologie zur Steigerung des Automatisierungsgrades in der Produktion eingesetzt. Die vierte industrielle Revolution (vgl. MAIER G. n. W. et al. 2020: 4-5) wird durch den vermehrten Einsatz von Cyber-physischen Systemen gekennzeichnet. Die vernetzten technischen Systeme werden immer autonomer.

Die Digitalisierung kann in zwei Zeitsparten eingeteilt werden. Zum einen die 80er und 90er Jahre, in welchen das klassische Internet öffentlich nutzbar wurde. Das „Internet der Personen“ entwickelte sich zu einer weltweiten Vernetzung in dem Menschen ortsunabhängig miteinander virtuell kommunizieren konnten. In der heutigen Zeit werden IT-Netzwerke und physische Komponenten vermehrt vernetzt und interagieren im „Internet der Dinge“ zusammen. Die Vernetzung der Gesellschaft wird immer weiter vorangetrieben. (vgl. MAINZER K. 2020: 167)

Wie in Abbildung 22 dargestellt, bestehen im Übergang der mechatronischen Systeme zum Cloud-basiertem Internet der Dinge, die cyber-physischen Systeme hauptsächlich aus

- Aktuatoren und elektromechanischen Systemen (physisch) sowie
- Steuerelektronik und Sensoreinheiten (cyber).

Das Cyber-System wie auch das physische System werden in einander integriert und interagieren zusammen als ein CPS-System. Mit der notwendigen Kommunikation zu

der Außenwelt erhöht sich auch das Potential für einen externen böswilligen Angriff. (vgl. JAMALUDIN J. und ROHANI J. 2018: 1-2)

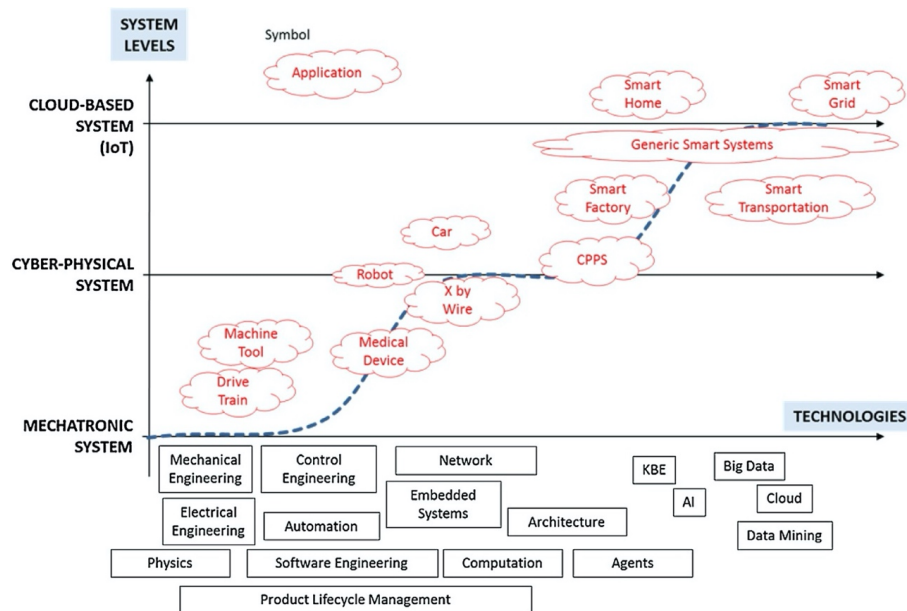


Abbildung 22: Transition process from Mechatronics to CPS to Internet of Things (Quelle: HEHENBERGER P. et al. 2016: 274)

Der Begriff cyber-physische Systeme wurde zu Beginn des 21. Jahrhunderts entwickelt. (vgl. TAHA W. et al. 2020: 5 & 9)

„Der Begriff cyber-physische Systeme bezieht sich auf eine neue Generation von Systemen mit integrierten rechnerischen und physischen Fähigkeiten, die über viele neue Modalitäten mit dem Menschen interagieren können“ (BAHETI R. und GILL H. 2011: 1).

In cyber-physischen Systemen (Abbildung 23) werden neben den rechnerischen und physischen Fähigkeiten auch kommunizierende so wie vernetzte Fähigkeiten integriert. (vgl. TAHA W. et al. 2020: 5)

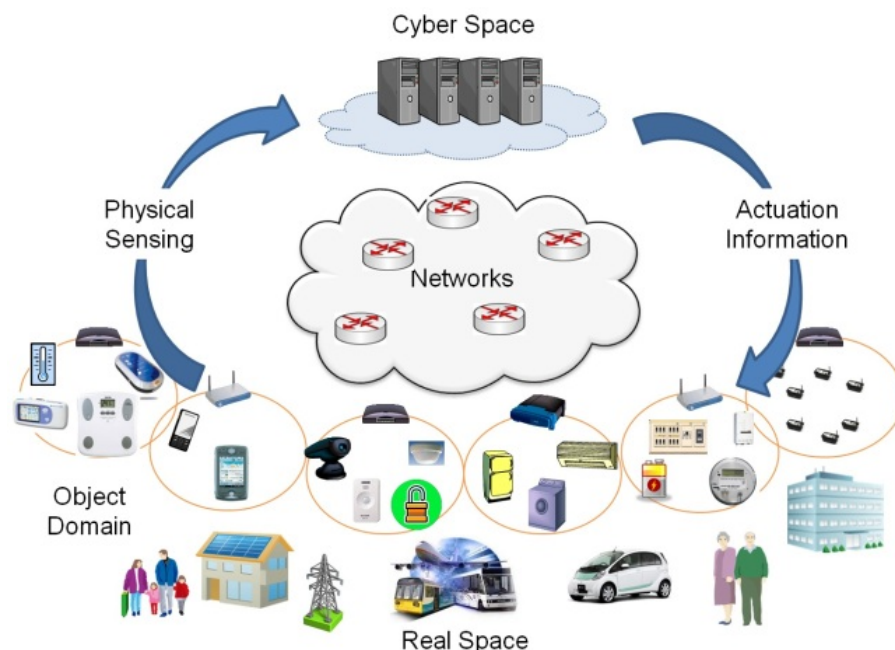


Abbildung 23: Cyber-Physical System (Quelle: EROARKE 2014)

Im Rahmen der Gesellschaft 4.0 werden im Folgenden verschieden relevante cyber-physische Konzepte vertieft.

Die intelligente Mobilität (Smart Mobility) setzt sich aus mehreren intelligenten Mobilitätsinnovationen zusammen (Abbildung 24). (vgl. MARSDEN G. und REARDON L. 2018: 2-4) Die Elektrifizierung von Fahrzeugen, autonome Fahrzeuge, mobilen Endgeräten für die Navigation mit einer Datenübertragung und Kommunikation in beide Richtungen sind nur einige angewandte cyber-physische System. Aber auch in innovativen Konzepten wie das Nutzen von Fahrzeugen, statt deren Besitz, müssen intelligente Infrastrukturen auf Basis von cyber-physischen Systemen mit allen Akteuren interagieren. Fahrzeuge werden heutzutage als mobile Endgeräte in Mobilitätsnetze eingesetzt. (vgl. MAINZER K. 2020: 168) Fahrzeuge werden längst nicht mehr nur aus mechanischen und elektrischen Komponenten hergestellt, sondern werden immer mehr zu Computern auf Rädern mit einer Vielzahl von Sensoren und Aktuatoren zur Überwachung, Automatisierung und autonomer Steuerung der Fahrt.

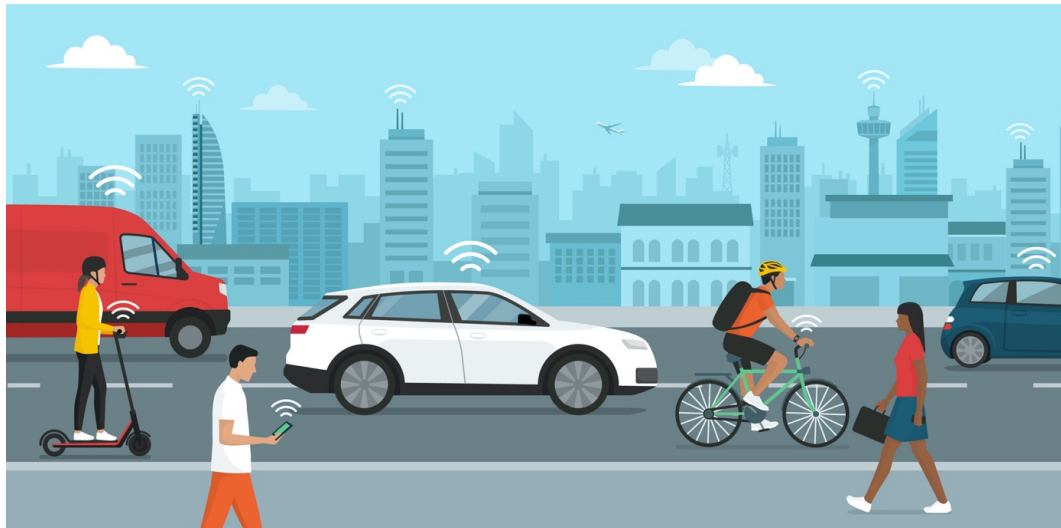


Abbildung 24: Smart Mobility (Quelle Shutterstock)

Unter intelligente Stromnetze (Smart Grids) (vgl. MAINZER K. 2020: 168) werden die intelligente Vernetzung zwischen elektrischen Erzeugungssystemen und Endverbrauchern verstanden. Wie in Abbildung 25 dargestellt, bildet der grüne Bereich die Stromproduktion mit den unterschiedlichsten Kraftwerkstypen ab und der blaue Bereich wird durch die verschiedensten Verbraucher charakterisiert. Im Zentrum des intelligenten Netzwerkes werden die Kontrollzentren mit Überwachungs-, Steuerungs- und Kommunikationssystemen, zur Gewährleistung der Energieversorgung, betrieben. Die Kombination von komplexen physischen Netzwerksystem und den Cyber-Systemen ist eine Voraussetzung, damit die intelligente Stromverteilung länderübergreifend funktionieren kann. Bedingt durch die Zunahme der vielen kleineren dezentralen Stromproduzenten und Endverbraucher sowie den großen Produktionskraftwerk und den Großkunden müssen die Stromflüsse bidirektional gesteuert werden können. Daraus resultiert, dass die Interaktionen zwischen den physischen Netzwerksystemen und die Cyber-Systeme ausgebaut werden müssen. Auch werden Simulationen eingesetzt um die Stromproduktion vorausschauend zu planen. Hierfür wird auf cyber-physische Systeme wie Sensoren, Informations- und Kommunikationstechnik zurückgegriffen, um die benötigten Daten für die Simulation in Echtzeit bereit zu stellen. (vgl. YU X. und XUE Y. 2016: 1058-1059; 1061)

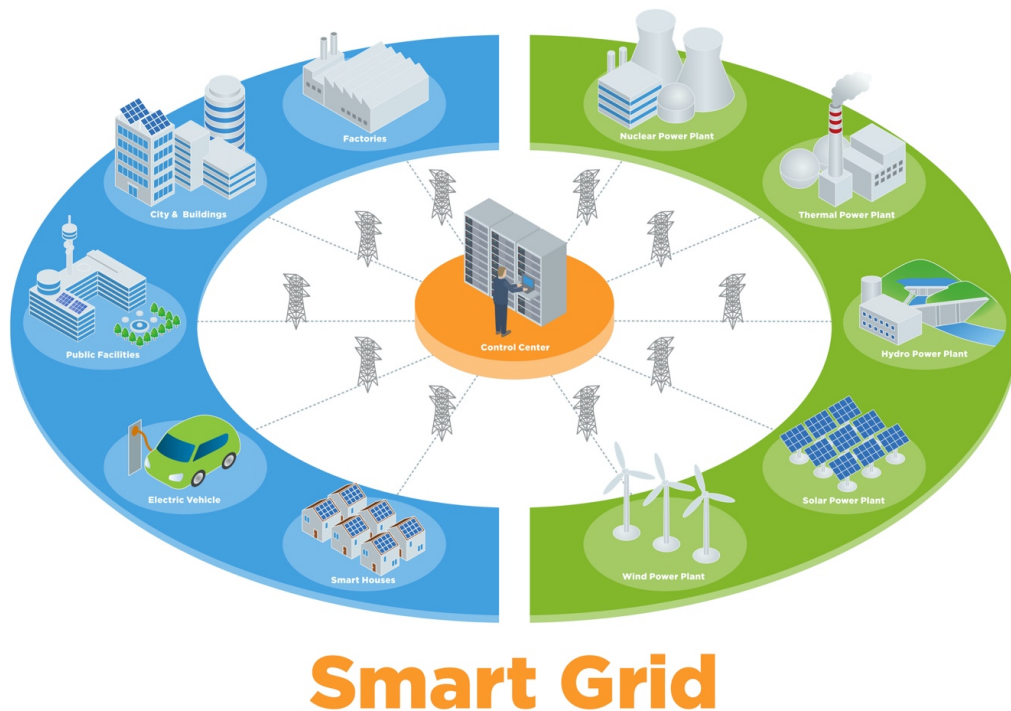


Abbildung 25: Smart Grid (Quelle: Shutterstock)

Die Verknüpfung von unterschiedlichen cyber-physischen Systemen wie u.a. Smart Mobility und Smart Grid zu einem übergeordneten Netzwerk (Abbildung 26), entspricht dem Ursprung für eine intelligente Stadt (Smart City).

„Eine Smart City setzt systematisch digitale Technologien ein, um den Ressourceneinsatz zu reduzieren, die Lebensqualität der Menschen zu verbessern und die Wettbewerbsfähigkeit der regionalen Wirtschaft nachhaltig zu steigern. Sie beinhaltet den Einsatz intelligenter Lösungen für Infrastruktur, Energie, Wohnen, Mobilität, Dienstleistungen und Sicherheit, die auf integrierter Sensorik, Konnektivität, Datenanalyse und eigenständig funktionierenden Wertschöpfungsprozessen basieren“ (GASSMANN O. et al. 2019: 25).

In einer intelligenten Stadt werden alle Lebenssituationen der Bewohner durch die vernetzten Systeme beeinflusst. (vgl. GASSMANN O. et al. 2019: 61).

Zur intelligenten Stadt gehört auch das intelligente Gesundheitssystem „Smart Health“ und in diesem sind wiederum intelligente Krankenhäuser „Smart Hospital“ ein Bestandteil. Im Folgenden wird die kritische Infrastruktur Krankenhaus 4.0 näher betrachtet.



Abbildung 26: Smart City (Quelle Shutterstock)

5.2 Digitalisierung in kritischen Infrastrukturen – Krankenhaus 4.0

Die Informationstechnologie und die Digitalisierung sind allgegenwärtig und stellen einen Megatrend in unserer Gesellschaft dar. Alle Bereiche der Gesellschaft sind betroffen und sie durchdringen alle Segmente einer Organisation. (vgl. PRITI S. 2017: 12); (vgl. DEITERS W. et al. 2018: 1031)

„Steigende Anforderungen an Speicherung, Datenschutz, Verarbeitungsprioritäten und Berichtswesen haben die Anwendung neuer Technologien (Virtualisierung, Cloud Computing, mobile Geräte und soziale Netzwerke) mit sich gebracht, die neue Herausforderungen, Risiken und Chancen mit sich bringen, die entweder angegangen oder genutzt werden müssen“ (PRITI S. 2017: 13).

Im intelligenten Krankenhaus (Smart Hospital) werden immer mehr medizintechnische Insellösungen zu standardisierten, offen vernetzten Systemen (Abbildung 27). In Krankenhäusern werden Algorithmen, Daten und Sensoren eingesetzt um die Patientenversorgung durch Ärzte und Pfleger sowie mit Hilfe von medizintechnischen Geräten und Dienstleistungen aufeinander abzustimmen. (vgl. MAINZER K. 2020: 167) Dabei werden sensible Patientendaten in zentralen Datenbanken gespeichert und über unterschiedliche Kommunikationswege internen wie externen Nutzern zur Verfügung gestellt. Medizintechnische Geräte werden durch die Vernetzung untereinander interagieren und die Daten können schneller verarbeitet werden, wodurch neue Möglichkeiten und Herausforderungen für den Gesundheitssektor entstehen. Hierfür steht u.a. nachfolgende Auflistung (vgl. BAHETI R. und GILL H. 2011: 3-4): Bildgesteuerte Operationen, neuronal gesteuerte Prothesen, auf den Patienten angepassten intelligente medizintechnischen Geräte, intelligente Operationssäle mit vernetzten Infusionspumpen, Beatmungsgeräten inkl. Sauerstoffzufuhr, vernetzte Sensoren zur Überwachung des Patienten. (vgl. JAMALUDIN J. und ROHANI J. 2018: 4)



Abbildung 27: Smart Hospital (Quelle Shutterstock)

Zur Darstellung der Digitalisierung in kritischen Infrastrukturen wird im nachfolgenden auf die Ausarbeitung der Krankenhausgesellschaft Nordrhein-Westfalen näher eingegangen.

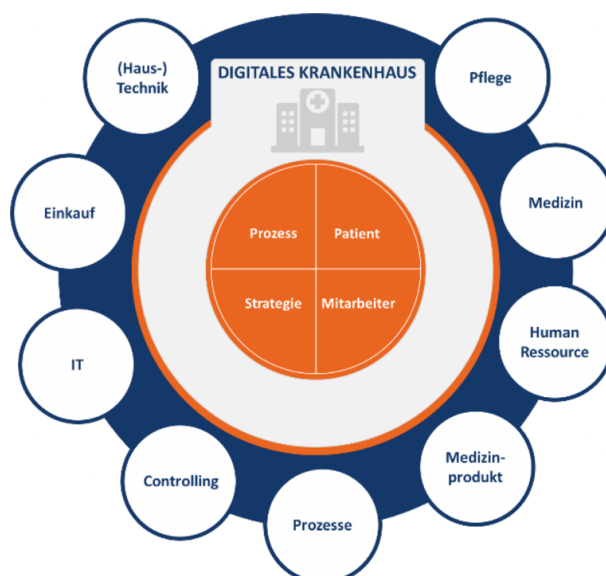


Abbildung 28: Kompetenzen des selbstbestimmten, souveränen digitalen Krankenhauses (Quelle: BURMANN A. et al. 2019: 10)

In der Digitalisierung im Krankenhaus ist die Radiologie ein Vorreiter. Hier werden die Aufnahmen digitalisiert, archiviert und den Endnutzern mit Hilfe von Visualisierungssoftware angezeigt (vgl. DEITERS W. et al. 2018: 1032). Mit dem Einsatz der vernetzten Technologien und der Kommunikation in Echtzeit wurde das Zeitalter Krankenhaus 4.0 eingeläutet (vgl. JUHRA C. und BORN J. 2020: 1038).

Um den Anforderungen an das Krankenhaus 4.0 gerecht zu werden hat die „Healthcare Information an Management Systems Society (HIMSS) Europe“ ein Model Namens „Electronic Medical Record Adoption Model (EMRAM)“ entwickelt. Seit 2015

(vgl. JUHRA C. und BORN J. 2020: 1039-1041) ist dieses Modell zum weltweiten Standard geworden. Krankenhäuser werden entsprechend dem Grad der Digitalisierung in 7 Stufen eingeteilt. Diese reichen von der Stufe 0, wo die Abteilungen Labor, Apotheke und Radiologie noch nicht mit informatischen Hilfsprogrammen ausgestattet sind über die Stufe 4 wo 50% aller medizinischen Anordnungen elektronisch erfasst werden und wo die Dokumentation der Patientenakte zu 90% erreicht wird, zu der letzten Stufe 7 wo keine Patientendaten zur Patientenversorgung mehr auf Papier verwaltet werden und klinische Informationen können über standardisierte elektronische Transaktionen mit Einrichtungen, Behörden oder anderen Stakeholder ausgetauscht werden.

Der digitale Wandel wird früher oder später in die Krankenhäuser einziehen. Bereits jetzt werden immer mehr informatische Systeme in der Patientenversorgung eingesetzt. Die medizinischen Daten werden in zentralen vernetzten Datenbanken archiviert und für alle berechtigten Akteure zur Verfügung gestellt. Zu diesen informatischen Systemen gehören u.a. das RIS (Radiologie Information System), das PACS (Picture Archiving and Communication System), das KIS (Krankenhausinformationssystem), das LIS (Laboratory Information System) und vielen herstelllerspezifischen Systeme aus der Medizintechnik und Patientenversorgung. Wie in Abbildung 29 dargestellt, gehören in die durchgängige Vernetzung der Systeme ebenfalls die Versorgungs-, Logistik- und Verwaltungssysteme.

Mit zunehmender Vernetzung nehmen die Gefahren für Hacker-Angriffe deutlich zu. Im Kapitel 6 wird die Verwundbarkeit von kritischen Infrastrukturen verdeutlicht. Bei Angriffen auf digitale Systeme müssen kritische Infrastrukturen dafür sorgen, dass diese Angriffe idealerweise, nicht stattfinden oder zumindest rechtzeitig abgewehrt werden können. Nicht nur mobile Endgeräte stellen hier eine große Gefahr dar, sondern auch das Verhalten der Benutzer dieser Endgeräte kann zu Problemen führen. In einem Krankenhaus werden mobile Endgeräte von allen Akteuren (Mitarbeiter, Besucher, Patienten und externe Partner) genutzt. In öffentlichen Bereichen und insbesondere in Wartezonen, werden für die „Kundenzufriedenheit“ offenen WLAN-Zugängen zur Verfügung gestellt. Auch in den Patientenzimmern werden immer öfters WLAN-Zugänge freigeschaltet. Aus neuen Anwendungen werden neue Möglichkeiten für die Verarbeitung und Zurverfügungstellung von Daten geschaffen. Allerdings entstehen auch immer wieder neue Gefahren für Datenlecks. (vgl. JUHRA C. und BORN J. 2020: 1049-1050)

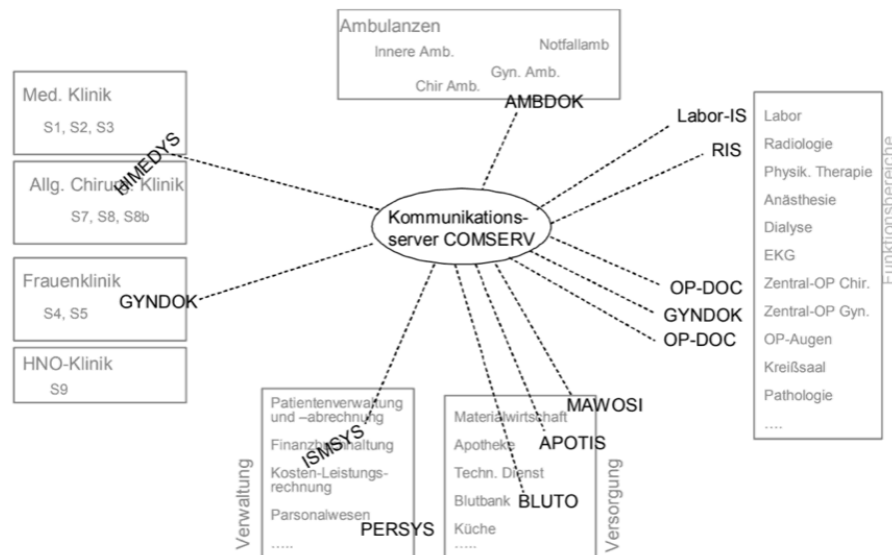


Abbildung 29: Beispiel für logisches Topologiemodell eines KIS (fiktive Produktnamen) (Quelle: HAAS P. 2005: 63)

Bedingt durch die sich ständig erweiternde vierte Revolution und der damit verbundenen Zunahme an cyber-physischen Systemen, wächst die Gefahr einer externen Bedrohung dieser Netzwerksysteme. Dadurch könnten größere Schäden mit den damit verbundenen finanziellen Verlusten entstehen. (vgl. JAMALUDIN J. und ROHANI J. 2018: 1)

Im folgenden Kapitel werden die Verwundbarkeiten, Abhängigkeiten und die Auswirkungen eingehender beschrieben.

6 Verwundbarkeiten und deren Auswirkungen

Kritische Infrastrukturen sind verwundbar und vielen Gefährdungen ausgesetzt. Wie im Kapitel 4.1 bereits beschrieben, ziehen der Teil- oder Gesamtausfall von kritischen Dienstleistungen u.a. aus dem Gesundheitswesen, der Lebensmittelversorgung, der Energieversorgung und dem Bankwesen Einschränkungen und Auswirkungen für die Bevölkerung mit sich. Es gilt diesen Gefährdungen entgegenzuwirken. Im Vorfeld müssen die kritischen Infrastrukturen sich mittels präventivem Risikomanagement auf Bedrohungen einstellen und Maßnahmen zum Schutz der kritischen Infrastruktur vorsehen.

Im Folgenden werden die möglichen Gefährdungen und Verwundbarkeiten von kritischen Infrastrukturen am Beispiel Krankenhaus dargelegt.

6.1 Gefährdungen für kritische Infrastrukturen

In der Europäischen Verordnung von 2008 zum Schutz der kritischen Infrastrukturen rät der Rat der Europäischen Union den Mitgliedsstaaten einen alle Risiken abdeckenden Ansatz anzusetzen. Und neben den Bedrohungen durch den Terrorismus auch die Gefährdungen von Menschen ausgehenden technologischen Gefahren sowie Naturkatastrophen zu berücksichtigen.

Im Februar 2018 hat die luxemburgische Regierung eine neue großherzogliche Verordnung über die Erstellung eines Sicherheits- und Betriebskontinuitätsplanes für kritische Infrastrukturen verabschiedet (ME 2018b). Neben der Charakterisierung der kritischen Infrastruktur muss der Plan Auskunft über das eingesetzte Risikomanagement zur Identifikation, Analyse, Bewertung und Minderung der Risiken sowie eine Präventionsstrategie aufzeigen. Zusätzlich wird auch eine Beschreibung des Business Continuity Planes verlangt. Für die Risikoanalyse müssen mindestens die nachfolgenden Gefahrenkategorien berücksichtigt werden:

- Natur- und Umweltgefahren (z.B.: Unwetter, Überschwemmung);
- Gesundheitsgefahren (z.B.: Pandemie);
- Gefahren technischen Ursprungs (z.B.: Prozessausfall, Ausfall Stromversorgung, Ausfall der IT-Technik);
- Intentionale Gefahren (z.B.: Cyberangriff, Sabotage, Terroranschlag). (vgl. ME 2018b: A 151 - 2)

Mit dem aktuellen Handbuch Krankenhausalarm und -einsatzplanung hat das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) den Krankenhäusern in Deutschland eine Empfehlung für die Praxis ausgegeben. In diesem Handbuch empfiehlt das BBK die nachfolgenden Gefahrenlagen im Krankenhaus zu berücksichtigen:

- Evakuierung / Räumung des Krankenhauses,
- Massenanfall von Verletzten,
- CBRN (Chemisch, Biologisch, Radioaktiv, Nuklear)
- Polizeiliche Lagen (z.B.: Amoklauf, Terroranschlag, Bombendrohung, Geiselnahme),

- Brand im Krankenhaus,
- Naturgefahren (z.B.: Hochwasser, Starkregen),
- Störungen im Krankenhaus (Ausfall IT; Ausfall Versorgungssysteme; Versorgung Telekommunikation). (vgl. BBK 2020b: 69)

Welchen Gefährdungen eine kritische Infrastruktur ausgesetzt ist, hängt ebenfalls von den lokalen Randbedingungen ab. Um alle Gefährdungen zu definieren, bedarf es einer detaillierten Risikoidentifizierung und -analyse (siehe Kap. 7.1) auch in Bezug zur Verwundbarkeit der Infrastruktur. Ausgehend vom Resultat der Risikoanalyse müssen mehr oder weniger Gefährdungen betrachtet werden.

6.2 Verwundbarkeit von kritischen Infrastrukturen

Wie im vorherigen Kapitel beschrieben ist die Digitalisierung ein zentraler Treiber für cyber-physischen Systemen und Internet der Dinge. Durch die immer stärkere Vernetzung der kritischen Infrastrukturen wird das Gesamtsystem für Cyberangriffe immer komplexer und verwundbarer. Damit die Gefahr von Ausfällen in kritischen Infrastrukturen reduziert werden kann, müssen die Betreiber der Infrastrukturen sich entsprechend aufstellen, um diese Herausforderung anzugehen. (vgl. ARETZ A. und HIRSCHL B. 2017: 14)

In diesem Kapitel wird die Verwundbarkeit von kritischen Infrastrukturen am Beispiel eines Krankenhauses erarbeitet.

Der Autor kann aus eigener Erfahrung die Aussage von PFENNINGER E. und ADOLPH O. (2017: 673) teilen. In Krankenhäusern sind oft Notfallpläne für die Evakuierung im Brandfall und die Versorgung von Verletzten bei einem Massenanfall von Verletzten (MANV) vorhanden. Werden Verantwortliche Personen der Organisationsstruktur hinsichtlich Verwundbarkeit sensibilisiert und wird ein Leiter Krankenhausalarm und -einsatzplanung (Kümmerer, Risiko- oder Business Continuity Manager) im Krankenhaus eingesetzt, wird sich ein Krankenhaus präventiv auf andere Gefährdungen vorbereiten können. (vgl. WURMB T. et al. 2018: 81)

Damit die kritische Infrastruktur Gefahrenabwehrpläne erarbeiten kann, muss sie zuerst die kritischen Verwundbarkeitsfaktoren kennen. Im komplexen System „Krankenhaus“ (vgl. HUFSCHMIDT G. 2018: 66) sind diese Verwundbarkeitsfaktoren in allen Bereichen zu finden. Durch die multiplen Ressourcen und Prozesse müssen die Abhängigkeiten in die Verwundbarkeitsanalyse eingebunden werden. Dabei gilt es nicht nur auf die eigenen internen Bereiche zu schauen, sondern auch die externen Rahmenbedingungen wie u.a. politische, sozio-ökonomische und kulturelle Faktoren zu berücksichtigen. Auch müssen die Schutzziele „Schutz von Patienten, Mitarbeitern und alle anderen Betroffenen“, „Funktionalitätserhaltung“ und „Aufrechterhaltung der Behandlungskapazität“ (WURMB T. et al. 2018: 81) für ein Krankenhaus berücksichtigt werden. Mit der wachsenden Vernetzung wächst die Ressourcenabhängigkeit und entsprechend wächst die Verwundbarkeit. (vgl. PFENNINGER E. und ADOLPH O. 2017: 673);

6.3 Abhängigkeiten

Wie bereits erwähnt ist die kritische Infrastruktur Krankenhaus multiplen Gefährdungen ausgesetzt. Diese resultieren aus vielen Abhängigkeiten. Im Kapitel 5 wurden die Abhängigkeiten von der Digitalisierung bis zum intelligenten Krankenhaus beschrieben. Neben den Cyber-physischen Abhängigkeiten bestehen im komplexen System Krankenhaus zusätzliche Abhängigkeiten.

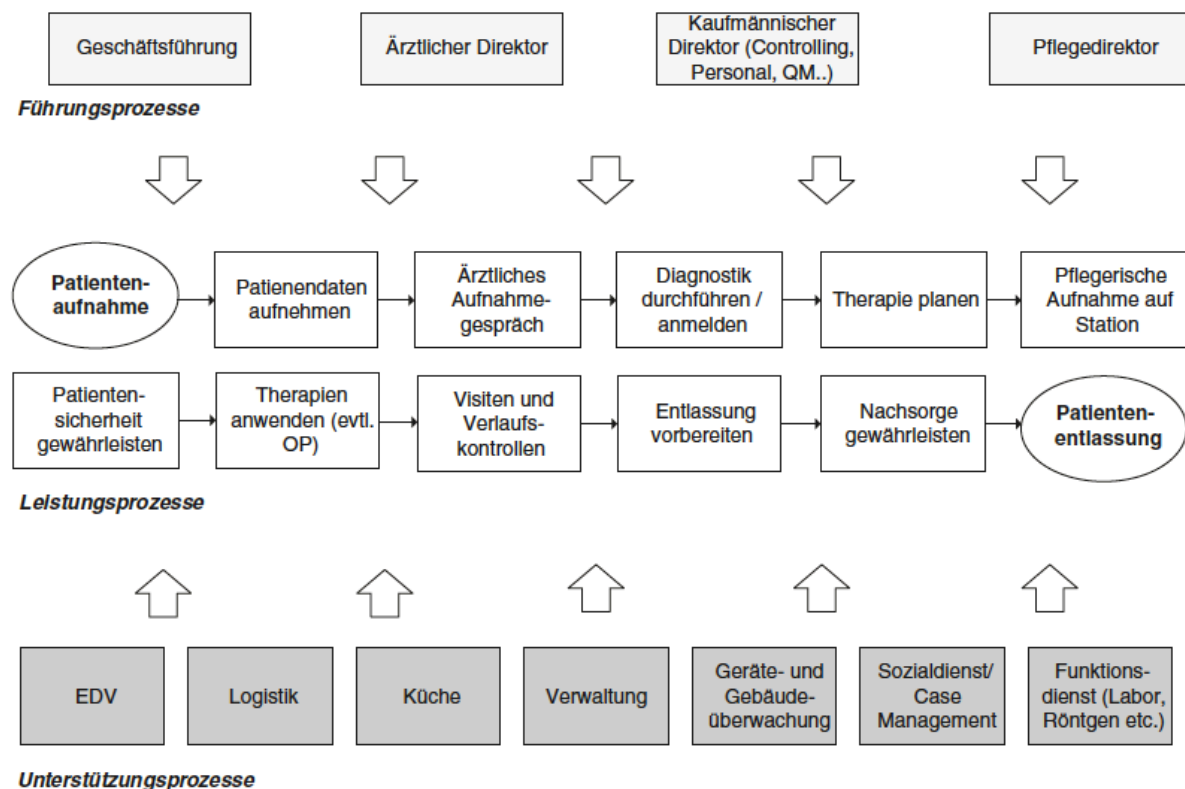


Abbildung 30: Beispiel Prozesslandschaft Krankenhaus (Quelle: KUNTSCHKE P. und BÖRCHERS K. 2017a: 108)

Um alle Abhängigkeiten in einer kritischen Infrastruktur zu bestimmen ist es wichtig alle Prozesse in der Organisation zu verstehen und deren Reihenfolge zu kennen. Eine Prozessanalyse (vgl. ANDLER N. 2015: 342) kann hier die benötigten Informationen liefern, da diese einen Einblick in das operative Geschäft gewährt. Je detaillierter eine Prozessanalyse durchgeführt wird, um so mehr Information (Abhängigkeiten) können definiert werden.

In Abbildung 30 ist eine beispielhafte Prozesslandkarte eines Krankenhauses dargestellt. Im Folgenden sind einige Abhängigkeiten beispielhaft aufgeführt:

- Trinkwasserversorgung
- Abwasserentsorgung
- Abfallentsorgung
- Lebensmittelversorgung
- Energieversorgung
 - o Stromversorgung
 - o Wärmeversorgung
 - o Kälteversorgung

- Dampfversorgung
- Informations- und Kommunikationsversorgung
- Architektonische Gegebenheiten
- Raumplanerische Gegebenheiten
- Personelle Ressourcen
 - Ärzteschaft
 - Internes Personal
 - Externes Personal
- Interne Dienstleistungen, z.B.:
 - Apotheke
 - Labor
 - Aufbereitungseinheit für Medizinprodukte
 - Reinigung
 - Materialverwaltung
 - EDV
 - Technik
 - Administration
 - Patientenbetreuung und -fürsorge
- Externe Partner, z.B.:
 - Wäscherei
 - Lebensmittelproduktion
 - Wachdienst
 - Wartungsfirmen
- Externe Dienstleistungen, z.B.
 - Zulieferer Verbrauchsmaterial
 - Zulieferer Medikamente

Aus der obigen Liste wird ersichtlich, dass das Krankenhaus von vielen externen wie auch internen Ressourcen abhängig ist. Dem entsprechend werden im Schadenfall die Kaskadeneffekte wie im Kapitel 4.3 beschrieben zum Tragen kommen und die Auswirkungen werden sich bedingt durch die Abhängigkeiten ausbreiten.

6.4 Auswirkungen von Zwischenfällen auf kritische Infrastrukturen

Auswirkungen von Kaskadeneffekten (siehe Kapitel 4.3) und Sektor übergreifende Ausfälle werden mit den Zunahmen an vernetzten Infrastrukturen immer wahrscheinlicher. In Abbildung 31 werden die Abhängigkeiten zwischen kritischen Infrastrukturen und den benötigten Ressourcen dargestellt. Insbesondere der Ausfall von Energieversorgungssystemen und Telekommunikationssystemen erhöhen das Schadenpotential. (vgl. BARTELS M. und LORENZ D. F. 2017: 27)

In Abbildung 31 sind Abhängigkeiten von einigen kritischen Infrastrukturen und einigen kritischen Ressourcen dargestellt, wobei die Abhängigkeit der Zeile von den Spalten mit einem „X“ gekennzeichnet ist. (vgl. EHLEN M. und VARGAS V. 2013: 7)

Infrastruktur	Infrastructure															
	Agriculture & Food	Banking & Finance	Chemicals & Hazardous Materials	Commercial Facilities	Critical Manufacturing	Dams	Defense Industrial Base	Emergency Services	Energy / Electric Power	Energy / Natural Gas	Energy / Petroleum	Government Facilities	Healthcare & Public Health	Information Technology	Nuclear Facilities	Postal & Shipping
Agriculture & Food	x	x	x			x			x	x	x					x
Banking & Finance		x							x				x			x
Chemicals & Hazardous Materials		x	x						x	x	x		x		x	x
Commercial Facilities	x	x	x	x	x			x	x	x			x	x	x	x
Critical Manufacturing		x	x	x	x			x	x	x			x		x	x
Dams						x										x
Defense Industrial Base		x					x								x	x
Emergency Services								x	x		x		x		x	x
Energy / Electric Power		x				x			x	x	x		x	x		x
Energy / Natural Gas		x							x	x	x		x			x
Energy / Petroleum		x							x		x		x		x	x
Government Facilities		x		x			x	x	x	x	x	x	x	x	x	x
Healthcare & Public Health	x	x	x	x	x			x	x	x	x	x	x	x	x	x
Information Technology		x							x		x		x	x		x
Nuclear Facilities					x			x	x				x	x	x	x

Abbildung 31: Infrastruktur-Abhängigkeiten: Auswahl kritischer Infrastrukturen und wichtiger Ressourcen (Quelle: Ehlen M. und VARGAS V. 2013: 7)

In der Cybersicherheit ist eine wesentliche Herausforderung, die Angriffe von aussen abzuwehren. Diese Abwehr zu garantieren, wird mit der zunehmenden Vernetzung von Prozessen, Ressourcen, Produkten und Geräten immer aufwendiger. Insbesondere müssen Mitarbeiter sensibilisiert werden, denn öfters sind geöffnete Anhänge von E-Mails die Ursache, dass Cyberangriffe Erfolg haben. (vgl. MAIER S. und AENGENHEYSER S. 2020: VII-VIII; XIII)

Das Gesundheitswesen ist eine der Branchen, welche am meisten von Cyberkriminellen angegriffen werden. Zum Beispiel wurde im Mai 2017 das Gesundheitswesen in Großbritannien angegriffen (vgl. ARGAW S. T. et al. 2020: 1-2). Dabei kam es zu Verzögerungen in der Behandlung, zentrale Notaufnahmen mussten geschlossen und die Rettungswagen umgeleitet werden. Der Zugang zum Krankenhausinformationssystem wurde unterbrochen. Neben den Verzögerungen gab es auch finanzielle Schäden und das Gesundheitswesen hat Langzeit-Imageschäden erlitten. Andere Schäden könnten der Klau von Patientendaten sein. Im Dark-Net werden die Patientendaten für das 10- bis 20-fach vom Wert der Sozialversicherungsnummer oder Kreditkartennummer gehandelt. Neben den vielen vernetzten medizintechnischen Geräte können Cyberangriffe auch andere Dienstleistungen wie z.B. vernetzte, technische Anlagen in einem Krankenhaus betreffen. Neben den klassischen Hackerangriffen können Cyberkriminelle auch „Stealth Malware“ (Virus versteckt sich aktiv vor dem Antivirenprogramm) in die vernetzte Krankenhaus IT-Landschaft einspielen, die dann zu einem gewünschten Zeitpunkt aktiviert wird. Hier könnte es passieren, dass die Cyberkriminellen einen besonders verwundbaren Zeitpunkt wie z.B. eine Naturkatastrophe abwarten, während der sie dann das Krankenhaus-System anzugreifen.

Im Folgenden werden drei Fallbeispiele dargestellt, bei denen ein Ereignis mehrere Auswirkungen verursacht hat. Die Fallbeispiele wurden dem Handbuch Krankenhausalarm- und -einsatzplanung (KAEP) des BBK entnommen. (siehe BBK 2020b: 143-145; 152-156)

Das erste Fallbeispiel zu einem Cyberangriff bezieht sich auf die Ausführungen von Dr. Klaus Reinartz Facharzt für Anästhesie; ehemaliger Leitender Arzt der Zentralambulanz am Lukaskrankenhaus Neuss. (siehe REINARTZ K. 2020: 143-145)

Das zweite Fallbeispiel zu einem Brand bezieht sich auf die Darstellungen von Robin Jopp Leiter Stabsstelle Unternehmenskommunikation am BG Universitätsklinikum Bergmannsheil in Bochum. (siehe JOPP R. 2020: 152-155)

Das dritte Fallbeispiel zu einem Stromausfall bezieht sich auf die Beschreibungen von Dr. med. Anja Greven Fachärztin für Anästhesiologie, ehem. Oberärztin der Zentralen Notaufnahme am Bundeswehr-Krankenhaus in Hamburg. (siehe GREVEN A. 2020: 155-156)

6.4.1 Fallbeispiel: Cyberangriff auf das Lukaskrankenhaus Neuss (D)

Vermutlich durch das Öffnen eines E-Mail Anhangs durch einen Mitarbeiter wurde das IT-System des Lukaskrankenhauses am 16. Februar 2016 mit einer „Ransomware“ angegriffen. Aufgefallen ist der Angriff in den Morgenstunden als unterschiedlichen Nutzern aufgefallen ist, dass die benutzen Systeme (u.a. KIS, PACS) besonders langsam liefen. Der IT-Abteilung ist ein besonderes hoher Datenverkehr im Netzwerk aufgefallen. Umgehend wurde vom IT-Abteilungsleiter entschieden alle hausinternen Systeme herunterzufahren. Einigen Nutzern ist beim morgendlichen starten der PCs eine Nachricht in schlechtem Englisch aufgefallen mit der Botschaft, dass die Daten verschlüsselt wären und gegen eine Zahlung in Bitcoin wieder freigeschaltet würden. Der Klinikleitung war es zu dem Zeitpunkt klar, dass es einen Cyberangriff gegeben hat.

Bedingt durch den kompletten Ausfall der IT-System, dieses wurde bewusst vom Abteilungsleiter IT abgeschaltet, musste das Krankenhaus die gesamte Patienten-Dokumentation auf Handbetrieb umstellen, was eine enorme Herausforderung darstellte. Unmittelbar wurde der interne Krisenstab einberufen und die Kommunikation mit den Mitarbeitern organisiert. Hierzu wurden Versammlungen, Aushänge, Flugblätter und persönlich Anweisungen genutzt.

Der Krankenhausleitung wurde schnell klar, dass diese Störung nicht innerhalb weniger Stunden behoben sein wird und dass der Krankenhausbetrieb erheblich gestört wurde. Daraufhin wurde das Krankenhaus bis auf Weiteres für die Notfallversorgung bei der Kreisleitstelle abgemeldet. Im Krankenhaus waren unterschiedlichste Prozesse und Ressourcen in fast allen Abteilungen betroffen. Das elektive Programm wurde abgesagt. Bedingt durch nicht Verfügbarkeit der digitalen Patientendaten mussten viele Untersuchungen abgesagt werden. Die bildgebenden Verfahren konnten nur solange betrieben werden bis die internen Speicherkapazitäten in den Geräten erreicht waren. Die Befundung der Bilder konnte ab dem Zeitpunkt nur mehr am Gerät selbst durchgeführt werden. Es mussten Notabläufe und Notbetriebe

organisiert und betrieben werden. Als der Handbetrieb bis eingespielt war, konnte vereinzelt Interventionen und Operationen wieder aufgenommen werden.

Kriminalistische sowie polizeibehördliche Ermittlungen standen im Gegensatz zum Krankenhausbetrieb. Die Polizei beschlagnahmte unterschiedliche IT-Hardware wobei das Krankenhaus schnellstmöglich wieder in Betrieb gehen wollte. Mit den Behörden sowie externen IT-Spezialisten musste aber zuerst das Virus identifiziert werden, anschließend wurde eine Gegensoftware erarbeitet.

Das Krankenhaus war für ca. 3 Wochen wesentlich eingeschränkt, während dieser Zeit war fast ausschließlich eine manuelle Bearbeitung der Patientendaten möglich. Am Ende konnten alle Daten wiederhergestellt werden und ein Datenmissbrauch wurde nicht festgestellt.

6.4.2 Fallbeispiel: Brand im BG Universitätskrankenhaus Bergmannsheil Bochum (D)

In den Nachtstunden des 30. Septembers 2016 löste die Brandmeldeanlage in der Pflegestation im 6. OG des achtstöckigen Bettenhauses 1 der Universitätsklinik Alarm aus. Das Bettenhaus 1 beherbergt im UG die Zentralküche, im EG einen Empfangsbereich, Ambulanzen und Verwaltungsbüros, OG1-6 Pflegestationen für 192 möglichen Patienten, im 7. OG einen Funktionsbereich mit zwei Operationssälen und im 8. OG eine Technikzentrale mit Lüftungsanlagen und den Aufzugsmaschinenräumen. Umgehend nach der Alarmierung wurde mit der Evakuierung der Patienten begonnen. Zu dem Zeitpunkt waren 150 Patienten im Bettenhaus 1 hospitalisiert. Ein erheblicher Teil war nicht mobil oder nur eingeschränkt gehfähig. Der Brand breitete sich schnell auf das 7. und 8. OG aus. Da die Feuerwehr ausschließlich in die Brandbekämpfung eingebunden war, wurde die Evakuierung durch die Polizei und das alarmierte Personal durchgeführt. Von den 150 Patienten konnten 148 Personen gerettet werden, wobei 8 Patienten verletzt wurden und 7 Patienten erlitten eine Rauchgasvergiftung. Die Verursacherin und der Patient aus dem Nachbarzimmer konnten nicht mehr gerettet werden und sind verstorben.

Während der Evakuierungsphase wurde in anderen Gebäuden der Universitätsklinik kurzfristig Versorgungsmöglichkeiten geschaffen. In den frühen Morgenstunden wurden andere Patienten, wo der Gesundheitszustand es erlaubte, entlassen, um die evakuierten Patienten wieder in Patientenzimmern hospitalisieren zu können.

Durch das eingesetzte Löschwasser wurde die Serverstruktur der Klinik sehr stark geschwächt, so dass verschiedene IT-Systeme nicht mehr funktionsfähig waren. Dadurch dass die Universitätsklinik mehrere Gebäude auf einem Campus betreibt, konnte der reguläre Krankenhausbetrieb aufrechterhalten bleiben. Durch die Schäden vom Löschwasser waren die Zentralküche sowie die Bettenzentrale ausgefallen, hier wurden Ersatzmaßnahmen durch eine Zulieferung einer externen Küche. In einer Sporthalle wurde die Bettenzentrale provisorisch eingerichtet.

Die Löscharbeiten konnten nach ca. 14,5 Stunden abgeschlossen werden.

6.4.3 Fallbeispiel: Stromausfall am Bundeswehr-Krankenhaus Hamburg

Während größeren Umbauarbeiten auf dem Campus des Bundeswehr-Krankenhauses, kam es am 16. August 2017 in den Morgenstunden zu einer Durchtrennung einer Mittelspannungsringleitung. Dies bedingte einen größeren Stromausfall auf dem gesamten Gelände. Die Notstromversorgung hat die Stromversorgung übernommen. Bedingt durch eine Überspannung schalteten drei von neun Energiezentralen auch die Notstromversorgung automatisch ab. Zwischen Energiezentrale 2 und 3 war die Ringleitung unterbrochen, jedoch war hiervon keine Kenntnis vorhanden und dadurch konnte die Redundanz einer Ringleitung nicht genutzt werden. Durch den Ausfall der drei Energiezentralen waren die betroffenen Bereiche stromlos und ein erheblicher Teil der Liegenschaft war ohne Stromversorgung. Durch den Stromausfall auf dem Gelände der Klinik kam es zu einer Überspannung und die Stromversorgung im Stadtteil Wandsbek wurde kaskadenartig abgeschaltet. Hiervon betroffen war ein weiteres Krankenhaus. Auf dem Klinikgelände waren die Auswirkungen unterschiedlich, da einige Energiezentralen im Notbetrieb betrieben werden konnten. Notstromversorgt waren die Intensivstation, die Röntgenabteilung, die zentrale Notaufnahme und das Labor. Im OP-Bereich gab es einige Funktionsausfälle. Davon betroffen waren u.a. der Stabsraum, viele IT-Endgeräte, berührungslose Waschbeckenarmaturen und die digitale Schließanlage. Störungen gab es ebenfalls in der zentralen Aufbereitungseinheit für Medizinprodukte und in der Apotheke. Nach einer Ausfallzeit von ca. 1,5 Stunden konnte die Stromzufuhr wieder hergestellt werden und alles konnte wieder in Betrieb genommen werden.

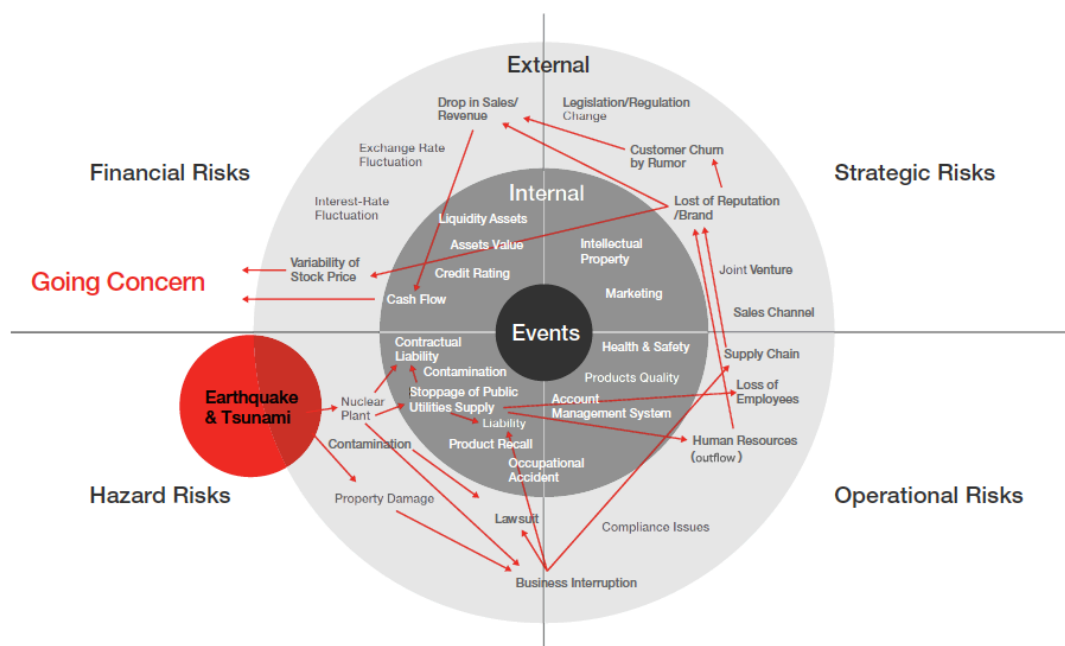
Aus den drei Fallbeispielen sowie den Erläuterungen zu den Verwundbarkeiten, Abhängigkeiten und möglichen Auswirkungen ist es ersichtlich, dass sich kritische Infrastrukturen, zu denen auch Krankenhäuser gehören, im Vorfeld von möglichen Ereignissen vorbereiten müssen. Im folgenden Kapitel 7 werden Management Systeme und Werkzeuge zur Steigerung der Resilienz beschrieben.

7 Risikomanagement und Business Continuity Management

7.1 Risikomanagement

Durch die weltweite Vernetzung der Gesellschaft ist das Gesamtsystem der kritischen Infrastrukturen so komplex geworden, dass es bei einer Verkettung von Auswirkungen zu systemischen Risiken kommen kann.

Ein gutes Beispiel zur Darstellung der vernetzten Gesellschaft und der Kaskadeneffekte ist das Seebeben am 11. März 2011 vor der Sanriku-Küste in Japan. Das Seebeben als auslösendes Ereignis hat einen Tsunami mit bis zu 38 Meter hohen Wellen und Überschwemmungen sowie verschiedene Unfällen an Kernkraftwerken an der Ostküste Japans ausgelöst. Dies führte zur Nuklearkatastrophe von Fukushima mit anschließenden Produktionsausfällen und Lieferstopps. Hiervon war die weltweite Automobilindustrie sehr stark betroffen. In Abbildung 32 werden die Kaskadeneffekte nach dem Ereignis dargestellt und bedingt durch die komplexen Abhängigkeiten in der Gesellschaft breiten dieses sich in allen Risikokategorien aus. (vgl. ROMEIKE F. 2018: 206-208)



Source: Marsh Inc., 2011

Abbildung 32: Example of Business and Operational Risks and their Domino Effects (vgl. World Economic Forum 2012: 32)

Damit Organisationen sich besser auf externe wie interne Abhängigkeiten vorbereiten können ist ein allumfassendes Risikomanagement notwendig.

Wenn Leistungen verbessert, Innovationen angeregt und Ziele erreicht werden sollen um Werte zu schaffen oder zu bewahren, kann das Risikomanagement angewandt werden (vgl. ISO 2018: 2).

Mit der ISO 31000:2018 „Risk Management – Principles and Guidelines“ gibt es einen weltweiten Standard was das Risikomanagement anbelangt. (vgl. KUNTSCHKE P. und BÖRCHERS K. 2017b: 171)

Die Abbildung 33 veranschaulicht die Grundsätze im Risikomanagement gemäß der ISO 31000:2018. Anhand dieser kann das Risikomanagement in einer Organisation eingeführt und betrieben werden. Ebenso kann die Basis für die Erstellung einer organisationsinternen Politik und für den Umgang mit Risiken gelegt werden. Mit der Umsetzung der ISO 31000 sind Organisationen bestmöglich vorbereitet, um gegen die Auswirkungen von Ereignissen zu bestehen. (vgl. ISO 2018: 2)



Abbildung 33: Grundsätze des Risikomanagement nach ISO 31000:2018 – eigene Darstellung
(Quelle: ISO 2018: 3-4)

Grundsätzliches Ziel des Risikomanagement ist es Risiken zu vermeiden, zu mindern, zu akzeptieren oder zu transferieren und so Nachteile für die Organisation zu vermeiden. (vgl. STOLZENBURG K. und KOWALZIK B. 2018: 74); (vgl. SCHMOLA G. 2016: 289)

Nach SCHMOLA G. (2016: 289) besteht das Risiko aus den beiden Komponenten Schadenshöhe und Eintrittswahrscheinlichkeit. Für SCHMOLA G. (2016: 290) wird das Risikomanagement neben dem Fehlermanagement auch für eine vorausschauende Analyse von möglichen Problemen eingesetzt. Die Erfüllung der Anforderungen von Stakeholdern wie u.a. Patienten und Mitarbeitern erfordert eine zielgerichtete Reaktion auf mögliche Risiken um somit eine dauerhafte Sicherung der Organisationsexistenz zu erreichen.

Die Organisationsexistenz, im Kontext eines Krankenhauses, setzt sich aus 2 Kategorien zusammen. Zum einen die klinische Organisation und zum anderen die betriebswirtschaftliche Organisation. Zum Erfüllen der genannten Anforderungen muss das Risikomanagement für beide Kategorien in Betracht gezogen werden. Wobei beim klinischen Risikomanagement die medizinische Patientenversorgung und beim betriebswirtschaftlichen Risikomanagement die ökonomische Organisation im Vordergrund stehen werden. Krankenhäuser verwenden öfters zusätzliche Motive um ein allumfassendes Risikomanagement zu betreiben. Für die Folgenden Motive kann ein Risikomanagement als sinnvoll erachtet werden:

- Abwendung eines potenziellen Schadens von einem Patienten – Sicherstellung der Patientenversorgung;
- Förderung der Arbeitssicherheit und des Gesundheitsschutzes für Mitarbeiter;
- Reduzierung der Folgekosten möglicher medizinischer Behandlungsfehler;
- Erfüllung gesetzlicher Anforderungen u.a. aus dem Sozialrecht, dem Unternehmensrecht, dem Datenschutzrecht, dem IT-Sicherheitsrecht und der Gesetzgebung über die kritischen Infrastrukturen;
- Erfüllung von Vorgaben beim Qualitätsmanagement;
- Erreichen besserer Konditionen beim Versicherer. (vgl. SCHMOLA G. 2016: 289-295)

In der kommunalen und regionalen Gesundheitsversorgung (vgl. FIEDLER M. et al. 2019: 2) sind Krankenhäuser in die Gefahrenabwehr stark eingebunden und erbringen wesentliche Dienste (vgl. STOLZENBURG K. und KOWALZIK B. 2018: 72). Aus politischer, betriebswirtschaftlicher, sozialer und gesellschaftlicher Sicht werden diese in einem sehr dynamischen und komplexen Umfeld mit unterschiedlichsten Stakeholdern betrieben. In vielen Regionen werden Krankenhäuser zu den größten Arbeitgebern gezählt.

Damit diese Anforderungen erfüllt werden können wird in einem immer wiederkehrenden Prozess (Abbildung 2), dem PDCA Zyklus nach DEMING W. E. (1982: .) das Risikomanagementsystem betrieben.

Plan – Aufbauen	Auftrag und Verpflichtung der Organisation mit der daraus zu erstellenden Risikopolitik
Do – Implementieren	Betreiben des eigentlichen Risikomanagementprozesses mit den wesentlichen Schritten „Identifizieren“, „Analysieren“, „Bewerten“ und „Bewältigen“
Check – Überwachen und Prüfen	Umsetzung der Risikobewältigungsstrategie

Act – Verbessern

Anpassungen an die
Risikobewältigungsstrategie (vgl. KUNTSCHKE P.
und BÖRCHERS K. 2017b: 172-173)

Um ein Risikomanagementsystem gemäß der ISO 31000:2018 etablieren zu können, müssen von der Organisation einige Anforderungen umgesetzt werden. In einer Risikopolitik müssen Ziele und Strategien für die operative und prozessgesteuerte Aktivitäten festgelegt werden. In einem Krankenhaus müssen z.B. patientenorientierte Aktivitäten und eine fehlerfreie Behandlung als Ziele beachtet werden. In die Beschreibung der Risikopolitik gehört auch die Festlegung der Verantwortlichkeiten und die dazu gehörigen Aufgaben. Für die Identifikation der Risiken während der Implementierung des Risikomanagementprozesses und um die kritischen Prozesse zu identifizieren ist es sinnvoll eine Prozesslandkarte zu entwickeln. Die Analyse und Bewertung der Risiken werden im folgenden Unterkapitel beschrieben. Die Kommunikation in der Organisation darf nicht vernachlässigt werden und alle Stakeholder sollten frühzeitig eingebunden werden. (vgl. KUNTSCHKE P. und BÖRCHERS K. 2017b: 173-174)

7.1.1 Risikoidentifikation, -analyse und -bewertung

Um Risiken bewältigen zu können müssen bei der Identifikation, Analyse und Bewertung die Qualität der Ergebnisse stimmen. Werden während diesen Prozessen Fehler gemacht oder wichtige Informationen sind nicht verfügbar, hat es eine direkte Auswirkung auf die Bewältigung. (vgl. ROMEIKE F. 2018: 55)

In der Praxis müssen die richtigen Methoden für die Risikoidentifikation, -analyse und -bewertung gefunden werden. Ebenso muss für die Problemlösungsfindung die richtige Methodik ausgewählt werden. Bei der Vielzahl an Methoden wird dies als Herausforderung angesehen. Im Folgende wird näher auf Ansätze und Methoden eingegangen. (vgl. KUNTSCHKE P. und BÖRCHERS K. 2017b: 174)

Wie in Tabelle 2 dargestellt, unterteilt ROMEIKE F. (2018: 56) die Methoden in „Kollektionsmethoden“ und „Suchmethoden“, wobei die Suchmethoden nochmals in analytische Methoden und Kreativitätsmethoden unterteilt werden.

Sind die Risiken bereits bekannt, aus einer vorherigen Analyse oder durch Vorgaben, z.B. im Rahmen von kritischen Infrastrukturen (siehe Kapitel 6.1) werden vornehmlich die Kollektionsmethoden angewendet. Dem gegenüber stehen die Suchmethoden, welche insbesondere für unbekannte Risiken eingesetzt werden. Aufgrund von Parallelen in den Prozessstrukturen zwischen dem Risikomanagement und dem Qualitätsmanagement konnten die analytischen Methoden aus dem Qualitätsmanagement übernommen werden und mit diesen Methoden können insbesondere Risikoprozesse analysiert werden. In den Kreativitätsmethoden werden überwiegend kreative Prozesse angewendet um das Denken chaotisch werden zu lassen und somit bisher unbekannte Risikopotenziale identifizieren zu können. (vgl. ROMEIKE F. 2018: 56 & 58)

Tabelle 2: Methoden der Risikoidentifikation, -analyse und -bewertung (Quelle: ROMEIKE F. 2018: 56)

Kollektions- methoden	Suchmethoden	
	Analytische Methoden	Kreativitätsmethoden
– Checkliste – Schadenfall-Datenbank – SWOT-Analyse – Self-Assessment – Risiko-Identifikations-Matrix (RIM) – Interview	– Bow-tie Analysis – Empirische Datenanalyse – Fehlerbaumanalyse (Fault Tree Analysis, FTA) – Fehlermöglichkeits- und Einflussanalyse (FMEA) – Hazard and operability studies (HAZOP) – Business impact analysis – Fehler-Ursachen-Analyse (Root cause analysis, RCA) – Ereignis-Baumanalyse (Event tree analysis) – Cause-and-effect analysis – Ishikawa-Diagramm – Markov analysis/Bayesian statistics and Bayes Nets – Consequence/probability matrix – Social Network Analysis	– Morphologische Analyse – Brainstorming – Brainwriting – Methode 635 – Brainwriting Pool – Mind Mapping – KJ-Methode – Flip-Flop-Technik (Kopfstandtechnik) – World-Café – Delphi-Methode – Business Wargaming – Deterministische Szenarioanalyse – Stochastische Szenarioanalyse (stochastische Simulation) – System Dynamics

Wie in Tabelle 3 dargestellt, werden in der „ONR 49002-2 Risikomanagement für Organisationen und Systeme Teil 2: Leitfaden für die Methoden der Risikobeurteilung Anwendung von ISO/DIS 31000 in der Praxis“ ähnliche Methoden aufgeführt. In dieser Tabelle werden die Methoden gemäß den drei Kategorien „Identifikation“, „Bewertung“ und „Bewältigung“ aufgelistet. Wobei die Methoden für die Kategorie Bewertung in drei zusätzliche Unterkategorien „Auswirkungen“, „Wahrscheinlichkeit“ und „Risikohöhe“ aufgeführt werden. (vgl. AUSTRIAN-STANDARDS 2008b: 5)

Tabelle 3: Übersicht der Methoden im Risikomanagement-Prozess (Quellen: AUSTRIAN-STANDARDS 2008b: 5)

Methode	Prozess Risikomanagement				
	Identifikation	Bewertung			Bewältigung
		Auswirkungen	Wahrscheinlichkeit	Risikohöhe	
Brainstorming	+++	+	+		+
Delphi-Technik		++	++		++
Morphologie	+				+++
Schadensanalyse	++	+	+		++
Fehlerbaum- und Ablaufanalyse		++	+++	+	+
Szenario-Analyse	+++	+++	++	++	++
CIRS (Critical Incident Reporting System)	+++		+		+
CBRM (Change Based Risk Management)	+++	+			
FMEA (Failure Mode and Effects Analysis)	+++	++	++	+	++
Gefährdungsanalyse	++	+++	++	++	++
HAZOP (Hazard and Operability Study)	+++	+++	++	+	++
HACCP (Hazard and Critical Control Point)	++	++			++
Standardabweichung		++	+++	++	
Konfidenzintervall		++	+++	++	
Monte-Carlo-Simulation	+	++	+++	++	

Die Beschreibung jeder einzelnen dieser Methoden würde den Rahmen dieser Arbeit übersteigen. In den Kapiteln 3 und 8 zur Methodik und der Fallstudie werden lediglich die angewandten Ansätze und Methoden beschrieben.

Die Risikobewertung wird üblicherweise mit den Angaben, wie wahrscheinlich ist ein Ereignis und welche mögliche Schadenshöhe kann beim Eintritt des Ereignisses erwartet werden, beschrieben:

$$\text{RISIKO} = \text{EINTRITTSWAHRSCHEINLICHKEIT} \times \text{SCHADENSHÖHE (AUSWIRKUNG)}$$

Ist eine quantitative Einschätzung nicht möglich, so kann auch eine qualitative Beschreibung der Größen durchgeführt werden. Für die Darstellung des Risikoportfolios kann auf eine Visualisierung zurückgegriffen werden. (vgl. KRYSTEK U. und FIEGE S. 2013)

KUNTSCHKE P. und BÖRCHERS K. (2017b: 174) geben an, dass die Risikomatrix eine verbreitete Methode für die Darstellung des Risikoprofils ist. In der Risikomatrix können die einzelnen Ergebnisse der Risikoanalysen verglichen werden. Anhand der Grafik können auch Priorisierungen für die Risikobewältigung sehr gut festgelegt werden. Wurden Risiken mit einer hohen Eintrittswahrscheinlichkeit und einem hohen Schadensausmaß analysiert, sollten in der Bewältigung, diese Risiken den Risiken

gegenüber den Risiken mit einer geringeren Eintrittswahrscheinlichkeit und einem geringeren Schadensausmaß, vorgezogen werden. Idealerweise werden zielgerichtete Schutzmaßnahmen in der Bewältigungsphase eingesetzt um die Risiken gegen Null zu reduzieren. (vgl. BBK 2020b: 30-31)

Während der Risikobewertung müssen auch die Zusammenwirkungen einzelner Risiken für eine Organisation berücksichtigt werden. Diese Bewertung ist um so wichtiger, da aus wenig gefährdenden Einzelrisiken in Interaktion mit anderen Risiken ein erhebliches Risiko für die Organisation entstehen könnte. Schutzmaßnahmen für die präventive Risikobewältigung müssen entsprechend auf die Einzelrisiken aber auch auf die interagierenden Risiken definiert werden.

7.1.2 Risikobewältigung

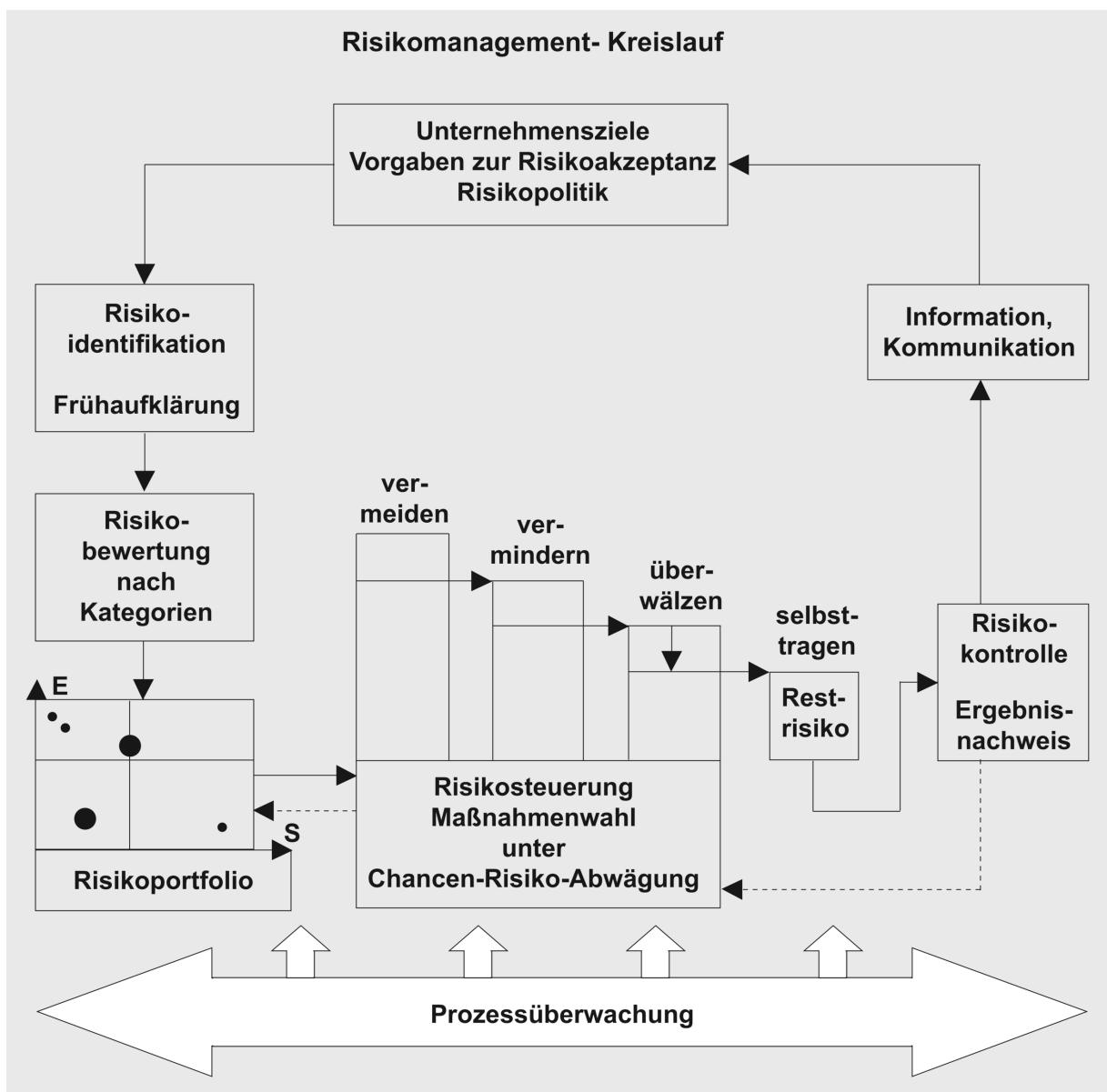


Abbildung 34: Risikomanagement-Kreislauf (Quelle: KRYSTEK U. und FIEGE S. 2013)

Zur Umsetzung der Risikopolitik der Organisation sowie zur Reduzierung des Risikos müssen für die identifizierten und bewerteten Risiken Schutzmaßnahmen oder andere

Möglichkeiten entwickelt werden. In der Risikosteuerung werden unterschiedliche Strategien angewandt, die in Einklang mit der Organisationsstrategie stehen. Für eine Risikobewältigung oder Risikosteuerung stehen vier Strategien (vgl. KRYSTEK U. und FIEGE S. 2013) zur Verfügung:

- Vermeiden** Verzicht von Aktivitäten in der Organisation, das daraus resultierende Risiko wird die Organisation nicht mehr betreffen;
- Vermindern** Reduzierung der Eintrittswahrscheinlichkeit oder Reduzierung des Schadensausmaßes, entsprechende Maßnahmen zur Senkung des Risikos müssen umgesetzt werden;
- Überwälzen** Das Risiko wird auf einen anderen Akteur oder Partner übertragen, z.B.: Outsourcing oder Abtragung an einen Versicherer;
- Selbst tragen** Restrisiken wird es in einer Organisation immer geben, die Organisation muss die entsprechenden Mittel haben, um das verbleibende Restrisiko zu tragen;

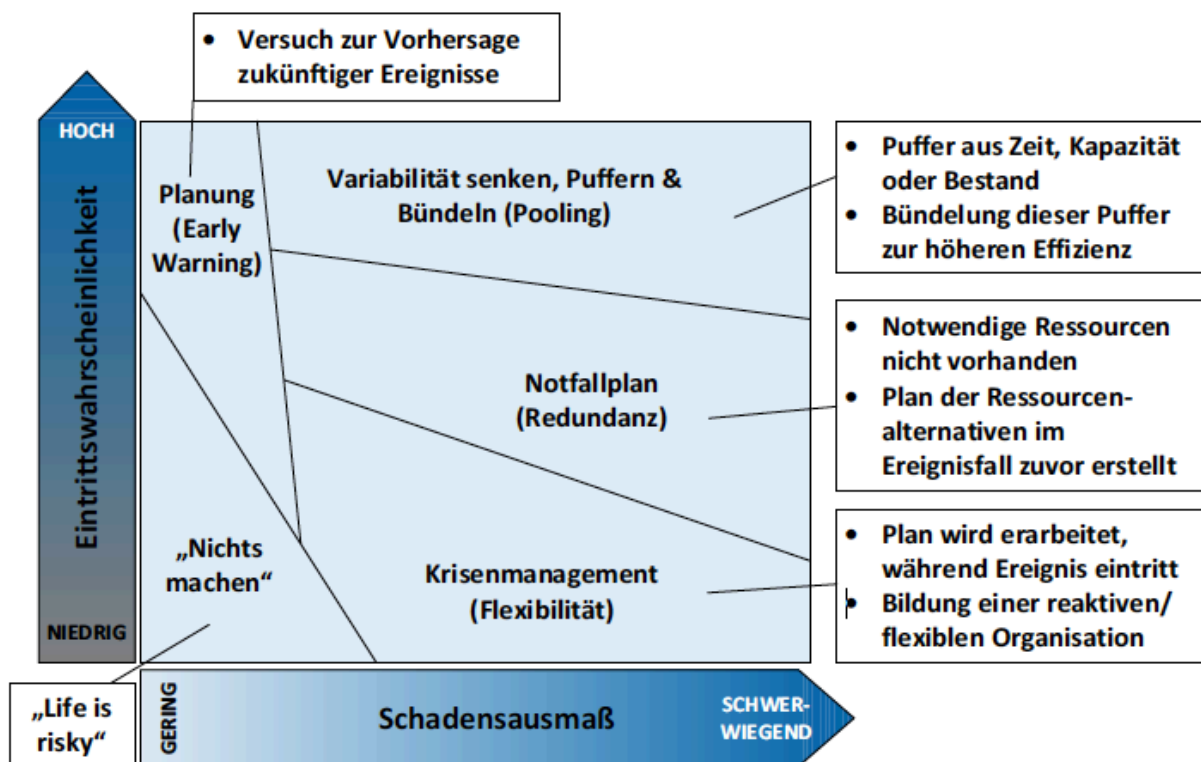


Abbildung 35: Grundsätzliche Strategien zur Risikosteuerung (Quelle: ROMEIKE F. 2018: 47)

In Abbildung 35 werden mögliche Strategien zur Risikosteuerung dargestellt und mit den angegebenen Maßnahmen können Risiken in der Organisation bewältigt werden. (vgl.: ROMEIKE F. 2018: 46)

Die bisher beschriebenen Herausforderungen und die damit verbundenen Anforderungen verlangen eine zunehmend effizientere Organisation. Die Abhängigkeiten von der Informationstechnik, den externen Dienstleistern, Lieferanten und Dritten sowie den vernetzten Infrastrukturen in der Verfügbarkeit der

Geschäftsprozesse entwickeln sich zu Existenzfragen für die Organisation. (vgl. BSI 2021: 6)

Aufbauend auf dem Risikomanagement werden noch anderen Konzepte u.a. das Business Continuity Management (BCM) und IT-Sicherheitsmanagementsystem (ISMS) für den Umgang mit Unsicherheiten in der Praxis angewendet. (vgl. MÜLLER-SEITZ G. 2014: 111)

7.2 Business Continuity Management

Neben den bereits behandelten Risikoaspekten aus dem Risikomanagement werden beim Business Continuity Management eher noch schwieriger zu quantifizierende Risikoquellen berücksichtigt. Um mit den worst-Case Risiken (vgl. SPÖRRER S. 2014: V) umgehen zu können, reicht es nicht nur diese zu identifizieren, sondern werden auch organisatorische Möglichkeiten benötigt. Mit dem Business Continuity Management wird das strategische Management einer Organisation proaktiv unterstützt. (vgl. MÜLLER-SEITZ G. 2014: 112)

Eine Organisation sollte sich in der Risikopolitik nicht nur das alleinige Ziel setzen ein maximales Sicherheitsniveau zu erreichen, sondern vielmehr Ziele setzen, die ein betriebswirtschaftliches optimales Sicherheitsniveau erreichen. Dafür müssen Betriebsstörungen reduziert werden (vgl. SPÖRRER S. 2014: 2-3). Eine Organisation ist u.a. den Gefährdungen aus Kapitel 6.1 ausgesetzt, zusätzlich müssen aber u.a. auch Störungen wie Krankheitsausfällen, lokal-regionale Ereignisse, Lieferkettenbeeinträchtigungen berücksichtigt werden. Kann eine Organisation nicht angemessen auf unerwartete Betriebsstörungen reagieren, dann schädigt sie ihren Ruf.

Die Identifikation von potenziellen Bedrohungen (ebd.: 3), die Umsetzung von geeigneten Schutzmaßnahmen für finanzielle, operative, legale Schäden oder Reputationsschäden, die angemessene Reaktion auf Gefährdungen stellen das Rahmenwerk für ein Business Continuity Management dar. Damit die Geschehnisse idealerweise bewältigt werden können, werden im Business Continuity Management bereits im Vorfeld von eventuellen Vorfällen Analysen durchgeführt (ebd.: 8). Während den Analysen sollte nicht nur die interne Organisation betrachtet werden, sondern sollten die externen wesentlichen Partner in die Analyse integriert werden (ebd.: 11). Zur Erfüllung dieser Anforderungen kann auf die ISO 22301 „Security and resilience — Business continuity management systems — Requirements“ als internationale Norm zurückgegriffen werden.

Ziel des Business Continuity Management sollte sein bei erheblichen Schadenereignissen den Geschäftsprozess nicht zu unterbrechen indem präventive Schutzmaßnahmen bestehen oder den Geschäftsprozess nach einer kurzen Ausfallzeit wieder angemessen fortführen zu können. Hierfür bedarf es einer reaktiven Vorplanung mit den entsprechenden Business Continuity Plänen. Schutzmaßnahmen können personeller, baulicher, organisatorischer wie auch technischer Natur sein und sollten in Abstimmung mit anderen Managementsystemen ausgearbeitet werden. (vgl. BSI 2021: 7)

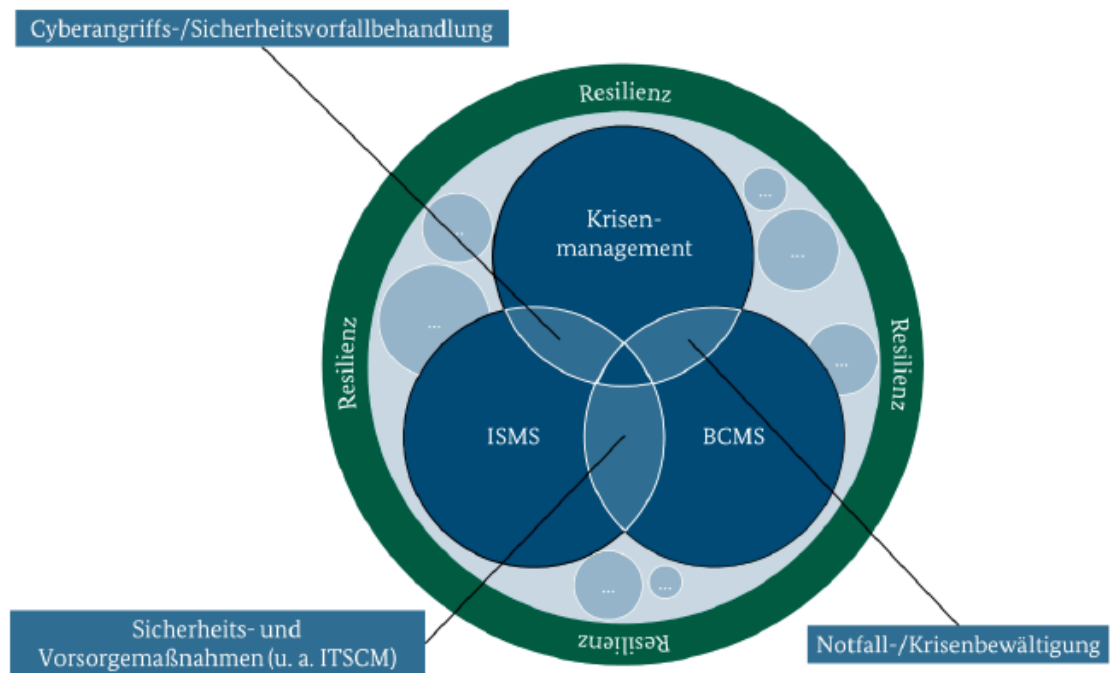


Abbildung 36: Resilienz schaffen durch verschiedene Sicherheitsthemen (Quelle: BSI 2021: 7)

Kann eine Organisation interne und externe Veränderungen erkennen und auf diese reagieren, umso besser können Risiken abgewehrt und Chancen genutzt werden. Diese Fähigkeit wird „organisatorische Resilienz“ (BSI 2021: 7) bezeichnet. Die organisatorische Resilienz wird, wie in Abbildung 36 dargestellt, durch mehrere Managementsysteme geschaffen. Hierzu zählen neben dem Business Continuity Management u.a. auch das Krisenmanagement, das IT-Sicherheitsmanagement, das Risikomanagement, das Qualitätsmanagement, das Arbeitssicherheits- und Gesundheitsmanagement sowie der Perimeter- und Gebäudeschutz. (vgl. BSI 2021: 7) Dadurch können bei der Datensammlung Synergieeffekte spielen, die anschließend bei der Risikoidentifikation und -analyse Verwendung finden. Bei der Risikobewertung können die einzelnen Abhängigkeiten im Gesamtsystem betrachtet werden. In der Risikobewältigungsphase können die Ergebnisse in gemeinsamen Schutzmaßnahmen einfließen.

Im Business Continuity Management System werden, wie in Abbildung 37 dargestellt, die Elemente BCM-Organisation, -Methoden, -Prozess, -Ressourcen und Dokumentation angewendet. Die Schnittstellen zu anderen Managementsysteme werden für die Abstimmung der Methoden und Prozesse benötigt. Dadurch kann das BCMS in der organisatorischen Resilienz einer Organisation verwendet werden. (vgl. BSI 2021: 12&15)

Für die BCM-Organisation müssen der Geltungsbereich, die allgemeinen Ziele sowie die Prioritäten festgehalten werden. Zusätzlich müssen Vorgaben, Aktivitäten, Methoden und Handlungen konkretisiert sowie die Rollen der verantwortlichen Personen definiert werden. Die BCM-Methoden beschreiben die Werkzeuge zur Umsetzung. Zu diesen Werkzeugen werden die Business Impact Analyse, die BCM-Risikoanalyse sowie andere Strategien und Lösungen gezählt. Damit das Business Continuity Management System aufgebaut und kontinuierlich vorangetrieben werden kann, bedarf es einem BCM-Prozess. Dieser Prozess folgt dem PDCA-Zyklus. Zum

Betreiben eines BCMS werden personelle, organisatorische, finanzielle sowie zeitliche BCM-Ressourcen benötigt. In der BCM-Dokumentation werden sämtliche Dokumente, welche das BCMS beschreiben, abgelegt. Dazu gehören auch Pläne für die Notfallbewältigung und die Beschreibung der Wiederaufnahme der Aktivität. (vgl. BSI 2021: 13-14)

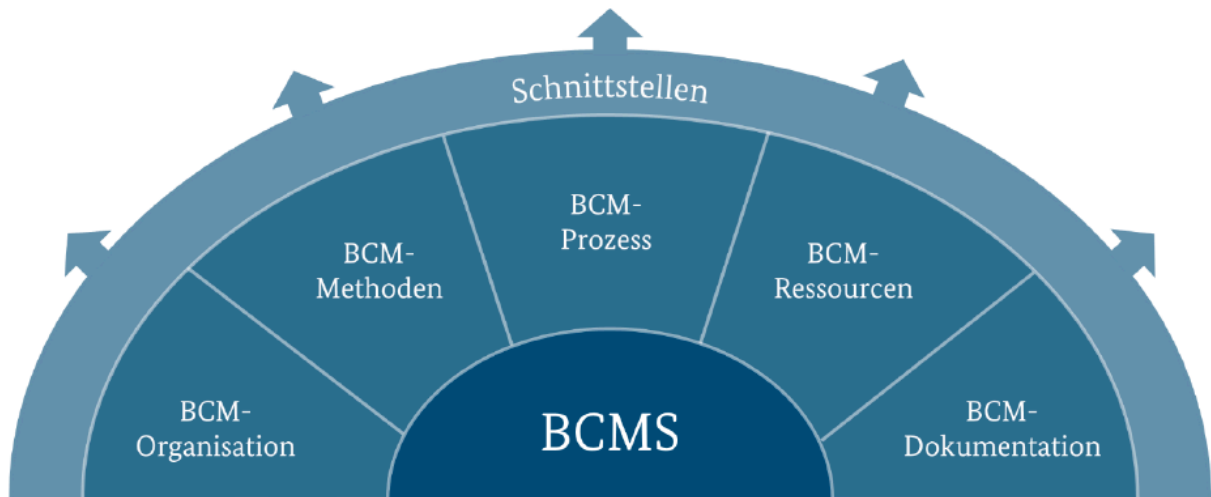


Abbildung 37: BCMS-Bestandteile (Quelle: BSI 2021: 13)

In Tabelle 4 werden die einzelnen Aktivitäten im PDCA-Zyklus des BCM-Prozesses beschrieben.

Tabelle 4: PDCA-Zyklus im BCM-Prozess (vgl. BSI 2021: 145)

Plan	▪ Analyse der Anforderungen an das BCMS, ▪ Festlegung der BCM-Politik, ▪ Ausrichtung auf die Bedürfnisse und Anforderungen der Interessengruppen, ▪ Definition der Dokumentationsstrategie, ▪ Festlegung der BCMS Leitlinien durch die Organisationsleitung.
Do	▪ Etablierung einer besonderen Aufbauorganisation (Krisenstab) für den Not- und Krisenfall, ▪ angemessenen Absicherung der zeitkritische Geschäftsprozesse: ○ Business Impact Analyse für zeitkritische Prozesse zur Definition der maximalen Ausfallzeit und der notwendigen Ressourcen für einen Notbetrieb, ○ Soll-Ist-Vergleich mit der Feststellung ob die benötigten Ressourcen ausreichend abgesichert sind, ○ BCM-Risikoanalyse mit der Durchführung von Untersuchungen zur Absicherung der identifizierten zeitkritischen Prozesse und Ausarbeitung von entsprechenden Business Continuity Strategien und Lösungen, ○ Festlegung der Geschäftsfortführungspläne und Wiederanlaufpläne mit Handlungsschritten zur Weiterführung der zeitkritischen Prozesse im Notfall,

	○ Beschreibung der Wiederherstellungspläne mit Handlungsanweisungen für die Rückkehr in den Normalbetrieb.
Check	▪ Praktische Überprüfung der beschriebenen Maßnahmen während Übungen und Tests, ▪ Überprüfung der gesetzten Anforderungen und Ziele.
Act	▪ Überführung von identifizierten Verbesserungen in konkrete Maßnahmen.

Wird das gesamte BCMS inkl. des kontinuierlichen PDCA-Kreislaufes umgesetzt, so wird das Business Continuity Management System der ISO 22301 entsprechen. (vgl. BSI 2021: 145)

Wie in Tabelle 4 beschrieben, bildet die Do-Phase ähnlich wie beim Risikomanagement in Kapitel 7.1 den eigentlichen Prozess zur Identifizierung der kritischen Prozesse. Ebenfalls müssen die Daten analysiert und bewertet werden. Gemäß der ISO 22301 betreffend das BCM wird sich für die Risikobeurteilung an der ISO 31000 zum Risikomanagement orientiert. Somit gibt es hier ein sehr enge Verzahnung der beiden Management System. (vgl. SPÖRRER S. 2014: 104)

SPÖRRER S. (2014: 104) beschreibt die Business Impact Analyse als eine Aktivität, die es erlaubt kritische Prozesse, welche Schlüsselprodukte erstellen oder Schlüsseldienstleistungen erbringen, zu identifizieren. Auch Abhängigkeiten zwischen erforderlichen Prozessen und Ressourcen können identifiziert werden.

Im Business Continuity Management sind die Business Impact Analyse und die Risikobewertungen essenziell damit die benötigten Business Continuity Pläne erstellt werden können. Dazu ist es nötig die Organisation zu verstehen. (TORABI S. A. et al. 2014)

Die CERBERUS Systemarchitektur kann sowohl zwischen vernetzten kritischen Infrastrukturen eingesetzt werden als auch innerhalb Organisationen, in denen kritische Prozesse untereinander vernetzt sind. Für die besonderen Betrachtungen der Kaskadeneffekte innerhalb des fiktiven Krankenhauses und in Anbetracht der Identifikation, Analyse und Bewertung der kritischen Prozesse und Ressourcen, wurde in der vorliegenden Arbeit die Business Impact Analyse als geeignetes Werkzeug für die statische Risikoanalyse ausgewählt.

7.3 Business Impact Analyse

Eine Business Impact Analyse liefert dem Management einer Organisation die nötigen Informationen über Schwachstellen, die Auswirkungen auf wertschöpfende Prozesse nach einem Ereignis und biete eine Basis für Wiederherstellungspläne. (vgl. TAARUP-ESBENSEN J. 2020: 2)

„Die Business Impact Analyse liefert idealerweise folgende Schlüsselergebnisse:

- Identifikation aller kritischen Prozesse und Ressourcen des Unternehmens.
- Identifikation aller kritischen Geschäftsprozesse.
- Identifikation der Zeit, innerhalb derer kritische Prozesse wiederhergestellt werden müssen, um die Kontinuität des Betriebs aufrechtzuerhalten.

- Kartierung aller eingesetzten IT-Ressourcen und aller Anwendungen, die auf den Unternehmenssystemen laufen.
- Identifizierung des Ziels für den Wiederherstellungspunkt (die Zeit, bis zu der, Transaktionen oder Daten wiederhergestellt werden müssen).
- Identifizierung von wichtigen Materialien und Aufzeichnungen, die für die Wiederherstellung oder Fortführung des Betriebs erforderlich sind.
- Identifizierung der Risikobereitschaft der Organisation.
- Auflistung aller Bedrohungen und Zuordnung der Auswirkungen auf das Unternehmen, entweder qualitativ oder quantitativ.
- Identifizierung der finanziellen und nicht-finanziellen Kosten“ (PRITI S. 2017: 29).

TORABI S. A. et al. (2014: 311) haben in ihrem Rahmenwerk für die Durchführung einer Business Impact Analyse die nachfolgenden Schritte definiert:

- Identifizierung der Schlüsselprodukte der Organisation
- Zerlegung der Schlüsselprodukte in kleinste wesentliche Funktionen,
- Identifizierung der geschäftskritischen Funktionen,
- Ermittlung der Kontinuitätsparameter:
 - Maximum Tolerable Period of Disruption (MTPD) und
 - Minimum Business Continuity Objective (MBCO)

In einer Business Impact Analyse müssen alle Schlüsselprozesse identifiziert werden, die nach einer Unterbrechung unbedingt wiederhergestellt werden müssen, um prioritäre kritische Funktionen funktionsfähig zu betreiben. Die Identifizierung von kritischen Funktionen kann anhand von verschiedenen Gliederungen wie Abteilungsgliederung, Kostengliederung und Ressourcengliederung erfolgen. (TORABI S. A. et al. 2014: 312)

Durch dieses Rahmenwerk können alle Schlüsselprodukte und deren erforderliche Funktionen identifiziert werden. Dies ist insbesondere wichtig, wenn die Organisation nicht in der Lage ist alle gestörten Funktionen gleichzeitig wiederherzustellen. Mit dieser Methode können erforderliche Funktionen priorisiert werden und entsprechende kritische Funktionen identifiziert werden. (TORABI S. A. et al. 2014: 313)

Bei der praktischen Umsetzung einer Business Impact Analyse ist es unerlässlich das Geschäft einer Organisation und deren vielfältigen Abhängigkeiten sowie Beziehungen zu verstehen. Eine Prozesslandkarte mit einer Einteilung in Aktivitäten und Unteraktivitäten eignet sich hierfür ausgezeichnet.

TAARUP-ESBENSEN J. (2020: 4) beschreibt in seiner Struktur zur Durchführung einer Business Impact Analyse die Abfolge der Aktivitäten zur fundierten Analyse der Herausforderungen in Bezug auf das Business Continuity Management, mit dem eine Organisation konfrontiert ist.

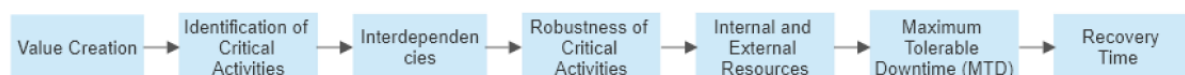


Abbildung 38: Struktur zur Durchführung einer BIA (Quellen: TAARUP-ESBENSEN J. 2020: 4)

Im nachfolgenden werden die einzelnen Schritte zur Durchführung einer BIA nach TAARUP-ESBENSEN J. (2020: 4-5) kurz beschrieben:

1. Wertschöpfung (Value Creation):

- Die Beschreibung der Wertschöpfungsprozesse ist von zentraler Bedeutung, um zu verstehen was die Organisation leistet.
 - Diese Beschreibung beinhaltet alle Aktivitäten, die zur Erreichung der gesetzten Organisationsziele nötig sind.
2. Identifizierung der kritischen Aktivitäten (Identification of Critical Activities):
- Während der Analyse der Aktivitäten muss bei allen Prozessschritten, welche zur Aktivität gehören untersucht werden, welche Prozessschritte einen wesentlichen Anteil zur Erreichung der Ziele für diese Aktivität haben.
3. Interdependenzen (Interdependencies):
- Als Interdependenzen wird die Verbindung sowie die Abhängigkeit zwischen den kritischen Aktivitäten beschrieben.
 - Die Prozesslandkarte einer Organisation kann zur Analyse hinzugezogen werden, indem die primären Aktivitäten und sekundären (unterstützenden) Aktivitäten auf ihre Abhängigkeiten untersucht werden.
4. Robustheit der kritischen Aktivitäten (Robustness of Critical Activities):
- Mit der Robustheit einer kritischen Aktivität wird die Fähigkeit beschrieben, wie störende Ereignisse absorbiert werden können, um die Aktivität so wenig wie möglich zu beeinträchtigen.
 - Mit dem Robustheitsgrad wird eine Abschätzung in Abhängigkeit des Eintretens von störenden Ereignissen getätigt.
 - Mit der Robustheit der kritischen Aktivität wird die Vulnerabilität der Aktivität beschrieben.
5. Interne und externe Ressourcen (Internal and External Resources):
- Wesentliche interne wie externe physische wie intellektuelle (Kompetenzen) Ressourcen müssen identifiziert werden damit die kritische Aktivität betrieben werden kann, ohne einen Wertschöpfungsverlust zu erleiden.
6. Maximal tolerierbare Ausfallzeit (Maximum Tolerable Downtime - MTD):
- Für die maximal tolerierbare Ausfallzeit wird die Zeit ab einem Ereignis, welche die Aktivität einschränkt oder ganz ausfallen lässt, bis zum Zeitpunkt wo die Beeinträchtigung der Aktivität nicht mehr akzeptable ist, definiert.
 - Die maximal tolerierbare Ausfallzeit kann bei der Entscheidungsfindung von Prioritäten für die Behebung des Ereignisses eingesetzt werden.
 - Die „Maximum Tolerable Downtime“ kann mit der „Maximum Tolerable Period of Disruption“ (MTPD) gleich gesetzt werden.
7. Wiederherstellungszeit (Recovery Time):
- Mit der Wiederherstellungszeit wird die Zeit beschrieben, ab dem Eintreten eines Ereignisses bis zum Zeitpunkt wo damit begonnen wird die

beeinträchtigte Aktivität wieder herzustellen. Diese Wiederherstellungszeit wird als „Recovery Time Objective“ (RTO) bezeichnet.

- Die Wiederherstellungszeit kann auch genutzt werden, den maximal zu tolerierenden Datenverlust nach einem Ereignis zu beschreiben. In diesem Fall wird die Wiederherstellungszeit „Recovery Point Objective“ (RPO) bezeichnet.

In Abbildung 39 werden die Faktoren „Recovery Point Objective“, „Recovery Time Objective“ und die „Maximum Tolerable Period of Disruption“ zum besseren Verständnis dargestellt.

Defining RTO, RPO and MTPOD

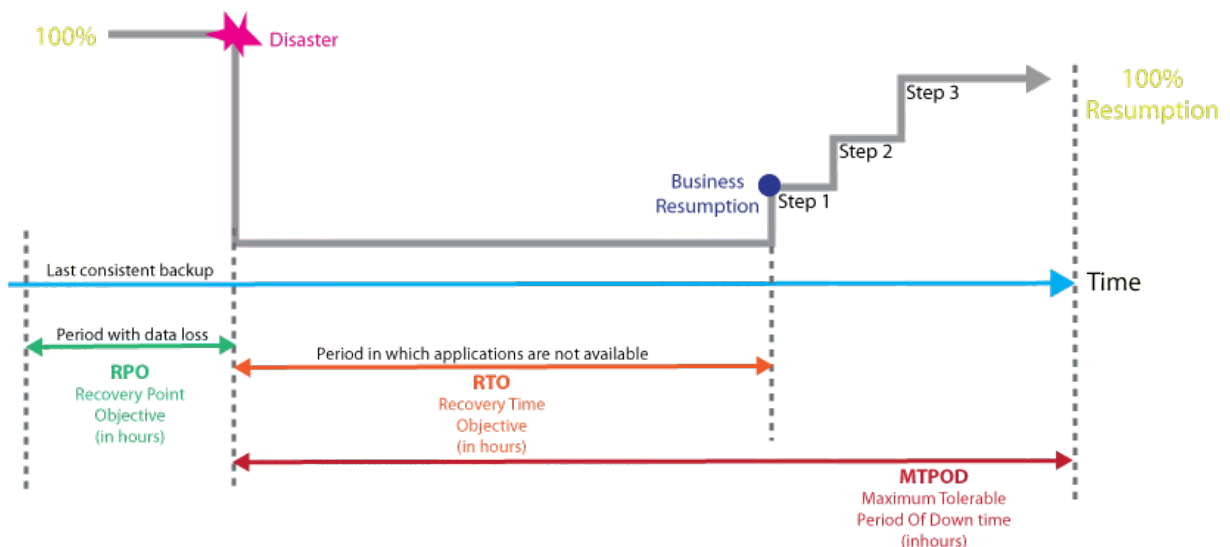


Abbildung 39: Erläuterung der Kenngrößen MTPD (MTPOD), RTO, RPO (Quelle: Goh M. H. 2011)

Wie aus den obigen Erläuterungen zu erkennen ist, gibt es keinen Standard-Ansatz (vgl. TAARUP-ESBENSEN J. 2020: 1) für eine Business Impact Analyse, sondern jede Organisation muss hier ihre Vorgehensweise, abhängig der zu analysierenden kritischen Prozesse und Ressourcen, definieren. Die Vorgehensweise sollte so festgelegt werden, dass die wertschöpfenden Prozesse mit den entsprechenden Faktoren bewertet werden. Damit die organisatorische Resilienz in einer Organisation zum Tragen kommt, muss jede Organisation die Schnittstellen zwischen den einzelnen Managementsystemen festlegen und beschreiben.

7.4 Risikomanagement und Business Continuity Management in kritischen Infrastrukturen

MEISSNER J. O. (2017: 53-54) beschreibt das Management organisationaler Resilienz als Risiko- und Sicherheitskultur in einem Resilienztrichter (Abbildung 40) von der präventiven bis zur reaktiven Strategie, Führung und Organisation. In diesem Resilienztrichter werden als Eingangsbedingungen u.a. das betriebliche Gesundheitsmanagement (BGM), das Qualitätsmanagement, das Risikomanagement, Kontinuitätsmanagement, Notfall- & Krisenmanagement bis hin zum öffentlichen Katastrophenmanagement berücksichtigt. Daraus folgt, dass das Management der organisationalen Resilienz nicht nur von einer Abteilung in einer

Organisation abhängig sein kann, sondern dass alle betroffenen Abteilung interdisziplinär zusammen arbeiten müssen um die Resilienz zu fördern.

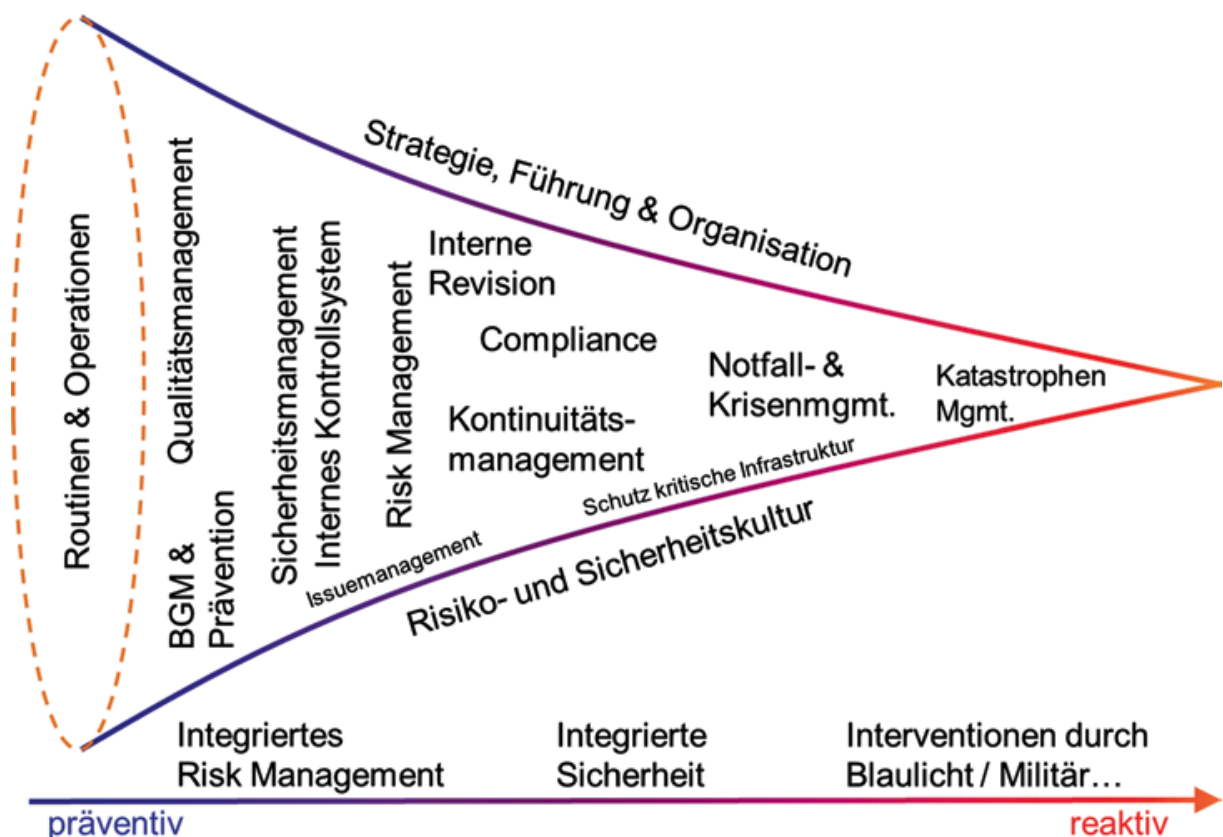


Abbildung 40: Der Resilienztrichter (Quelle: MEISSNER J. O. 2017: 53)

Das Modell des Resilienztrichters kann für kritische Infrastrukturen sowie für komplexe Krankenhausinfrastrukturen sehr interessant sein, da diese in der heutigen modernen vernetzten Gesellschaft für die Versorgung von wesentlichen Dienstleistungen und Waren unverzichtbar sind (vgl. WILLISEGGER J. 2017: 61). Demzufolge müssen kritische Infrastrukturen gezielt auf Betriebsunterbrechungen reagieren um im Ereignisfall Schäden und deren Folgen abwehren zu können. Das Business Continuity Management ist dafür ausgelegt mögliche Betriebsstörungen oder -unterbrechungen zu identifizieren und im Vorfeld eines möglichen Ereignisses präventive Schutzmaßnahmen zu definieren um im Notfall die Kontinuität der Geschäftsaktivitäten zu gewährleisten. Wo hingegen das Risikomanagement dafür ausgelegt ist Risiken zu identifizieren, zu analysieren und zu bewerten um anschließend Risikobewältigungsstrategien, wie in Abbildung 34 dargestellt, einzusetzen. (vgl. WILLISEGGER J. 2017: 73-74)

BAUMANN S. und VON RÖSSING R. (2017: 190) geben an, dass sowohl Business Continuity Management als auch Risikomanagement das Ziel haben strategische Geschäftsprozesse zu schützen. Entsprechend werden Risiken für potenzielle Betriebsunterbrechungen identifiziert und Schutzmaßnahmen gemanagt. In beiden Systemen werden zum Teil die gleichen Elemente genutzt. Beide Systeme sollen idealerweise in einer Organisation gleichberechtigt betrieben werden.

Für die Analyse von vernetzten „systemischen Risiken“ (BAUMANN S. und VON RÖSSING R. 2017: 192) kann das Business Continuity Management gut eingesetzt werden. Hier

fehlen dem Risikomanagement die nötigen Möglichkeiten diese zu analysieren. Im Kapitel 5 wurde eingehend auf die heutigen Gefährdungen von vernetzten cyber-physischen Systeme eingegangen. Die Vernetzung und daraus resultierenden Abhängigkeiten müssen zukünftig mehr denn je von kritischen Infrastrukturen und im besonderen Maße von Krankenhäusern (Patientenversorgung) berücksichtigt werden.

Wie eben dargestellt können der simultane Einsatz des Business Continuity Managements und des Risikomanagements nützliche Synergieeffekte in einer kritischen Infrastruktur generieren. Zum Schutz der Infrastruktur und zur Förderung der organisatorischen Resilienz hinsichtlich Betriebskontinuität, auch bei Störfällen, ist der Einsatz der beiden System absolut berechtigt und eine Verzahnung der System sicherlich sinnvoll. (vgl. BAUMANN S. und VON RÖSSING R. 2017: 193)

In komplexen vernetzten Krankenhausinfrastrukturen können die beiden Systeme zu einem Mehrwert in der organisatorischen Resilienzsteigerung beitragen.

8 Fallstudie am Bsp. der zentralen Aufbereitungseinheit für Medizinprodukte

In der vorliegenden Arbeit wird für die Fallstudie ein fiktives Krankenhaus als Grundlage verwendet. Das fiktive Krankenhaus basiert auf einer realen Krankenhausorganisation, allerdings wurden die Daten anonymisiert. Bevor die Informationsbeschaffung und die Risikoanalysen beschrieben werden, folgen einige allgemeine Informationen zum besseren Verständnis des fiktiven Krankenhauses, der Aufbereitungseinheit für Medizinprodukte (AEMP) und eine Prozesslandkarte.

8.1 Beschreibung des fiktiven Krankenhauses und der AEMP

Zur Verdeutlichung der Ausgangslage wird folgende Größenordnung angenommen:

- 2 Standort mit einer Entfernung von ca. 25 km
- 1.050 Mitarbeiter
- 160 zugelassenen Ärzte
- Hauptstandort:
 - o Zentrale Notaufnahme
 - o Verschiedene Ambulanzen
 - o Bildgebende Abteilung
 - o 6 Operationssäle
 - o Zentrale Aufbereitungseinheit für Medizinprodukte
 - o Reanimationsabteilung mit 16 Betten
 - o Entbindungsstation
 - o Dialysestation
 - o 277 Betten in zehn Pflegeeinheiten mit verschiedenen medizinischen Fachspezialitäten
- Nebenstandort:
 - o Eine Ambulanz
 - o Bildgebende Abteilung
 - o 2 Operationssälen
 - o 80 Betten in drei Pflegestationen mit verschiedenen medizinischen Fachspezialitäten

8.1.1 Die Gebäudestruktur

Der Hauptstandort unterteilt sich in verschiedene Gebäudeteile mit zwei großen Sektoren, zum einen der Sektor Nord mit den Bauteilen BT1.1, BT1.2, BT1.3 und BT2.0 und zum anderen der Sektor Süd mit den Bauteilen BT3.1, und BT3.2. Die Organisationseinheiten wurden folgendermaßen aufgeteilt:

BT1.1: Lager, verschiedene Ambulanzen, Dialyse, Bettenhaus mit 4 Pflegestationen

BT1.2: Apotheke, Labor, verschiedenen Ambulanzen, Bettenhaus mit 5 Pflegestationen

BT1.3: Administrative Abteilungen

BT2.0: Zentraler Gebädetrakt, Eingang, Anmeldung, verschiedene Ambulanzen, 1 Pflegestation

BT3.1: Zentrale Küche, zentrale Notaufnahme, Reanimationsabteilung, **Aufbereitungseinheit für Medizinprodukte**

BT3.2: Zentrales Archiv, Bildgebende Abteilung, Operationsbereich

Die Operations-(OP)-bereiche werden in einem Krankenhaus als wesentliche Organisationseinheiten angesehen (vgl. SCHMECK J. et al. 2008: 805). Wegen der zentralen Bedeutung der OP-Bereiche ist ein reibungsloser Ablauf und eine gute Abstimmung mit allen Stakeholdern unabdingbar. Einer der Stakeholder ist die Aufbereitungseinheit für Medizinprodukte (AEMP). Die AEMP bereitet wiederverwendbare Medizinprodukte (MP) für den OP-Bereich aber auch für alle anderen Abteilungen (u.a. Reanimationsabteilung, Zentrale Notaufnahme, Ambulanzen, Pflegestationen, ...) auf. Zusätzlich ist die AEMP zuständig für die Aufbereitung von flexiblen Endoskopen, welche in der Endoskopie-Abteilung benutzt werden.

8.1.2 Die Aufbereitungseinheit für Medizinprodukte

Als zentrale wichtige interne Dienstleistungsabteilung (vgl. BEYN M. und LÜTHI R. 2020: 479) ist die zentrale AEMP eine der kritischen Dienstleistungen im Krankenhaus. Für die aktuelle Arbeit ist die AEMP am Hauptstandort des fiktiven Krankenhauses untergebracht.

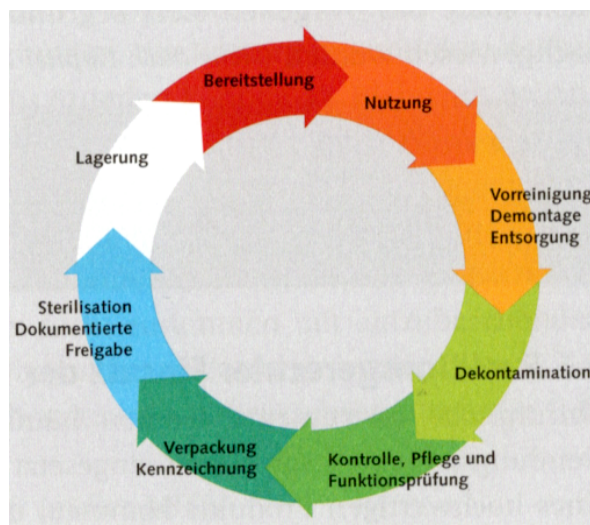


Abbildung 41: Aufbereitungskreislauf für Medizinprodukte (Quelle: KIRMSE G. und WILD R. 2020: 123)

In Abbildung 41 ist der Aufbereitungskreislauf der AEMP dargestellt. Welche Prozesse der AEMP zufallen und welche Aufgaben den Benutzer-Abteilungen zufallen, wird von der Krankenhausorganisation festgelegt. Hier müssen organisatorische wie auch räumliche Gegebenheiten berücksichtigt werden. Im aktuellen fiktiven Krankenhaus werden die Prozesse „Dekontamination“, „Kontrolle, Pflege & Funktionsprüfung“, „Verpackung & Kennzeichnung“ sowie „Sterilisation, Dokumentieren & Freigabe“ durch die AEMP ausgeführt.

Das Raumkonzept einer AEMP sieht drei verschiedene Funktionsbereiche mit entsprechenden Schleusen vor, so dass eine Rekontamination bestmöglich ausgeschlossen werden kann. (BEYN M. und LÜTHI R. 2020)

Wie in Abbildung 42 dargestellt, gehören zu den drei Funktionsbereichen (vgl. BEYN M. und LÜTHI R. 2020: 482-484):

- Anliefer- und Dekontaminationsbereich - „ unreiner Bereich “
 - o Annahme der Medizinprodukte (MP)
 - o Manuelle Vorreinigung
 - o Vorbereitung für die maschinelle Reinigung und Desinfektion
- Packbereich – „ reiner Bereich “
 - o Reinigungs- und Desinfektionsgeräte (RDG) im Übergangsbereich vom Dekontaminationsbereich
 - o Kontrollieren der MP nach der Desinfektion
 - o Pflege der MP
 - o Funktionskontrolle der MP
 - o Verpackung der MP
 - o Vorbereitung zur Sterilisation
- Sterilgut-Bereich
 - o Sterilisatoren im Übergangsbereich von der Packzone
 - o Freigabe der MP
 - o Zwischenlagerung vor dem Abtransport

Im Übergang zwischen Dekontaminationsbereich und Packbereich sind die Reinigungs- und Desinfektionsgeräte (RDG) sowie die Reinigungs- und Desinfektionsgeräte Endoskopie (RDG-E) installiert. Zwischen dem Packbereich und dem Sterilgut-Bereich werden die Sterilisationsgeräte betrieben. Für die Endoskope wird ein spezifischer Plasmasterilisator betrieben. Zusätzlich werden noch Sozialräume, Personalschleusen, Lagerflächen und administrative Räume benötigt.

In dieser Fallstudie ist die AEMP im Bauteil 3.2 im ersten Obergeschoss angeordnet, in kurzer Distanz zum OP-Bereich.

Aus betriebswirtschaftlichen Gründen und wegen hoher Ausfallkosten im OP-Bereich fordern BEYN M. und LÜTHI R. (2020: 489) die Schaffung von nötigen Redundanzen bezüglich Prozessgeräten und Medienversorgung. Dies insbesondere in kleinen Aufbereitungseinheiten für Medizinprodukte wo der Ausfall eines Gerätes ein größeres Risiko birgt. Für die kritische Infrastruktur Krankenhaus ist es wesentlich den Prozess der AEMP aufrecht zuhalten um auch im Not- oder Katastrophenfall die gesundheitliche Versorgungsdienstleistung der Bevölkerung über das Krankenhaus anbieten zu können. Neben den technischen Ressourcen und kritischen Prozessgeräten sind die fachkundigen Personen in der AEMP ebenso wesentlich, da der Betriebsablauf gemäß BEYN M. und LÜTHI R. (2020: 489) überwiegend aus manueller Tätigkeit besteht, wobei die AEMP-Prozessgeräte „Reinigungs- und Desinfektion“ sowie „Sterilisation“ nicht zu vernachlässigen sind.

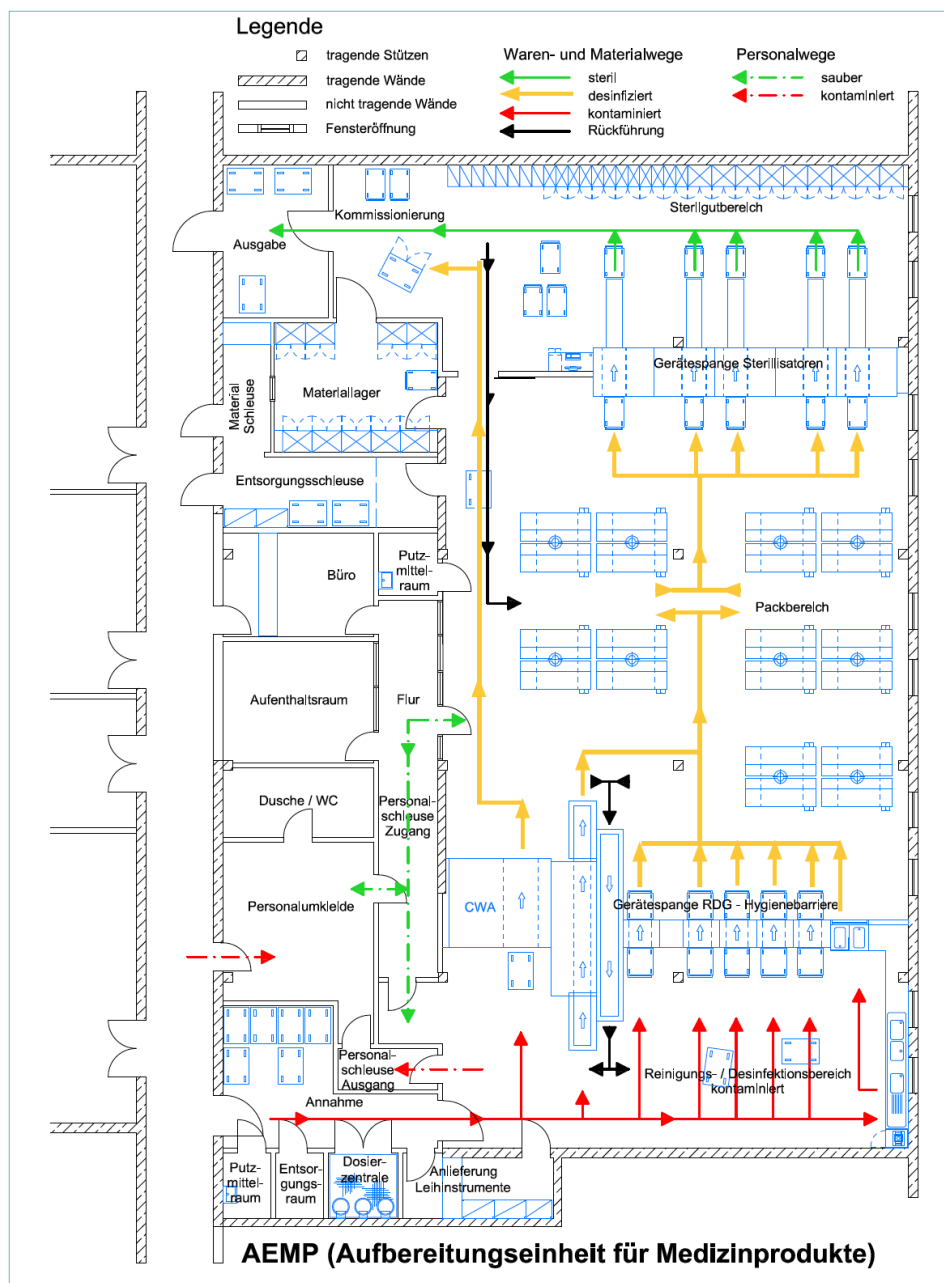


Abbildung 42: Raumkonzept einer AEMP (Quelle: CARTER A. et al. 2015: 6)

Neben den technischen und personenbezogenen Ressourcen werden auch vermehrt cyber-physische Systeme im Krankenhaus und der AEMP eingesetzt.

8.1.3 Digitalisierung im Krankenhaus und insbesondere in der AEMP

Wie in Abbildung 29 dargestellt, ist das intelligente Krankenhaus bereits allgegenwärtig. Immer mehr Systeme werden vernetzt und Daten müssen ausgetauscht werden.

Aus legaler Sicht der Medizinproduktegesetzgebung, um eine gleichbleibende hohe Qualität in Aufbereitungseinheiten für Medizinprodukte zu garantieren und eine detaillierte Ausführung der Einzelschritte zu dokumentieren, ist der Einsatz eines Qualitätsmanagementsystems unabdingbar. (vgl. SCHMECK J. et al. 2008: 808)

Die Medizinprodukte im Aufbereitungskreislauf werden, bis auf Einzelverpackungen, chargenweise als Set den Prozess durchlaufen. Dafür werden die einzelnen

Medizinprodukte vor der Verpackung immer in der gleichen Position in Siebe gelegt. Dies garantiert dem Operateur im OP-Saal identische Zusammensetzung und Reihenfolge der Medizinprodukte (Instrumentarium) in einem Sieb vorzufinden. Ebenfalls kann die OP-Vorbereitung immer nach demselben Standard ablaufen.

Alle Prozessgeräte sind mit EDV-Systemen zum Betreiben und Dokumentieren der einzelnen Prozessschritte ausgestattet. An jedem Arbeitsplatz befinden sich EDV-Systeme zur elektronischen Datenerfassung der einzelnen Chargen. In einer integrierten QM-Software, welche mit den Benutzerabteilungen vernetzt ist, können neben der Dokumentation für das Qualitätsmanagement auch Chargenverwaltungen sowie die Priorisierung in der Aufbereitung automatisch gesteuert werden. Eine Vernetzung mit dem Krankenhausinformationssystem ist möglich wird aber im aktuellen Fallbeispiel nicht berücksichtigt, wenngleich die verantwortlichen Personen der AEMP auf das Krankenhausinformationssystem zugreifen, um die nötigen Informationen zum geplanten OP-Programm abzugreifen und um die Aufbereitung der notwendigen Siebe manuell zu steuern.

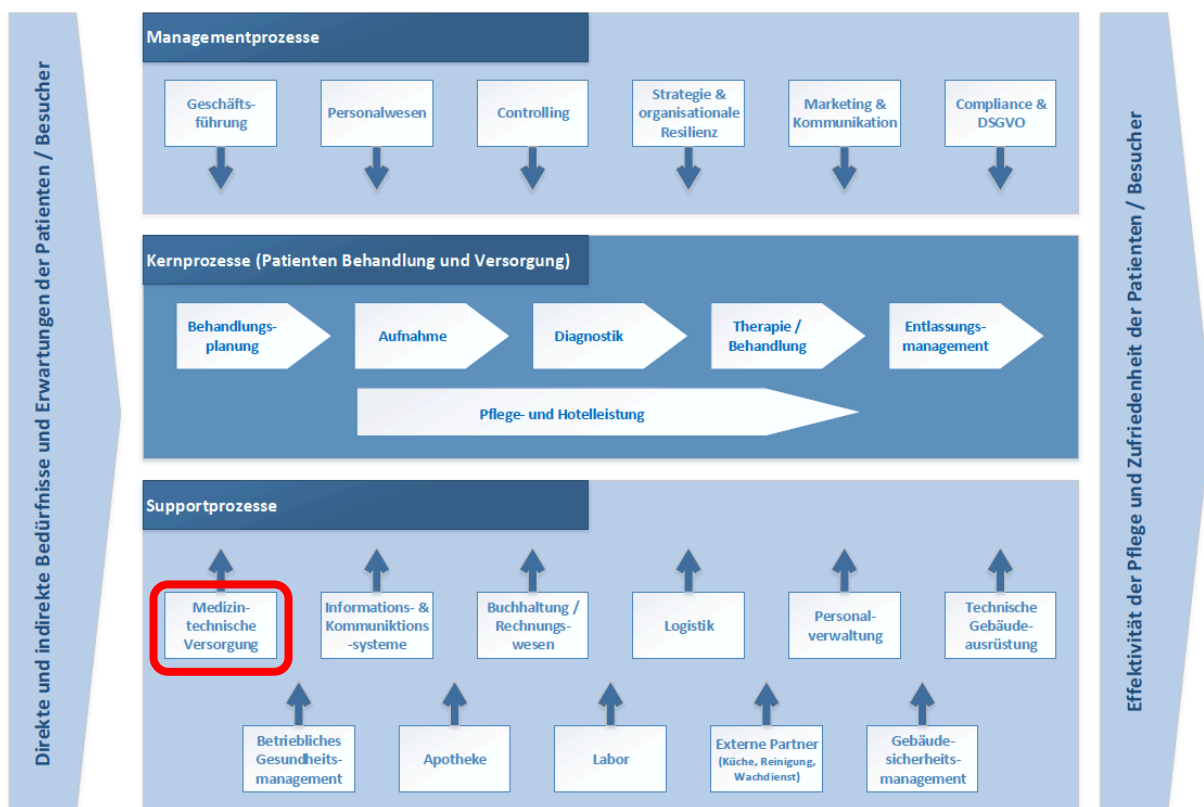


Abbildung 43: Prozesslandkarte fiktives Krankenhaus

Neben den Prozessgeräten sind auch die haustechnischen Versorgungsanlagen zur Überwachung und Steuerung mit der EDV-basierten Gebäudeleittechnik vernetzt.

8.1.4 Prozesslandkarte

An Anlehnung an (KUNTSCHE P. und BÖRCHERS K. 2017a: 108), (MÖLLER E. B. 2016: 39) und (ROITSCH M. et al. 2020: 547) wurde für das fiktive Krankenhaus eine angepasste Prozesslandkarte erstellt.

In der Prozesslandkarte aus Abbildung 43 ist die AEMP im Supportprozess „Medizin-technische Versorgung“ anzusehen (Markierung) und stellt somit einen unterstützenden Prozess dar, der die Kernprozesse Aufnahme, Diagnostik, Therapie und Behandlung mit wiederverwendbaren sterilen Medizinprodukten versorgt.

Für die anschließende Datensammlung ist es wichtig zu wissen wie die AEMP in der gesamten Prozesslandschaft integriert ist, um die Abhängigkeiten der kritischen Prozessen und Ressourcen bestimmen zu können.

8.2 Datensammlung zu den wesentlichen Prozessen

Die Vorgehensweise zur Datensammlung wurde im Kapitel 3.3 zur Informationsbeschaffung beschrieben.

In einem ersten Interview mit der Leiterin, der QM-Beauftragten und dem Bereichsleiter der Pflegedirektion im Oktober 2020 wurden erste Informationen zur Funktionsweise der AEMP eingeholt. Als Ergebnis der anschließenden Analyse entstand der vereinfachte Kreislauf zur Benutzung und Aufbereitung von wiederverwendbare Medizinprodukte mit den wesentlichen Schritten in der AEMP (siehe Abbildung 44).

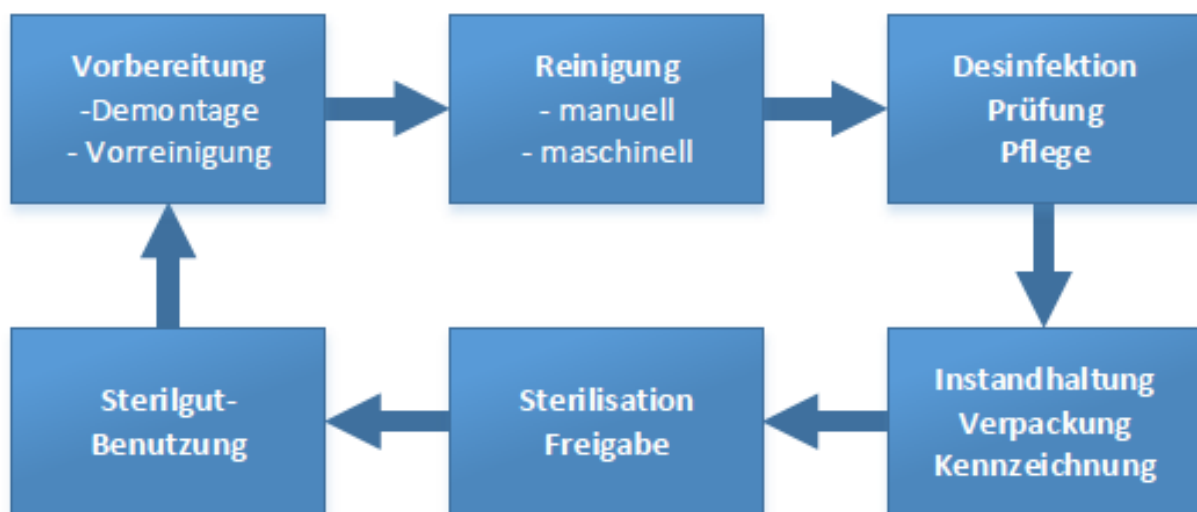


Abbildung 44: vereinfachter Kreislauf der wiederverwendbaren Medizinprodukte

In einem weiteren Interview Ende Januar 2021 mit der QM-Beauftragten wurden die einzelnen Prozessschritte im Detail durchgenommen. Aus diesem Interview wurden die kritischen Prozessschritte für die Aufbereitung der Medizinprodukte und der Endoskope ermittelt. Die benötigten Ressourcen, von denen die einzelnen Prozessschritte abhängig sind, wurden so gut wie möglich durch die QM-Beauftragte zusammengestellt.

Wie in Kapitel 3.3 beschrieben wurden die einzelnen Prozessschritte entweder den Benutzerabteilungen, der AEMP oder der Logistik zugeteilt. Aus dieser Zuteilung wurden die kritischen Prozesse, wie in Tabelle 5 dargestellt, definiert. Im Anschluss wurden die wesentlichen Ressourcen der kritischen Prozesse in sechs Kategorien aufgeteilt.

1. Internes Personal (Rollen)
2. Externe Partner

3. IT Software
4. Prozessgeräte
5. Versorgung / Anlagen
6. Sicherheitstechnik

Für jede Ressourcen-Kategorie wurden kritische Ressourcen und eine erste Beschreibung vorgenommen. (siehe Tabelle 6 bis Tabelle 11)

Tabelle 5: kritische Prozessschritte der AEMP

Kritische Prozesse	Beschreibung
1. Transport gebrauchte Medizinprodukte & Endoskope	Transport benutzte MP & Endoskope aus den Verbrauchsabteilung zur AEMP, Scannen der Transportsiebe
2a. Vorreinigung & Vorbereitung MP	Auspacken der Siebe, grobe Vorreinigung, wenn nötig, Vorbereitung der Geräteträger mit MP
2b. Vorreinigung & Vorbereitung Endoskope	Grobe Vorreinigung der Endoskope und Vorbereitung für die maschinelle Reinigung
3a. Maschinelle Reinigung & Desinfektion MP	Maschinelle Reinigung: 10 min bei 55°C, Desinfektion 5min bei 90°C, Trocknung 45-60 min
3b. Maschinelle Reinigung & Desinfektion Endoskope	Maschinelle Reinigung:
4a. Sichtprüfung & manuelle Trocknung MP	Übernahme der desinfizierten MP vom Geräteträger, Prüfung auf Sauberkeit
4b. Sichtprüfung & Trockenschrank Endoskope	Übernahme der desinfizierten Endoskope, Prüfung auf Sauberkeit
5a. Freigabe nach Prüfung Medizinprodukte	Freigabe zur Funktionskontrolle nach der Sichtprüfung
5b. Freigabe nach Prüfung Endoskope	Freigabe zur Funktionskontrolle nach der Sichtprüfung
6a. Funktionskontrolle & Pflege MP	Funktionskontrolle zum Teil mit unterstützenden Geräten, Pflege (z.B. ölen), Ersetzen verbrauchte MP
6b. Funktionskontrolle & Pflege Endoskope	Funktionskontrolle und Pflege der Endoskope
7a. Verpackung Medizinprodukte	Manuelle Verpackung von kompletten Sieben und Vorbereitung Sterilisation
7b. Verpackung Endoskope	Vorbereitung Endoskope für die Plasmasterilisation
8a. Sterilisation Medizinprodukte	Sterilisation verpackter Siebe
8b. Plasmasterilisation Endoskope	Plasmasterilisation verpackter Endoskope (Niedertemperatur)
9a. Freigabe nach Sterilisation MP	Freigabe der Siebe nach der Sterilisation für den Transport
9b. Freigabe nach Sterilisation Endoskope	Freigabe der Endoskope nach der Plasmasterilisation für den Transport
10. Transport sterile Medizinprodukte & Endoskope	Transport sterilisierte MP und Endoskope von der AEMP zum internen Lager je Verbrauchsabteilung

Tabelle 6: Ressourcen-Kategorie Internes Personal

Internes Personal (Rollen)	Beschreibung
Logistiker	Intern für die Verteilung innerhalb der Standorte, Extern für den Transport zw. den Standorten
Leiter Abteilung Einkauf / Lager / Logistik	Verantwortlich für die interne wie externe Logistik
Fachkundige in der Aufbereitung von MP	Bearbeitung der Prozessschritte 2 bis 9

8 Fallstudie am Bsp. der zentralen Aufbereitungseinheit für Medizinprodukte

AEMP Stammdatenadministrator	Pflegen der Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope
Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Verantwortlich für das exklusive Qualitätsmanagement in der AEMP und ist gleichzeitig Stellv. Leiterin AEMP
Leitung der AEMP	Verantwortlich für die Organisation der AEMP
Bereichsleiter Pflegedirektion	Mittelmanagement in der Pflegedirektion zuständig unter anderem für die AEMP
Technischer Dienst	Verantwortlich für den technischen Zustand der AEMP-Ausstattung und der techn. Versorgung (Strom, Wasser, ...)
IT-Hardwarespezialisten	Verantwortlich für die IT-Hardware Ausstattung der AEMP
IT-Softwarespezialisten	Verantwortlich für die Schnittstellen zw. der anlagenspezifischen Software und der QM- / KIS-Software
Abteilungsleiter (der Benutzer-Abteilungen)	Verantwortlich für die reibungslosen Vorbereitung der MP / Endoskope zum Abtransport
Reinigungskräfte	Internes Reinigungspersonal für die Oberflächenreinigung und maschinelle Reinigung der Handwagen
Leiter Reinigung	Verantwortlich für das interne Reinigungspersonal

Tabelle 7: Ressourcen-Kategorie Externe Partner

Externe Partner	Beschreibung
Externer Transportunternehmer	Transport der benutzten und sterilen MP in spezifischen Transportwagen zw. Den Standorten
Wartungsfirma RDG	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma RDG-E	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma Einschweißgerät	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma Sterilisator	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma Plasmasterilisator	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma Versorgungsanlagen	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma Sicherheitstechnische Anlagen	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma IT-Hardware	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung
Wartungsfirma IT-Software	Wartung, Reparatur, Instandsetzung gemäß Wartungsvertrag, gesonderte Bestellung

Tabelle 8: Ressourcen-Kategorie IT-Software & Prozessgeräte

IT-Software	Beschreibung
Qualitätsmanagement Software	13 Arbeitsplätze an den versch. Stationen in der AEMP
Krankenhausinformationssystem	3 Arbeitsstationen mit Zugriff auf das KIS
klassische IT-Office Software	3 Arbeitsstationen mit Zugriff auf klassische IT-Office Software

8 Fallstudie am Bsp. der zentralen Aufbereitungseinheit für Medizinprodukte

anlagen spezifische Software	Software welche spezifisch für die Funktionsfähigkeit des Gerätes / der Anlage programmiert ist
Verwaltung Leihgeräte	Hausinterne Software zur Verwaltung der Leihgeräte MP
Internetzugang nach extern	3 Arbeitsstationen mit Zugang ins öffentliche WorldWideWeb

Tabelle 9: Ressourcen-Kategorie IT-Software & Prozessgeräte

Prozessgeräte	Beschreibung
Waschbecken für manuelle Reinigung	Waschbecken mit Handbrause, Trinkwasser / VE-Wasser
Ultraschallbecken	Ultraschalltischgerät
Reinigungs- & Desinfektionsgeräte (RDG)	RDG zur automatisierten Reinigung, Desinfektion und Trocknung der MP
Reinigungs- & Desinfektionsgeräte Endoskope	RDG-E zur automatisierten Reinigung und Desinfektion von Endoskopen
Packtische	höhenverstellbare Arbeitstische für die Sichtprüfung, man. Trocknung, Funktionsprüfung, Pflege und Verpackung
Sterilisatoren	Sterilisatoren für die Siebe mit MP, und die
Plasmasterilisatoren	Niedertemperatur - Plasmasterilisator nur für verschiedenen Endoskope
Einschweißgerät	Einschweißgerät für einzelne MP
unterstützende Geräte zur Funktionskontrolle	Kleingeräte für die Funktionskontrolle

Tabelle 10: Ressourcen-Kategorie Versorgung / Anlagen

Versorgung / Anlagen	Beschreibung
AV-Stromversorgung	Einspeisung Stromversorgung vom BHKW
SV-Stromversorgung	Einspeisung Sicherheitsstromversorgung vom BHKW
Reindampf	Herstellung Reindampf aus Hausdampf in Eigenproduktion
Hausdampf	Einspeisung Hausdampf vom BHKW
Druckluft 5 BAR	Produktion von Druckluft über die eigenen Druckluftversorgungsanlage
Kälte	Einspeisung Kälteversorgung vom BHKW
Trinkwasser	Einspeisung Trinkwasser durch den Wasserversorger
VE Wasser	Herstellung VE Wasser in Eigenproduktion aus Trinkwasser
Abwasser	Abwassersammelleitung im UG 2 inkl. Abpumpen mit Abwasserhebeanlage ins öffentliche Abwassernetz
IT-Hardware	Strategische Verteilung der PC's inkl. Zubehör, Handscanner, Drucker
IT-Netzwerk	Anbindung PC's und Großgeräte am IT-Netzwerk
Lüftungsanlage	zentrale Lüftungsanlage für die gesamte AEMP Reinraumklasse 2
Aufzüge	4 Bettenlifte mit 3 verschiedenen Maschinenräumen.
Gebäudeleittechnik	Gebäudeleittechnik ist eine Überwachungssoftware für alle technischen Versorgungsressourcen

Tabelle 11: Ressourcen-Kategorie Sicherheitstechnik

Sicherheitstechnik	Beschreibung
Gefahrenmanagementsystem	Gefahrenmanagement ist eine Überwachungssoftware für die sicherheitstechnischen Anlagen
Brandmeldeanlage	BMA zur Überwachung der AEMP Räume
Zutrittskontrolle	Zutrittskontrolle für die verschiedenen Eingänge der AEMP

Damit die Daten für die statische wie auch dynamischen Risikoanalyse vervollständigt und alle wichtigen Informationen strukturiert gesammelt werden können, wurde im Anschluss an das Gespräch ein Fragebogen inkl. allgemeine Beschreibung der Vorgehensweise und eine BIA-Matrix, in Form einer Excel-Datei mit mehreren Blättern, erstellt.

8.2.1 Erstellung des Fragebogens

Zur Erklärung der Vorgehensweise einer Business Impact Analyse wurde eine Beschreibung ausgearbeitet, so dass Personen, die an der Erstellung der BIA-Matrix beteiligt sind und selten mit einer BIA arbeiten ein Verständnis dafür entwickeln können. Die Beschreibungen wurden auf drei verschiedene Blätter in der Datei erstellt Deckblatt (siehe Anhang 14.2), Allgemeine Informationen (siehe Anhang 14.3), und Prozessbeschreibung (siehe Anhang 14.4). Nachfolgende Beschreibungen wurden integriert.

Was versteht man unter einer Business Impact Analyse (BIA)?

Damit das Krankenhaus Risiko- und Business Continuity Management betreiben kann, müssen kritische Prozesse identifiziert, analysiert und bewertet werden. In diesem Zusammenhang wird eine BIA eingesetzt. Die BIA ist ein Werkzeug, das Informationen zu Schwachstellen liefern kann. Werden diese Schwachstellen identifiziert, können entsprechende Gegenmaßnahmen eingeleitet (Risikoreduktion) und Kontinuitätspläne erstellt werden.

Ablauf der BIA - Datensammlung:

Die Datensammlung dient dazu, ein all umfassendes Verständnis zu den kritischen Prozessen zu erhalten. Anschließend kann eine Business Impact Analyse für diese Prozesse durchgeführt werden. Folgende Schritte sind dafür notwendig:



- 1) Prozessbeschreibung zum allgemeinen Verständnis,
- 2) Identifikation von kritischen Prozessschritten,
- 3) Identifikation von internen und externen Partnern, sowie allen Ressourcen,

- 4) Bestimmung der Abhängigkeiten zwischen den Prozessschritten, den Partnern und den Ressourcen,
- 5) Beschreibung der Robustheit von Prozessen, Partnern und Ressourcen (Ausfallsicherheit, Redundanzen),
- 6) Bestimmung der Schadensklassen für (Operate, Legal, Finance, Image),
- 7) Bestimmung des Recovery Point Objective (RPO),
- 8) Bestimmung des Recovery Time Objective (RTO),
- 9) Bestimmung des maximal tolerierbaren Ausfallzeitraumes (MTPD).

Schadensklassen

Die Schadensklassen wurden dem BSI-Standard 200-4 Business Continuity Management (siehe: BSI 2021: 201-202) entnommen.

Managebar - Gering:

Allgemeine Beschreibung: Ein Ausfall hat geringe, kaum spürbare Auswirkungen.

Operate: Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb wird unwesentlich beeinträchtigt.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen Konsequenzen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution unerheblich.

Image: Negative Innen- und Außenwirkung (Imageschaden): In Einzelfällen ist eine geringe, nicht andauernde Ansehensbeeinträchtigung zu erwarten.

Signifikant - Mittel:

Allgemeine Beschreibung: Ein Ausfall hat spürbare Auswirkungen.

Operate: Beeinträchtigung der Aufgabenerfüllung: Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen. Verstöße können zu Konsequenzen führen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution tolerabel, aber nicht unerheblich.

Image: Negative Innen- und Außenwirkung (Imageschaden): Eine Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. Der Schaden kann durch interne Mittel begrenzt werden, z.B. durch eine angepasste Kommunikation.

Kritisch - Hoch:

Allgemeine Beschreibung: Ein Ausfall hat nicht tolerierbare Auswirkungen

Operate: Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist massiv und über längere Zeit eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand oder zusätzlichen Ressourcen zu kompensieren.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze verstoßen, Verpflichtungen zum Betrieb der kritischen Infrastruktur können nicht eingehalten werden. Verstöße führen zu erheblichen Konsequenzen, z. B. Bußgelder. Patientenschäden führen zu hohen Strafen oder Konsequenzen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.

Image: Negative Innen- und Außenwirkung (Imageschaden): Eine erhebliche, nachhaltige Ansehen- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.

Verfügbarkeitszeiten RTO, RPO, MTPD

Die Verfügbarkeitszeiten wurden bereits im Kapitel 7.3 erläutert. Diese werden ebenfalls in den Allgemeinen Beschreibungen genutzt. (siehe Anhang 14.3)

Damit die Prozessbeschreibung und die Datenerfassung wie in Abbildung 7 dargestellt erfolgen kann, wurden nachstehende Fragen ausgearbeitet. Die Ausarbeitung der Fragen wurde in einem kontinuierlichen Prozess mehrere Expert*Innenbefragungen durchgeführt. Die Rückmeldungen wurden umgehend eingearbeitet und die Fragen entsprechend angepasst. Die Fragen wurden so ausgewählt, dass die Antworten direkt in die BIA-Matrix eingegeben werden können.

1) Kunden

- a) Welche Abteilungen mit direkter Patientenversorgung hängen von den zu bewertenden Prozessen ab?
- b) Welche Abteilungen mit indirekter Patientenversorgung hängen von den zu bewertenden Prozessen ab?

2) Kritische Prozessschritte / Ressourcen

- a) Welche kritischen Prozessschritte werden durch die Abteilung ausgeführt?
- b) Welche kritischen (physische und personenbezogene) Ressourcen werden für die Ausführung der kritischen Prozesse benötigt?
- c) Welche externen Partner werden für die Ausführung von kritischen Prozessen benötigt?
- d) Welche externen Partner werden für die Bereitstellung von kritischen Ressourcen benötigt?

3) Partner- und Kundenbeziehung

- a) Haben Sie Verträge (Service Level Agreement) mit den internen Kunden-Abteilungen und Partnern?

- b) Haben Sie Verträge (Service Level Agreement) mit den externen Kunden-Abteilungen und Partnern?
- c) Werden Prozesse zur Erfüllung des Auftrages der Abteilung werden durch externe Partner ausgeführt (Outsourcing)?
- 4) Robustheit der Prozesse und Ressourcen
 - a) Können störende Ereignisse absorbiert werden (Ausfallsicherheit)?
 - b) Existieren Redundanzen?
 - c) Gibt es Mindestanforderungen an die Prozessleistung, welche zur Erfüllung des Auftrages erreicht werden müssen?
- 5) Finanzaspekte
 - a) Welche durchschnittlichen Kosten müssen für einen Prozessdurchlauf aufgewendet werden?
 - b) Gibt es Wartungsverträge für die kritischen Geräte & Anlagen? Wenn ja, bitte beschreiben und die Kosten angeben.
 - c) Gibt es Ausfallkonzepte mit externen Partnern? Wenn ja, bitte beschreiben und die Kosten angeben.
- 6) Schadensklassen (3 Kategorien)
 - a) Welche Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?
 - b) Welche Auswirkungen haben der Verstoß gegen Gesetze, Vorschriften und Verträge?
 - c) Welche finanziellen Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?
 - d) Welche imageschädigenden Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?
- 7) Ausfallzeiten
 - a) Bis zu welchem rückwirkenden Zeitpunkt vor einem Ereignis, dürfen die notwendigen informatischen Daten ausfallen ohne dass sie wieder hergestellt werden müssen? – Recovery Point Objective (RPO)?
 - b) Ab welchem Zeitpunkt nach einem Ereignis muss der Prozess spätestens wiederanlaufen? – Recovery Time Objective (RTO)
 - c) Welche maximal tolerierbare Unterbrechungsdauer in der der Prozess nicht oder nur eingeschränkt verfügbar ist wird akzeptiert, bevor die Auswirkungen als inakzeptabel eingestuft werden? – Maximum Tolerable Period of Disruption (MTPD)

8.2.2 Erstellung der BIA-Matrix

Aus den Interviews, den Befragungen und den Workshops wurde eine BIA-Matrix mit den kritischen Prozessen und den kritischen Ressourcen für die Abteilung Aufbereitung von Medizinprodukten erstellt. Die BIA-Matrix wurde kontinuierlich

verbessert, angepasst und vervollständigt. Die Abhängigkeiten zwischen den Prozessen und Ressourcen wurden nur in eine Richtung eingetragen, außer bei den Fällen wo die Abhängigkeit in beide Richtungen zum Tragen kommt.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
1	► ► Liste der Prozesse & Ressourcen			kritische Prozessschritte												internes Personal (Rollen)							
2	BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			1 Transport gebrauchte Medizinprodukte	2 Vorreinigung & Vorbereitung MP	3 maschinelle Reinigung & Desinfektion MP	4 Sichtprüfung & manuelle Trocknung MP	5 Freigabe nach Prüfung Medizinprodukte	6 Funktionskontrolle & Pflege MP	7 Verpackung Medizinprodukte	8 Sterilisation Medizinprodukte	9 Freigabe nach Sterilisation MP	10 Transport sterile Medizinprodukte	0	Logistiker	Fachkundige in der Aufbereitung von MP	AEMP Stammdatenadministrator	Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Leitung der AEMP	Technischer Dienst	IT-Hardwarespezialisten	IT-Softwarespezialisten	
3																							
4	kritische Prozessschritte	1 Transport gebrauchte Medizinprodukte																					
5		2 Vorreinigung & Vorbereitung MP	x																				
6		3 maschinelle Reinigung & Desinfektion MP		x																			
7		4 Sichtprüfung & manuelle Trocknung MP			x																		
8		5 Freigabe nach Prüfung Medizinprodukte				x																	
9		6 Funktionskontrolle & Pflege MP					x																
10		7 Verpackung Medizinprodukte						x															
11		8 Sterilisation Medizinprodukte							x														
12		9 Freigabe nach Sterilisation MP								x													
13		10 Transport sterile Medizinprodukte									x												
14																							
15	internes Personal (Rollen)	Logistiker																					
16		Fachkundige in der Aufbereitung von MP																					
17		AEMP Stammdatenadministrator																					
18		Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)																					
19		Leitung der AEMP																					
20		Technischer Dienst																					
21		IT-Hardwarespezialisten																					
22		IT-Softwarespezialisten																					

Abbildung 45: Auszug BIA-Matrix - Darstellung der Abhängigkeiten

In Abbildung 45 sind auszugsweise die Abhängigkeiten in der BIA-Matrix dargestellt. In Spalte C sind die einzelnen kritischen Prozesse und Ressourcen aufgelistet. Die Eingabe in der Spalte C ergibt eine Übertragung in die Zeile 3. Die Abhängigkeiten werden anschließend mit einem **X** eingetragen. Dabei sind die Prozesse und Ressourcen aus Spalte C abhängig von den Prozessen und Ressourcen aus Zeile 3 (orange Pfeile). Dieser Vorgang wurde für alle Prozesse und Ressourcen durchexerziert und im Anschluss kontrolliert.

8 Fallstudie am Bsp. der zentralen Aufbereitungseinheit für Medizinprodukte

A B C			CN	CO
►► Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Beschreibung der Prozesse & Ressourcen	Beschreibung der Robustheit * Ist ein Prozess oder Anlage robust, kann sie störende Ereignisse absorbieren und die betriebliche Integrität erhalten. * z.B. ein Prozess mit nur einer Anlage / einem Gerät weist eine geringere Robustheit auf als ein Prozess mit mehreren Anlagen / Geräten → Redundanzen angeben ⇒ Mit den Angaben zur Robustheit, * kann die Verwendbarkeit und dem entsprechend das Mindestbetriebsniveau (MBCO) für einen kritischen Prozess bestimmt werden. * können Prozesse identifiziert werden, die als anfällig gelten
kritische Prozessschritte	1	Transport gebrauchte Medizinprodukte	Transport benutzte MP & Endoskope aus den Verbrauchsstellen zur AEMP, Annahme der Transportseile	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner
	2	Vorreinigung & Vorbereitung MP	Auspacken der Siebe, grobe Vorreinigung wenn möglich, Vorbereitung der Geräteeinheit mit MP	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	3	maschinelle Reinigung & Desinfektion MP	Maschinelle Reinigung von Medizinprodukten	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	4	Sichtprüfung & manuelle Trocknung MP	Übernahme der desinfizierten MP vom Geräteräger, Prüfung auf Sauberkeit	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	5	Freigabe nach Prüfung Medizinprodukte	Freigabe zur Funktionskontrolle nach der Sichtprüfung	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	6	Funktionskontrolle & Pflege MP	Funktionskontrolle zum Teil mit unterstützenden Geräten, Pflege (z.B. Ölen), Ersetzen verbrauchte MP	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	7	Verpackung Medizinprodukte	komplette Siebe werden manuelle verpackt und für die Sterilisation vorbereitet	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	8	Sterilisation Medizinprodukte	Verpackte Siebe werden sterilisiert	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	9	Freigabe nach Sterilisation MP	Freigabe der Siebe nach der Sterilisation für den Transport	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäuser
	10	Transport sterile Medizinprodukte	Transport sterilisierte MP und Endoskope von der AEMP zu den Verbrauchsstellen	Ausfallkonzept (F: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner
interne Personal (Rollen)	Logistiker	Bearbeitet die Prozessschritte 1 & 10 (interner Transport) innerhalb der beiden Standorte	mehrere interne Logistiker	
	Fachkundige in der Aufbereitung von MP	Bearbeiten die Prozessschritte 1 (Warennahme) & 2 bis 9	15 Personen in der AEMP in allen Bereichen einsetzbar	
	AEMP Stammdatenadministrator	Pflegen die Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope	2 Stammdatenadministratoren	
	Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Verantwortet das Qualitätsmanagement exklusiv in der AEMP und ist gleichzeitig Stellv. Leiterin AEMP	QM hat keinen Stellvertreter	
	Leitung der AEMP	Verantwortet die Organisation der AEMP	hat einen Stellvertreter	
	Technischer Dienst	Verantwortlich für den technischen Zustand der AEMP-Ausstattung und der techn. Versorgung (Strom, Wasser, ...)	Bereitschaft - innerhalb 30 min vor Ort (5 Elektriker) / Prozeduren zur Fehlerbehebung vorhanden	
	IT-Hardwarespezialisten	Verantwortlich für die IT Hardware Ausstattung der AEMP	Bereitschaft - innerhalb 60 min vor Ort (5 Hardware Spezialisten) / Dokumente & Beschreibungen sind vorhanden	
	IT-Softwarespezialisten	Verantwortlich für die Schnittstellen zw. der anlagenspezifischen Software und der QM - / KS-Software	Bereitschaft - innerhalb 60 min vor Ort (4 Software Spezialisten) / Dokumente & Beschreibungen sind vorhanden	

Abbildung 46: Auszug BIA-Matrix - Beschreibung und Robustheit

Im Tabellenkalkulationsprogramm befinden sich rechts neben der BIA-Matrix zwei Spalten (siehe Abbildung 46), zum einen mit der Beschreibung und zum anderen mit der Robustheit in Bezug auf die Prozesse bzw. die Ressourcen angeordnet. Ebenfalls wurden im rechten Verlauf der Tabelle vier Spalten für die Schadensklassen eingestellt (siehe Abbildung 47).

A B C			CP	CQ	CR	CS
►► Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Operate Die Schadensklasse "Operate" beschreibt die Beeinträchtigung der Aufgabenerfüllung, Ziele können nicht erreicht werden. ⇒ Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Legal Die Schadensklasse "Legal" beschreibt den Verstoß gegen Gesetze, Vorschriften und Verträge. ⇒ Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Finance Die Schadensklasse "Finance" beschreibt die finanziellen Auswirkungen, wie z.B. Verluste, Bussgelder, Strafen. ⇒ Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Image Die Schadensklasse "Image" beschreibt die negativen Innen- und Aussenwirkungen (Imageschaden). ⇒ Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch
kritische Prozessschritte	1	Transport gebrauchte Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
	2	Vorreinigung & Vorbereitung MP	Signifikant	Managebar	Managebar	Managebar
	3	maschinelle Reinigung & Desinfektion MP	Signifikant	Managebar	Managebar	Managebar
	4	Sichtprüfung & manuelle Trocknung MP	Signifikant	Managebar	Managebar	Managebar
	5	Freigabe nach Prüfung Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
	6	Funktionskontrolle & Pflege MP	Signifikant	Managebar	Managebar	Managebar
	7	Verpackung Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
	8	Sterilisation Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
	9	Freigabe nach Sterilisation MP	Signifikant	Managebar	Managebar	Managebar
	10	Transport sterile Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
interne Personal (Rollen)	Logistiker		Managebar	Managebar	Managebar	Managebar
	Fachkundige in der Aufbereitung von MP		Managebar	Managebar	Managebar	Managebar
	AEMP Stammdatenadministrator		Managebar	Managebar	Managebar	Managebar
	Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)		Managebar	Managebar	Managebar	Managebar
	Leitung der AEMP		Managebar	Managebar	Managebar	Managebar
	Technischer Dienst		Managebar	Managebar	Managebar	Managebar
	IT-Hardwarespezialisten		Managebar	Managebar	Managebar	Managebar
	IT-Softwarespezialisten		Managebar	Managebar	Managebar	Managebar

Abbildung 47: Auszug BIA-Matrix - Schadensklassen

Im weiteren Verlauf der Tabelle wurde im rechten Anschluss an die Schadensklassen drei Spalten mit den Faktoren RPO, RTO und MTPD eingefügt (siehe Abbildung 48).

A B C			CT	CU	CV
► ► Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Recovery Point Objective (RPO) RPO ist die Zeit, in der ein Datenverlust für die Wiederaufnahme des Prozesses oder der Dienstleistung hingenommen werden kann. Prinzipiell ist es die Zeit zwischen zwei Datenspeicherungen. ⇒ zum besseren Verständnis, siehe Grafik im Blatt Allgemeine Informationen "Definition RTO, RPO, MTPD" ⇒ Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	Recovery Time Objective (RTO) RTO ist die Wiederherstellungszeit, die benötigt wird um nach einem Ereignis den Prozess oder die Dienstleistung wieder Schrittweise aufzunehmen. ⇒ zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD" ⇒ Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	Maximum tolerable Period of Disruption (MTPD) MTPD ist die maximal tolerierbare Unterbrechungsdauer bevor negative Auswirkungen auf die nachfolgenden Prozesse oder Dienstleistungen entstehen. ⇒ zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD" ⇒ Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage
kritische Prozessschritte	1	Transport gebrauchte Medizinprodukte	30 Minuten	30 Minuten	24 Stunden
	2	Vorreinigung & Vorbereitung MP	30 Minuten	30 Minuten	24 Stunden
	3	maschinelle Reinigung & Desinfektion MP	1 Stunden	30 Minuten	24 Stunden
	4	Sichtprüfung & manuelle Trocknung MP	30 Minuten	30 Minuten	24 Stunden
	5	Freigabe nach Prüfung Medizinprodukte	30 Minuten	30 Minuten	24 Stunden
	6	Funktionskontrolle & Pflege MP	30 Minuten	30 Minuten	24 Stunden
	7	Verpackung Medizinprodukte	30 Minuten	30 Minuten	24 Stunden
	8	Sterilisation Medizinprodukte	2 Stunden	30 Minuten	24 Stunden
	9	Freigabe nach Sterilisation MP	30 Minuten	30 Minuten	24 Stunden
	10	Transport sterile Medizinprodukte	30 Minuten	30 Minuten	24 Stunden
Interne Personal (Rollen)		Logistiker	---	2 Stunden	4 Stunden
		Fachkundige in der Aufbereitung von MP	---	2 Stunden	4 Stunden
		AEMP Stammdatenadministrator	---	24 Stunden	3 Tage
		Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	---	3 Tage	7 Tage
		Leitung der AEMP	---	3 Tage	7 Tage
		Technischer Dienst	---	30 Minuten	1 Stunden
		IT-Hardware spezialisten	---	1 Stunden	2 Stunden
		IT-Software spezialisten	---	1 Stunden	2 Stunden

Abbildung 48: Auszug BIA-Matrix - RPO, RTO, MTPD

Die einzelnen Tabellen der BIA-Matrix, so wie hier auszugsweise vorgestellt, sind in den Anhängen 14.5, 14.6, 14.7 und 14.8 zu finden.

Bedingt durch die sehr komplexe Struktur der technischen Versorgungssysteme im Krankenhauskomplex mit sechs Gebäudeteilen (BT) und vielen unterschiedlichen Versorgungssystemen, wurde zur Klärung der Abhängigkeiten ein Datenmodell ausgearbeitet. Dieses Datenmodell befindet sich im Anhang 14.9. In Abbildung 49 ist ein Auszug aus dem Datenmodell für die AEMP dargestellt.

Tabelle 12: Technische Versorgungssysteme der AEMP

- AV: Allgemeine Stromversorgung	- HD: Hausdampf
- AW: Abwasser	- KA: Kälte
- DL-T: Technische Druckluft	- RD: Reindampf
- DL-M: Medizinische Druckluft	- SV: Sicherheitsstromversorgung
- EDV: EDV-Netzwerk	- TR: Trinkwasser
- FL: Frischluft	- USV: Unterbrechungsfreie Stromversorgung
	- VE: Vollentsalztes Wasser

In Tabelle 12 sind die technischen Versorgungssysteme inkl. Beschreibung der Abkürzungen, wie in Abbildung 49 angewendet, aufgelistet. Diese Versorgungssysteme müssen im Gebäudekomplex verteilt werden.

Ein externes Blockheizkraftwerk (BHKW), betrieben durch einen externen Partner, liefert AV-, SV-Strom, Hausdampf, Kälte und Wärme. Der AV- und SV-Stromübergabepunkt befindet sich im UG 1 des BT3.2. Hausdampf, Kälte und Wärme werden für die Bauteile Nord im UG 1 des BT1.1 und für die Bauteile Süd im UG 2 vom BT3.2 übergeben.

Die Trinkwasserversorgung ist im UG 2 BT1.1 an das öffentliche Trinkwassernetz angeschlossen.

Die Anbindung an das Telekomnetz für Telefonie und Internet-Verbindung befindet sich im UG1 BT2.0 und im UG 1 BT3.2.

Das UG 2 ist als Verteilerkanal für alle Medien ausgebaut einschließlich Technikzentralen (z.B.: Abwasserhebeanlagen, Rohrpostverteilung) und unterhalb den Bauteil 1.1, 1.2, 2.0 und 3.1 einen Schachtverteiler für die Elektro-Versorgung der Etagenverteiler dieser Bauteile.

Im UG 1 BT1.1 sind die Technikzentralen für Druckluft, Osmose-Anlage sowie Wärme- und Kälteverteilung für die Bauteile Nord untergebracht.

Im UG 1 BT3.2 befinden sich die AV- und SV-Hausanschlüsse inkl. der Hauptverteilungen für die einzelnen Bauteile bzw. Etagen. Auch befindet sich im UG1 die Kälte- und Wärmeverteilung für die Bauteile Süd. Im selben Bereich befindet sich einer von 2 Serverräumen, der zweite Serverraum befindet sich im UG 1 von BT1.3.

Das BT1.3 ist nicht über einen Schachtverteiler im UG 2 sondern im UG 1 an die Hauptverteilung angeschlossen.

Im UG 1 von BT2.0 befinden sich die Technikzentralen für Sicherheits- und Kommunikationsanlagen.

Im relationalen Datenmodell aus Anhang 14.9 sind alle Abhängigkeiten wie im vorherigen Abschnitt beschrieben zwischen den technischen Versorgungssystemen und der AEMP aufgezeigt. Die AEMP ist direkt oder indirekt abhängig zu den grau hinterlegten Versorgungssystemen. Das Datenmodell ist die Grundlage zur Bestimmung der Abhängigkeiten zwischen den Versorgungsanlagen und diente zur Eintragung der Abhängigkeiten in die BIA-Matrix.

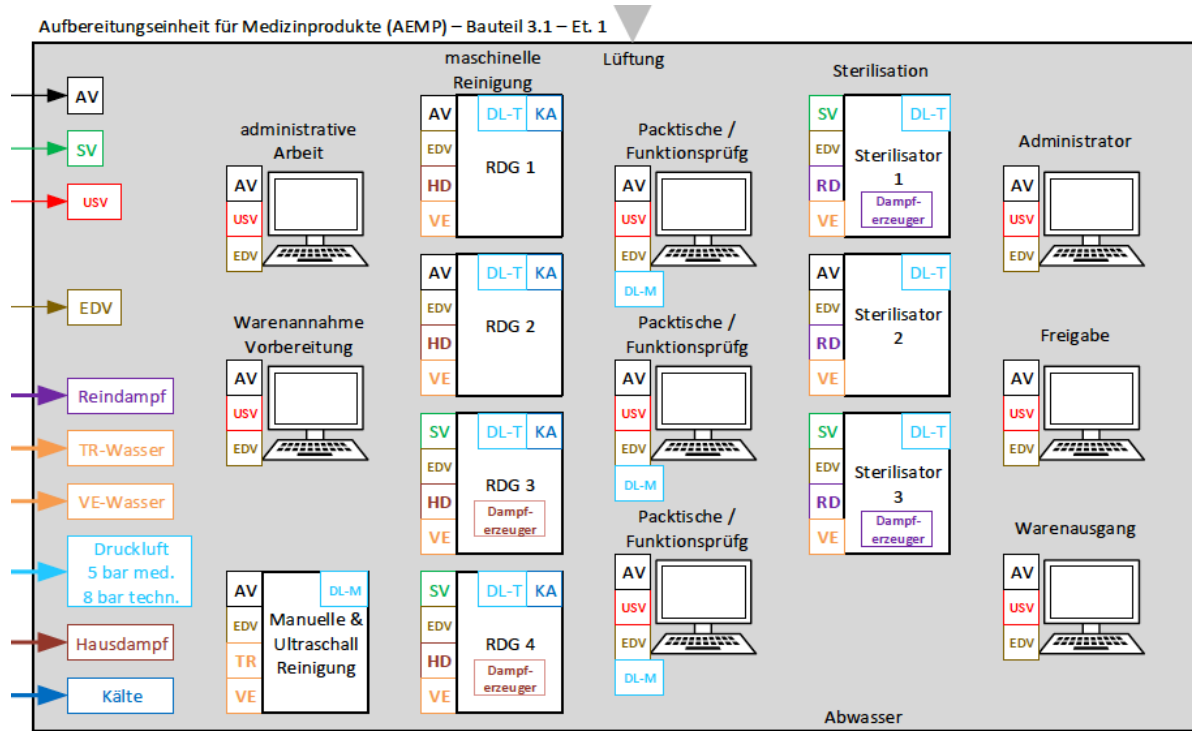


Abbildung 49: Versorgung der AEMP - Auszug aus dem Datenmodell der Versorgungssystem (siehe Anhang 14.9)

Nach der kompletten Sammlung der Daten wurde festgestellt, dass die Prozessschritte zur Aufbereitung der Endoskope bis auf die wenigen anderen Prozessgeräte identisch mit der Aufbereitung der Medizinprodukten sind. Damit die BIA-Matrix für die weitere Bearbeitung etwas schlanker gehalten werden kann ohne dabei die Business Impact Analyse zu verfälschen wurden die Prozesse und Ressourcen, welche die Aufbereitung der Endoskope beschreiben aus der BIA-Matrix gelöscht. Ebenfalls wurden verschiedenen Ressourcen, die nicht in direkt Abhängigkeit mit den Aufbereitungsprozessen der Medizinprodukte stehen, gelöscht.

Die endgültige Fassung der BIA Matrix inkl. aller Beschreibungen und Einstellungen der Faktoren ist, wie bereits erwähnt, in den Anhängen 14.5, 14.6, 14.7 und 14.8 zu finden. Die Faktoren, Abhängigkeiten und Beschreibungen der vorliegenden BIA-Matrix können für die Parametrierung der bcNAVIGATOR Software benutzt werden.

In den anschließenden statischen wie auch dynamischen Risikoanalysen werden die Parametrierung sowie die Durchführung von Szenarien beschrieben. Hierfür werden 2 Szenarien durchgespielt.

8.3 Szenarien für die dynamischen Risikoanalysen

8.3.1 Szenario 1: Überschwemmung UG 2

Für das Szenario 1 wird folgendes angenommen: Der Krankenhauscampus liegt in einem Überschwemmungsgebiet. Zum Hochwasserschutz wurde oberhalb der Ortschaft im Zufluss-Bereich des Fließgewässers ein Regenrückhaltebecken für ein 30-jähriges Hochwasser gebaut. Zusätzlich wurde zum Schutz des Gebäudes ein natürlicher Erdwall zwischen dem Gewässer und den Krankenhausgebäuden gebaut. Dadurch soll das Eindringen von Wasser bei in das Krankenhausgebäude verhindert

werden, wenn das Fließgewässer über die Ufer tritt. Das EG befindet sich auf gleicher Höhe wie der Erdwall. Das UG 1 befindet sich auf der Ebene des Wirtschaftshofes und der Parkplatzfläche. Da das Krankenhaus mit den nördlichen Gebäudeteilen an eine Hanglage stößt besteht bei Starkregenereignissen, das Risiko, dass Wasser vom Hang in den Hof-Bereich des Krankenhauses läuft. Bedingt durch den Erdwall, kann das Hangwasser nur über die Kanalisation abgeführt werden. Die Kanalisation wird bei einem Starkregenereignis das Oberflächenwasser nicht komplett abführen können und somit wird der Hof und die angrenzende Parkplatzfläche mit Wasser überschwemmt. Auf dieser Ebene befinden sich auch die externen Treppenabgänge in das Technikverteilergeschoss UG 2, in dieses das Wasser eindringen kann. In diesem Technikgeschoss befinden sich für die Gebäudeteile BT1.1, BT 1.2, BT 2.0 und BT 3.1 Elektro-Schachtverteiler mit den Stromverteilern für die Versorgung der Elektro-Etagenverteiler oberhalb UG 2. Ab einer Wasserstandshöhe von 50 cm ist es wahrscheinlich, dass die Elektroverteilerschränke abgeschaltet werden müssen. Für das fiktive Krankenhaus wird eine Überschwemmung > 1 Meter zu einer kompletten Abschaltung aller Verteilerschränke in den Schachtverteilern führen. Das bedeutet für diese Anlagenteile einen Totalausfall der elektrischen Energieverteilung.

8.3.2 Szenario 2: Cyberangriff

Für das Szenario 2 wird als Grundlage das Fallbeispiel vom Lukaskrankenhaus aus Kapitel 6.4.1 angenommen: Das fiktive Krankenhaus betreibt ein komplexes vernetztes EDV-System an dem sowohl medizintechnische Geräte (z.B. bildgebende Geräte, Anästhesie-Geräte als auch Perfusoren), Patienten-Überwachungssysteme und technische Gebäudeanlagen angeschlossen sind. In der AEMP sind alle Prozessgeräte mit dem EDV-System vernetzt um u.a. Chargendaten und Produktionskennzahlen in die Datenbank einzuspielen. In diesem Szenario wird davon ausgegangen, dass das EDV-System einen Cyberangriff erlebt hat und das Netzwerk mit einem Virus infiziert wurde, so dass alle Server und das gesamte Netzwerk abgeschaltet werden musste um die Verbreitung vom Virus zu unterbinden.

8.4 Statische Risikoanalyse

Für die statische Risikoanalyse mit dem Software Tool bcNAVIGATOR werden die Abhängigkeiten, die Schadensklassen, und die BIA-Faktoren RPO, RTO und MTPB aus der BIA-Matrix in das Modul bcIMPACT eingepflegt. Im Anschluss an die Parametrierung und Dateneingabe können die Analysen durchgeführt werden. Die Einstellungen (Parametrierung) und Eingabe der Daten zu den Ressourcen sowie Prozessen sind im Anhang 14.10 in einer Schritt-für-Schritt Anleitung aufgeführt.

Für die statische Risikoanalyse werden zwei verschiedenen Tabellen ausgewertet. Zum einen können im Modul bcIMPACT die Abhängigkeiten zu den kritischen Prozessen und zum anderen zu den kritischen Ressourcen analysiert werden.

Das Resultat der statischen Analyse betreffend die kritischen Prozesse ist im Anhang 14.13.1 in Tabellenform dargestellt. In der Übersicht in Tabelle 17 werden die übernommenen Informationen aus der BIA-Matrix dargestellt. In Tabelle 18 sind pro Teilprozesse der AMEP die Ressourcen-Abhängigkeiten nach Ressourcen-Kategorien

aufgeteilt. Die RTO-Verfügbarkeitszeit unterhalb der Zeitskala wird pro Ressource mit einer „1“ angegeben. Aus dieser Tabelle können die kritischen Ressourcen welche unbedingt für einen Prozess funktionieren müssen ermittelt werden.

Das Ergebnis der Auswertung zu den kritischen Ressourcen ist im Anhang 14.13.2 in einzelnen Tabellen aufgeführt. Jede Tabelle steht für eine Ressourcen-Kategorie. In jeder Tabelle sind für diese Kategorie die kritischen Ressourcen aufgelistet, dies mit den Abhängigkeiten zu den Teilprozessen der AEMP. Zusätzlich werden in der Zeitskala die Zeiten angegeben (Eintrag „1“) ab wann diese Ressource für den spezifischen Teilprozess zur Verfügung stehen muss.

Mit dieser Auswertung stehen der Organisation die Informationen bezüglich der kritischen Prozesse und kritischen Ressourcen zur Verfügung.

Bedingt durch die statische Risikoanalyse werden hier nur die statischen Abhängigkeiten zwischen den Ressourcen und Prozessen berücksichtigt. Diese Art der Bewertungen benötigt dafür keine expliziten Szenarien.

Die Auswertung der Resultate im Vergleich zu der dynamischen Risikoanalyse wird im Kapitel 8.6 erläutert.

8.5 Dynamische Risikoanalyse

Der dynamischen Risikoanalyse liegt die BIA-Matrix aus Kapitel 8.2.2 zu Grunde. Aus der Matrix wurden die Abhängigkeiten gemäß Abbildung 45 übernommen und in der SAURON Propagation Engine die Netzwerkstruktur erstellt. Jeder Prozess oder jede Ressource wird in einem Knotenpunkt und die Abhängigkeiten werden als Verbindungslinien dargestellt. Eine Schritt-für-Schritt Anleitung zur Eingabe der Knotenpunkte und der Abhängigkeiten befindet sich im Anhang 14.11.

Zur Modellierung der einzelnen Knotenpunkte und der Übergänge zu anderen Knoten müssen verschiedenen Parameter je Knotenpunkt eingetragen werden.

Die Abhängigkeiten müssen „nach vorne gerichteten“ parametrisiert werden. D.h. der ausgewählte Knotenpunkt (A) zeigt auf die Knotenpunkte die vom Knotenpunkt (A) abhängig sind. Für jeden Knotenpunkt wurden die Abhängigkeiten in der Dropdownliste aller Knotenpunkte ausgewählt. Aus diesen Festlegungen wird das Netzwerk (siehe Abbildung 50) generiert.



Abbildung 50: Abhängigkeits-Netzwerk der AMEP (graphische Darstellung in der SAURON Propagation Engine)

Zur Bestimmung der Knotenzustände müssen die Übergänge programmiert werden und können drei verschiedene Zustände annehmen:

1. Der Knoten ist funktionsfähig und unberührt vom Vorfall.
2. Der Knoten ist in seiner Funktion beeinträchtigt, kann aber noch funktionieren.
3. Der Knoten fällt aus und ist nicht mehr funktionsfähig.

Je Knoten können mehrere Übergänge beschrieben werden. Der Standard-Ausgangswert ist „1“. Alle Übergänge wurden zur Übersicht in einem neuen Arbeitsblatt in der Excel-Datei eingepflegt. Zur Bestimmung der Parameter wurden die Prozess- oder Ressourcenbeschreibungen, die Schadensklasse „Operate“ sowie die Beschreibungen der Robustheit als Grundlage genommen und anschließend von dem Expert*Innen geschätzt.

- **Szenario 1**

- Für das Szenario 1 – Überschwemmung UG 2, wurden zur Initialisierung der Simulation die drei Knotenpunkte :

1. Schachtverteiler BT1.1 Et.-2
2. Schachtverteiler BT2.0 Et.-2
3. Schachtverteiler BT3.1 Et.-2

mit dem Trigger „Überschwemmung >1m“ angesetzt und 1.000 Durchläufe gestartet.

- **Szenario 2**

- Für das Szenario 2 – Cyberangriff, wurden zur Initialisierung der Simulation die vier Knotenpunkte :

1. Serverraum Nord BT1.3. Et. -1
2. Serverraum Süd BT3.2. Et. -1
3. EDV-Netzwerk redundant
4. EDV-Netzwerk nicht redundant

mit dem Trigger „Cyberangriff - SD“ angesetzt und 1.000 Durchläufe gestartet.

Die Definition der Abhängigkeiten zu den anderen Knoten wurde nach dem „worst-case“ eingestellt, d.h. wenn für einen Knoten mehrere Abhängigkeiten anliegen, wird die Abhängigkeit mit der größten Auswirkung ausgehend vom Szenario für den Übergang der Knoten genutzt. Die Übergänge zwischen den Knotenpunkten werden mit Wahrscheinlichkeitswerten angegeben, d.h. wie wahrscheinlich ist es, dass der Knotenpunkt den Eingangszustand in den vorgegebene Ausgangszustand ändert. Daraus entstanden die Übergänge wie in der Tabelle im Anhang 14.12 dargestellt. Diese wurden in der Simulationsdatei entsprechend eingesetzt.

8.6 Auswertung der Ergebnisse

Die detaillierten Ergebnisse der Auswertung der statischen sowie der dynamischen Risikoanalysen befinden sich im Anhang 14.13. Bedingt durch die unterschiedlichen Verfahren in der Bewertung, sind die Ergebnisse nicht vergleichbar.

Die statische Risikoanalyse liefert eine Übersicht der Schadensklassen und der BIA-Faktoren (siehe Anhang 14.13.1) sowie in der BIA-Matrix angegeben. Dies resultiert daraus, dass die Angaben aus der BIA-Matrix identisch in die eingesetzte Software übernommen wurden. Für jeden Prozess der AEMP wurden die direkt abhängigen Ressourcen mit den jeweiligen mindest Wiederanlaufzeiten nach einem Ereignis angegeben. Diese Übersicht gibt der Organisation eine klar strukturierte Information welcher Prozess von welchen Ressourcen abhängig sind. Die BIA-Matrix in Tabellenform liefert diese Information auch, aber je aufwendiger die BIA-Matrix wird, je mehr Einträge wird es geben und so unübersichtlicher wird die Darstellung in Tabellenform. Eine zweite Darstellungsform bietet die Software in Form einer Auflistung der Ressourcen, welche eine direkte Verbindung zu den Prozessen der AEMP haben (siehe Anhang 14.13.2). Je Ressource werden die abhängigen Prozesse aufgelistet, inklusive der Wiederanlaufzeit, d.h. ab wann diese Ressource dem aufgeführten Prozess zur Verfügung stehen muss. Diese beiden Darstellungsformen liefern allerdings nur die Abhängigkeiten in direktem Bezug zu den Prozessen. Alle anderen Abhängigkeiten sind in der Software eingepflegt, werden aber in diesen Ansichten nicht dargestellt. Entsprechend müssen die Abhängigkeiten unterhalb der jeweiligen Ressourcen einzeln in der Eingabemaske der Ressourcenabhängigkeiten eingesehen werden.

Die dynamische Risikoanalyse bewertet die Ergebnisse wahrscheinlichkeitsbasiert aus. Dies ist ein ganz anderer Ansatz als die statische Risikoanalyse. Auch wurden hier keine Wiederanlaufzeiten berücksichtigt. Die Abhängigkeiten zwischen den Prozessen und Ressourcen (Knotenpunkten) erfolgt unidirektional, außer für einige wenige Übergänge die bidirektional abhängig sind. Das Resultat, nach einer Simulation von 1.000 Rechenzyklen (siehe Kapitel 3.6), liefert eine Aussage wie wahrscheinlich ein möglicher Ausfall oder eine mögliche Einschränkung des Prozesses oder der Ressource ist. Die Simulation liefert pro Szenario die Ergebnisse.

Für das Szenario „Überschwemmung UG 2 > 1m“ (siehe Anhang 14.13.3) und für das Szenario „Cyberangriff“ (siehe Anhang 14.13.4) sind die Knotenpunkte vom wahrscheinlichen Ausfall absteigend zum unwahrscheinlichen Ausfall gelistet. Das Ergebnis zeigt ganz klar welche Prozesse und Ressourcen nicht widerstandsfähig

sind. Andere Prozesse sind resilienter gegen einen möglichen Ausfall. Der mittlere Teil der Liste beschreibt die Prozesse, welche anfälliger gegen Beeinträchtigungen oder Ausfälle sind. Der Schluss der Liste beinhaltet die Prozesse oder Ressourcen welche eher nicht ausfallen. Die Simulation der beiden Szenarien ergeben unterschiedliche Auswertungen.

Wie Eingangs beschrieben, sind es unterschiedliche Ansätze und die beiden Risikoanalysen können nicht untereinander verglichen werden. Die Auswertungen ergeben für die statische Risikoanalyse eine prozessabhängige Darstellung der Ressourcenabhängigkeiten mit Wiederanlaufzeiten. Wo hingegen die dynamische Risikoanalyse eher eine Auflistung der Prozesse und Ressourcen mit Angaben zur Resilienz liefert. Die Simulation der beiden Szenarien ergab unterschiedliche Auswirkungen.

9 Diskussion der Ergebnisse

Das Forschungsfeld zur Betrachtung von Abhängigkeiten und Kaskadeneffekten zwischen kritischen Infrastrukturen, nimmt immer mehr an Relevanz zu. Diese Forschungsansätze können auch innerhalb der kritischen Infrastrukturen eingesetzt werden. Die vorliegende Arbeit hat sich diesem Thema gewidmet und an dem Fallbeispiel eines fiktiven Krankenhauses die Forschungsansätze angewandt. Das Krankenhaus als kritische Infrastruktur, muss die medizinische Grundversorgung für die Bevölkerung sicherstellen. Daraus resultiert die Verantwortung auch in Notsituation eine Grundversorgung sichern zu können. Als einer der unverzichtbaren zentralen Dienstleistungen im Krankenhaus, wurde spezifisch die Aufbereitungseinheit für Medizinprodukte (AEMP) für das Fallbeispiel ausgewählt. Die Aufbereitung von Medizinprodukten (z.B. Instrumentarium) besteht aus einer Reihe von manuellen, intellektuellen und maschinellen Vorgänge. Oberstes Ziel der AEMP ist es, den Benutzerabteilungen wiederverwendbare, sterile und funktionsfähige Medizinprodukte zur Verfügung zu stellen.

Die Bearbeitung der Forschungsfragen wurde anhand von Teilaspekten des Risiko- und Business Continuity Managements durchgeführt und insbesondere wurde die Business Impact Analyse angewandt.

Gemäß der zwei Hypothesen aus Kapitel 1.4 ist es wichtig die Kenntnisse über kritische Prozesse und Ressourcen sowie deren Abhängigkeiten und kaskadenartigen Auswirkungen auf den Gesamtprozess der Aufbereitung von Medizinprodukten zu erwerben. Dies um die Aufrechterhaltung der Dienstleistung bestmöglich sicherstellen zu können. Im Nachfolgenden werden die Forschungsfragen aus der Einleitung überprüft.

Die vier Fragen sind eng mit dem Forschungsgebiet der Kaskadeneffekte zwischen kritischen Infrastrukturen verknüpft. Aus diesem Forschungsgebiet wurde die CERBERUS-Systemarchitektur als Systemmodell zur Beantwortung der Fragen gewählt. Dazu wurde die Systemarchitektur, wie im Kapitel 3.2 beschrieben, an die Bedürfnisse der eingesetzten Werkzeuge angepasst.

9.1 Unterforschungsfrage 1

Welche kritischen Prozesse betreffend die Aufbereitung von Medizinprodukten werden identifiziert?

Zur Identifikation der kritischen Prozesse in der AEMP wurden unterschiedliche Methoden in der Informationsbeschaffung eingesetzt, u.a. wurden Interviews und ein Fragebogen genutzt um Informationen zu sammeln. Nachdem alle einzelnen Prozessschritte ermittelt waren, wurden zusammen mit den Expert*Innen die nachfolgenden zehn kritischen Prozesse ermittelt, welche für die Wertschöpfung der Dienstleistung am wichtigsten waren.

1. Transport von gebrauchten Medizinprodukten (MP)
2. Vorreinigung & Vorbereitung MP
3. Maschinelle Reinigung & Desinfektion MP

4. Sichtprüfung & manuelle Trocknung MP
5. Freigabe nach Prüfung Medizinprodukte
6. Funktionskontrolle & Pflege MP
7. Verpackung Medizinprodukte
8. Sterilisation Medizinprodukte
9. Freigabe nach Sterilisation MP
10. Transport der sterilen MP

Zur weiteren Verarbeitung der Informationen für die kommenden Forschungsfragen wurden die zehn Prozesse in eine Business Impact Analyse-Matrix (Anhang 14.5) eingetragen. Zum allgemeinen Verständnis und zur weiteren Verarbeitung der gesammelten Daten wurden die Prozessfunktion und die Robustheit des Prozesses beschrieben. Mit diesem Ergebnis konnte die erste Forschungsfrage beantwortet werden.

9.2 Unterforschungsfrage 2

Welche kritischen Ressourcen auf der digitalen (cyber), der physischen sowie der personenbezogenen Ebene werden zum Betreiben der kritischen Prozesse benötigt?

Zur Identifikation der kritischen Ressourcen, wurden diese zuerst in sechs Kategorien eingeteilt:

1. Internes Personal (Rollen)
2. Externe Partner
3. IT Software
4. Prozessgeräte
5. Versorgung / Anlagen
6. Sicherheitstechnik

Anschließend wurde jeder der zehn Prozesse anhand dieser sechs Kategorien durch die Expert*Innen analysiert. Als Grundlage der Bewertung diente die fiktive Prozesslandkarte aus Abbildung 43 und das relationale Datenmodell aus Anhang 14.9. Im Anschluss an diese Analyse wurden die kritischen Ressourcen ermittelt (siehe hierfür die BIA-Matrix im Anhang 14.5). Ebenfalls für die weiterführende Verarbeitung der Informationen wurde jede Ressourcenfunktion und Robustheit in der Matrix beschrieben.

Mit der Auflistung der kritischen Ressourcen in der BIA-Matrix konnte die zweite Forschungsfrage beantwortet werden.

9.3 Unterforschungsfrage 3

Welche Abhängigkeiten bestehen zwischen den identifizierten kritischen Prozessen und Ressourcen?

Aufbauend auf der Identifizierung und den Informationen der kritischen Prozesse und Ressourcen, wurden die Abhängigkeiten geprüft. Insbesondere die komplexe Vernetzung sowie die verteilte technische Infrastruktur, über alle Gebäudeteile, war ohne zusammenhängenden Plan nur sehr schwierig zu überblicken. Damit die Abhängigkeiten optimal analysiert werden konnten, wurde vom Autor in Abstimmung

mit den Expert*Innen ein grafisches relationales Datenmodell gezeichnet. Mit diesem Datenmodell konnten die Abhängigkeiten in die BIA-Matrix im Anhang 14.5 eingetragen werden. Damit konnte die dritte Forschungsfrage beantwortet werden.

Gemäß der CERBERUS Systemarchitektur konnten mit den drei Forschungsfragen die Datensammlung und Datenbereinigung abgeschlossen werden. Die vierte Forschungsfrage zielt auf die statische wie auch dynamische Risikoanalyse und deren Ergebnisse ab.

9.4 Unterforschungsfrage 4

Wie können die Abhängigkeiten zwischen den kritischen Prozessen und Ressourcen analysiert werden um die Kaskadeneffekte darzustellen?

Für die statische Risikoanalyse wurde als Werkzeug eine Business Impact Analyse genutzt. Dem gegenüber wurde die SAURON Propagation Engine aus dem SAURON Forschungsprojekt für die dynamische Risikoanalyse eingesetzt.

Für die Business Impact Analyse wurden zusätzliche Daten zu Schadensklassen und den BIA-Faktoren RPO, RTO und MTPD benötigt. Diese Daten und Faktoren wurden zusammen mit den Expert*Innen in Workshops ausgearbeitet und in die BIA-Matrix eingetragen (siehe Anhang 14.7 und 14.8). Die BIA-Matrix wurde als Grundlage genutzt, um die Daten in eine softwarebasierte Business Impact Analyse zu übertragen. Als Software wurde das Modul bcIMPACT genutzt. Für die angewandte statische Risikoanalyse konnten in der Software die Abhängigkeiten in direkter Verbindung mit den zehn kritischen Prozessen visualisiert werden (siehe Anhang 14.13.1 und 14.13.2).

Im Simulationswerkzeug SAURON Propagation Engine wurde eine Netzwerkstruktur mit Knotenpunkten aus den kritischen Prozessen und Ressourcen der BIA-Matrix erstellt. Die Abhängigkeiten zwischen den Knotenpunkten wurden, bis auf ein paar wenige Ausnahmen, unidirektional parametrisiert. Zur Simulation der Auswirkungen an den einzelnen Knotenpunkte, können diese drei verschiedenen Zustände (funktionsfähig, Funktion eingeschränkt oder nicht mehr funktionsfähig) einnehmen. Zur Visualisierung der Kaskadeneffekte wurden 2 verschiedene Szenarien beispielhaft simuliert. Die Ergebnisse lieferten für jeden Prozess oder jede Ressource eine Angabe wie wahrscheinlich ein Ausfall dieses Knotenpunkte im Netzwerk ist. In den beiden Szenarien konnten die Kaskadeneffekte dargestellt werden (siehe Anhang 14.13.3 und 14.13.4).

Durch die Betrachtung der statischen und der dynamischen Risikoanalyse der CERBERUS Systemarchitektur konnten die direkten Abhängigkeiten zu den kritischen Prozessen mit der Software bcIMPACT und die Kaskadeneffekte für die kritischen Prozesse und Ressourcen mit der SAURON Propagation Engine dargestellt werden. Bedingt durch die beiden unterschiedlichen Programme konnte eine zusammenhängende Darstellung beider Ergebnisse nicht realisiert werden.

Dementsprechend konnte die Forschungsfrage vier nur teilweise beantwortet werden. Für die Beantwortung dieser Frage und die zusammenhängende Darstellung der Ergebnisse wären zusätzliche Untersuchungen nötig.

10 Zusammenfassung

Ende der 1990er-Jahre haben verschiedene Länder angefangen sich mit der Thematik zum Schutz kritischer Infrastrukturen zu beschäftigen, darunter waren die USA und Deutschland (siehe Kapitel 4.2). Verschiedene Ereignisse aus dieser Zeit zeigen, wie verwundbar die Bevölkerung ist, wenn unterschiedliche wesentlichen Infrastrukturen ausfallen. Der Schutz kritischer Infrastrukturen wurde immer wichtiger, u.a. der Terroranschlag „09/11“ auf die Zwillingstürme des World Trade Centers in New York im Jahre 2001 hat in der Europäischen Union ein Umdenken bewirkt. Mitte der 2000-er Jahre hat die Europäische Kommission an einer Richtlinie zum Schutz kritischer Infrastrukturen gearbeitet und elf Sektoren sowie auch sieben-und-dreißig Teilsektoren definiert. Es wurden allerdings Ende 2008 nur die beiden Sektoren Transport und Energie in der Richtlinie aufgenommen (siehe Kapitel 4.1). Die damaligen Grundanforderungen wurden von den Mitgliedsstaaten unterschiedlich umgesetzt. Jeder Mitgliedstaat kann zusätzliche kritische Infrastrukturen selbst definieren. Dadurch können die einzelnen Strategien der Mitgliedsstaaten nicht untereinander verglichen werden. Allerdings gibt es standardisierte internationale Verfahren, die bestimmen wie die kritischen Infrastrukturen ihre Verwundbarkeit beurteilen und reduzieren können.

Störungen in kritischen Infrastrukturen sollten nur ausnahmsweise, kurzzeitig und lokal begrenzt auftreten.

Damit die Lebensgrundlage der Bevölkerung bestmöglich geschützt werden kann, haben z.B. Deutschland und Luxemburg unterschiedliche Sektoren definiert (siehe Kapitel 4.1.1). Hierzu gehören unter anderem die Lebensmittelversorgung, die Energieversorgung, das Finanzwesen und die Gesundheitsversorgung. Ziel dieser Länder war es auch in Notfallsituationen ihre Dienstleistungen oder Wertschöpfung aufrechterhalten zu können. Diese Infrastrukturen sind den unterschiedlichsten Gefahren wie z.B. Naturgefahren, intentionale, technischen oder menschlichen Gefahren (siehe Kapitel 6.1) ausgesetzt. Wie verschiedene größere Notfallsituationen in der Vergangenheit gezeigt haben, sind die unterschiedlichen Infrastrukturen der einzelnen Sektoren abhängig voneinander.

Im Sektor Gesundheitsversorgung sind Krankenhäuser, u.a. neben Rettungsdienst, niedergelassenen Ärzten, Laboren, ein zentraler Partner in der Rettungskette und gehören zu den kritischen Infrastrukturen (siehe Kapitel 4.1.2). Damit die kritische Infrastruktur Krankenhaus den Anforderungen gerecht wird, muss die Infrastruktur auch in Notfallsituationen funktionsfähig bleiben. Ein Krankenhaus ist ein hoch sensibles und komplexes System und ist von vielen internen wie externen Kooperationspartnern, Funktionsbereichen und Ressourcen abhängig.

Die vorliegende Arbeit befasst sich mit den „Besonderen Betrachtungen der Kaskadeneffekten in Bezug auf das Risikomanagement von kritischen Infrastrukturen am Beispiel eines Krankenhauses“. Innerhalb eines Krankenhauses sind unterschiedliche Prozesse, ähnlich wie kritische Infrastrukturen stark voneinander abhängig sind.

Für die Gesellschaft sind vernetzte, abhängige kritische Infrastrukturen eine erhebliche Schwachstelle. Die sechs Dimensionen „Interdependenzen“, „Umfeld“, „Verbindungen und Reaktionsverhalten“, „Störungen“, „Charakteristik der Infrastruktur“ und „Betriebszustand“ beschreiben die Abhängigkeiten einer kritischen Infrastruktur (siehe Kapitel 4.2). Wie sich die Auswirkungen einer Infrastruktur auf andere Infrastrukturen ausbreiten, hängt vom Maß der Interdependenzen zwischen den Infrastrukturen ab. kaskadenartige Ausfälle finden meistens ihre Ursache in Ausfällen von einzelnen Ressourcen oder Prozessen. Zur Analyse der Kaskadeneffekte (siehe Kapitel 4.3) können die internationalen standardisierten Verfahren „Business Continuity Management“ und „Risikomanagement“, unter der Anwendung der CERBERUS Systemarchitektur, eingesetzt werden. Diese kann sowohl für die Analyse von Auswirkungen im Netzwerk der kritischen Infrastrukturen, als auch innerhalb einer Infrastruktur genutzt werden.

In der CERBERUS Systemarchitektur (siehe Kapitel 4.3.1) wird neben der statischen Risikoanalyse, eine dynamische Risikoanalyse in Form einer Simulation durchgeführt. Für die Simulation müssen alle Prozesse und Ressourcen in Knotenpunkten in einem Netzwerk abgebildet werden. Gemäß der Parametrierung des Netzwerkes können die einzelnen Knotenpunkte ihre Zustände ändern. Für die Simulation der Zustandsänderungen werden stochastische Markov-Ketten genutzt. Die SAURON Prorogation Engine wendet ebenfalls die Markov-Ketten zur Simulation von Netzwerken an. Dadurch passt dieses Simulationswerkzeug ideal in die CERBERUS Systemarchitektur. Zusätzlich zur Simulation von kaskadenartigen Auswirkungen werden im SAURON-Rahmenwerk (siehe 4.3.2) auch die Analyse von Cyber-physischen Systeme durchgeführt.

Wir leben aktuell im Zeitalter der vierten industriellen Revolution (siehe Kapitel 5.1), in der die Cyber-Physischen Systeme eingeführt wurden. Aus der Digitalisierung und dem Internet der Personen, hat sich das vernetzte und interagierende Internet der Dinge, als Cyber-Physisches System entwickelt. Daraus entsteht die Gesellschaft 4.0 mit unterschiedlichen Cyber-physischen Konzepten wie z.B. die intelligente Mobilität (Smart Mobility) und die intelligenten Stromnetze (Smart Grids), welche u.a. den Ursprung zur intelligenten Stadt (Smart City) bilden. Zu diesen Cyber-physischen Systemen gehört auch das intelligente Krankenhaus (Smart Hospital).

Im Krankenhaus 4.0 (siehe Kapitel 5.2) werden, aus medizintechnischen Insellösungen, offene vernetzte cyber-physische Systeme, die untereinander interagieren und Daten selbstständig austauschen können. Zu diesen Systemen gehören u.a. Bildgesteuerte Operationen, neuronal gesteuerte Prothesen, auf den Patienten angepassten intelligente medizintechnische Geräte, intelligente Operationssäle mit vernetzten Infusionspumpen, Beatmungsgeräte inkl. Sauerstoffzufuhr, vernetzte Sensoren zur Überwachung des Patienten und unterschiedliche Informationssysteme im Krankenhaus.

Kritische Infrastrukturen sind den unterschiedlichsten Gefahren (siehe Kapitel 6.1), wie bereits etwas weiter oben beschrieben, ausgesetzt. Durch die Erweiterung der Vernetzung innerhalb von kritischen Infrastrukturen aber auch zwischen unterschiedlichen kritischen Infrastrukturen, erhöht sich die Gefahr von Cyberangriffen

und der Verwundbarkeit (siehe Kapitel 6.2). Damit eine Organisation Gefahrenabwehrpläne erstellen kann, muss sie die unterschiedlichen Verwundbarkeitsfaktoren kennen. Hierzu dürfen nicht nur die internen Faktoren berücksichtigt werden, sondern auch die externen Faktoren. Damit diese Faktoren ermittelt werden können müssen die Schutzziele der kritischen Infrastruktur definiert werden. Dafür ist es wichtig die Abläufe in einer Organisation zu kennen. Eine Prozesslandkarte aller wichtigen Abläufe, welche in einem Krankenhaus zur Patientenversorgung beitragen, wird benötigt. Damit die kritische Infrastruktur die Grundversorgung von Patienten gewährleisten kann, werden aus der Prozesslandkarte die Abhängigkeiten mit den dafür benötigten kritischen Prozessen und Ressourcen ermittelt. Die kritische Infrastruktur Krankenhaus ist von vielen externen wie auch internen Ressourcen abhängig (siehe Kapitel 6.3).

Das System „Krankenhaus 4.0“ ist ein sehr komplexes vernetztes System, in dem es viele Abhängigkeiten zwischen kritischen Prozessen und kritischen Ressourcen gibt. Es wird zwischen personellen, architektonischen, technischen, cyber-physischen, internen sowie externen Ressourcen unterschieden. Durch den hohen Vernetzungsgrad innerhalb und außerhalb des Krankenhauses und zwischen dem Krankenhaus und den externen kritischen Infrastrukturen, wirken sich Ausfälle von einzelnen Ressourcen kaskadenartig auf andere Ressourcen bzw. Prozesse aus und können über die Organisationsgrenze auch andere kritische Infrastrukturen beeinflussen (siehe Kapitel 6.4).

Damit Krankenhäuser und im Allgemeinen kritische Infrastrukturen die möglichen Auswirkungen erkennen und resilienter werden können, stehen verschiedene internationale standardisierte Werkzeuge zur Verfügung. Zum einen sollten Organisationen zur Schaffung und zum Schutz von Werten auf mögliche Auswirkungen von Ereignissen vorbereitet sein. Als geeignetes Werkzeug kann das Risikomanagement gemäß ISO 31000 eingesetzt werden. Das wesentlich präventive Ziel vom Risikomanagement ist es Risiken zu vermeiden, zu mindern, zu akzeptieren oder zu transferieren (siehe Kapitel 7.1). Dafür müssen die Risiken identifiziert, analysiert und bewertet werden. Abhängig von den Risiken können zur Identifikation und Analyse unterschiedliche Methoden angewandt werden. Das Risiko wird üblicherweise mit den beiden Faktoren Eintrittswahrscheinlichkeit und Schadenshöhe (Auswirkung) in einer Risikomatrix dargestellt.

Neben dem Erkennen und Bewältigen von Risiken, müssen Krankenhäuser, als kritische Infrastruktur, zum anderen ebenfalls die Kontinuität der Patientengrundversorgung in Notfallsituation vorsehen. Dazu müssen präventive Schutzmaßnahmen bestehen oder müssen Kontinuitätspläne, zur maximalen Reduzierung der Ausfallzeit von Prozessen vorhanden sein. Zur Aufrechterhaltung des Business Continuity Management gilt die ISO 22301 als internationales standardisiertes Werkzeug, welches in dieser Arbeit angewandt wurde (siehe Kapitel 7.2). Der Business Continuity Management Prozess wird in einem klassischen PDCA Zyklus kontinuierlich durchlaufen. Ähnlich wie beim Risikomanagement wird in der DO-Phase die Identifikation, Analyse und Bewertung der kritischen Prozesse durchgeführt.

Die Anwendung der CERBERUS Systemarchitektur innerhalb einer Organisation und die Betrachtung der besonderen Kaskadeneffekten bedingt die Identifikation, Analyse und Bewertung von vernetzten kritischen Prozessen und Ressourcen im fiktiven Krankenhaus. Zur Durchführung der statischen Risikoanalyse wurde in der vorliegenden Arbeit eine Business Impact Analyse (BIA) angewandt (siehe Kapitel 7.3). Diese hat als Ziel, Schwachstellen und Auswirkungen auf kritische Prozesse zu identifizieren sowie Grundlagen für Wiederherstellungspläne zu liefern. Da jede Organisation eine andere Strategie verfolgt, anders organisiert ist oder andere Strukturen hat, muss die BIA an jede Organisation individuell angepasst werden. In der angewandten BIA wurden insbesondere kritische Prozesse und Ressourcen identifiziert, deren Robustheit beschrieben, Schadensklassen sowie die drei BIA-Faktoren „Recovery Point Objective“, „Recovery Time Objective“ und „Maximum Tolerable Period of Disruption“ bestimmt

Die kombinierte Anwendung der unterschiedlichen Management-Systeme wie z.B. Risikomanagement, Business Continuity Management, Qualitätsmanagement IT-Sicherheitsmanagement, Krisen- und Notfallmanagement innerhalb einer Organisation steigern die organisationale Resilienz (siehe Kapitel 7.4). Gilt es doch die vielen unterschiedlichen Gefährdungen abzuwenden, kann in komplexen vernetzten Systemen, wie einem Krankenhaus, diese Risiko- und Sicherheitspolitik von Nutzen sein, um mögliche Unterbrechungen in der Patientengrundversorgung bestmöglich vorzubeugen.

Zur besonderen Betrachtung der Kaskadeneffekte in Bezug auf das Risikomanagement von kritischen Infrastrukturen wurde in der vorliegenden Arbeit die Aufbereitungseinheit für Medizinprodukte (AEMP) in einem fiktiven Krankenhaus für das Fallbeispiel ausgewählt. Die AEMP ist eine zentrale wichtige interne Dienstleistungsabteilung (siehe Kapitel 8.1.2) mit den drei unterschiedlichen Arbeitsbereichen „Anliefer- und Dekontaminationsbereich“, „Packbereich“ und „Sterilgut-Bereich“. Die AEMP ist sehr stark von vielen verschiedenen technischen Versorgungssystemen abhängig. Auch EDV-gestützte Systeme wie u.a. das Qualitätsmanagement werden eingesetzt. Durch die Vernetzung innerhalb der AEMP entstehen vermehrt cyber-physische Systeme (siehe Kapitel 8.1.3). In der fiktiven Prozesslandkarte wird die AEMP unter den Supportprozessen als „medizintechnische Versorgung“ geführt (siehe Kapitel 8.1.4).

Anhand von Interviews, Befragungen und Workshops mit Expert*Innen wurden die Daten zu den wesentlichen Prozessen gesammelt. Dazu wurde der Kreislauf der wiederverwendbaren Medizinprodukten analysiert und es konnten zehn kritische Prozesse identifiziert werden. Zur Bestimmung der kritischen Ressourcen wurden diese in fünf Kategorien „internes Personal“, „externe Partner“, „IT-Software“, „Prozessgeräte“ und „Versorgung / Anlagen“ eingeteilt. Um alle relevanten Informationen zu sammeln, wurde ein Fragebogen ausgearbeitet. Sämtliche Daten zur Beschreibung, Robustheit, der Schadensklasse sowie der BIA-Faktoren RPO, RTO und MTPD wurden in eine BIA-Matrix eingetragen. Zur Identifikation und Beurteilung der Abhängigkeiten zwischen den einzelnen Prozessen oder Ressourcen wurden die fiktive Prozesslandkarte sowie auch relationale Datenmodell der technischen Anlagen

genutzt. Dadurch konnten die Abhängigkeiten der AMEP sehr deutlich und detailliert ausgearbeitet werden (siehe Kapitel 8.2).

Für die dynamische Risikoanalyse wurden zwei Szenarien ausgearbeitet.

Zum einen wurde ein Szenario „Überschwemmung UG 2 > 1m“ (siehe Kapitel 8.3.1), bedingt durch eine Sturzflut, ausgearbeitet. Dabei würde das 2. Kellergeschoss mit Wasser geflutet. Das 2. Kellergeschoss ist eine Verteilerebene für Kabel und Rohrleitungen. In dieser Ebene sind auch unterschiedliche technische Anlagen, wie z.B.: Schachtverteiler, Rohrpostzentrale, Abwasserhebeanlage, vorhanden. Bedingt durch die Überflutung und zur Verhinderung eines Kurzschlusses, müssen alle Anlagen vom Netz abgeschaltet werden. Dies bedeutet für diese Anlagenteile der Totalausfall der elektrischen Energieversorgung.

Zum anderen wurde ein Szenario „Cyberangriff“ (siehe Kapitel 8.3.2) ausgearbeitet. Abhängig der komplexen, vernetzten Krankenhausstrukturen, wie u.a. EDV-Systeme, medizintechnischen Geräten, Prozessgeräte, elektronischen Patientendaten und technische Gebäudeanlagen ergeben sich viele Abhängigkeiten und mögliche Eingänge für einen Cyberangriff. Um die Ausbreitung eines Virus nach einem Cyberangriff zu verhindern, müssen alle Netzwerke und Serverlandschaften ausgeschaltet werden. Dies bedeutet ein Totalausfall der gesamten IT-Landschaft.

Die statische Risikoanalyse als Business Impact Analyse, wurde auf der Grundlage der BIA-Matrix mit Zuhilfenahme der Software bcIMPACT durchgeführt. Hier wurden die Schadensklassen und die BIA-Faktoren bewertet. Die Software lieferte die direkt abhängigen Ressourcen, welche die zehn kritischen Ressourcen betreffen. Die Prozesse und die direkt abhängigen Ressourcen, werden in Tabellenform dargestellt. (siehe Kapitel 8.4)

Für die dynamische Risikoanalyse wurde die Abhängigkeiten aus der BIA-Matrix in eine Graphen-basierte Netzwerkstruktur programmiert. Knotenpunkte stellen die Prozesse und Ressourcen dar, mit den Verbindung zwischen den Knotenpunkten werden die Abhängigkeiten dargestellt. Die SAURON Propagation Engine basiert auf einer stochastischen Zustandsveränderung der Knotenpunkte. Damit die Knotenpunkte eine von drei unterschiedliche Statusmeldungen annehmen, müssen die Übergänge pro Knotenpunkt mit den Wahrscheinlichkeitswerten angepasst werden. Als Ergebnis lieferte die Software eine Liste der betroffenen Knotenpunkte, welche komplett ausfallen bis zu den Knotenpunkten, die zu 100% funktionsfähig bleiben. (siehe Kapitel 8.5)

Mit der Anwendung der CERBERUS Systemarchitektur, der statischen Risikoanalyse in Form einer Business Impact Analyse und der dynamischen Risikoanalyse anhand der SAURON Propagation Engine konnten die kritischen Prozesse und Ressourcen ermittelt werden. Mit der fiktiven Prozesslandkarte und dem relationalen Datenmodell konnten die Abhängigkeiten zwischen den Prozessen und den Ressourcen ermittelt werden. Neben der Bewertung von Ausfallzeiten und Schadensklassen in der Business Impact Analyse und der Identifikation der direkten Abhängigkeiten pro Prozess konnten mit der Graphen-basierten Netzwerkstruktur auch die Kaskadeneffekte innerhalb des Netzwerks identifiziert werden. (siehe Kapitel 8.6)

11 Perspektive – Ausblick

Bedingt durch die unterschiedlichen Ansätze, der statischen und dynamischen Risikoanalyse, ergeben die Auswertungen unterschiedliche Schlussfolgerungen. Das Fallbeispiel hat gezeigt, dass die beiden Ansätze in der Praxis eingesetzt werden können. Werden allerdings mehr und mehr kritische Prozesse und Ressourcen analysiert, stößt die Darstellung mittels klassischer Tabellenkalkulationsprogrammen schnell an ihre Grenzen. Für komplexe, vernetzte kritische Infrastrukturen wie beispielsweise ein Krankenhaus kann die Analyse von Kaskadeneffekten nur softwarebasiert durchgeführt werden.

Idealerweise müsste ein softwarebasiertes Analysewerkzeug, angelehnt an die CERBERUS Systemarchitektur, entwickelt werden. Dadurch könnten Synergieeffekte bei der Datenerfassung ein Vorteil bringen. Eine kombinierte Betrachtung der Abhängigkeiten aller Netzwerkknoten und die entsprechende Darstellung in der statischen Risikoanalyse, würden auch die untergeordneten Ressourcen zu den kritischen Prozessen anzeigen. Dadurch könnten die kaskadenartigen Abhängigkeiten in der statischen Risikoanalyse besser dargestellt werden. In der dynamischen Risikoanalyse könnten die stochastischen Analysen mit faktorbasierte Daten der statischen Risikoanalyse durchgeführt werden. Dadurch würde die dynamischen Simulation nicht mehr nur mittels Wahrscheinlichkeitsbasierten Daten, sondern näher an den realen Abhängigkeitsfaktoren ausgeführt werden können. Auch die Datenerfassung könnte softwarebasiert durchgeführt werden. Dadurch könnten die Daten durch die Expert*Innen direkt in das System integriert werden.

Die Komplexität der Vernetzung von kritischen Prozessen und Ressourcen würden den Einsatz einer Software mit der Integration von beiden Ansätzen erfordern.

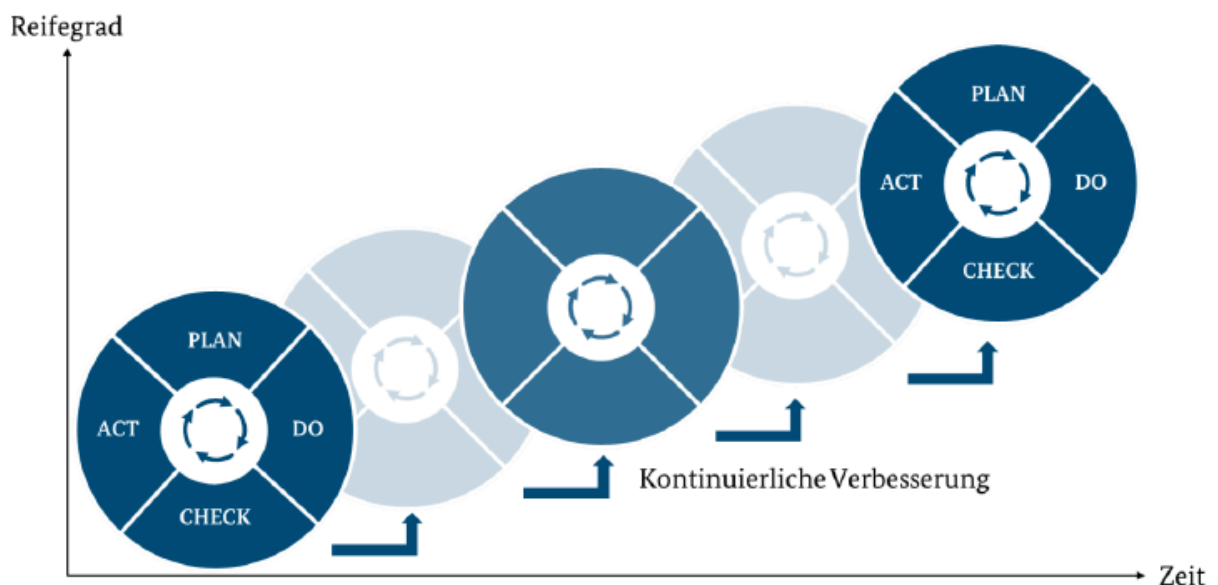


Abbildung 51: PDCA-Zyklus eines Managementsystems (Quelle: BSI 2021: 14)

Die Erkenntnisse aus der Datenerfassung hat gezeigt, dass die Expert*Innen aus den spezifischen Abteilungen mehr oder weniger Erfahrungen mit Business Impact Analysen hatten. Abbildung 51 stellt die Steigerung des Reifegrades in Abhängigkeit

der steigenden Anzahl von PDCA-Zyklen dar. In Anwendung dieser Abbildung, steigert sich die Erfahrung der Expert*Innen. Dadurch kann die Resilienz einer Organisation gesteigert werden. Für eine Organisation bedeutet dies, dass eine kontinuierliche Anpassung vom Risiko- und Business Continuity Management stattfinden muss.

Das durchgeführte Fallbeispiel wurde anhand einer spezifischen Dienstleistung innerhalb eines Krankenhauses durchgeführt. Die Analyse und Bewertung basierte auf den grundlegenden Ressourcen der Energie- und Versorgungssystemen eines Krankenhauses. Für eine Organisation, welche das erste Mal Risiko- und Business Impact Analysen durchführt, zeigt sich die Anwendung der Top-Down Methode als bester Ansatz gegenüber dem Bottom-Up Ansatz. Die Erfahrungen aus dem Fallbeispiel haben gezeigt, dass es schwieriger ist die Datenanalyse durchzuführen ohne die genauen Abhängigkeiten aus den übergeordneten Prozessen zu kennen. Durch die Top-Down Analyse sind die Kaskadeneffekte der nebengeordneten Prozesse bekannt und können gegebenenfalls mit berücksichtigt werden. Auch müssen die externen Abhängigkeiten auf die kritische Infrastruktur bekannt sein, damit diese Kaskadeneffekte in die Analysen einbezogen werden können. Fällt z.B. die Stromversorgung aus, ist ein Krankenhaus mit Notstromaggregaten abgesichert. Trotz Einschränkungen, muss der Betrieb nicht gleich eingestellt werden. Ist die Stromversorgung, bedingt durch einen „Blackout“, längerfristig unterbrochen, fallen eventuell noch andere Versorgungssystem im Krankenhaus aus. Aus diesem Grund sind die Risiko- und Business Impact Analysen nicht nur innerhalb der kritischen Infrastruktur durchzuführen, sondern müssen in der regulatorischen Ebene ebenfalls durchgeführt werden. Durch die Bewertung der komplexen vernetzten kritischen Infrastruktursysteme, ergeben sich Kenntnisse über Kaskadeneffekte, welche sich auf die einzelnen kritischen Infrastrukturen auswirken.

Durch die Betrachtung der externen wie auch internen Abhängigkeiten und Kaskadeneffekte, wird eine Organisation resilienter gegenüber von Gefährdungen. Insbesondere die Betrachtung der dokumentierten Cyberangriffe und der vernetzten cyber-physischen Systeme erfordern eine ganzheitliche Betrachtung der Zusammenhänge.

Die Europäische Kommission hat Ende 2020 eine „neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen“ vorgestellt. (vgl. EU 2020a)

In der Anlage 5 zum Vorschlag einer Richtlinie über die Resilienz kritischer Einrichtungen, wurden die öffentlichen oder privaten Einrichtungen folgendermaßen in Sektoren und Teilsektoren festgelegt:

Tabelle 13: Vorschlag einer EU-Richtlinie über die Resilienz kritischer Einrichtungen - Sektoren & Teilsektoren (vgl. EU 2020b: 74)

Sektor	Teilsektor
1. Energie	a. Strom b. Fernwärme und -kälte c. Erdöl

	d. Erdgas e. Wasserstoff
2. Verkehr	a. Luftfahrt b. Schienenverkehr c. Schifffahrt d. Straßenverkehr
3. Bankwesen	
4. Finanzmarktinfrastrukturen	
5. Gesundheit	
6. Trinkwasser	
7. Abwasser	
8. Digitale Infrastruktur	
9. Öffentliche Verwaltung	
10. Weltraum	

Mit der neuen Strategie möchte die EU die digitale wie auch physische Widerstandsfähigkeit erhöhen.

Die nachfolgenden beiden Zitate sind sehr aussagekräftig.

„Der für die Förderung unserer europäischen Lebensweise zuständige Vizepräsident, Margaritis **Schinias**, ergänzte: *„Cybersicherheit ist ein zentraler Bestandteil der Sicherheitsunion. Es gibt keine Unterscheidung mehr zwischen Online- und Offline-Bedrohungen. Digitale und physische Risiken sind inzwischen untrennbar miteinander verbunden. Das heutige Maßnahmenpaket zeigt, dass die EU bereit ist, alle ihre Ressourcen und ihr Fachwissen zu nutzen, um auf physische Bedrohungen und Cyberbedrohungen gleichermaßen vorbereitet zu sein und mit dem gleichen Maß an Entschlossenheit auf sie zu reagieren.“* (EU 2020a)

„Ylva **Johansson**, Kommissarin für Inneres, ergänzte: *„Unsere Krankenhäuser, Abwassersysteme oder Verkehrsinfrastruktur sind nur so stark wie ihre schwächsten Anbindungen; Störungen in einem Teil der Union können sich auf die Erbringung wesentlicher Dienstleistungen anderswo auswirken. Um das reibungslose Funktionieren des Binnenmarkts und die Existenzgrundlage der in Europa lebenden Menschen zu gewährleisten, muss unsere zentrale Infrastruktur gegen Risiken wie Naturkatastrophen, Terroranschläge, Unfälle und Pandemien wie die, die wir heute erleben, gewappnet sein. Mein Vorschlag zur kritischen Infrastruktur dient genau hierzu.“* (EU 2020a)

Mit diesen Aussagen und dem Vergleich zu vernetzten komplexen länderübergreifenden Abhängigkeiten, stellt sich die Frage ob das Europäische Parlament und der Europäische Rat anstelle der 2 europäischen Richtlinien nicht eher den Weg europäischer Verordnungen einschlagen sollten?

12 Kurzzusammenfassung - Abstract

Forschungsansätze betreffend Abhängigkeiten und Kaskadeneffekten zwischen kritischen Infrastrukturen, werden zunehmend eingesetzt. Kritische Infrastrukturen sind unterschiedlichsten Gefahren ausgesetzt. Dabei sollten Störungen nur ausnahmsweise, kurzzeitig und lokal begrenzt auftreten. Über den Sektor Gesundheitsversorgung gehören Krankenhäuser zu kritischen Infrastrukturen und müssen die Patientengrundversorgung auch in Notfallsituationen sicherstellen. Ein Krankenhaus ist ein hoch sensibles und komplexes System und ist von vielen internen wie externen Kooperationspartner, Funktionsbereichen und Ressourcen abhängig. Wie sich Auswirkungen einer Infrastruktur und Ressource auf andere Infrastrukturen und Ressourcenausbreiten, hängt vom Maß der Interdependenzen zwischen den Infrastrukturen und Ressourcen ab. Im stark vernetzten Krankenhaus 4.0 spielen cyber-physische Systeme eine wesentliche Rolle und dürfen bei der Betrachtung der Abhängigkeiten und Kaskadeneffekte nicht vernachlässigt werden.

Ziel dieser Forschungsarbeit ist es, Kenntnis über kritische Teilprozesse und Ressourcen sowie deren Abhängigkeiten und kaskadenartigen Auswirkungen auf den Gesamtprozess einer Aufbereitung von Medizinprodukten zu erwerben, damit die Aufrechterhaltung der Dienstleistung innerhalb eines fiktiven Krankenhauses bestmöglich durchgeführt werden kann.

Dazu wurden Teilaspekten vom Risiko- und Business Continuity Management für die Bearbeitung der Forschungsfragen eingesetzt und insbesondere wurde die Business Impact Analyse sowie das SAURON Rahmenmodell angewandt. Die CERBERUS Systemarchitektur diente als grundlegendes Modell zur Bearbeitung.

Anhand von Interviews, Befragungen und Workshops wurden für die AEMP zehn kritische Prozesse identifiziert. Zur Identifikation der Prozessabhängigkeiten wurden die Ressourcen in sechs unterschiedliche Kategorien eingeteilt. Zu diesen Prozessen und Ressourcen konnten Beschreibungen, Robustheit, Schadensklassen und BIA-Faktoren ermittelt werden. Zur Ermittlung der Daten wurden u.a. eine fiktive Prozesslandkarte zur Darstellung der übergeordneten und nachbarlichen Prozesse sowie ein relationales Datenmodell zur Darstellung der technischen Versorgungssysteme für die AEMP eingesetzt. In einer statischen Risikoanalyse konnten die direkt abhängigen Ressourcen pro Prozess ermittelt werden. Mit zwei Szenarien „Überschwemmung UG 2“ und „Cyberangriff“ konnten in einer dynamischen Risikoanalyse die Kaskadeneffekte zwischen den kritischen Prozessen und Ressourcen ermittelt und grafisch in einem Netzwerkdiagramm dargestellt werden.

Research projects of interdependencies and cascading effects between critical infrastructures are increasingly used within infrastructures. Critical infrastructures are exposed to a wide range of hazards. Disruptions should only occur exceptionally, briefly, and locally. In the healthcare sector, hospitals are critical infrastructures and must ensure basic patient care even in emergency situations. A hospital is a highly sensitive and complex system and is dependent on many internal and external cooperation partners, functional departments and resources. Incidents affecting one infrastructure and resource spread to other infrastructures and resources depending on the degree of interdependencies between the infrastructures and resources. In the highly interconnected Hospital 4.0, cyber-physical systems play an essential role and must not be neglected when considering interdependencies and cascade effects.

The aim of this research work is to acquire knowledge about critical sub-processes and resources as well as their dependencies and cascading effects on the overall process of reprocessing of medical devices. This to ensure that this service within a fictitious hospital can be guaranteed in the best possible way.

For this purpose, partial aspects of risk and business continuity management were used to address the research questions and, in particular, the business impact analysis of the SAURON framework model were applied. The CERBERUS system architecture served as a basic model for processing.

Based on interviews, surveys and workshops, ten critical processes were identified for the reprocessing unit for medical devices. To identify the process dependencies, the resources were divided into six different categories. For these processes and resources, descriptions, robustness, damage classes and BIA factors could be determined. To determine this data, a fictitious process map was used to represent the higher-level and neighboring processes. A relational data model was used to represent the technical supply systems for the reprocessing unit for medical devices. In a static risk analysis, the directly dependent resources per process were identified. In a dynamic risk analysis, the cascade effects between the critical processes and resources were identified by means of two scenarios "Flood Basement 2" and "Cyber-attack". The effects were graphically represented in a network diagram.

13 Literaturverzeichnis

- ALEXANDER D. E. (2002): Principles of emergency planning and management. - Edinburgh,
- ANDLER N. (2015): Tools für Projektmanagement, Workshops und Consulting : Kompendium der wichtigsten Techniken und Methoden. - Erlangen,
- ANT M. (2018): Effizientes strategisches Management - Die 10 Phasen einer erfolgreichen Unternehmensentwicklung. - Wiesbaden,
- ARETZ A. UND HIRSCHL B. (2017): Resilienz und Vulnerabilität von Infrastrukturen. - In: Ökologisches Wirtschaften - Fachzeitschrift 32, 14.
- ARGAW S. T., TRONCOSO-PASTORIZA J. R., LACEY D., FLORIN M.-V., CALCAVECCHIA F., ANDERSON D., BURLESON W., VOGEL J.-M., O'LEARY C., ESHAYA-CHAUVIN B. UND FLAHAULT A. (2020): Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. - In: BMC Medical Informatics and Decision Making 20, 146.
- AUSTRIAN-STANDARDS ONR 49000:2008, Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen
- AUSTRIAN-STANDARDS ONR 49002-2:2008, Risikomanagement für Organisationen und Systeme - Leitfaden Methoden der Risikobeurteilung
- BABS (2018): Leitfaden Schutz kritischer Infrastrukturen. Bern (CH): Bundesamt für Bevölkerungsschutz.
- BAHETI R. UND GILL H. (2011): Cyber-physical systems. - In: The impact of control technology 12, 161-166.
- BARTELS M., BECKER T., HAHNE M., HEMPEL L., KOLBE T. H. UND LIEB R. (2014): Simulation von Kaskadeneffekten beim Ausfall von Infrastrukturen. - In: ZfV-Zeitschrift für Geodäsie, Geoinformation und Landmanagement 4/2014.
- BARTELS M. UND LORENZ D. F. (2017): Resilienz und Vulnerabilität von Infrastrukturen ohne Bürger? - Infrastruktursicherheit als gesellschaftliche Herausforderung. - In: Ökologisches Wirtschaften 4.2017.
- BAUMANN S. UND VON RÖSSING R. (2017): Business Continuity Management – unverzichtbares Element eines angemessenen Risikomanagements. In: Hunziker Stefan und Meissner Jens O. (Hrsg.): Ganzheitliches Chancen- und Risikomanagement: Interdisziplinäre und Praxisnahe Konzepte. - Wiesbaden,
- BBK (2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus - Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen

Infrastrukturen des Gesundheitswesens. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

BBK (2011): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden. Berlin: Bundesministerium des Innern.

BBK (2020a): 10 Jahre "KRITIS-Strategie". Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

BBK (2020b): Handbuch Krankenhausalarm und -einsatzplanung (KAEP): Empfehlungen für die Praxis zur Erstellung eines individuellen Krankenhausalarm und -einsatzplans. - Bonn,

BBK (2021a): Online Glossar - Gefahr [Online]. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Available: https://www.bbk.bund.de/DE/Infothek/Glossar/functions/glossar.html?nn=19742&cms_lv2=19764 [Abfragedatum: 17.08.2021].

BBK (2021b): Online Glossar - Gefährdung [Online]. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Available: https://www.bbk.bund.de/DE/Infothek/Glossar/functions/glossar.html?nn=19742&cms_lv2=19764 [Abfragedatum: 17.08.2021].

BBK (2021c): Online Glossar - Verwundbarkeit [Online]. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Available: https://www.bbk.bund.de/DE/Infothek/Glossar/functions/glossar.html?nn=19742&cms_lv2=19848 [Abfragedatum: 17.08.2021].

BBK UND BSI. (2021a): Kritische Infrastrukturen - Sektoren- und Brancheneinteilung. In: (Hrsg.): Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik -

BBK UND BSI (2021b): Sektoren und Branchen KRITIS [Online]. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Bundesamt für Sicherheit in der Informationstechnik. Available: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sectoren_node.html [Abfragedatum: 10.08.2021].

(2020): bcIMPACT - Administration Guide. (Hrsg.): Consulting BC - Melk (A).

BC-CONSULTING (2021a): Business Continuity Management [Online]. Available: <https://www.bc-consulting.at/bcm/> [Abfragedatum: 06.08.2021].

BC-CONSULTING (2021b): Business Impact Analyse [Online]. Available: <https://www.bc-consulting.at/business-impact-analyse/> [Abfragedatum: 06.08.2021].

BEYN M. UND LÜTHI R. (2020): Funktionale und bauliche Voraussetzungen in der AEMP. In: Wismer Guido und Zanette Toni (Hrsg.): Sachgerechte Aufbereitung von Medizinprodukten. - Wiesbaden,

- BJA UND BM.I (2014): Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP). Wien: Bundeskanzleramt Österreich, Bundesministerium für Inneres.
- BMLRT-FFG (2021): KIRAS Sicherheitsforschung - Kooperative Projekte > 2016 - CERBERUS [Online]. Wien: Bundesministerium für Landwirtschaft, Regionen und Tourismus (BMLRT) - FFG - Österreichische Forschungsförderungsgesellschaft mbH. Available: https://www.kiras.at/index.php?id=173&L=0.2121121121212.1%27A%3D0&tx_tnews%5Btt_news%5D=596&cHash=67631ae82822bd120f83392913a75ba2 [Abfragedatum: 17.07.2021].
- BOURDY L. (2021): Cyberattaque à l'hôpital de Dax : 4 mois après, "l'œil du cyclone est passé, mais il y a toujours de la houle". Dax: France Bleu.
- BRÜDERKRANKENHAUS (2017): Stromausfall am Montagabend – erste Hintergründe. Trier: Krankenhaus der Barmherzigen Brüder Trier.
- BSI (2021): BSI-Standard 200-4 - Business Continuity Management - Community Draft - 200-4, Bonn: Bundesamt für Sicherheit in der Informationstechnik.
- BURMANN A., BRINKKÖTTER N., FISCHER B. UND MEISTER S. (2019): Das Digitale Krankenhaus: Online-Erhebung, Handlungsbedarf, Roadmap. - Düsseldorf,
- CARTER A., JONES A., LINNEN M.-T., LUTZENBERGER S., SCHERRER M., STENGER F., WENTZLER A. UND WIESE K. (2015): Anforderungen für den Bau oder Umbau einer Aufbereitungseinheit für Medizinprodukte (AEMP), Teil 3 - Räume und deren Zuordnung. - In: Zentralsterilisation 5/2015.
- DEITERS W., BURMANN A. UND MEISTER S. (2018): Digitalisierungsstrategien für das Krankenhaus der Zukunft. - In: Urologe. Ausgabe A 57, 1039.
- DEMING W. E. (1982): Quality, productivity, and competitive position massachusetts: Massachusetts institute of technology. - In: Center for Advanced Engineering Study, USA.
- EHLIN M. UND VARGAS V. (2013): Multi-hazard, multi-infrastructure, economic scenario analysis. - In: Environment Systems & Decisions Vol. 33.
- EROARKE (2014): DEVICESMART PLATFORM – CYBER-PHYSICAL SYSTEMS [Online]. Available: <https://devicesmart.wordpress.com/2014/05/05/devicesmart-platform-cps-cyber-physical-systems-are-a-natural-consequence-of-an-increasingly-connected-physical-world/> [Abfragedatum: 15.08.2021].
- EU (2005): Grünbuch über ein europäisches Programm für den Schutz kritischer Infrastrukturen. KOM(2005) 576 endgültig, Brüssel: Europäische Kommission.
- EU. (2008): RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die

Bewertung der Notwendigkeit, ihren Schutz zu verbessern. In: Rat der Europäischen Union. (Hrsg.): - Brüssel

EU (2020a): Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen [Online]. Brüssel: Europäische Kommission. Available: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2391 [Abfragedatum: 30.08.2021].

EU (2020b): Vorschlag für eine Richtlinie des Europäischen Parlamentes und des Rates über die Resilienz kritischer Infrastrukturen. 220/0365 (COD), Brüssel: Europäische Kommission.

FIEDLER M., SILLER H. UND STIERLE J. (2019): Einleitung: Das Krankenhaus als besonderer Dienstleister. In: Stierle Jürgen, Siller Helmut, Fiedler Manfred und Ortner Sonja (Hrsg.): Handbuch Strategisches Krankenhausmanagement. - Wiesbaden,

(2012): The Global Risks Report, 7. Aufl. Bd. 2012. (Hrsg.): World Economic Forum - Geneva.

GAERTNER R. (2020): Großalarm in Krankenhaus : Feuer in Klinik-Keller – 85 Menschen gerettet. In: Hamburger Morgenpost, 13.12.2020.

GASSMANN O., BÖHM J. UND PALMIÉ M. (2019): Smart cities : : introducing digital innovation to cities. - United Kingdom ;,

GLADE T., ANDERSON M. UND CROZIER M. J. (2005): Landslide hazard and risk. - Chichester, West Sussex, England,

GOH M. H. (2011): Recovery Objectives RTO RPO and MTPD. Recovery Objectives RTO RPO and MTPD.png, Singapore: BCM Institute.

GOOGLE-SCHOLAR (2021): Identifying, understanding, and analyzing critical infrastructure interdependencies [Online]. Google Scholar. Available: https://scholar.google.com/scholar?lookup=0&q=Identifying,+understanding,+and+analyzing+critical+infrastructure+interdependencies&hl=de&as_sdt=0,5 [Abfragedatum: 04.09.2021].

GREVEN A. (2020): Stromausfall am Bundeswehrkrankenhaus Hamburg. Handbuch Krankenhausalarm und -einsatzplanung (KAEP): Empfehlungen für die Praxis zur Erstellung eines individuellen Krankenhausalarm und -einsatzplans. - Bonn, 175

GUEYE A., MBAYE B., FALL D., DIOP A. UND KASHIHARA S. (2020): A Matrix Model to Analyze Cascading Failure in Critical Infrastructures. -,

- GÜNTHER E. (2018): Resilienz [Online]. Wiesbaden: Gabler Wirtschaftslexikon. Available: <https://wirtschaftslexikon.gabler.de/definition/resilienz-52429/version-275567> [Abfragedatum: 04.09.2021].
- HAAS P. (2005): Medizinische Informationssysteme und elektronische Krankenakten. - Heidelberg,
- HABEGGER B. UND KMIECIK S. (2010): Der Schutz kritischer Infrastrukturen: Gegenwart und Zukunft - Ergebnisse eines Expertendialogs. In: Crisis and Risk Network (CRN) - Center for Security Studies (CSS) ETH Zürich (Hrsg.), Zürich (CH): Center for Security Studies (CSS) der ETH Zürich.
- HEHENBERGER P., VOGEL-HEUSER B., BRADLEY D., EYNARD B., TOMIYAMA T. UND ACHICHE S. (2016): Design, modelling, simulation and integration of cyber physical systems: Methods and applications. - In: Computers in industry Vol. 82, 289.
- HINES P., DOBSON I. UND REZAEI P. (2017): Cascading power outages propagate locally in an influence graph that is not the actual grid topology. -,
- HUFSCHMIDT G. (2018): Verwundbarkeit und Resilienz für ein ganzheitliches Risiko- und Krisenmanagement im Krankenhaus. In: Scholtes K., Wurmb T. und Rechenbach P. (Hrsg.): Risiko- und Krisenmanagement im Krankenhaus - Alarm- und Einsatzplanung. - Stuttgart,
- ISO 31000:2018(F), Management du risque - Lignes directrices; Risk management - Guidelines
- ISO 22301:2019 (F), Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences
- ISO/TS 22317:2015, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- JAMALUDIN J. UND ROHANI J. (2018): Cyber-Physical System (CPS): State of the Art. -,
- JOPP R. (2020): Brand im BG Universitätsklinikum Bergmannsheil Bochum. Handbuch Krankenhausalarm und -einsatzplanung (KAEP): Empfehlungen für die Praxis zur Erstellung eines individuellen Krankenhausalarm und -einsatzplans. - Bonn, 175
- JUHRA C. UND BORN J. (2020): Klinik 4.0 – Das digitale Krankenhaus. Berlin, Heidelberg.
- KAMPS U. (2018): stochastischer Prozess [Online]. Wiesbaden: Gabler Wirtschaftslexikon. Available: <https://wirtschaftslexikon.gabler.de/definition/stochastischer-prozess-45652/version-268941> [Abfragedatum: 04.09.2021].

- KIRMSE G. UND WILD R. (2020): Instrumentenkunde und -pflege. In: Wismer Guido und Zanette Toni (Hrsg.): Sachgerechte Aufbereitung von Medizinprodukten. - Wiesbaden,
- KRYSTEK U. UND FIEGE S. (2013): Risikomanagement [Online]. Gabler Wirtschaftslexikon. Available: <https://wirtschaftslexikon.gabler.de/definition/risikomanagement-42454/version-173114> [Abfragedatum: 22.08.2021].
- KUNTSCHKE P. UND BÖRCHERS K. (2017a): Grundlagen des Qualitäts- und Risikomanagements. In: Kuntsche Peter und Borchers Kirstin (Hrsg.): Qualitäts- und Risikomanagement im Gesundheitswesen: Basis- und integrierte Systeme, Managementsystemübersichten und praktische Umsetzung. - Berlin, Heidelberg, 51-118
- KUNTSCHKE P. UND BÖRCHERS K. (2017b): Qualitäts- und Risikomanagement im Gesundheitswesen : Basis- und integrierte Systeme, Managementsystemübersichten und praktische Umsetzung. - Berlin, Heidelberg,
- LANGER C. (o.J.): Wissenschaftliches Arbeiten - Methoden und Technik. 3. Auflage, Rostock.
- MACDERMOTT Á., HURST W., SHI Q. UND MERABTI M. (Hrsg.) (2014): Simulating Critical Infrastructure Cascading Failure. Proceedings - UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, UKSim 2014, 2014 of Conference, -.
- MAIER G. N. W., ENGELS G. UND STEFFEN E. (2020): Einleitung. In: Maier Günter W., Engels Gregor und Steffen Eckhard (Hrsg.): Handbuch Gestaltung digitaler und vernetzter Arbeitswelten. - Berlin, Heidelberg, 163-188
- MAIER S. UND AENGENHEYSER S. (2020): Cyber-Security und Resilienz verstehen. Wiesbaden.
- MAINZER K. (2020): Technikgestaltung und Ethik für die Arbeitswelt 4.0. In: Maier Günter W., Engels Gregor und Steffen Eckhard (Hrsg.): Handbuch Gestaltung digitaler und vernetzter Arbeitswelten. - Berlin, Heidelberg, 163-188
- MARSDEN G. UND REARDON L. (2018): Governance of the Smart Mobility Transition. - Bingley, UK ;,
- ME. (2018a): Règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques. In: Journal officiel du Grand-Duché de Luxembourg. (Hrsg.): Ministère de l'État - Luxembourg
- ME. (2018b): Règlement grand-ducal du 21 février 2018 fixant la structure des plans de sécurité et de continuité de l'activité des infrastructures critiques. In: Journal officiel du Grand-Duché de Luxembourg. (Hrsg.): Ministère de l'État - Luxembourg

- MEIKE R., CARSTEN R., SARAH M., STEVE B., MICHAEL H., CARYS S., MURRAY A. S., PAUL J. P., JOHN F., CLAIRE I., DAVID S., DANIEL S., URSULA R., BENJAMIN G., DOLORES O., TAYRNE B., NURIA DE L., JUAN R. UND JUAN A. (2017): Road2CPS priorities and recommendations for research and innovation in cyber-physical systems. -,
- MEILINGER S. (2012): Verursachungsgerechte Kostenverteilung in der zentralen Sterilgutversorgungsabteilung (ZSVA): Optimale Umlage der Aufbereitungskosten von Medizinprodukten. - Hamburg,
- MEISSNER J. O. (2017): Risikomanagement und Organisationale Resilienz. In: Hunziker Stefan und Meissner Jens O. (Hrsg.): Ganzheitliches Chancen- und Risikomanagement: Interdisziplinäre und Praxisnahe Konzepte. - Wiesbaden,
- MÖLLER E. B. (2016): Prozessplanung in Akut-Krankenhäusern : Robuste zyklische Operationspläne mit szenariobasierter Modellierung von Unsicherheit. - Wiesbaden :,
- MÜLLER-SEITZ G. (2014): Von Risiko zu Resilienz — Zum Umgang mit Unerwartetem aus Organisationsperspektive. - In: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung Vol. 68, 102-122.
- NCTV. (2018): Resilient critical infrastructure. In: (Hrsg.): National Coordinator for Security and Counterterrorism - Ministry of Justice and Security - The Hague
- NORDHAUSEN T. UND HIRT J. (2018): Manual zur Literaturrecherche in Fachdatenbanken. - Halle (Saale),
- PESCAROLI G. UND ALEXANDER D. (2015): A definition of cascading disasters and cascading effects: Going beyond the “toppling dominos” metaphor. - In: Planet@ risk Vol. 3, 58-67.
- PETERS J. (2020): Stromausfall: Keine Auswirkungen im Apenrader Krankenhaus. In: Der Nordschleswiger, 15.09.2020.
- PFENNINGER E. UND ADOLPH O. (2017): Memorandum – Zur Vulnerabilität kritischer Infrastrukturen an Bundesdeutschen Kliniken. - In: Notfall & Rettungsmedizin Vol. 20, 681.
- PORTMANN A. UND HIRSCHI O. (2017): Cybersecurity in Schweizer Unternehmen. In: Birrer Thomas K., Rupp Markus und Spillmann Martin (Hrsg.): Corporate Treasury Management - Konzepte für die Unternehmenspraxis. - Wiesbaden, 456-473
- PRITI S. (2017): Practitioner's Guide to Business Impact Analysis. - Boca Raton, FL,
- RECHENBACH P. (2018): Die Kritische Infrastruktur Krankenhaus. In: Scholtes K., Wurmb T. und Rechenbach P. (Hrsg.): Risiko- und Krisenmanagement im Krankenhaus - Alarm- und Einsatzplanung. - Stuttgart,

- REDAKTION-MOPO (2020): Alarm nach Mitternacht: Feuer im Hamburger Bundeswehrkrankenhaus ausgebrochen. In: Hamburger Morgenpost, 14.10.2020.
- REINARTZ K. (2020): Cyberangriff auf das Lukaskrankenhaus Neuss. Handbuch Krankenhausalarm und -einsatzplanung (KAEP): Empfehlungen für die Praxis zur Erstellung eines individuellen Krankenhausalarm und -einsatzplans. - Bonn, 175
- RESEARCHGATE (2021): Identifying, understanding, and analyzing critical infrastructure interdependencies - Stats [Online]. ResearchGate GmbH. Available: https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies/stats [Abfragedatum: 04.09.2021].
- RINALDI S. M., PEERENBOOM J. UND KELLY T. K. (2001): Identifying, understanding, and analyzing critical infrastructure interdependencies. - In: Control Systems, IEEE 21, 11-25.
- ROITSCH M., WEINIG F. UND WEPF M. (2020): Qualitätsmanagement. In: Wismer Guido und Zanette Toni (Hrsg.): Sachgerechte Aufbereitung von Medizinprodukten. - Wiesbaden,
- ROMEIKE F. (2018): Risikomanagement. - Wiesbaden,
- RUMPOLT P. A. UND GLADE T. (2012): Zitierempfehlung des Instituts für Geographie und Regionalforschung der Universität Wien. Ein Leitfaden für korrektes Zitieren im wissenschaftlichen Kontext. - Wien,
- SAURON (2020): Forschungsprojekt SAURON [Online]. Available: <https://www.sauronproject.eu> [Abfragedatum: 25/10/2020].
- SCHAUER S., KÖNIG S., RASS S., GRAFENAUER T., WACHTER J., SCHABERREITER T., QUIRCHMAYR G., POLEDNA S., LATZENHOFER M., STOLLNBERGER R. UND STEINNOCHER K. 2018: Risikobewertung für vernetzte kritische Infrastrukturen. D-A-CH Security, Location, - Place, 313-322.
- SCHAUER S., RAINER B., MUSEUX N., DAVID F., HINGANT GÓMEZ J., RODRIGO F., BEYER S., PERIS R. UND LOPEZ S. (2019): Conceptual Framework for Hybrid Situational Awareness in Critical Port Infrastructures: 13th International Conference, CRITIS 2018, September 24-26, 2018, Revised Selected Papers. - Kaunas, Lithuania, 191-203
- SCHMECK J., SCHMECK S. B., KOHNEN W., WERNER C., SCHAFER M. UND GERVAIS H. (2008): Bedeutung der Materiallogistik im Schnittstellenmanagement der Operationsabteilungen - Ist die Sterilgutversorgung ein neues Geschäftsfeld der OP-Organisation? - In: Der Anaesthesist Vol. 57.

- SCHMOLA G. (2016): Grundlagen und Instrumente des Risikomanagements. In: Schmola Gerald und Rapp Boris (Hrsg.): Compliance, Governance und Risikomanagement im Krankenhaus: Rechtliche Anforderungen – Praktische Umsetzung – Nachhaltige Organisation. - Wiesbaden,
- SCHUSTER C. (2019): Brand in einem Patientenzimmer des Marienhospitals - 19 Verletzte und 100 Betroffene durch Rettungsdienst und Feuerwehr versorgt - ein 77-jähriger Mann verstarb vor Ort. In: Düsseldorf Feuerwehr (Hrsg.), Düsseldorf: Feuerwehr Düsseldorf.
- SPÖRRER S. (2014): Business Continuity Management : ISO 22301 und weitere Normen im Rahmen der Informationstechnologie. - Wiesbaden,
- STOLZENBURG K. UND KOWALZIK B. (2018): Risikomanagement und Krankenhausalarmplanung aus der Sicht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe. In: Scholtes K., Wurmb T. und Rechenbach P. (Hrsg.): Risiko- und Krisenmanagement im Krankenhaus - Alarm- und Einsatzplanung. - Stuttgart,
- SZ (2021): Technischer Defekt löste vermutlich Kraftwerks-Brand aus. In: SZ, 11.02.2021.
- T3N (2020): Cyberangriff legt tschechisches Krankenhaus mit größtem Corona-Testlabor des Landes lahm. In: t3n digital pioneers, 19.03.2020.
- TAARUP-ESBENSEN J. (2020): The Business Impact Analysis, Working paper no 1. University College Copenhagen, Emergency and Risk management programme.
- TAHA W., TAHA A.-E. UND THUNBERG J. (2020): What is a Cyber-Physical System? Cyber-Physical Systems: A Model-Based Approach, -, 3-18
- TORABI S. A., REZAEI SOUFI H. UND SAHEBJAMNIA N. (2014): A new framework for business impact analysis in business continuity management (with a case study). - In: Safety science 68, 309-323.
- UKD (2020a): Krankenhaus derzeit nur sehr eingeschränkt erreichbar – Patientenversorgung eingeschränkt. Universitätsklinikum Düsseldorf.
- UKD (2020b): Wieder normale Patientenzahlen nach IT-Ausfall. Universitätsklinikum Düsseldorf.
- WAGENBACH E. (2021): Hochwasser „Um 3:35 Uhr haben wir das Krankenhaus aufgegeben“. In: mbH Bibliomed-Medizinische Verlagsgesellschaft (Hrsg.), Melsungen: Bibliomed-Medizinische Verlagsgesellschaft mbH.
- WALDMANN K.-H. UND HELM W. E. (2016a): Markov-Ketten. Berlin, Heidelberg.

- WALDMANN K.-H. UND HELM W. E. (2016b): Simulation stochastischer Systeme - Eine anwendungsorientierte Einführung. - Berlin, Heidelberg,
- WARUM M., RAINER B., SCHAUER S., KÖNIG S., GRAFENAUER T. UND RASS S. (2020): SAURON Propagation Engine Editor [Online]. Available: <https://atlas.ait.ac.at/sauron/#/> [Abfragedatum: 25.10.2020].
- WILLISEGGER J. (2017): Schutz kritischer Infrastrukturen. In: Hunziker Stefan und Meissner Jens O. (Hrsg.): Ganzheitliches Chancen- und Risikomanagement: Interdisziplinäre und Praxisnahe Konzepte. - Wiesbaden,
- WURMB T., SCHOLTES K., KOLIBAY F. UND DERSCH D. (2018): Projektplan. In: Scholtes K., Wurmb T. und Rechenbach P. (Hrsg.): Risiko- und Krisenmanagement im Krankenhaus - Alarm- und Einsatzplanung. - Stuttgart,
- YU X. UND XUE Y. (2016): Smart Grids: A Cyber-Physical Systems Perspective. - In: Proceedings of the IEEE Vol. 104, 1070.

14 Anhang

14.1 Prozessabhängigkeiten der AEMP

Im Anschluss an die Erstellung der Prozesslandkarte für das fiktive Krankenhaus wurden die Prozessabhängigkeiten der Aufbereitungseinheit für Medizinprodukte graphisch dargestellt.

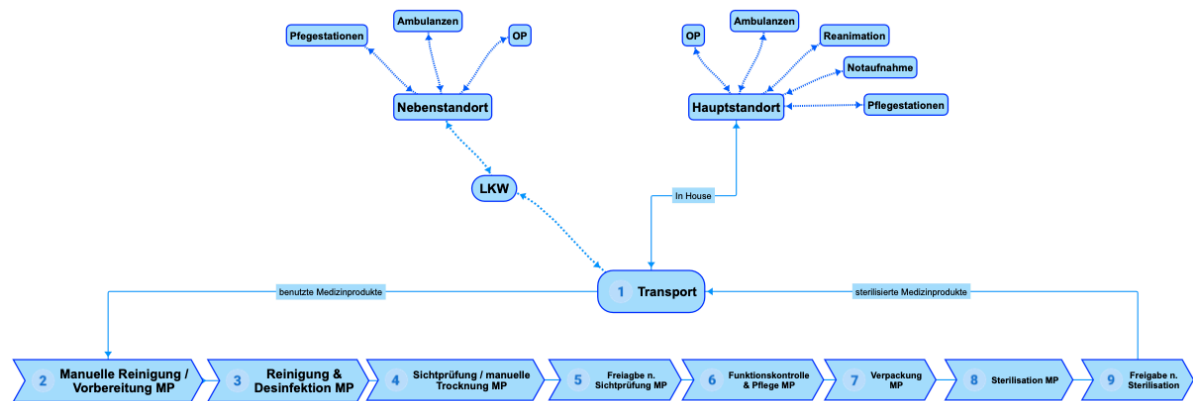


Abbildung 52: Prozessabhängigkeiten AEMP

14.2 BIA-Datensammlung - Deckblatt

BUSINESS IMPACT ANALYSE (BIA) Daten- und Informationsbeschaffung Expert*Innenbefragungen

Abteilung:	Aufbereitungseinheit Medizinprodukte
Prozess:	Aufbereitung von Medizinprodukten
Prozessverantwortliche(r):	Leiter AEMP
	16.02.2021
	24.02.2021
Termine der Befragungen & Workshops:	19.03.2021
	01.04.2021
	07.05.2021
	20.05.2021
Teilnehmer der Datensammlung:	* Bereichsleiter der Plegedirektion * Leiterin AEMP * Qualitätsbeauftragte AEMP * Leiter Technik * Leiter EDV * Leiter Lenkungsausschuss BCM * Leiter Arbeitssicherheit, Gesundheits- und Brandschutz

Was versteht man unter einer Business Impact Analyse (BIA)?

Damit das Krankenhaus Risiko- und Business Continuity Management betreiben kann, müssen kritische Prozesse identifiziert, analysiert und bewertet werden. In diesem Zusammenhang wird eine BIA eingesetzt. Die BIA ist ein Werkzeug, das Informationen zu Schwachstellen liefern kann. Werden dies Schwachstellen identifiziert, können entsprechende Gegenmaßnahmen eingeleitet (Risikoreduktion) und Kontinuitätspläne erstellt werden.

Die Datei ist in mehrere Blätter unterteilt:

- Deckblatt
- Allgemeine Informationen zum Ablauf der Datensammlung und Beschreibung von Begriffen
- Prozessbeschreibungen und -abfragen in Form eines Fragebogen
- BIA-Matrix mit den Prozess- und Ressourcenabhängigkeiten sowie den Beschreibungen, Schadensklassen und Ausfallzeiten für die anschließende Risikoanalyse
- Dokumentation der Simulationsparameter für die anschließende dynamische Risikoanalyse

14.3 BIA-Datensammlung - Allgemeine Informationen

Ablauf der BIA - Datensammlung

Die Datensammlung dient dazu ein all umfassendes Verständnis zu den kritischen Prozessen zu erhalten. Anschließend kann eine Business Impact Analyse für diese Prozesse durchgeführt werden. Folgende Schritte sind dafür notwendig:



- 1) Prozessbeschreibung zum allgemeinen Verständnis,
- 2) Identifikation von kritischen Prozessschritten,
- 3) Identifikation von internen und externen Partnern sowie allen Ressourcen,
- 4) Bestimmung der Abhängigkeiten zwischen den Prozessschritten, den Partnern und den Ressourcen,
- 5) Beschreibung der Robustheit von Prozessen, Partnern und Ressourcen (Ausfallsicherheit, Redundanzen),
- 6) Bestimmung der Schadensklassen für (Operate, Legal, Finance, Image),
- 7) Bestimmung des Recovery Point Objective (RPO) (siehe Grafik),
- 8) Bestimmung des Recovery Time Objective (RTO) (siehe Grafik),
- 9) Bestimmung des maximal tolerierbaren Ausfallzeitraumes (MTPD) (siehe Grafik).

Schadensklassen

Die Schadensklassen wurden dem BSI-Standard 200-4 Business Continuity Management entnommen.

Quelle: BSI (2021): BSI-Standard 200-4 - Business Continuity Management - Community Draft - 200-4, Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.

Managebar - Gering:

Allgemeine Beschreibung: Ausfall hat geringe, kaum spürbare Auswirkungen.

Operate: Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb wird unwesentlich beeinträchtigt.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen Konsequenzen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution unerheblich.

Image: Negative Innen- und Außenwirkung (Imageschaden): In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten.

Signifikant - Mittel:

Allgemeine Beschreibung: Ausfall hat spürbare Auswirkungen.

Operate: Beeinträchtigung der Aufgabenerfüllung: Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution tolerabel.

Image: Negative Innen- und Außenwirkung (Imageschaden): Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.

Kritisch - Hoch:

Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen

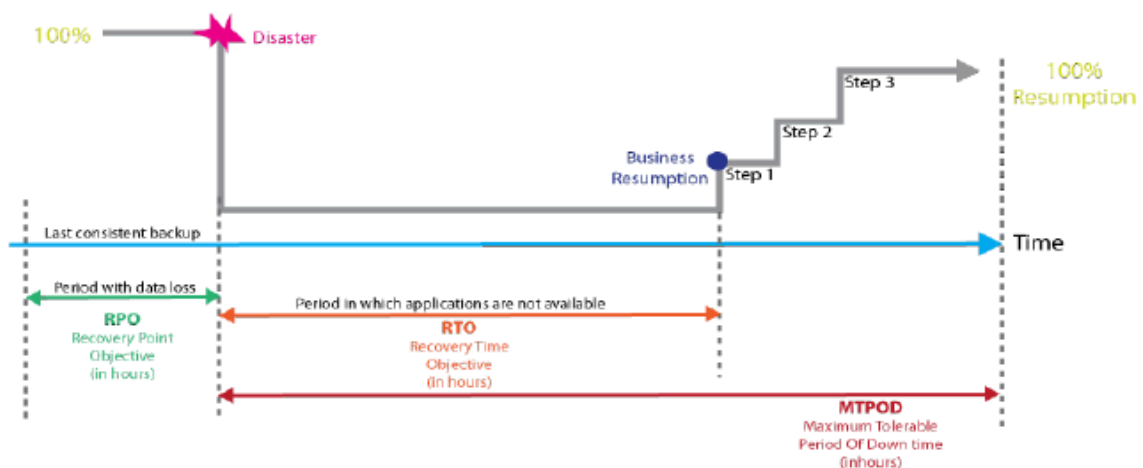
Operate: Beeinträchtigung der Aufgabenerfüllung: Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.

Legal: Verstoß gegen Gesetze, Vorschriften und Verträge: Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.

Finance: Finanzielle Auswirkungen: Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.

Image: Negative Innen- und Außenwirkung (Imageschaden): Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.

Ausfallzeiten RTO, RPO, MTPD



Quelle: GOH M. H. (2011): Recovery Objectives RTO RPO and MTPD. Recovery Objectives RTO RPO and MTPD.png, Singapore: BCM Institute.

Definition der Kennwerte gemäss ISO 22317

Quelle: ISO/TS 22317:2015, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

RPO:

Recovery Point Objective or
MDL: Maximum Data Loss

RPO ist die Zeit, in der ein Datenverlust für die Wiederaufnahme des Prozesses oder der Dienstleistung hingenommen werden kann. Prinzipiell ist es die Zeit zwischen zwei Datenspeicherungen.

RTO:

Recovery Time Objective

RTO ist die Wiederherstellungszeit, die benötigt wird um nach einem Ereignis den Prozess oder die Dienstleistung wieder Schrittweise aufzunehmen.

MTPoD or MTPD:

Maximum Tolerable Period of Disruption

MTPD ist die maximal tolerierbare Unterbrechungsdauer bevor negative Auswirkungen auf die nachfolgenden Prozesse oder Dienstleistungen entstehen.

14.4 BIA-Datensammlung – Prozessbeschreibung

Prozessbeschreibung

Die nachfolgende Prozessbeschreibung dient dazu Verständnis über den wertschöpfenden Beitrag zum Gesamtprozess der Patientenversorgung im Krankenhaus zu bekommen.

Durch das Verständnis der Prozessbeschreibung ist es möglich, zu analysieren, wie sich die Folgen von Gefährdungen auf die Fähigkeit eines Prozesses zur Wertschöpfung und anschließend auf die Gestaltung von Schutzmaßnahmen auswirken werden.

Die folgenden Leitfragen dienen dazu das Brainstorming für die Datensammlung der BIA anzuregen. Gegebenenfalls werden die Antworten in der BIA-Matrix (nachfolgendes Arbeitsblatt) an entsprechender Stelle eingetragen.

Zentrale Leitfrage:

Wenn ein(e) Prozess / Ressource ausfällt, mit welchem Schadenpotenzial ist zu rechnen?

1. Kunden

a) Welche Abteilungen mit direkter Patientenversorgung hängen von den zu bewertenden Prozessen ab?

- 1) Hauptstandort:** OP, Endoskopie, Urologie, ZNA, Polikliniken, Pflegestationen, Reanimation, Aufwachraum, ambulanten Untersuchungsbereiche, Physiotherapie,
- 2) Nebenstandort:** OP, Endoskopie, Polikliniken, Pflegestationen
- 3) Extern:** private Hebamme

b) Welche Abteilungen mit indirekter Patientenversorgung hängen von den zu bewertenden Prozessen ab?

keine

2. kritische Prozessschritte / Ressourcen

- a) Welche kritischen Prozessschritte werden durch die Abteilung ausgeführt?
- b) Welche kritischen (physische und personenbezogene) Ressourcen werden für die Ausführung der kritischen Prozesse benötigt?
- c) Welche externen Partner werden für die Ausführung von kritischen Prozessen benötigt?
- d) Welche externen Partner werden für die Bereitstellung von kritischen Ressourcen benötigt?

>>> Bezeichnung der kritischen Prozesse und Ressourcen in Spalte C der Matrix eintragen.
>>> Beschreibung in die entsprechende Teile der Spalte "Beschreibung der Prozesse und Ressourcen" eintragen.

3. Partner- und Kundenbeziehung

a) Haben Sie Verträge (Service Level Agreement) mit den internen Kunden-Abteilungen und

- * keine Service Level Agreement vorhanden
- * regelmässige Besprechungen mit OP, Endoskopie/Urologie

b) Haben Sie Verträge (Service Level Agreement) mit den externen Kunden-Abteilungen und Partnern?

- * Service Level Agreement vorhanden
- * Ausfallkonzept mit 2 anderen Kliniken für alle Tätigkeiten
- >>> Beschreibung in Spalte "Robustheit" eintragen

c) Werden Prozesse zur Erfüllung des Auftrages der Abteilung werden durch externe Partner ausgeführt (Outsourcing)?

- * Transport zwischen den beiden Standorten durch externen Transportpartner
- >>> Beschreibung in Spalte "Robustheit" eintragen

4. Robustheit der Prozesse und Ressourcen

a) Können störende Ereignisse absorbiert werden (Ausfallsicherheit)?

b) Existieren Redundanzen?

c) Gibt es Mindestanforderungen an die Prozessleistung, welche zur Erfüllung des Auftrages erreicht werden müssen?

- >>> Beschreibung in Spalte "Robustheit" eintragen

5. Finanzaspekte

a) Welche durchschnittlichen Kosten müssen für einen Prozessdurchlauf aufgewendet werden?

keine Informationen vorhanden

b) Gibt es Wartungsverträge für die kritischen Geräte & Anlagen? Wenn ja, bitte beschreiben und die Kosten angeben.

Es gibt Wartungsverträge für die Geräte der AEMP, allerdings sehen diese Verträge keine Reaktions- als auch Einsatzzeiten vor Ort vor.

c) Gibt es Ausfallkonzepte mit externen Partnern? Wenn ja, bitte beschreiben und die Kosten

Ein Ausfallkonzept besteht mit 2 anderen Krankenhasträgern. Im Notfall, bei Ausfällen, unterstützen sich diese 3 Partner gegenseitig. Die Unterstützung ist unendgültlich. Die Kosten für Transport und zusätzlichem Personal für den internen Mehraufwand müssen vom Träger bei dem der Notfall eingetreten ist aufgewendet werden. Service Level Agreement mit den anderen Krankenhasträgern ist vorhanden.
=> siehe Spalte "Robustheit"

6. Schadensklassen (3 Kategorien)

a) Welche Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?

b) Welche Auswirkungen haben der Verstoß gegen Gesetze, Vorschriften und Verträge?

c) Welche finanziellen Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?

d) Welche imageschädigenden Auswirkungen haben Beeinträchtigungen der Aufgabenerfüllung?

- >>> Auswahl in der entsprechenden Spalte der "Schadensklassen" eintragen:

- * Managebar - Gering
- * Signifikant - Mittel
- * Kritisch - Hoch

7. Ausfallzeiten

a) Bis zu welchem rückwirkenden Zeitpunkt vor einem Ereignis, dürfen die notwendigen informatischen Daten ausfallen ohne dass sie wieder hergestellt werden müssen? – Recovery Point Objective (**RPO**)?

b) Ab welchem Zeitpunkt nach einem Ereignis muss der Prozess spätestens wiederanlaufen? – Recovery Time Objective (**RTO**)

c) Welche maximal tolerierbare Unterbrechungsdauer in der der Prozess nicht oder nur eingeschränkt verfügbar ist wird akzeptiert, bevor die Auswirkungen als inakzeptabel eingestuft werden? – Maximum Tolerable Period of Disruption (**MTPD**)

>>> Auswahl in der entsprechenden Spalte der "RPO", "MTPD" oder "RTO" eintragen:

- * 10 Minuten
- * 30 Minuten
- * 1 Stunden
- * 2 Stunden
- * 4 Stunden
- * 8 Stunden
- * 12 Stunden
- * 24 Stunden
- * 3 Tage
- * 7 Tage

14.5 BIA-Matrix – Abhängigkeiten

Auf den folgenden 4 Seiten sind die Abhängigkeiten dargestellt.

[illegible]

Liste der Prozesse & Ressourcen			Interne & Externe kritische Ressourcen		Versorgung / techn. Anlagen	
BUSINESS IMPACT ANALYSE (BIA)						
MATRIX						
Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen						
▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung						
Interne & Externe kritische R	Versorgung / techn. Anlagen	BHKW AV Stromversorgung				
		AV Übergabe & Etagenverteiler BT 3.2 Et.-1	x			
		BHKW SV Stromversorgung				
		SV Übergabe & Etagenverteiler BT 3.2 Et.-1		x		
		Etagenverteiler BT 3.2 Technikzentrale 1B	x	x		
		Schachtverteiler BT 3.1 Et. -2	x	x		
		Etagenverteiler BT 3.1 Et. 1				
		Etagenverteiler BT 3.1 Et. 2			x	
		Etagenverteiler BT 3.1 Technikzentrale 1A			x	
		Schachtverteiler BT 2.0 Et.-2	x	x		
		Etagenverteiler BT 2.0 Et.-1			x	
		Schachtverteiler BT 1.3 Et. -1	x	x		
		Etagenverteiler BT 1.3 Et. -1			x	
		Schachtverteiler BT 1.1 Et. -2	x	x		
		Etagenverteiler BT 1.1 Et. -1				x
		USV Stromversorgung Südtrakt Et. 2			x	
		BHKW Hausdampfversorgung				
		Hausdampfübergabe Süd BT 3.2 Et.2			x	
		Reindampfversorgung Süd BT 3.2 Et. 2			x	
		BHKW Wärmeversorgung				
		Wärmeübergabe Süd BT 3.2 Et. -2	x	x		
		BHKW Kälteversorgung				
		Kälteübergabe Süd BT 3.2 Et. -2	x	x		
		Kälteübergabe Nord BT 1.1 Et. -1			x	
		Lüftungsanlage 17A Südtrakt Et. 2			x	
		Produktion Med. Druckluft 5 bar BT 1.1 Et. -1			x	
		Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1			x	
		Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2				
		TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1			x	
		TR-W Enthärtung BT 1.1 Et. -1			x	
		Osmoseanlage BT 1.1 Et. -1			x	
		Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1				
		Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2		x		
		Abwasserhebeanlage BT 2.0 Et. -2				
		Aufzüge A4-A6 BT 2.0				
		Aufzug A7 BT 3.1				
		Versorgung durch Telekomanbieter BT 2.0 Et. -1				
		EDV-Netzwerk redundant		x		
		EDV-Netzwerk nicht redundant		x		
		Serverraum Nord BT 1.3. Et. -1				
		Serverraum Süd BT 3.2 Et. -1	x	x		
		Schwachstromsicherheitsanlagen BT 2.0 Et. -1				
		Telekomanlage BT 2.0 Et. -1				
		elektr. Zutrittskontrolle BT 2.0 Et. -1				

14.6 BIA-Matrix – Prozess- und Ressourcenbeschreibung, Beschreibung der Robustheit

Auf den folgenden 2 Seiten sind die Beschreibungen der Prozesse, Ressourcen und Robustheit aufgelistet.

▶▶ Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Beschreibung der Prozesse & Ressourcen	Beschreibung der Robustheit
kritische Prozessschritte		1 Transport gebrauchte Medizinprodukte	Transport benutzte MP & Endoskope aus den Verbrauchsabteilung zur AEMP, Annahme der Transportsiebe	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner
		2 Vorreinigung & Vorbereitung MP	Auspacken der Siebe, grobe Vorreinigung wenn nötig, Vorbereitung der Geräteträger mit MP	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		3 maschinelle Reinigung & Desinfektion MP	Maschinelle Reinigung von Medizinprodukten	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		4 Sichtprüfung & manuelle Trocknung MP	Übernahme der desinfizierten MP vom Geräteträger, Prüfung auf Sauberkeit	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		5 Freigabe nach Prüfung Medizinprodukte	Freigabe zur Funktionskontrolle nach derSichtprüfung	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		6 Funktionskontrolle & Pflege MP	Funktionskontrolle zum Teil mit unterstützenden Geräten, Pflege (z.B. ölen), Ersetzen verbrauchte MP	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		7 Verpackung Medizinprodukte	komplette Siebe werden manuelle verpackt und für die Sterilisation vorbereitet	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		8 Sterilisation Medizinprodukte	Verpackte Siebe werden sterilisiert	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		9 Freigabe nach Sterilisation MP	Freigabe der Siebe nach der Sterilisation für den Transport	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
		10 Transport sterile Medizinprodukte	Transport sterilisierte MP und Endoskope von der AEMP zu den Verbrauchsabteilung	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner
Interne & Externe kritische Ressourcen	internes Personal (Rollen)	Logistiker	Bearbeitet die Prozessschritte 1 & 10 (interner Transport) innerhalb der beiden Standorte	mehere intere Logistiker
		Fachkundige in der Aufbereitung von MP	Bearbeiten die Prozessschritte 1 (Warenannahme) & 2 bis 9	15 Personen in der AEMP in allen Bereichen einsetzbar
		AEMP Stammdatenadministrator	Pflegen die Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope	2 Stammdatenaministratoren
		Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Verantwortet das Qualitätsmanagement exklusiv in der AEMP und ist gleichzeitig Stellv Leiterin AEMP	QM hat keinen Stellvertreter
		Leitung der AEMP	Verantwortet die Organisation der AEMP	hat einen Stellvertreter
		Technischer Dienst	Verantwortlich für den technischen Zustand der AEMP-Ausstattung und der techn. Versorgung (Strom, Wasser, ...)	Bereitschaft - innerhalb 30 min vor Ort (5 Elektriker) / Prozeduren zur Fehlerbehebung vorhanden
		IT-Hardwarespezialisten	Verantwortlich für die IT Hardware Ausstattung der AEMP	Bereitschaft - innerhalb 60 min vor Ort (5 Hardware Spezialisten) / Dokumente & Beschreibungen sind vorhanden
		IT-Softwarespezialisten	Verantwortlich für die Schnittstellen zw. der anlagenspezifischen Software und der QM- / KIS-Software	Bereitschaft - innerhalb 60 min vor Ort (4 Software Spezialisten) / Dokumente & Beschreibungen sind vorhanden
	externe Partner	Ausfallkonzept mit 2 anderen Krankenhäusern	Falls Prozesse in der AEMP ausfallen und nicht umgehend behoben werden können	die 2 externen AEMP stehen an 2 verschiedenen Standorten unentgeltlich zur Verfügung - SLA vorhanden
		Externer Transportunternehmer	Transport der benutzten und sterilen MP in spezifischen Transportwagen zw. den Standorten	Ersatzfahrer / Ersatz-LKW
		Wartungsfirma RDG	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	keine Angaben über Reaktionszeit und mind. Einsatzzeit vor Ort
		Wartungsfirma Einschweißgerät	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	/
		Wartungsfirma Sterilisator	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	keine Angaben über Reaktionszeit und mind. Einsatzzeit vor Ort
		Wartungsfirma Versorgungsanlagen	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	/
		Wartungsfirma Sicherheitstechnische Anlagen	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	Wartungsvertrag mit 3h Vororteinsatz
		Wartungsfirma IT-Hardware (Netz, DB, Server, ...)	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	/
		Wartungsfirma IT-Software	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	Wartungsvertrag: Hotline (Mo-Fr 08:00-16:00)
		BHKW Betreiber	BHKW Eigentümer = Gemeinde; BHKW Betreiber = externe Firma	externe Firma mit Bereitschaftsdienst
	IT Software	Trinkwasserversorger	Trinkwasserversorgung durch die Gemeinde	Bereitschaftsdienst der Gemeinde
		Telekomversorger	Telekomnetzversorger für die Bereiche Telefonie und EDV Anbindung an das WWW	Bereitschaftsdienst des Telekomversorgers
		Qualitätsmanagement Software	13 Arbeitsplätze an den versch. Stationen in der AEMP	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank; Redundanz = Ausfallkonzept
		Krankenhausinformationssystem	3 Arbeitsstationen mit Zugriff auf das KIS	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank; Redundanz = Abstimmung OP
		klassische IT-Office Software	13 Arbeitsstationen mit Zugriff auf klassische IT Office Software	Software = Lokal gespeichert, Verbindung über Netzwerk zum Dateiserver
		anlagen spezifische Software	Software welche spezifisch für die Funktionsfähigkeit des Gerätes / der Anlage programmiert ist	RDG & Sterilisatoren=> Datenbank: VMServer = Master & lokaler PC = Slave / Plasmasterilisator => Datenbank: VMServer, Dateiserver
	Prozessgeräte	Verwaltung Leihsets	Hausinterne Software zur Verwaltung der Leihsets MP	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank
		Gebäudeleittechnik	Gäudeleittechnik ist eine Überwachungssoftware für alle technischen Versorgungsressourcen	Parameter sind in der Feldebene gespeichert; Redundante VM-Serverstruktur; nur Visualisierung
		Waschbecken für Vorreinigung	Waschbecken mit Handbrause, Trinkwasser / VE-Wasser	
		Ultraschallbecken	Ultraschalltischgerät	2 identische Ultraschallbecken
		Reinigungs- & Desinfektionsgeräte (RDG)	RDG zur automatisierten Reinigung, Desinfektion und Trocknung der MP	2/4 Geräten mit Elektrowärmeerzeuger; 2 Geräte mit AV- & 2 Geräte mit SV-Versorgung
		Packtische	höhenverstellbare Arbeitstische für die Sichtprüfung, man. Trocknung, Funktionsprüfung, Pflege und Verpackung	6 identische Packtische
		Sterilisatoren	Sterilisatoren für die Siebe mit MP, und die	2/3 Sterilisatoren mit Elektrodampferzeuger;1 Gerät mit AV- & 2 Geräte mit SV-Versorgung
		Einschweissgerät	Einschweißgerät für einzelne MP	2 Geräte
		unterstützende Geräte zur Funktionskontrolle	Kleingeräte für die Funktionskontrolle	keine Redundanz, Ausfallkonzept mit 2 anderen KH
		EDV Hardware (Desktop PC in der AEMP)	PC's inkl. Zubehör, Hands scanner an jedem Prozessschritt, Drucker strategisch verteilt	Redundanzen für lokale PC, der virtuellen Serverstruktur, die Storage sind vorhanden
		BHKW AV Stromversorgung	AV-Stromversorgung dient der normalen Versorgung aller System, Anbindung BHKW-KH erfolgt im BT Süd	BHKW: 3 MSpg-Einspeisungen; Redundanz mit 3 Gasmotoren; Einspeisung BHKW-HK im BT Süd
		AV Übergabe & Etagenverteiler BT 3.2 Et.-1	AV-Sammelschiene zur Verteilung an die Schachtverteiler und die Etagenverteiler im BT 3.2	Koppelschalter zur Verbindung der Sammelschienen SV-AV
		BHKW SV Stromversorgung	SV-Stromversorgung dient als Sicherheitsversorgung wenn AV ausfällt, Anbind. BHKW-KH erfolgt im BT Süd	Regelbetrieb durch AV-Versorgung; Netzausfall: 2 Dieselgeneratoren; Einspeisung BHKW-HK im BT Süd
		SV Übergabe & Etagenverteiler BT 3.2 Et.-1	SV-Sammelschiene zur Verteilung an die Schachtverteiler und die Etagenverteiler im BT 3.2	Koppelschalter zur Verbindung der Sammelschienen SV-AV
		Etagenverteiler BT 3.2 Technikzentrale 1B	Etagenverteiler zur Versorgung der Technikzentrale 1B	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Schachtverteiler BT 3.1 Et. -2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 3.1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m
		Etagenverteiler BT 3.1 Et. 1	EDV Etagenverteiler zur Versorgung BT 3.1 Etage 1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Etagenverteiler BT 3.1 Et. 2	Etagenverteiler zur Versorgung BT 3.1 Etage 1 & 2	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Etagenverteiler BT 3.1 Technikzentrale 1A	Etagenverteiler zur Versorgung der Technikzentrale 1A	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Schachtverteiler BT 2.0 Et.-2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 2.0	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m
		Etagenverteiler BT 2.0 Et.-1	Etagenverteiler zur Versorgung BT 2.0 Etage -1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Schachtverteiler BT 1.3 Et. -1	Schachtverteiler zur Versorgung der Etagenverteiler im BT 1.3	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m
		Etagenverteiler BT 1.3 Et. -1	Etagenverteiler zur Versorgung BT 2.0 Etage -1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage
		Schachtverteiler BT 1.1 Et. -2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 1.1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m
		Etagenverteiler BT 1.1 Et. -1	Etagenverteiler zur Versorgung BT 1.1 Etage -1	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage

▶▶ Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung		Beschreibung der Prozesse & Ressourcen	Beschreibung der Robustheit
Versorgung / techn. Anlagen	USV Stromversorgung Südtrakt Et. 2	AEMP nur mit USV versorgt	SV versorgt USV Anlage, Ausfall SV Versorgung => Übernahme durch USV bis SV wieder einspeist
	BHKW Hausdampfversorgung	Einspeisung Süd: AEMP und Reindampfproduktion Süd; Einspeisung Nord: Reindampfproduktion Nord	/
	Hausdampfübergabe Süd BT 3.2 Et.2	Hausdampfübergabe im BT 3.2 zur Versorgung der AEMP und der Reindampfversorgung Süd	keine Redundanz
	Reindampfversorgung Süd BT 3.2 Et. 2	Reindampf wird für die Desinfektion von MP und zur Befeuchtung in den Lüftungsanlagen benötigt	VE Wassereinspeisung aus BT Nord über eine nicht redundante Druckerhöhung; keine Redundanz
	BHKW Wärmeversorgung	Einsatz Wärme: Temperaturerhöhung in den Lüftungsanlagen	/
	Wärmeübergabe Süd BT 3.2 Et. -2	Einspeisung Wärmeversorgung BHKW-KH im im BT Süd für Lüftungsanlagen und Küche	keine Redundanz
	BHKW Kälteversorgung	Einsatz Kälte: Temperatursenkung in den Lüftungsanlagen; Deckenkonvektoren; Kühlung RDG's	/
	Kälteübergabe Süd BT 3.2 Et. -2	Einspeisung Kälteversorgung BHKW-KH im BT Süd	keine Redundanz
	Kälteübergabe Nord BT 1.1 Et. -1	Einspeisung Kälteversorgung BHKW-KH im BT Nord	keine Redundanz
	Lüftungsanlage 17A Südtrakt Et. 2	separate Lüftungsanlage für die gesamte AEMP - Reinraumklasse 1 / 2	Redundante Zu- & Ab-Luft für insgesamt 10 verschiedene Lüftungsanalge im Bauteil Süd; Anlage 17A nicht redundant ausgelegt
	Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	med. Druckluft wird für die man. Trocknung und die Funktionsprüfung versch. MP benötigt	2 redundante Druckluftherzeuger im Bauteil Nord
	Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1	Druckluftproduktion und -Versorgung im KH, Druckluft wird für die Automatismen der Sterilisatoren benötigt	2 redundante Druckluftherzeuger im Bauteil Nord
	Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2	Trinkwasser wird durch den Wasserversorger eingespeist, TW wird für die Herstellung von VE Wasser benötigt	1 TW Einspeisung ins KH ohne Redundanz im Bauteil Nord
	TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1	UV-Behandlung und Chlorierung zur Reinigung des Trinkwassers	keine Redundanz
	TR-W Enthärtung BT 1.1 Et. -1	Wasserenthärtungsanlage	3 parallel funktionierende Enthärtungsanlagen
	Osmoseanlage BT 1.1 Et. -1	Herstellung von VE Wasser	keine Redundanz
	Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1	Druckerhöhung VE Wasser für die Prozessschritten Vorreinigung, maschinelle Reinigung und Sterilisation	2 parallel funktionierende Pumpen
	Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2	Druckerhöhung zur Einspeisung der Reindampfversorgung im BT 3.2 Et. 2	keine Redundanz
	Abwasserhebeanlage BT 2.0 Et. -2	Abwasserleitungen ins UG 2 und von dort mit einer Abwasserhebeanlage ins öffentliche Abwassernetz	2 Abwasserhebeanlagen
	Aufzüge A4-A6 BT 2.0	3 Bettenlifte, Transport vun MP & Endoskopen vom EG <=> OG	2 verschiedenen Maschinenenräumen
	Aufzug A7 BT 3.1	1 Bettenlift, Transport von MP & Endoskopen vom EG <=> OG;	Redundanz zu A8
	Versorgung durch Telekomanbieter BT 2.0 Et. -1	Anbindung an das öffentliche Telekommunikationsnetz und Verdinung ins Internet	2 getrennte Kabelwege in das Hauptgebäude
	EDV-Netzwerk redundant	internes LWL Netzwerk vom Netzanachluss über die beiden Serverräume zu den Etagenverteiler	komplett redundant verkabelte Netzwerkstruktur (CoreSwitch, Glasfaserverkabelung, Etagenswitch...)
	EDV-Netzwerk nicht redundant	Verbindung vom Etagenverteiler zu den perioheren Switches, PC's und Grossgeräte	keine Redundanz; einfache Single-Verkabelung
	Serverraum Nord BT 1.3. Et. -1	Serverraum mit Core-Switch; Datenspeicherung und Serverlandschaft	Redundanz zum Serverraum Nord
	Serverraum Süd BT 3.2 Et. -1	Serverraum mit Core-Switch; Datenspeicherung und Serverlandschaft	Redundanz zum Serverraum Süd
	Schwachstromsicherheitsanlagen BT 2.0 Et. -1	Technikraum mit allen Schwachstromsicherheitsanlagen: GMS, BMA, ZUKO, CCTV, Telekom,	
	Telekomanlage BT 2.0 Et. -1	Telekommunikationsanlage für Festnetzanschlüsse und DECT telefonie, Verkabelung über EDV-Netz	Anlage ist nicht redundant, komplett redundant verkabelte Netzwerkstruktur (CoreSwitch, Glasfaserverkabelung, Etagenswitch...)
	elektr. Zutrittskontrolle BT 2.0 Et. -1	Zutrittskontrolle für die verschiedenen Eingänge der AEMP	Eigenständige Anlage an SV-Versorgung angeschlossen

14.7 BIA-Matrix – Schadensklassen

Auf den folgenden 2 Seiten sind die Schadensklassen aufgelistet.

▶▶ Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung		Schadensklassen				
		Operate	Legal	Finance	Image	
		Die Schadensklasse "Operate" beschreibt die Beeinträchtigung der Aufgabenerfüllung, Ziele können nicht erreicht werden.	Die Schadensklasse "Legal" beschreibt den Verstoss gegen Gesetze, Vorschriften und Verträge.	Die Schadensklasse "Finance" beschreibt die finanziellen Auswirkungen, wie z.B. Verluste, Bussgelder, Strafen.	Die Schadensklasse "Image" beschreibt die negativen Innen- und Aussenwirkungen (Imageschaden).	
		=> Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	=> Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	=> Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	=> Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	
kritische Prozessschritte		1 Transport gebrauchte Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
		2 Vorreinigung & Vorbereitung MP	Signifikant	Managebar	Managebar	Managebar
		3 maschinelle Reinigung & Desinfektion MP	Signifikant	Managebar	Managebar	Managebar
		4 Sichtprüfung & manuelle Trocknung MP	Signifikant	Managebar	Managebar	Managebar
		5 Freigabe nach Prüfung Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
		6 Funktionskontrolle & Pflege MP	Signifikant	Managebar	Managebar	Managebar
		7 Verpackung Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
		8 Sterilisation Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
		9 Freigabe nach Sterilisation MP	Signifikant	Managebar	Managebar	Managebar
		10 Transport sterile Medizinprodukte	Signifikant	Managebar	Managebar	Managebar
& Externe kritische Ressourcen	internes Personal (Rollen)	Logistiker	Managebar	Managebar	Managebar	Managebar
		Fachkundige in der Aufbereitung von MP	Managebar	Managebar	Managebar	Managebar
		AEMP Stammdatenadministrator	Managebar	Managebar	Managebar	Managebar
		Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Managebar	Managebar	Managebar	Managebar
		Leitung der AEMP	Managebar	Managebar	Managebar	Managebar
		Technischer Dienst	Managebar	Managebar	Managebar	Managebar
		IT-Hardwarespezialisten	Managebar	Managebar	Managebar	Managebar
		IT-Softwarespezialisten	Managebar	Managebar	Managebar	Managebar
	externe Partner	Ausfallkonzept mit 2 anderen Krankenhäusern	Managebar	Managebar	Managebar	Managebar
		Externer Transportunternehmer	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma RDG	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma Einschweißgerät	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma Sterilisator	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma Versorgungsanlagen	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma Sicherheitstechnische Anlagen	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma IT-Hardware (Netz, DB, Server, ...)	Managebar	Managebar	Managebar	Managebar
		Wartungsfirma IT-Software	Managebar	Managebar	Managebar	Managebar
		BHKW Betreiber	Managebar	Managebar	Managebar	Managebar
		Trinkwasserversorger	Managebar	Managebar	Managebar	Managebar
		Telekomversorger	Managebar	Managebar	Managebar	Managebar
	IT Software	Qualitätsmanagement Software	Signifikant	Managebar	Managebar	Managebar
		Krankenhausinformationssystem	Signifikant	Managebar	Managebar	Managebar
		klassische IT-Office Software	Managebar	Managebar	Managebar	Managebar
		anlagen spezifische Software	Signifikant	Managebar	Managebar	Managebar
		Verwaltung Leihsets	Signifikant	Managebar	Managebar	Managebar
		Gebäudeleittechnik	Managebar	Managebar	Managebar	Managebar
	Prozessgeräte	Waschbecken für Vorreinigung	Managebar	Managebar	Managebar	Managebar
		Ultraschallbecken	Managebar	Managebar	Managebar	Managebar
		Reinigungs- & Desinfektionsgeräte (RDG)	Signifikant	Managebar	Managebar	Managebar
		Packtische	Signifikant	Managebar	Managebar	Managebar
		Sterilisatoren	Signifikant	Managebar	Managebar	Managebar
		Einschweissgerät	Signifikant	Managebar	Managebar	Managebar
		unterstützende Geräte zur Funktionskontrolle	Signifikant	Managebar	Managebar	Managebar
		EDV Hardware (Desktop PC in der AEMP)	Signifikant	Managebar	Managebar	Managebar
		BHKW AV Stromversorgung	Signifikant	Managebar	Managebar	Managebar
		AV Übergabe & Etagenverteiler BT 3.2 Et.-1	Signifikant	Managebar	Managebar	Managebar
		BHKW SV Stromversorgung	Kritisch	Managebar	Managebar	Managebar
		SV Übergabe & Etagenverteiler BT 3.2 Et.-1	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 3.2 Technikzentrale 1B	Kritisch	Managebar	Managebar	Managebar
		Schachtverteiler BT 3.1 Et. -2	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 3.1 Et. 1	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 3.1 Et. 2	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 3.1 Technikzentrale 1A	Kritisch	Managebar	Managebar	Managebar
		Schachtverteiler BT 2.0 Et.-2	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 2.0 Et.-1	Kritisch	Managebar	Managebar	Managebar

▶▶ Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼ ▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Schadensklassen			
			Operate Die Schadensklasse "Operate" beschreibt die Beeinträchtigung der Aufgabenerfüllung, Ziele können nicht erreicht werden. => Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Legal Die Schadensklasse "Legal" beschreibt den Verstoß gegen Gesetze, Vorschriften und Verträge. => Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Finance Die Schadensklasse "Finance" beschreibt die finanziellen Auswirkungen, wie z.B. Verluste, Bussgelder, Strafen. => Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch	Image Die Schadensklasse "Image" beschreibt die negativen Innen- und Aussenwirkungen (Imageschaden). => Dropdown Auswahl: * Managebar = Gering * Signifikant = Mittel * Kritisch = Hoch
Interne	Versorgung / techn. Anlagen	Schachtverteiler BT 1.3 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 1.3 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Schachtverteiler BT 1.1 Et. -2	Kritisch	Managebar	Managebar	Managebar
		Etagenverteiler BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		USV Stromversorgung Südtrakt Et. 2	Kritisch	Managebar	Managebar	Managebar
		BHKW Hausdampfversorgung	Kritisch	Managebar	Managebar	Managebar
		Hausdampfübergabe Süd BT 3.2 Et.2	Kritisch	Managebar	Managebar	Managebar
		Reindampfversorgung Süd BT 3.2 Et. 2	Kritisch	Managebar	Managebar	Managebar
		BHKW Wärmeversorgung	Signifikant	Managebar	Managebar	Managebar
		Wärmeübergabe Süd BT 3.2 Et. -2	Signifikant	Managebar	Managebar	Managebar
		BHKW Kälteversorgung	Kritisch	Managebar	Managebar	Managebar
		Kälteübergabe Süd BT 3.2 Et. -2	Kritisch	Managebar	Managebar	Managebar
		Kälteübergabe Nord BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Lüftungsanlage 17A Südtrakt Et. 2	Kritisch	Managebar	Managebar	Managebar
		Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2	Kritisch	Managebar	Managebar	Managebar
		TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		TR-W Enthärtung BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Osmoseanlage BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1	Kritisch	Managebar	Managebar	Managebar
		Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2	Kritisch	Managebar	Managebar	Managebar
		Abwasserhebeanlage BT 2.0 Et. -2	Kritisch	Managebar	Managebar	Managebar
		Aufzüge A4-A6 BT 2.0	Signifikant	Managebar	Managebar	Managebar
		Aufzug A7 BT 3.1	Signifikant	Managebar	Managebar	Managebar
		Versorgung durch Telekomanbieter BT 2.0 Et. -1	Signifikant	Managebar	Managebar	Managebar
		EDV-Netzwerk redundant	Signifikant	Managebar	Managebar	Managebar
		EDV-Netzwerk nicht redundant	Signifikant	Managebar	Managebar	Managebar
		Serverraum Nord BT 1.3. Et. -1	Signifikant	Managebar	Managebar	Managebar
		Serverraum Süd BT 3.2 Et. -1	Signifikant	Managebar	Managebar	Managebar
		Schwachstromsicherheitsanlagen BT 2.0 Et. -1	Signifikant	Managebar	Managebar	Managebar
		Telekomanlage BT 2.0 Et. -1	Signifikant	Managebar	Managebar	Managebar
		elektr. Zutrittskontrolle BT 2.0 Et. -1	Managebar	Managebar	Managebar	Managebar

14.8 BIA-Matrix – RPO, RTO, MTPD

Auf den folgenden 2 Seiten sind die BIA-Faktoren aufgelistet.

►► Liste der Prozesse & Ressourcen		Recovery Point Objective (RPO)	Recovery Time Objective (RTO)	Maximum tolerable Period of Disruption	
BUSINESS IMPACT ANALYSE (BIA)		RPO ist die Zeit, in der ein Datenverlust für die Wiederaufnahme des Prozesses oder der Dienstleistung hingenommen werden kann. Prinzipiell ist es die Zeit zwischen zwei Datenspeicherungen.	RTO ist die Wiederherstellungszeit, die benötigt wird um nach einem Ereignis den Prozess oder die Dienstleistung wieder Schrittweise aufzunehmen.	MTPD ist die maximal tolerierbare Unterbrechungsdauer bevor negative Auswirkungen auf die nachfolgenden Prozesse oder Dienstleistungen entstehen.	
MATRIX		=> zum besseren Verständnis, siehe Grafik im Blatt Allgemeine Informationen "Definition RTO, RPO, MTPD"	=> zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD"	=> zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD"	
Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen		=>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	=>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	=>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	
kritische Prozessschritte		1 Transport gebrauchte Medizinprodukte	30 Minuten	24 Stunden	
		2 Vorreinigung & Vorbereitung MP	30 Minuten	24 Stunden	
		3 maschinelle Reinigung & Desinfektion MP	1 Stunden	24 Stunden	
		4 Sichtprüfung & manuelle Trocknung MP	30 Minuten	24 Stunden	
		5 Freigabe nach Prüfung Medizinprodukte	30 Minuten	24 Stunden	
		6 Funktionskontrolle & Pflege MP	30 Minuten	24 Stunden	
		7 Verpackung Medizinprodukte	30 Minuten	24 Stunden	
		8 Sterilisation Medizinprodukte	2 Stunden	24 Stunden	
		9 Freigabe nach Sterilisation MP	30 Minuten	24 Stunden	
		10 Transport sterile Medizinprodukte	30 Minuten	24 Stunden	
Interne & Externe kritische Ressourcen	internes Personal (Rollen)	Logistiker	---	2 Stunden	4 Stunden
		Fachkundige in der Aufbereitung von MP	---	2 Stunden	4 Stunden
		AEMP Stammdatenadministrator	---	24 Stunden	3 Tage
		Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	---	3 Tage	7 Tage
		Leitung der AEMP	---	3 Tage	7 Tage
		Technischer Dienst	---	30 Minuten	1 Stunden
		IT-Hardwarespezialisten	---	1 Stunden	2 Stunden
		IT-Softwarespezialisten	---	1 Stunden	2 Stunden
	externe Partner	Ausfallkonzept mit 2 anderen Krankenhäusern		3 Tage	7 Tage
		Externer Transportunternehmer	---	3 Tage	7 Tage
		Wartungsfirma RDG	---	3 Tage	7 Tage
		Wartungsfirma Einschweißgerät	---	3 Tage	7 Tage
		Wartungsfirma Sterilisator	---	3 Tage	7 Tage
		Wartungsfirma Versorgungsanlagen	---	3 Tage	7 Tage
		Wartungsfirma Sicherheitstechnische Anlagen	---	3 Tage	7 Tage
		Wartungsfirma IT-Hardware (Netz, DB, Server, ...)	---	3 Tage	7 Tage
		Wartungsfirma IT-Software	---	3 Tage	7 Tage
		BHKW Betreiber		1 Stunden	4 Stunden
		Trinkwasserversorger		1 Stunden	4 Stunden
		Telekomversorger		1 Stunden	4 Stunden
	IT Software	Qualitätsmanagement Software	30 Minuten	30 Minuten	24 Stunden
		Krankenhausinformationssystem	30 Minuten	24 Stunden	3 Tage
		klassische IT-Office Software	---	24 Stunden	3 Tage
		anlagen spezifische Software	30 Minuten	24 Stunden	3 Tage
		Verwaltung Leihsets	30 Minuten	24 Stunden	3 Tage
		Gebäudeleittechnik	---	24 Stunden	3 Tage
	Prozessgeräte	Waschbecken für Vorreinigung	---	1 Stunden	8 Stunden
		Ultraschallbecken	---	1 Stunden	8 Stunden
		Reinigungs- & Desinfektionsgeräte (RDG)	1 Stunden	1 Stunden	2 Stunden
		Packtische	---	1 Stunden	8 Stunden
		Sterilisatoren	2 Stunden	1 Stunden	2 Stunden
		Einschweissgerät	---	1 Stunden	2 Stunden
		unterstützende Geräte zur Funktionskontrolle	---	1 Stunden	4 Stunden
		EDV Hardware (Desktop PC in der AEMP)	---	1 Stunden	4 Stunden
	versorgung / techn. Anlagen	BHKW AV Stromversorgung	---	1 Stunden	4 Stunden
		AV Übergabe & Etagenverteiler BT 3.2 Et.-1		1 Stunden	4 Stunden
		BHKW SV Stromversorgung	---	1 Stunden	4 Stunden
		SV Übergabe & Etagenverteiler BT 3.2 Et.-1		1 Stunden	4 Stunden
		Etagenverteiler BT 3.2 Technikzentrale 1B		1 Stunden	4 Stunden
		Schachtverteiler BT 3.1 Et. -2		1 Stunden	4 Stunden
		Etagenverteiler BT 3.1 Et. 1		1 Stunden	4 Stunden
		Etagenverteiler BT 3.1 Et. 2		1 Stunden	4 Stunden
		Etagenverteiler BT 3.1 Technikzentrale 1A		1 Stunden	4 Stunden
		Schachtverteiler BT 2.0 Et.-2		1 Stunden	4 Stunden
		Etagenverteiler BT 2.0 Et.-1		1 Stunden	4 Stunden
		Schachtverteiler BT 1.3 Et. -1		1 Stunden	4 Stunden
		Etagenverteiler BT 1.3 Et. -1		1 Stunden	4 Stunden
		Schachtverteiler BT 1.1 Et. -2		1 Stunden	4 Stunden
		Etagenverteiler BT 1.1 Et. -1		1 Stunden	4 Stunden
		USV Stromversorgung Südtrakt Et. 2	---	1 Stunden	4 Stunden
		BHKW Hausdampfversorgung	---	1 Stunden	4 Stunden
		Hausdampfübergabe Süd BT 3.2 Et.2		1 Stunden	4 Stunden
		Reindampfversorgung Süd BT 3.2 Et. 2	---	1 Stunden	4 Stunden
		BHKW Wärmeversorgung	---	1 Stunden	8 Stunden
		Wärmeübergabe Süd BT 3.2 Et. -2		1 Stunden	8 Stunden
		BHKW Kälteversorgung	---	1 Stunden	4 Stunden
		Kälteübergabe Süd BT 3.2 Et. -2		1 Stunden	4 Stunden
		Kälteübergabe Nord BT 1.1 Et. -1	---	1 Stunden	4 Stunden
		Lüftungsanlage 17A Südtrakt Et. 2	---	1 Stunden	4 Stunden
		Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	---	1 Stunden	4 Stunden
		Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1	---	1 Stunden	4 Stunden
		Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2	---	1 Stunden	4 Stunden

▶▶ Liste der Prozesse & Ressourcen BUSINESS IMPACT ANALYSE (BIA) MATRIX Abhängigkeiten, Beschreibungen und Beziehungen zw. Prozessen und Ressourcen ▼▼ Prozesse und Ressourcen sind abhängig von der horizontalen Auflistung			Recovery Point Objective (RPO) RPO ist die Zeit, in der ein Datenverlust für die Wiederaufnahme des Prozesses oder der Dienstleistung hingenommen werden kann. Prinzipiell ist es die Zeit zwischen zwei Datenspeicherungen. => zum besseren Verständnis, siehe Grafik im Blatt Allgemeine Informationen "Definition RTO, RPO, MTPD" =>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	Recovery Time Objective (RTO) RTO ist die Wiederherstellungszeit, die benötigt wird um nach einem Ereignis den Prozess oder die Dienstleistung wieder Schrittweise aufzunehmen. => zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD" =>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage	Maximum tolerable Period of Disruption MTPD ist die maximal tolerierbare Unterbrechungsdauer bevor negative Auswirkungen auf die nachfolgenden Prozesse oder Dienstleistungen entstehen. => zum besseren Verständnis, siehe Grafik Deckblatt "Definition RTO, RPO, MTPD" =>Dropdown Auswahl: 10 Min, 30 Min, 1 h, 2h, 4h, 8h, 12h, 24h, 3 Tage, 7 Tage
>		TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1		1 Stunden	4 Stunden
		TR-W Enthärtung BT 1.1 Et. -1		1 Stunden	4 Stunden
		Osmoseanlage BT 1.1 Et. -1		1 Stunden	4 Stunden
		Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1	---	1 Stunden	4 Stunden
		Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2		1 Stunden	4 Stunden
		Abwasserhebeanlage BT 2.0 Et. -2	---	1 Stunden	4 Stunden
		Aufzüge A4-A6 BT 2.0		1 Stunden	4 Stunden
		Aufzug A7 BT 3.1		1 Stunden	4 Stunden
		Versorgung durch Telekomanbieter BT 2.0 Et. -1		1 Stunden	4 Stunden
		EDV-Netzwerk redundant		1 Stunden	4 Stunden
		EDV-Netzwerk nicht redundant	---	1 Stunden	4 Stunden
		Serverraum Nord BT 1.3. Et. -1		1 Stunden	4 Stunden
		Serverraum Süd BT 3.2 Et. -1		1 Stunden	4 Stunden
		Schwachstromsicherheitsanlagen BT 2.0 Et. -1		1 Stunden	4 Stunden
		Telekomanlage BT 2.0 Et. -1		1 Stunden	4 Stunden
		elektr. Zutrittskontrolle BT 2.0 Et. -1	---	1 Stunden	8 Stunden

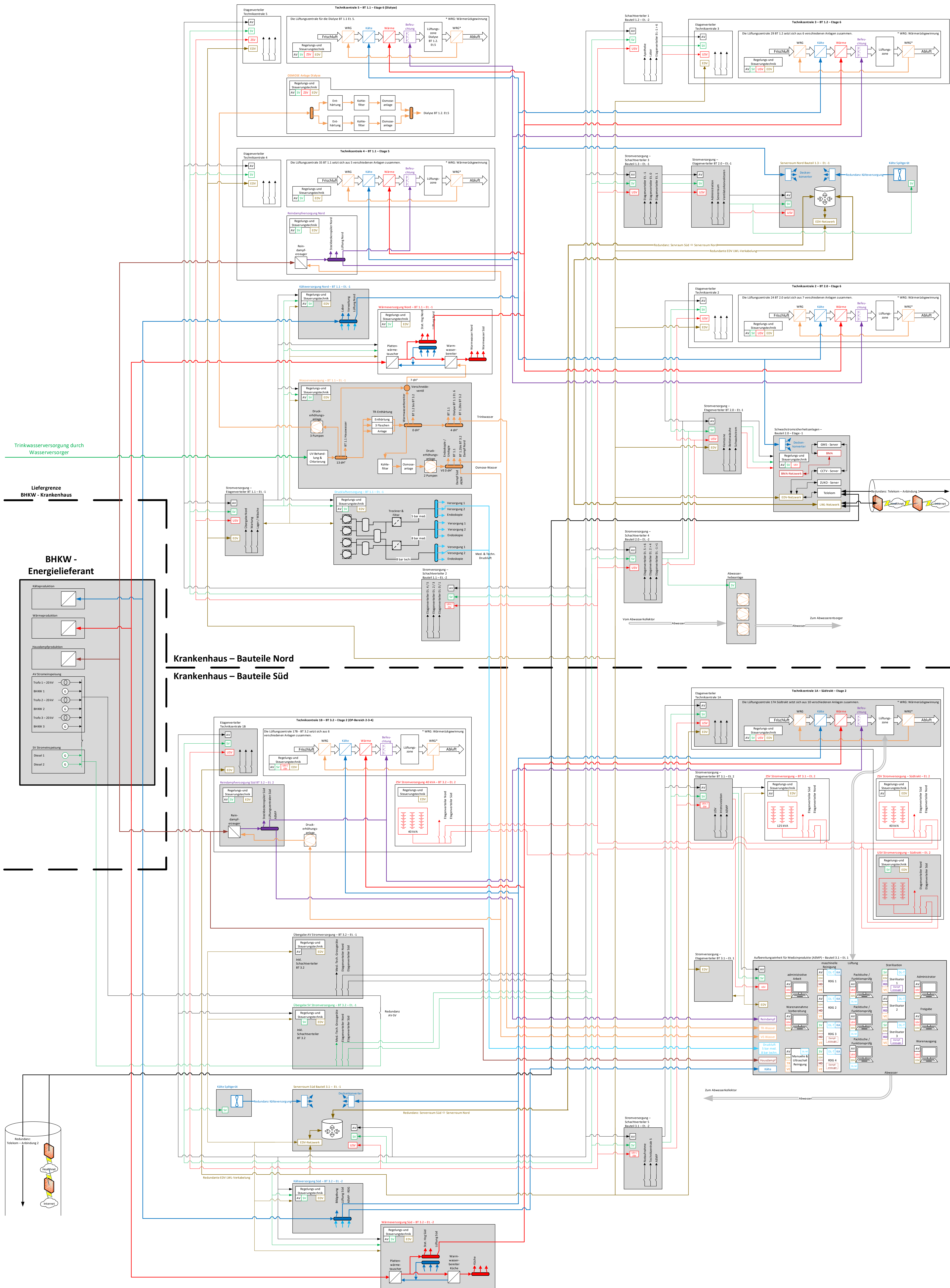
14.9 Relationales Datenmodell der Versorgungssystem im fiktiven Krankenhaus

Auf der folgenden Seite ist das relationale Datenbankmodell dargestellt.

Zur Visualisierung und besseren Übersicht wird angeraten das relationale Datenmodell mindestens in DIN A1 Format auszudrucken.

Relationales Datenmodell der technischen Versorgung in einem fiktiven Krankenhaus
Darstellung der Abhängigkeiten am Bsp. der Aufbereitungseinheit für Medizinprodukte

Version 5 - Erstellt durch C. Frauenberg – 24.05.2021



14.10 Parametrierung bcIMPACT

Nachfolgend wird das Werkzeug bcIMPACT mittels eigener erstellten Bildschirmabbildungen dargestellt. Die Reihenfolge der Abbildungen beschreibt ebenfalls die Vorgehensweise zur Parametrierung der Software und zur Eingabe der Daten für die Business Impact Analyse. (siehe BC-CONSULTING 2020)

Im Startfenster (Abbildung 53) sind 4 Silos, die für die angewandte Business Impact Analyse genutzt wurden. Das Silo „Interview“ ist in der Ausarbeitung und wird später in der Software zur Verfügung stehen. Die Datenbeschaffung kann aus diesem Grund noch nicht im Werkzeug dokumentiert werden.

Einstellungen	Ressourcen	Prozesse	Interviews	Bericht BIA
Prozesstypen	Organisationen	Liste	Liste	Dashboard
Prozesskritikalitäten	Rollen	Hierarchie	Anlegen	Kritische Prozesse
Prozessfelder	Standorte	Anlegen		Kritische Ressourcen
Prozesskritikalitätskategorien	Personen			Bericht BIA
	Partner			Bericht Prozesse
	Konfigurierbare Ressourcen			

Abbildung 53: Menüfenster bcIMPACT

- **Einstellungen**

Im Menü „Einstellungen“ wird die einmalige Basis-Parametrierung für die Business Impact Analyse vorgenommen.

- **Prozesstypen**

In der Maske „Prozesstypen“ werden die unterschiedlichen Prozessebenen gemäß der vorhandenen Prozesslandkarte parametriert.

Bezeichnung	Beschreibung	Verwendet
Prozesskategorie (Ebene 1)	Managementprozesse; Schlüsselprozesse; Supportprozesse	0
Hauptprozesse (Ebene 2)	Strategie, Personalwesen, Finanzwesen, IT, Infrastruktur, Programmierte stationäre Patientenversorgung, Nicht-Programmierte stationäre Patientenversorgung, Programmierte ambulante Patientenversorgung, Nicht-Programmierte ambulante Patientenversorgung, Prozesse mit einer direkten Verbindung zur Patientenversorgung, Prozesse mit einer direkten Verbindung zur Patientenversorgung	0
Teilprozess (Ebene 3)	Fachgebiete, Patientenversorgung (Terminvergabe, Voraufnahme, Aufnahme, Klinische Untersuchungen, Therapie, Pflege und Überwachung, Diagnose, Ausgang)	0
Fachaktivität (Ebene 4)	zentrale Fachaktivitäten in der Abteilung	0
Fachaktivität (Ebene 5)	detailliertere Fachaktivität in der Abteilung	0

Abbildung 54: bcIMPACT - Prozesstypen

- **Prozesskritikalitäten**

In der Maske „Prozesskritikalitäten“ werden die einzelnen Kritikalitäten festgelegt. Die Kategorie wird in der Maske „Prozesskritikalitätskategorien“ parametriert.

Bezeichnung	Sequenz	Beschreibung	Feld Typ	Kategorie
Finanz	1	Finanzielle Schäden (Ertragsentgang, Sachschäden, etc.)	Time range	Schadensklassen
Regular	2	Regulatorische Schäden (Nichtbeachtung von nationalem Recht, Aufsichtsrechtlichen Vorschriften, internen Vorschriften, etc.)	Time range	Schadensklassen
Image	3	• Image Schäden (Reputationsverlust, Negative Eigentümerreaktionen, etc.)	Time range	Schadensklassen
Operate	4	• Operational Schäden (Vertragsstrafen, Geldstrafen, Rückerstattungen, etc.)	Time range	Schadensklassen
RTO	5	Recovery Time Objective Wie lange darf ein Geschäftsprozess/System ausfallen? Bei der Recovery Time Objective handelt es sich um die Zeit, die vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse (Wiederherstellung von: Infrastruktur – Daten – Nacharbeitung von Daten – Wiederaufnahme der Aktivitäten) vergehen darf. Der Zeitraum kann hier von 0 Minuten (Systeme müssen sofort verfügbar sein), bis mehrere Tage (in Einzelfällen Wochen) betragen	Option	Verfügbarkeit
RPO	6	Recovery Point Objective Wie viel Datenverlust kann in Kauf genommen werden? Bei der Recovery Point Objective handelt es sich um den Zeitraum, der zwischen zwei Datensicherungen liegen darf, das heißt, wie viele Daten/Transaktionen dürfen zwischen der letzten Sicherung und dem Systemausfall höchstens verloren gehen. Wenn kein Datenverlust hinnehmbar ist, beträgt die RPO 0 Sekunden.	Option	Verfügbarkeit
MTPD	7	Die maximal tolerierbare Unterbrechungsdauer (MTPD) ist die maximal zulässige Zeit, in der wichtige Prozesse oder Dienstleistungen der Organisation nicht verfügbar sind oder nicht geliefert werden können, bevor die Auswirkungen als inakzeptabel eingestuft werden.	Option	Verfügbarkeit
Integrität	8	Datenintegrität Der Begriff Datenintegrität bezieht sich auf die Korrektheit, Vollständigkeit und Konsistenz von Daten. Auch die Sicherheit von Daten mit Blick auf regulatorische Anforderungen, wie z. B. die Datenschutz fallen unter diesen Begriff. Um Datenintegrität zu gewährleisten, werden in der Designphase verschiedene Prozesse, Regeln und Standards implementiert. Ist die Integrität der Daten so erst einmal sichergestellt, bleiben die in einer Datenbank gespeicherten Informationen dauerhaft korrekt, vollständig und vertrauenswürdig, ganz gleich, wie oft auf sie zugegriffen wird. Zudem sorgt Datenintegrität dafür, dass Ihre Daten vor externen Einflüssen geschützt sind.	Option	Informationssicherheit
Vertraulichkeit	9	Die im Prozess verwendeten Daten sind vertraulich	Option	Informationssicherheit

Abbildung 55: bcImpact – Prozesskritikalitäten

- Schadensklassen

Für die Kategorie „Schadensklassen“ wurden folgende Zeitbereiche und Werte eingetragen:

Wert	Anzeigenname	Priorität	Sequenz	Beschreibung
1	5min	1	1	5 Minuten
1	1h	1	2	1 Stunde
4	4h	1	3	4 Stunden
24	1d	1	4	1 Tag
72	3d	1	5	3 Tage
168	1w	1	6	1 Woche
720	1m	1	7	1 Monat

Abbildung 56: bcIMPACT – Prozesskritikalität Schadensklasse-Zeitbereiche

Wert	Anzeigenname	Priorität	Sequenz	RtoPriority	Farbe	Beschreibung
1	Kritisch	1	1	-	Beispieltext	Kritisch
2	Signifikant	1	2	-	Beispieltext	Signifikant
0	Managebar	1	3	-	Beispieltext	Managebar

Abbildung 57: bcIMPACT – Prozesskritikalitäten Schadensklasse-Werte

- Verfügbarkeit

Für die Kategorie „Verfügbarkeit“ wurden folgende Zeitbereiche und Werte parametrisiert:

Wert	Anzeigename	Priorität	Sequenz	RtoPriority	Farbe	Beschreibung
1	5 Minuten	1	1	-	Beispieltext	5 Minuten
2	30 Minuten	1	2	-	Beispieltext	30 Minuten
3	1 Stunde	1	3	-	Beispieltext	1 Stunde
4	2 Stunden	1	4	-	Beispieltext	2 Stunden
5	4 Stunden	1	5	-	Beispieltext	4 Stunden
8	8 Stunden	0	6	-	Beispieltext	8 Stunden
24	24 Stunden	1	7	-	Beispieltext	24 Stunden
72	3 Tage	1	8	-	Beispieltext	3 Tage
168	7 Tage	1	9	-	Beispieltext	7 Tage

Abbildung 58: bcIMPACT – Prozesskritikalität Verfügbarkeit-Zeitbereiche

Wert	Anzeigename	Priorität	Sequenz	RtoPriority	Farbe	Beschreibung
1	Kritisch	1	1	-	Beispieltext	die eingesetzten Daten müssen kritisch beurteilt werden
2	Managebar	1	2	-	Beispieltext	die eingesetzten Daten sind managebar
3	Korrekt	1	3	-	Beispieltext	die eingesetzten Daten sind korrekt und auf den Prozess abgestimmt

Abbildung 59: bcIMPACT – Prozesskritikalität Verfügbarkeit-Werte

○ Prozessfelder

Hier können zusätzliche Prozessfelder frei definiert werden. Die nachfolgenden Felder wurden eingefügt, um die Prozesse besser beschreiben zu können. Dies hinsichtlich der Robustheit, ob die Prozesse outgesourced und der Prozess bereits analysiert wurde.

Bezeichnung	Reihenfolge	Beschreibung
Robustheit	1	Beschreibung der Robustheit des Prozesses
Outsourced	2	Dieser Prozess wird durch einen Partner durchgeführt (outsourced)
Prozess analysiert	3	Die Analyse wurde noch nicht abgeschlossen.

Abbildung 60: bcIMPACT - zusätzliche Prozessfelder

○ Prozesskritikalitätskategorien

Die Prozesskritikalitätskategorien, die in der Beschreibung der Prozesskritikalitäten benutzt werden, können hier frei definiert werden.

	Bezeichnung	Sequenz ↑	Priorität	Beschreibung
		↑ ↓	↑ ↓	↓
Bearbeiten	Schadensklassen	1	1	Zeitleiste der Schadensklassen
Bearbeiten	Verfügbarkeit	2	1	RTO, RPO, MTPD
Bearbeiten	Informationssicherheit	3	1	CIA

Abbildung 61: bcIMPACT - Prozesskritikalitätskategorien

- Ressourcen

Im Menü „Ressourcen“ wurden die einzelnen Ressourcen, die in Abhängigkeit zu den Prozessen stehen, hierarchisch-organisatorisch eingepflegt und beschrieben.

- Organisationen

In der Maske „Organisationen“ wurde eine fiktive hierarchische Organisationsstruktur des Krankenhauses eingestellt.

Bezeichnung
- Verwaltungsrat
- Geschäftsführung
- Medizinische Leitung
+ Stellvertretende Medizinische Leitung
- Pflegedienstleitung
- Stellvertretende Pflegedienstleitung
+ Medizintechnische Patientenversorgung
+ stationäre Patientenversorgung
Qualitätsmanagement
- Verwaltungsleitung
+ Abteilung Schutz & Prävention
Apotheke (Personal)
Datenschutzbeauftragter
Dienstleistungswesen (Hôtellerie)
+ Finanzwesen

Abbildung 62: bcIMPACT - Organisationen

- Rollen

In der Maske „Rollen“ wurden die wichtigsten fiktiven Rollen für die Funktionsfähigkeit der Aufbereitungseinheit für Medizinprodukte eingestellt, beschrieben und bewertet.

Bezeichnung	Beschreibung	Robustheit	Operate	Legal	Finanz	Image	RTO	MTPD
AEMP Stammdatenadministrator	Pflegen die Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope	2 Stammdatenadministratoren	Managebar	Managebar	Managebar	Managebar	24 Stunden	3 Tage
Fachkundige in der Aufbereitung von MP	Bearbeiten die Prozessschritte 1 (Wartungsaufnahme) & 2 bis 9	15 Personen in der AEMP in allen Bereichen einsetzbar	Managebar	Managebar	Managebar	Managebar	2 Stunden	8 Stunden
IT Hardwarespezialisten	Verantwortlich für die IT Hardware Ausstattung der AEMP	Bereitschaft: Innerhalb 60 min vor Ort (D: Hardware Spezialisten) / Dokumente & Beschreibungen sind vorhanden	Managebar	Managebar	Managebar	Managebar	1 Stunde	2 Stunden
IT Software spezialisten	Verantwortlich für die anlagenspezifischen Software und der QM- / KIS-Software	Bereitschaft: Innerhalb 60 min vor Ort (D: Software Spezialisten) / Dokumente & Beschreibungen sind vorhanden	Managebar	Managebar	Managebar	Managebar	1 Stunde	2 Stunden
Leitung der AEMP	Verantwortet die Organisation der AEMP	hat einen Stellvertreter	Managebar	Managebar	Managebar	Managebar	3 Tage	7 Tage
Logistiker	Bearbeitet die Prozessschritte 1 (interner Transport) innerhalb der beiden Standorte	mehrere intere Logistiker	Managebar	Managebar	Managebar	Managebar	2 Stunden	8 Stunden
Qualitätsmanager AEMP (Stellv. Leiter AEMP)	Verantwortet das Qualitätsmanagement exklusiv in der AEMP und ist gleichzeitig Stellv. Leiter AEMP	QM hat keinen Stellvertreter	Managebar	Managebar	Managebar	Managebar	3 Tage	7 Tage
Technischer Dienst	Verantwortlich für den technischen Zustand der AEMP- Ausstattung und der techn. Versorgung (Strom, Wasser,...)	Bereitschaft: Innerhalb 30 min vor Ort (D: Elektriker) / Prozeduren zur Fehlerbehebung vorhanden!	Managebar	Managebar	Managebar	Managebar	30 Minuten	1 Stunde

Abbildung 63: bcIMPACT - Rollen

* Bezeichnung

AEMP Stammdatenadministrator

Beschreibung

Pflegen die Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope

Robustheit

2 Stammdatenadministratoren

Operate

Managebar

Legal

Managebar

Finanz

Managebar

Image

Managebar

RTO

24 Stunden

MTPD

3 Tage

Abbildung 64: bcIMPACT – Rolle, Bsp.: AEMP Stammdatenadministrator

- Standorte

In der Maske „Standorte“ wurde eine fiktive hierarchische Struktur der Infrastruktur parametrier

Bezeichnung
- Hauptstandort
+ Bauteil 1.1
+ Bauteil 1.2
+ Bauteil 1.3
+ Bauteil 2.0
+ Bauteil 3.1
+ Bauteil 3.2
+ Bauteil 4.0
BHKW HS
Hubschrauberlandeplatz - Notarzt
+ Nebenstandort

Abbildung 65: bcIMPACT - Standorte

- Personen

Wegen der Analyse in einem fiktiven Krankenhaus, wurden in der Maske „Personen“ keine Einträge eingegeben. Falls Personen hier eingepflegt werden, können diese Personen den Rollen zugewiesen werden.

- Partner

In der Maske „Partner“ werden in diesem Fall die fiktiven externen Partner, welche zur Funktionsfähigkeit der Aufbereitungseinheit für Medizinprodukte benötigt werden, eingetragen und bewertet.

Bezeichnung	Beschreibung	Operate	Legal	Finanz	Image	RTO	MTPD
Ausfallkonzept mit 2 anderen Krankenhäusern	Falls Prozesse in der AEMP ausfallen und nicht umgehend behoben werden können	Managebar	Managebar	Managebar	Managebar	3 Tage	7 Tage
BHKW Betreiber	BHKW Eigentümer = Gemeinde, BHKW Betreiber = externe Firma	Managebar	Managebar	Managebar	Managebar	1 Stunde	4 Stunden
Externer Transportunternehmer	Transport der benutzten und sterilen MP in spezifischen Transportwagen zw. den Standorten	Managebar	Managebar	Managebar	Managebar	3 Tage	7 Tage
Telekomversorger	Telekomnetzversorger für die Bereiche Telefonie und EDV Anbindung an das WWW	Managebar	Managebar	Managebar	Managebar	1 Stunde	4 Stunden
Trinkwasserversorger	Trinkwasserversorgung durch die Gemeinde	Managebar	Managebar	Managebar	Managebar	1 Stunde	4 Stunden
Wartungsfirma Einschweisgerät	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	Managebar	Managebar	Managebar	Managebar	3 Tage	7 Tage

Abbildung 66: bcIMPACT - Partner

* Bezeichnung	Wartungsfirma RDG
Beschreibung	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung
Robustheit	keine Angaben über Reaktionszeit und mind. Einsatzzeit vor Ort
Operate	Managebar
Legal	Managebar
Finanz	Managebar
Image	Managebar
RTO	3 Tage
MTPD	7 Tage

Abbildung 67: bcIMPACT – Partner, Bsp.: Wartungsfirma RDG

- Konfigurierbare Ressourcen

In der Maske „konfigurierbare Ressourcen“ wurden zusätzliche Ressourcen zu den bereits Beschriebenen angelegt. Insbesondere IT-Software, Prozessgeräte sowie Versorgungs- und technische Anlage angelegt.

Ressourcen

Standard Ressourcen

Organisationen (93)

Rollen (8)

Standorte (204)

Personen

Partner (12)

Konfigurierbare Ressourcen

IT Software (6)

Prozessgeräte (8)

Sicherheitstechnik

Versorgung / techn. Anlagen (44)

Ressource hinzufügen

Ressourcenvorlage

Prozess - Ressourcenvorlage

Maßnahme - Ressourcenvorlage

Ressource - Ressourcenvorlage

Ressourcenvorlage hinzufügen

Bezeichnung	Beschreibung	Robustheit	Operate	Legal	Finanz	Image	RTO
Abwasserhebeanlage BT 2.0 Et. -2	Abwasserleitungen ins UG 2 und von dort mit einer Abwasserhebeanlage ins öffentliche Abwassernetz	1 od. 2 Abwasserhebeanlage (n) => Redundanz?	Kritisch	Managebar	Managebar	Managebar	1 Stunde
Aufzug A7 BT 3.1	1 Bettenlift, Transport von MP & Endoskopen vom EG => OG	Redundanz zu A8	Signifikant	Managebar	Managebar	Managebar	1 Stunde
Aufzüge A4-A6 BT 2.0	3 Bettenlifts, Transport von MP & Endoskopen vom EG => OG	2 verschiedenen Maschinenräumen	Signifikant	Managebar	Managebar	Managebar	1 Stunde
AV Übergabe & Etagenverteiler BT 3.2 Et.-1	AV-Sammelschiene zur Verteilung an die Schachtverteiler und die Etagenverteiler im BT 3.2	Koppelschalter zur Verbindung der Sammelschienen SV-AV	Signifikant	Managebar	Managebar	Managebar	1 Stunde

Abbildung 68: bcIMPACT - konfigurierbare Ressourcen

Speichern Abbrechen Löschen Ressourcenbeziehungen

Ressource bearbeiten

* Bezeichnung: Reinigungs- & Desinfektionsgeräte (RDG)

Beschreibung: RDG zur automatisierten Reinigung, Desinfektion und Trocknung der MP

Robustheit: 2/4 Geräten mit Elektrowärmeerzeuger, 2 Geräte mit AV- & 2 Geräte mit SV-Versorgung

Operate: Signifikant

Legal: Managebar

Finanz: Managebar

Image: Managebar

RPO: 1 Stunde

RTO: 1 Stunde

MTPD: 2 Stunden

Abbildung 69: bclIMPACT - konfigurierbare Ressourcen, Bsp.: Reinigungs & Desinfektionsgeräte (RDG)

- Ressourcenbeziehungen

In der Menüleiste zur Bearbeitung von Ressourcen, kann eine weitere Maske „Ressourcenbeziehungen“ geöffnet werden. In dieser Maske können dann die Abhängigkeiten zwischen den unterschiedlichen Ressourcen parametrisiert werden.

Ressourcenbeziehungen - Reinigungs- & Desinfektionsgeräte (RDG)

Zugewiesen	Bezeichnung
☒	anlagen spezifische Software
☐	Gebäudeleittechnik
☐	klassische IT Office Software
☐	Krankenhausinformationssystem
☒	Qualitätsmanagement Software
☐	Verwaltung Leihsets

Standard Ressourcen

- Rollen (2 / 8)
- Partner (1 / 12)

Konfigurierbare Ressourcen

- IT Software (2 / 6)**
- Versorgung / techn. Anlagen (7 / 44)

Abbildung 70: bclIMPACT – Ressourcenbeziehungen, Bsp.: Reinigungs- & Desinfektionsgeräte (RDG)

- Prozesse

Das Menü „Prozesse“ wird genutzt, um neue Prozesse anzulegen und um die bereits angelegten Prozesse in Listen hierarchisch geordnet darzustellen.

- Liste / Hierarchie

In den Masken „Liste“ werden die Prozesse in alphabetischer Reihenfolge oder in der Maske „Hierarchie“ die Prozesse gemäß den Prozessebenen entsprechend aufgelistet.

		Schadensklassen										Verfügbarkeit			Informationssicherheit			
Bezeichnung	Prozes...	Finanz		Regular		Image		Operate		RTD	RPO	MTPO	Integrität	Vertraulich...	KRITIK...	O...		
SuP 4.2.5 - Freigabe nach Prüfung Medizinpr...	Teilprozess (Ebene 3)	5min	1h	5min	1h	5min	1h	5min	1h	4h								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								
		4h	1d	4h	1d	4h	1d	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	1d	3d	1w	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	72 %		
		3d	1w	3d	1w	3d	1w	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								
SuP 4.2.6 - Funktionskontrolle & Pflege MP	Teilprozess (Ebene 3)	5min	1h	5min	1h	5min	1h	5min	1h	4h								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								
		4h	1d	4h	1d	4h	1d	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	1d	3d	1w	30 Minuten	30 Minuten	24 Stunden			72 %		
		3d	1w	3d	1w	3d	1w	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								
SuP 4.2.7 - Verpackung Medizinprodukte	Teilprozess (Ebene 3)	5min	1h	5min	1h	5min	1h	5min	1h	4h								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								
		4h	1d	4h	1d	4h	1d	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	1d	3d	1w	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	72 %		
		3d	1w	3d	1w	3d	1w	Signifikant	Signifikant	Signifikant								
		Managebar	Managebar	Managebar	Managebar	Managebar	Managebar	Signifikant	Signifikant	Signifikant								

Abbildung 71: bcIMPACT – Prozesshierarchie

○ Anlegen

Die Maske „Anlegen“ dient dazu neue Prozesse in die Prozesslandschaft zu integrieren und den Prozess, gemäß der Parametrierung in den Einstellungen, anzulegen und zu bewerten. Die Prozesslandkarte vom fiktiven Krankenhaus wurde als Grundlage für das Anlegen der Prozesse genutzt.

Abbildung 72: bclIMPACT - Prozess anlegen

- Prozessbeziehungen / Ressourcenbeziehungen

Nachdem ein Prozess angelegt ist, müssen die Beziehungen zu anderen Prozessen und Ressourcen gepflegt werden. Dadurch werden die Abhängigkeiten zwischen den Prozessen und den Ressourcen in die Abhängigkeitsmatrix eingetragen. Hierzu gibt es zwei Masken „Prozessbeziehungen“ und „Ressourcenbeziehungen“ in denen diese Abhängigkeiten eingetragen werden.

Abbildung 73: bclIMPACT - Menü Prozessabhängigkeiten

In der Maske „Prozessbeziehungen“ werden die Beziehungen zwischen der Prozesshierarchie gepflegt. Hier können übergeordnete und untergeordnete Prozesse eingetragen werden.

bcIMPACT / Prozesse / Prozess bearbeiten / Prozessbeziehungen ?

◀ Zurück

**Übergeordnete Prozesse für SuP 4.2 -
Aufbereitungseinheit für Medizinprodukte**

Bearbeiten

Bezeichnung
SuP - unterstützende Prozesse

**Untergeordnete Prozesse für SuP 4.2 -
Aufbereitungseinheit für Medizinprodukte**

Bearbeiten

Bezeichnung
SuP 4.2.1 - Transport gebrauchte Medizinprodukte
SuP 4.2.2 - Vorreinigung & Vorbereitung MP
SuP 4.2.3 - maschinelle Reinigung & Desinfektion MP
SuP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SuP 4.2.5 - Freigabe nach Prüfung Medizinprodukte
SuP 4.2.6 - Funktionskontrolle & Pflege MP
SuP 4.2.7 - Verpackung Medizinprodukte
SuP 4.2.8 - Sterilisation Medizinprodukte
SuP 4.2.9 - Freigabe nach Sterilisation MP
SuP 4.2.10 - Transport sterile Medizinprodukte

Abbildung 74: bcIMPACT – Prozessbeziehungen, Bsp.: Aufbereitungseinheit für Medizinprodukte

In der Maske „Ressourcenbeziehungen“ werden die Abhängigkeiten der Prozesse von den Ressourcen parametrisiert. Die Ressourcen wurden in der Maske „konfigurierbare Ressourcen“ eingepflegt. Dadurch, dass in der Maske „konfigurierbare Ressourcen“ die Ressourcenbeziehungen zwischen den einzelnen Ressourcen eingetragen wurden und an dieser Stelle die Abhängigkeiten der Prozesse von den Ressourcen eingetragen wurde, ist die Abhängigkeitsmatrix komplett in das informatische Werkzeug bcIMPACT eingetragen. Die Software ist in der Basis so programmiert, dass die Interdependenzen zwischen den Assets immer in beide Richtungen wirken.

Ressourcenbeziehungen - maschinelle Reinigung & Desinfektion MP

Ressource hinzufügen

- Standard Ressourcen
 - Rollen (1 / 8)
 - Partner (1 / 12)
- Konfigurierbare Ressourcen
 - IT Software (1 / 6)
 - Prozessgeräte (2 / 8)**
 - Versorgung / techn. Anlagen (2 / 44)

Zugewiesen	Bezeichnung	Verwendet
☐	EDV Hardware (Desktop PC in der AEMP)	
☐	Reinigungs- & Desinfektionsgeräte (RDG)	Ja

Abbildung 75: bcIMPACT – Ressourcenbeziehungen, Bsp: Prozess maschinelle Reinigung & Desinfektion MP

14.11 Parametrierung SAURON Propagation Engine

Nachfolgend wird die Parametrierung und Eingabe in die Propagation Engine anhand eigens erstellten Bildschirmausabbildungen beschrieben. Die Reihenfolge der Abbildungen beschreibt auch die Vorgehensweise zur Eingabe der Daten und der Parametrierung der Übergänge für die Simulation. Die Beschreibung basiert auf den Angaben in der Hilfe Kartei der SAURON Propagation Engine. (siehe WARUM M. et al. 2020)

- **Anlegen einer Simulationsdatei**

In der Maske „File“ können bereits erstellte Netzwerkdateien (Json-Datei) geladen werden oder die aktuelle Version gespeichert werden.

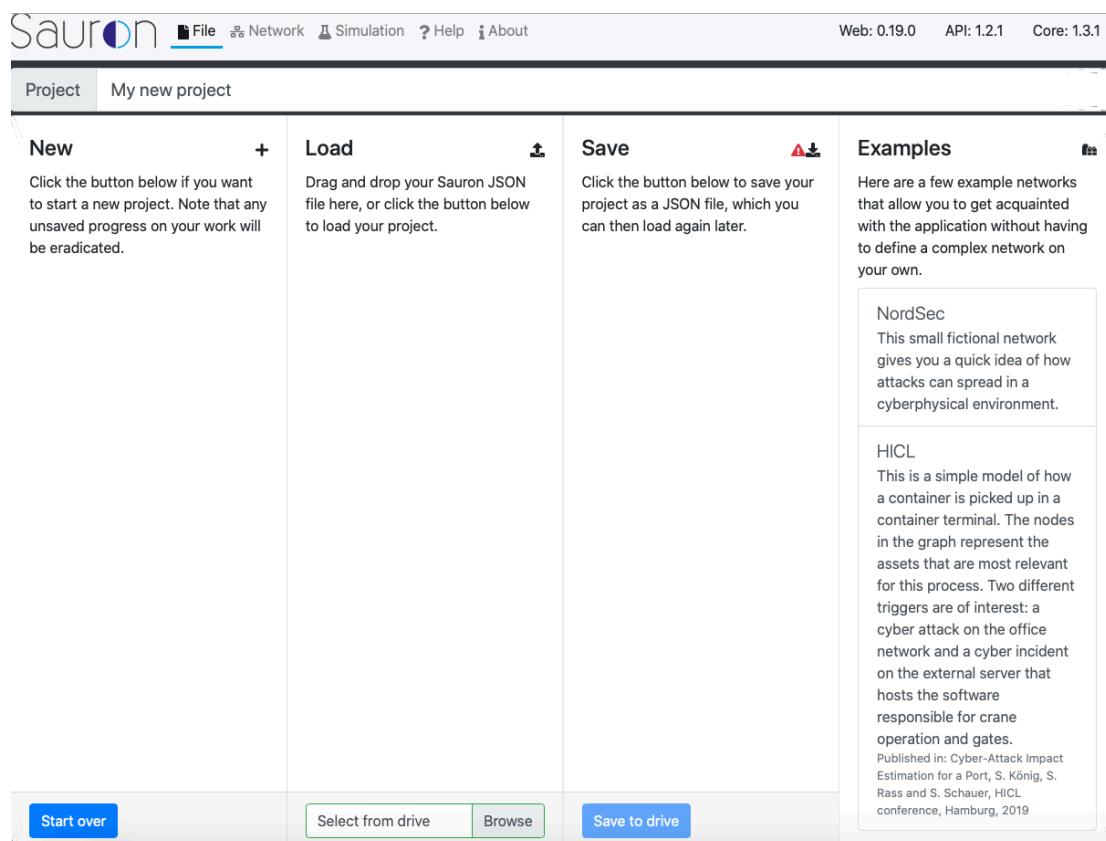


Abbildung 76: SAURON – Dateienverwaltung

- **Anlegen eines Netzwerkes**

In der Maske „Network“ wird das Netzwerk bestehend aus Prozessen und Ressourcen eingegeben und parametriert.

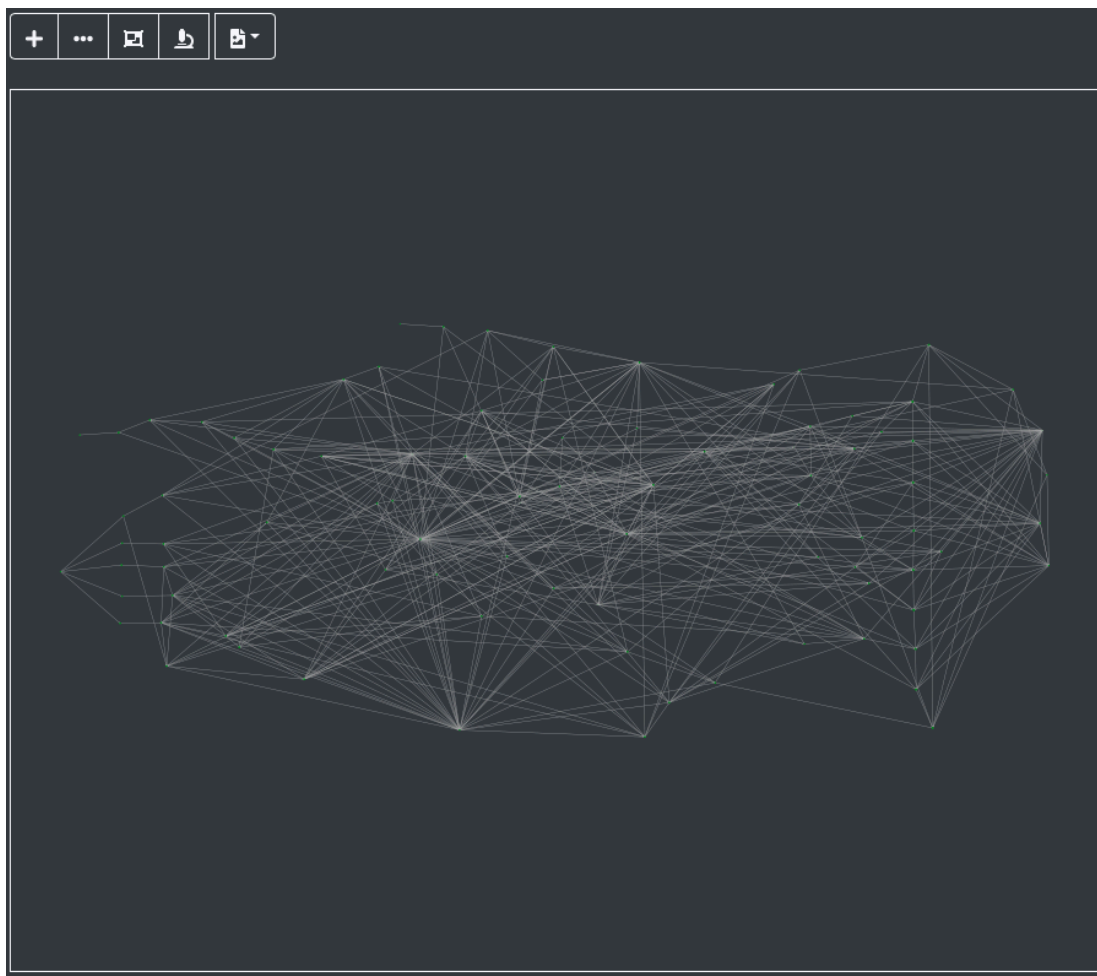


Abbildung 77: SAURON – Netzwerkeingabe, Bsp.: Netzwerk der Interdependenzen zur Aufbereitungseinheit von Medizinprodukten des fiktiven Krankenhauses

Die Netzwerkeingabe erfolgt über die nachfolgenden „Buttons“:

Tabelle 14: SAURON – Menüführung zur Netzwerkeingabe

	Einfügen eines einzelnen Netzwerkknotens
	Mehrfache Eingabe von Netzwerkknoten mit den Attributen für die gesamte Gruppe
	Automatische Positionierung der Netzwerkknoten
	Prüfung des Netzwerkes auf zyklische Abläufe innerhalb des Netzwerkes, um unendliche Schleifen oder sehr lange Prozesszeiten während der Simulation zu identifizieren
	Erzeugung einer SVG-Datei

Über die Mehrfacheingabe von Netzwerkknoten können Ressourcen und Prozesse einfach und schnell pro Gruppe importiert werden. Voraussetzung ist, dass im Vorfeld alle benötigten Daten in einer Textdatei oder Tabellen gesammelt wurden.

Add multiple nodes

Enter any and all nodes you wish to add at once. One per line. They will be randomly distributed.

Node names

Enter a list of nodes, one per line

Group

Existing:

(none)

New:

Enter group name

Copy style from

(none)

Copy properties from

(none)

Cancel

OK

Abbildung 78: SAURON - Mehrfacheingabe von neuen Netzwerkknoten

Sauron

File

Network

Simulation

Help

About

Web: 0.19.0

API: 1.2.1

Core: 1.3.1

+

...

🖨

🔍

📄

3 maschinelle Reinigung & Desinfektion MP

✓

select

Type in node names whole or partial. If the name exists the node is selectable. To select multiple nodes with a similar name, type only the letters they have in common.

i

🔥

👤

General information

Name

3 maschinelle Reinigung & Desinfektion MP

Group

AEMP - kritische Prozessschritte

new

Shape

star

apply to group

Description

Maschinelle Reinigung von Medizinprodukten

apply to group

🔥

🗑

Abbildung 79: SAURON – Netzwerkparametrierung

Die Parametrierung der Knoten erfolgt über die rechten Eingabefelder:

Tabelle 15: SAURON - Menüführung zur Parametrierung der Knoten

i	Allgemeinen Informationen
-	Knotenname

Universität Wien

OeRISK: Master-Thesis

163

- Knotengruppe
- Knotenform
- Beschreibung zum Knoten

Parametrierung der Übergänge

- Ausgangsstatus des Knotens
- Übergangsmatrix

Parametrierung der Interdependenzen

- Abhängigkeit vom aktuellen Knoten zum nächsten Knoten (Mehrfachauswahl möglich)

The screenshot shows a web-based configuration interface for a node in the SAURON system. The 'General information' tab is active. The node name is '3 maschinelle Reinigung & Desinfektion MP'. It is assigned to the group 'AEMP - kritische Prozessschritte'. The shape is set to 'star'. The description is 'Maschinelle Reinigung von Medizinprodukten'. There are buttons for 'new', 'apply to group', and a trash icon.

Abbildung 80: SAURON - Netzwerkknoten: Allgemeine Informationen

Die Knoten können drei verschiedene Zustände annehmen:

4. Der Knoten ist funktionsfähig und unberührt vom Vorfall.
5. Der Knoten ist in seiner Funktion beeinträchtigt, kann aber noch funktionieren.
6. Der Knoten fällt aus und ist nicht mehr funktionsfähig.

Je Knoten können mehrere Übergänge beschrieben werden. Der Standard-Ausgangswert ist 1. Die Eingabe der Übergänge erfolgt gemäß folgendem Schema:

Tabelle 16: SAURON - Parameter der Übergangsmatrix

Trigger	Auslöser für den Übergang von einem Zustand in den anderen Zustand.
From	Eingangszustand für den angegebenen Trigger. Wert zw. 1-3
Go To	Ausgangszustand für den angegebenen Trigger. Wert zw. 1-3
Output	Bei einer Zustandsänderung wird dieser Ausgang für den nächsten Knoten als Trigger genutzt.
%	Wahrscheinlichkeit mit derer die Zustandsänderung ausgelöst durch den Trigger erfolgt. Der Wert muss zwischen 0-100% gesetzt werden. Falls der gleiche Trigger mit dem gleichen Eingangszustand mehrfach angelegt wird, darf die Summe der

Wahrscheinlichkeit 100% nicht übersteigen. Ist die Summe der Wahrscheinlichkeit weniger als 100%, so besteht die Möglichkeit, dass ein Übergang zwischen Eingangszustand und Ausgangszustand zu Stande kommt.

State space of **3 maschinelle Reinigung & Desinfektion MP**

Initial state ✓ apply to group

Transition changes below are applied to all **7** other nodes in group **AEMP - kritische Prozessschritte !**

Trigger	From	Go To	Output	%
AV-SV Stromausfall	1	3	Ausfall AEMP	100%

eg. 'fire' ⓘ ✓ ✓ eg. 'fire' ⓘ % +

Abbildung 81: SAURON: Netzwerkknoten: Parametrierung der Übergänge

Die Abhängigkeit zwischen den Knoten wird vom Ausgangsknoten zum nächsten Knoten angegeben und ist unidirektional. Es können auch mehrere Knoten angewählt werden. Um eine bidirektionale Verknüpfung herzustellen, muss ebenfalls eine Abhängigkeit an dem zweiten Knoten eingestellt werden.

Connect **3 maschinelle Reinigung & Desinfektion MP** to...

Here is a list of all connected and disconnected nodes. To (connect to / disconnect from) another node, please click on the corresponding node.

1 Transport gebrauchte Medizinprodukte	✗
10 Transport sterile Medizinprodukte	✗
2 Vorreinigung & Vorbereitung MP	✗
4 Sichtprüfung & manuelle Trocknung MP	✓
5 Freigabe nach Prüfung Medizinprodukte	✗
6 Funktionskontrolle & Pflege MP	✗
7 Verpackung Medizinprodukte	✗
8 Sterilisation Medizinprodukte	✗
9 Freigabe nach Sterilisation MP	✗

Abbildung 82: SAURON - Netzwerkknoten: Parametrierung der Interdependenzen

- **Simulation des Netzwerkes**

Für die Simulation wird auf die zuvor eingestellten Knoten und Auslöser zurückgegriffen. An dieser Stelle wird das gewünschte Szenario mit der Beeinträchtigung oder dem Ausfall von Knoten (Alert source) eingestellt. Es können mehrere Knoten für den Start der Simulation ausgewählt werden. Auch können zu den unterschiedlichen Knoten, unterschiedliche Auslöser (Trigger) ausgewählt werden, sofern sie parametrisiert wurden. Sind alle Knoten und Auslöser ausgewählt und dem

Szenario hinzugefügt muss nur noch die Anzahl der Simulationszyklen festgelegt werden. Je mehr Zyklen durchlaufen werden, um so präziser wird das Ergebnis. Hier hat sich eine Zahl zwischen 100 und 1.000 Simulationszyklen bewährt. Anschließend kann die Simulation gestartet werden.

Step 1: Select initially compromised asset(s)
Add initial trigger(s) for your network elements to the simulation. If no valid triggers for an element exist (i.e., the transition table does not have any transitions originating in the element's current state), it will be disabled in the list below.

Alert source
Schachtverteiler BT 1.1 Et. -2 ✓ +

Trigger
Überschwemmung < 1m ✓ +

Step 2: Configure simulation scenario
Here you can find your constructed scenario of triggers initially affecting corresponding assets. You can disable triggers in order not to simulate them or remove them from the scenario by using the corresponding action buttons.

Order	Asset Name	Trigger	Actions
1.	Schachtverteiler BT 2.0 Et.-2	Überschwemmung < 1m	✓ ✕
2.	Schachtverteiler BT 3.1 Et. -2	Überschwemmung < 1m	✓ ✕

Step 3: Set simulation parameters and simulate
Set how many simulation runs you want to execute and, if preferred, a time step limit. The latter restricts each simulation run to the given amount of logical time steps. In order to simulate, at least one trigger has to be enabled in the scenario!

Number of simulations
-100 100 ✓ +100

Time step limit
1 ✓

simulate

Abbildung 83: SAURON – Simulationseingabe

Ist die Simulation durchgelaufen kann unter dem Reiter „Entity Analysis“ das Resultat visualisiert werden. Für jeden Knoten werden die möglichen Zustände farblich angezeigt und auch zahlenmäßig ausgedrückt. Dabei entspricht die Summe der Zahlen der Anzahl der Simulationszyklen.

Inspector Entity Analysis Network Cases Network Metrics Entity Prognosis

Show simulation until
1 ✓

The table below contains a quick summary about how often nodes ended up in what *final* state in those simulations and how much they deviate in average from the initial state of the corresponding node. Based on the standard deviation, a node's relative resilience is calculated where 1.0 means fully resilient and 0.0 not resilient at all to the simulated scenario. For more information about the properties displayed in the table take a look at the "Table Description". The shown node entities can be filtered and sorted by the given criteria in the collapsible menu of "Filter" and "Sort".

Entity	Initial	Distribution	Avg.	Std. Dev.	Max. Dev.	Vulnerability	Resilience
1 Transport gebrauchte Medizinprodukte	1	843 157	1.160	0.400	1	0.400	0.600
10 Transport sterile Medizinprodukte	1	852 148	1.150	0.380	1	0.380	0.620
2 Vorreinigung & Vorbereitung MP	1	667 333	1.670	1.150	2	0.575	0.425
3 maschinelle Reinigung & Desinfektion MP	1	667 333	1.670	1.150	2	0.575	0.425
4 Sichtprüfung & manuelle Trocknung MP	1	667 333	1.670	1.150	2	0.575	0.425
5 Freigabe nach Prüfung Medizinprodukte	1	667 333	1.670	1.150	2	0.575	0.425
6 Funktionskontrolle & Pflege MP	1	667 333	1.670	1.150	2	0.575	0.425
7 Verpackung Medizinprodukte	1	667 333	1.670	1.150	2	0.575	0.425
8 Sterilisation Medizinprodukte	1	667 333	1.670	1.150	2	0.575	0.425
9 Freigabe nach Sterilisation MP	1	1000	1.000	0.000	2	0.000	1.000
Abwasserhebeanlage BT 2.0 Et. -2	1	629 371	1.740	1.220	2	0.610	0.390
AEMP Stammdatenadministrator	1	872 128	1.130	0.360	1	0.360	0.640
anlagen spezifische Software	1	1000	1.000	0.000	1	0.000	1.000

Abbildung 84: SAURON - Ergebnisanzeige der Simulation

14.12 SAURON Übergangstabelle

Auf den folgenden 4 Seiten sind die Übergangsfaktoren der Knotenpunkte aufgelistet.

Simulations- MATRIX		Beschreibung der Prozesse & Ressourcen	Group	Input Trigger	Origin State	Destin- ation State	Output Symbol	Proba- bility %	Beschreibung der Robustheit
Beschreibungen, Trigger, Übergänge, Robustheit									
kritische Prozessschritte	1 Transport gebrauchte Medizinprodukte	Transport benutzte MP & Endoskope aus den Verbrauchsabteilung zur AEMP, Annahme der	Transport	Ausfall Aufzüge	1	2	Ausfall Aufzüge	20%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner
	2 Vorreinigung & Vorbereitung MP	Auspacken der Siebe, grobe Vorreinigung wenn nötig, Vorbereitung der Geräteträger mit MP	AEMP - kritische Prozesse	Ausfall Zutrittsstechnik	1	2	Ausfall Zutrittsstechnik	10%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
				AV-SV Stromausfall	1	3	Ausfall AEMP	100%	
				Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	
				Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%	
				Ausfall Lüftung	1	2	Ausfall Lüftung	30%	
				Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	30%	
				Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	
				Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%	
				Ausfall Druckluft	1	2	Ausfall Druckluft	10%	
				AV-SV Stromausfall	1	3	Ausfall AEMP	100%	
	3 maschinelle Reinigung & Desinfektion MP	Maschinelle Reinigung von Medizinprodukten	AEMP - kritische Prozesse	Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
				Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%	
				Ausfall Lüftung	1	2	Ausfall Lüftung	30%	
				Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%	
				Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	
				Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%	
				Ausfall Druckluft	1	2	Ausfall Druckluft	10%	
				AV-SV Stromausfall	1	3	Ausfall AEMP	100%	
				Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	
				Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%	
	4 Sichtprüfung & manuelle Trocknung MP	Übernahme der desinfizierten MP vom Geräteträger, Prüfung auf Sauberkeit	AEMP - kritische Prozesse	Ausfall Lüftung	1	2	Ausfall Lüftung	30%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
				Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%	
				Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	
				Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%	
				Ausfall Druckluft	1	2	Ausfall Druckluft	10%	
				AV-SV Stromausfall	1	3	Ausfall AEMP	100%	
				Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	
				Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%	
				Ausfall Lüftung	1	2	Ausfall Lüftung	30%	
				Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%	
	5 Freigabe nach Prüfung Medizinprodukte	Freigabe zur Funktionskontrolle nach derSichtprüfung	AEMP - kritische Prozesse	Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
				Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%	
				Ausfall Druckluft	1	2	Ausfall Druckluft	10%	
				AV-SV Stromausfall	1	3	Ausfall AEMP	100%	
				Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	
				Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%	
				Ausfall Lüftung	1	2	Ausfall Lüftung	30%	
				Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%	
				Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	
				Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%	
	6 Funktionskontrolle & Pflege MP	Funktionskontrolle zum Teil mit unterstützenden Geräten, Pflege (z.B. ölen), Ersetzen verbrauchte MP	AEMP - kritische Prozesse	Ausfall Druckluft	1	2	Ausfall Druckluft	10%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger
AV-SV Stromausfall				1	3	Ausfall AEMP	100%		
Ausfall VE-Wasser				1	2	Ausfall VE-Wasser	10%		
Ausfall Trinkwasser				1	3	Ausfall Trinkwasser	100%		
Ausfall Lüftung				1	2	Ausfall Lüftung	30%		
Ausfall Prozessgerät				1	3	Ausfall Prozessgerät	100%		
Ausfall Prozessgerät				1	2	Ausfall Prozessgerät	30%		
Ausfall Prozessgerät				2	3	Ausfall Prozessgerät	40%		
Ausfall Druckluft				1	2	Ausfall Druckluft	10%		
AV-SV Stromausfall				1	3	Ausfall AEMP	100%		
7 Verpackung Medizinprodukte	komplette Siebe werden manuelle verpackt und für die Sterilisation vorbereitet	AEMP - kritische Prozesse	Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger	
			Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%		
			Ausfall Lüftung	1	2	Ausfall Lüftung	30%		
			Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%		
			Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%		
			Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%		
			Ausfall Druckluft	1	2	Ausfall Druckluft	10%		
			AV-SV Stromausfall	1	3	Ausfall AEMP	100%		
			Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%		
			Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%		
8 Sterilisation Medizinprodukte	Verpackte Siebe werden sterilisiert	AEMP - kritische Prozesse	Ausfall Lüftung	1	2	Ausfall Lüftung	30%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger	
			Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%		
			Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%		
			Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%		
			Ausfall Druckluft	1	2	Ausfall Druckluft	10%		
			AV-SV Stromausfall	1	3	Ausfall AEMP	100%		
			Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%		
			Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%		
			Ausfall Lüftung	1	2	Ausfall Lüftung	30%		
			Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%		
9 Freigabe nach Sterilisation MP	Freigabe der Siebe nach der Sterilisation für den Transport	AEMP - kritische Prozesse	Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: 2 AEMP anderer Krankenhäusträger; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
			Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%		
			Ausfall Druckluft	1	2	Ausfall Druckluft	10%		
			AV-SV Stromausfall	1	3	Ausfall AEMP	100%		
			Ausfall VE-Wasser	1	2	Ausfall VE-Wasser	10%		
			Ausfall Trinkwasser	1	3	Ausfall Trinkwasser	100%		
			Ausfall Lüftung	1	2	Ausfall Lüftung	30%		
			Ausfall Prozessgerät	1	3	Ausfall Prozessgerät	100%		
			Ausfall Prozessgerät	1	2	Ausfall Prozessgerät	30%		
			Ausfall Prozessgerät	2	3	Ausfall Prozessgerät	40%		
10 Transport sterile Medizinprodukte	Transport sterilisierte MP und Endoskope von der AEMP zu den Verbrauchsabteilung	Transport	Ausfall Aufzüge	1	2	Ausfall Aufzüge	20%	Ausfallkonzept IT: Papierprozeduren und Vorlagen / Ausfallkonzept Prozess: externer Partner	
			Ausfall Zutrittsstechnik	1	2	Ausfall Zutrittsstechnik	10%		
m)	Logistiker	Bearbeitet die Prozessschritte 1 & 10 (interner Transport) innerhalb der beiden Standorte	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	mehere intere Logistiker
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Fachkundige in der Aufbereitung von MP	Bearbeiten die Prozessschritte 1 (Warenannahme) & 2 bis 9	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	15 Personen in der AEMP in allen Bereichen einsetzbar
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	AEMP Stammdatenadministrator	Pflegen die Stammdaten der Siebe ins Qualitätsmanagement, Managen Reparaturen der MP & Endoskope	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	2 Stammdatenaministratoren
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage

interne Personal (Rolle)	Qualitätsmanagerin AEMP (Stellv. Leiterin AEMP)	Verantwortet das Qualitätsmanagement exklusiv in der AEMP und ist gleichzeitig Stellv Leiterin AEMP	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	QM hat keinen Stellvertreter
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Leitung der AEMP	Verantwortet die Organisation der AEMP	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	hat einen Stellvertreter
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Technischer Dienst	Verantwortlich für den technischen Zustand der AEMP-Ausstattung und der techn. Versorgung (Strom, Wasser, ...)	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	Bereitschaft - innerhalb 30 min vor Ort (5 Elektriker) / Prozeduren zur Fehlerbehebung vorhanden
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	IT-Hardwarespezialisten	Verantwortlich für die IT Hardware Ausstattung der AEMP	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	Bereitschaft - innerhalb 60 min vor Ort (5 Hardware Spezialisten) / Dokumente & Beschreibungen sind vorhanden
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	IT-Softwarespezialisten	Verantwortlich für die Schnittstellen zw. der anlagenspezifischen Software und der QM- / KIS-Software	internes Personal (Rollen)	Ausfall Zutittstechnik	1	2	Ausfall internes Personal	20%	Bereitschaft - innerhalb 60 min vor Ort (4 Software Spezialisten) / Dokumente & Beschreibungen sind vorhanden
				AV-SV Stromausfall	1	2	AV-SV Stromausfall	10%	Telekomausfall; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
externe Partner	Ausfallkonzept mit 2 anderen Krankenhäusern	Falls Prozesse in der AEMP ausfallen und nicht umgehend behoben werden können	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	die 2 externen AEMP stehen an 2 verschiedenen Standorten unentgeltlich zur Verfügung - SLA vorhanden
	Externer Transportunternehmer	Transport der benutzten und sterilen MP in spezifischen Transportwagen zw. den Standorten	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	Ersatzfahrer / Ersatz-LKW
	Wartungsfirma RDG	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	keine Angaben über Reaktionszeit und mind. Einsatzzeit vor Ort
	Wartungsfirma Einschweißgerät	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	/
	Wartungsfirma Sterilisator	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	keine Angaben über Reaktionszeit und mind. Einsatzzeit vor Ort
	Wartungsfirma Versorgungsanlagen	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	/
	Wartungsfirma Sicherheitstechnische Anlagen	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	Wartungsvertrag mit 3h Vororteinsatz
	Wartungsfirma IT-Hardware (Netz, DB, Server, ...)	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	/
	Wartungsfirma IT-Software	Wartung, Reparatur, Instandsetzung gemäss Wartungsvertrag, gesonderte Bestellung	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	Wartungsvertrag: Hotline (Mo-Fr 08:00-16:00)
	BHKW Betreiber	BHKW Eigentümer = Gemeinde; BHKW Betreiber = externe Firma	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	externe Firma mit Bereitschaftsdienst
	Trinkwasserversorger	Trinkwasserversorgung durch die Gemeinde	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	Bereitschaftsdienst der Gemeinde
	Telekomversorger	Telekomnetzversorger für die Bereiche Telefonie und EDV Anbindung an das WWW	externe Partner	Ausfall Zutrittsstechnik	1	2	Ausfall ext. Partner	20%	Bereitschaftsdienst des Telekomversorgers
IT Software	Qualitätsmanagement Software	13 Arbeitsplätze an den versch. Stationen in der AEMP	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank; Redundanz = Ausfallkonzept EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	Krankenhausinformationssystem	3 Arbeitsstationen mit Zugriff auf das KIS	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank; Redundanz = Abstimmung OP EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	klassische IT-Office Software	13 Arbeitsstationen mit Zugriff auf klassische IT Office Software	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	Software = Lokal gespeichert, Verbindung über Netzwerk zum Dateiserver EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	anlagen spezifische Software	Software welche spezifisch für die Funktionsfähigkeit des Gerätes / der Anlage programmiert ist	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	RDG & Sterilisatoren=> Datenbank: VMServer = Master & lokaler PC = Slave / Plasmasterilisator => Datenbank: VMServer, Dateiserver EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	Verwaltung Leihsets	Hausinterne Software zur Verwaltung der Leihsets MP	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	Software = Lokal gespeichert, Verbindung über Netzwerk zur Datenbank EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	Gebäudeleittechnik	Gäudeleittechnik ist eine Überwachungssoftware für alle technischen Versorgungsressourcen	IT Software	Ausfall Server Nord	1	2	Ausfall Server Nord	20%	Parameter sind in der Feldebene gespeichert; Redundante VM-Serverstruktur; nur Visualisierung EDV Hardware; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	2	3	Ausfall Server Nord	100%	
				Ausfall Server Nord	1	3	Ausfall Server Nord	80%	
				Ausfall Server Süd	1	2	Ausfall Server Süd	20%	
				Ausfall Server Süd	2	3	Ausfall Server Süd	100%	
				Ausfall Server Süd	1	3	Ausfall Server Süd	80%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	
	Waschbecken für Vorreinigung	Waschbecken mit Handbrause, Trinkwasser / VE-Wasser	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%	
				Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%	
				Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%	
	Ultraschallbecken	Ultraschalltischgerät	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	2 identische Ultraschallbecken; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%	

Interne & Externe kritische Ressourcen	Prozessgeräte			Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%		
		Reinigungs- & Desinfektionsgeräte (RDG)	RDG zur automatisierten Reinigung, Desinfektion und Trocknung der MP	Prozessgeräte	Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%	2/4 Geräten mit Elektrowärmeerzeuger; 2 Geräte mit AV- & 2 Geräte mit SV-Versorgung; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
					AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	
					Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%	
					Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%	
					Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%	
		Packtische	höhenverstellbare Arbeitstische für die Sichtprüfung, man. Trocknung, Funktionsprüfung, Pflege und Verpackung	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	6 identische Packtische; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
					Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%	
					Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%	
					Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%	
	Sterilisatoren	Sterilisatoren für die Siebe mit MP, und die	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	2/3 Sterilisatoren mit Elektrodampferzeuger;1 Gerät mit AV- & 2 Geräte mit SV-Versorgung; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%		
				Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%		
				Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%		
	Einschweissgerät	Einschweißgerät für einzelne MP	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	2 Geräte; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%		
				Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%		
				Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%		
	unterstützende Geräte zur Funktionskontrolle	Kleingeräte für die Funktionskontrolle	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	keine Redundanz, Ausfallkonzept mit 2 anderen KH; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%		
				Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%		
				Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%		
	EDV Hardware (Desktop PC in der AEMP)	PC's inkl. Zubehör, Handscanner an jedem Prozessschritt, Drucker strategisch verteilt	Prozessgeräte	AV-SV Stromausfall	1	3	Ausfall Prozessgerät	100%	Redundanzen für lokale PC, der virtuellen Serverstruktur, die Storage sind vorhanden; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
				Ausfall Server Nord	1	2	Ausfall Prozessgerät	25%		
				Ausfall Server Süd	1	2	Ausfall Prozessgerät	25%		
			Ausfall EDV Netzwek	1	3	Ausfall Prozessgerät	100%			
Versorgung / techn. Anlagen	BHKW AV Stromversorgung	AV-Stromversorgung dient der normalen Versorgung aller System, Anbindung BHKW-KH erfolgt im BT Süd	BHKW					BHKW: 3 MSpg-Einspeisungen; Redundanz mit 3 Gasmotoren; Einspeisung BHKW-HK im BT Süd		
	AV Übergabe & Etagenverteiler BT 3.2 Et.-1	AV-Sammelschiene zur Verteilung an die Schachtverteiler und die Etagenverteiler im BT 3.2	AV Stromversorgung					Koppelschalter zur Verbindung der Sammelschienen SV-AV		
	BHKW SV Stromversorgung	SV-Stromversorgung dient als Sicherheitsversorgung wenn AV ausfällt, Anbind. BHKW-KH erfolgt im BT Süd	BHKW					Regelbetrieb durch AV-Versorgung; Netzausfall: 2 Dieselgeneratoren; Einspeisung BHKW-HK im BT Süd		
	SV Übergabe & Etagenverteiler BT 3.2 Et.-1	SV-Sammelschiene zur Verteilung an die Schachtverteiler und die Etagenverteiler im BT 3.2	SV Stromversorgung					Koppelschalter zur Verbindung der Sammelschienen SV-AV		
	Etagenverteiler BT 3.2 Technikzentrale 1B	Etagenverteiler zur Versorgung der Technikzentrale 1B	Etagenverteiler BT 3.2					Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage		
	Schachtverteiler BT 3.1 Et. -2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 3.1	Schachtverteiler Et.-2	Überschwemmung < 1m	1	2	AV-SV Stromausfall	30%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m	
				Überschwemmung < 1m	2	3	AV-SV Stromausfall	10%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung < 1m	1	3	AV-SV Stromausfall	5%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung > 1m	1	3	AV-SV Stromausfall	100%	Überschwemmung der Schutzbauteile in den Raum	
	Etagenverteiler BT 3.1 Et. 1	EDV Etagenverteiler zur Versorgung BT 3.1 Etage 1	Etagenverteiler	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage	
	Etagenverteiler BT 3.1 Et. 2	Etagenverteiler zur Versorgung BT 3.1 Etage 1 & 2	Etagenverteiler	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
	Etagenverteiler BT 3.1 Technikzentrale 1A	Etagenverteiler zur Versorgung der Technikzentrale 1A	Etagenverteiler	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage	
	Schachtverteiler BT 2.0 Et.-2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 2.0	Schachtverteiler Et.-2	Überschwemmung < 1m	1	2	AV-SV Stromausfall	30%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m	
				Überschwemmung < 1m	2	3	AV-SV Stromausfall	10%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung < 1m	1	3	AV-SV Stromausfall	5%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung > 1m	1	3	AV-SV Stromausfall	100%	Überschwemmung der Schutzbauteile in den Raum	
	Etagenverteiler BT 2.0 Et.-1	Etagenverteiler zur Versorgung BT 2.0 Etage -1	Etagenverteiler	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage	
	Schachtverteiler BT 1.3 Et. -1	Schachtverteiler zur Versorgung der Etagenverteiler im BT 1.3	Schachtverteiler					Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m		
	Etagenverteiler BT 1.3 Et. -1	Etagenverteiler zur Versorgung BT 2.0 Etage -1	Etagenverteiler 1.3					Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage		
	Schachtverteiler BT 1.1 Et. -2	Schachtverteiler zur Versorgung der Etagenverteiler im BT 1.1	Schachtverteiler Et.-2	Überschwemmung < 1m	1	2	AV-SV Stromausfall	30%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage, Überschwemmungsschutz an den Zugangstüren <1m	
				Überschwemmung < 1m	2	3	AV-SV Stromausfall	10%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung < 1m	1	3	AV-SV Stromausfall	5%	partielles Versagen des Überschwemmungsschutzes	
				Überschwemmung > 1m	1	3	AV-SV Stromausfall	100%	Überschwemmung der Schutzbauteile in den Raum	
	Etagenverteiler BT 1.1 Et. -1	Etagenverteiler zur Versorgung BT 1.1 Etage -1	Etagenverteiler	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	Trennung der einzelnen Schaltschränke mit 20 mm Promatplatten; Brandmeldeanlage	
	USV Stromversorgung Südtrakt Et. 2	AEMP nur mit USV versorgt	USV Stromversorgung					SV versorgt USV Anlage, Ausfall SV Versorgung => Übernahme durch USV bis SV wieder einspeist		
	BHKW Hausdampfversorgung	Einspeisung Süd: AEMP und Reindampfproduktion Süd; Einspeisung Nord: Reindampfproduktion Nord	BHKW					/		
	Hausdampfübergabe Süd BT 3.2 Et.2	Hausdampfübergabe im BT 3.2 zur Versorgung der AEMP und der Reindampfversorgung Süd	Dampf					keine Redundanz		
	Reindampfversorgung Süd BT 3.2 Et. 2	Reindampf wird für die Desinfektion von MP und zur Befeuchtung in den Lüftungsanlagen benötigt	Dampf	Ausfall VE-Wasser	1	3	Audfall Reindampf	100%	VE Wassereinspeisung aus BT Nord über eine nicht redundante Druckerhöhung; keine Redundanz	
	BHKW Wärmeversorgung	Einsatz Wärme: Temperaturerhöhung in den Lüftungsanlagen	BHKW					/		
	Wärmeübergabe Süd BT 3.2 Et. -2	Einspeisung Wärmeversorgung BHKW-KH im im BT Süd für Lüftungsanlagen und Küche	Wärmeversorgung	Überschwemmung < 1m	1	2	Ausfall Wärme Süd	15%	keine Redundanz	
				Überschwemmung < 1m	1	3	Ausfall Wärme Süd	5%		
				Überschwemmung > 1m	1	2	Ausfall Wärme Süd	35%		
				Überschwemmung > 1m	1	3	Ausfall Wärme Süd	65%		
				Überschwemmung > 1m	2	3	Ausfall Wärme Süd	40%		
	BHKW Kälteversorgung	Einsatz Kälte: Temperatursenkung in den Lüftungsanlagen; Deckenkonvektoren; Kühlung RDG's	BHKW					/		
	Kälteübergabe Süd BT 3.2 Et. -2	Einspeisung Kälteversorgung BHKW-KH im BT Süd	Kälteversorgung Süd	Überschwemmung < 1m	1	2	Ausfall Kälte Süd	15%	keine Redundanz	
				Überschwemmung < 1m	1	3	Ausfall Kälte Süd	5%		
				Überschwemmung > 1m	1	2	Ausfall Kälte Süd	35%		
				Überschwemmung > 1m	1	3	Ausfall Kälte Süd	65%		
				Überschwemmung > 1m	2	3	Ausfall Kälte Süd	40%		
	Kälteübergabe Nord BT 1.1 Et. -1	Einspeisung Kälteversorgung BHKW-KH im BT Nord	Kälteversorgung Nord	AV-SV Stromausfall	1	3	Ausfall Kälte Nord	100%	keine Redundanz; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
	Lüftungsanlage 17A Südtrakt Et. 2	separate Lüftungsanlage für die gesamte AEMP - Reinraumklasse 1 / 2	Lüftung	AV-SV Stromausfall	1	3	Ausfall Lüftung	100%	Redundante Zu- & Ab-Luft für insgesamt 10 verschiedene Lüftungsanalge im Bauteil Süd; Anlage 17A nicht redundant ausgelegt; Ausfall AV & SV Stromversorgung => Ausfall der Anlage	
				Ausfall Kälte Süd	1	2	Ausfall Kälte Süd	10%		
Ausfall Wärme Süd				1	2	Ausfall Wärme Süd	10%			
Ausfall Reindampf				1	2	Ausfall Reindampf	10%			
Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	med. Druckluft wird für die man. Trocknung und die Funktionsprüfung versch. MP benötigt	Druckluft	AV-SV Stromausfall	1	3	Ausfall Druckluft	100%	2 redundante Druckluftherzeuger im Bauteil Nord; Ausfall AV & SV Stromversorgung => Ausfall der Anlage		
Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1	Druckluftproduktion und -Versorgung im KH, Druckluft wird für die Automatismen der Sterilisatoren benötigt	Druckluft	AV-SV Stromausfall	1	3	Ausfall Druckluft	100%	2 redundante Druckluftherzeuger im Bauteil Nord; Ausfall AV & SV Stromversorgung => Ausfall der Anlage		
Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2	Trinkwasser wird durch den Wasserversorger eingespeist, TW wird für die Herstellung von VE Wasser benötigt	Wasserversorgung					1 TW Einspeisung ins KH ohne Redundanz im Bauteil Nord			

	TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1	UV-Behandlung und Chlorierung zur Reinigung des Trinkwassers	Trinkwasser	AV-SV Stromausfall	1	3	Ausfall Trinkwasser	100%	keine Redundanz; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	TR-W Enthärtung BT 1.1 Et. -1	Wasserenthärtungsanlage	Trinkwasser	AV-SV Stromausfall	1	3	Ausfall Trinkwasser	100%	3 parallel funktionierende Enthärtungsanlagen; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Osmoseanlage BT 1.1 Et. -1	Herstellung von VE Wasser	VE-Wasser	AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	keine Redundanz; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1	Druckerhöhung VE Wasser für die Prozessschritten Vorreinigung, maschinelle Reinigung und Sterilisation	VE-Wasser	Ausfall Trinkwasser	1	3	Ausfall VE-Wasser	100%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	2 parallel funktionierende Pumpen; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2	Druckerhöhung zur Einspeisung der Reindampfversorgung im BT 3.2 Et. 2	VE-Wasser	Ausfall Trinkwasser	1	3	Ausfall VE-Wasser	100%	
				AV-SV Stromausfall	1	3	AV-SV Stromausfall	100%	keine Redundanz; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	Abwasserhebeanlage BT 2.0 Et. -2	Abwasserleitungen ins UG 2 und von dort mit einer Abwasserhebeanlage ins öffentliche Abwassernetz	Abwasserhebeanlage	Ausfall Trinkwasser	1	3	Ausfall VE-Wasser	100%	
				AV-SV Stromausfall	1	3	Ausfall	100%	2 Abwasserhebeanlagen; Ausfall AV-SV Stromversorgung => Totalausfall
	Aufzüge A4-A6 BT 2.0	3 Bettenlifte, Transport von MP & Endoskopen vom EG <=> OG	Aufzüge	AV-SV Stromausfall	1	3	Abwasserhebeanlage	100%	
				AV-SV Stromausfall	1	3	Ausfall Aufzüge	100%	2 verschiedenen Maschinenräumen; Ausfall AV-SV Stromversorgung => Totalausfall
	Aufzug A7 BT 3.1	1 Bettenlift, Transport von MP & Endoskopen vom EG <=> OG;	Aufzüge	AV-SV Stromausfall	1	3	Ausfall Aufzüge	100%	
				AV-SV Stromausfall	1	3	Ausfall Aufzüge	100%	Redundanz zu A8; Ausfall AV-SV Stromversorgung => Totalausfall
	Versorgung durch Telekomanbieter BT 2.0 Et. -1	Anbindung an das öffentliche Telekommunikationsnetz und Verdinung ins Internet	Telekomversorgung	Cyberangriff - SD (Shutdown)	1	3	Ausfall Telekomversorgung	100%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall EDV Netzwerk	100%	2 getrennte Kabelwege in das Hauptgebäude
	EDV-Netzwerk redundant	internes LWL Netzwerk vom Netzanachluss über die beiden Serverräume zu den Etagenverteiler	EDV	AV-SV Stromausfall	1	3	Ausfall EDV Netzwerk	100%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall EDV Netzwerk	100%	komplett redundant verkabelte Netzwerkstruktur (CoreSwitch, Glasfaserverkabelung, Etagenswitch...); Ausfall AV-SV Stromversorgung => Totalausfall
	EDV-Netzwerk nicht redundant	Verbindung vom Etagenverteiler zu den perioheren Switches, PC's und Grossgeräte	EDV	AV-SV Stromausfall	1	3	Ausfall EDV Netzwerk	100%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall EDV Netzwerk	100%	keine Redundanz; einfache Single-Verkabelung; Ausfall AV-SV Stromversorgung => Totalausfall
	Serverraum Nord BT 1.3. Et. -1	Serverraum mit Core-Switch; Datenspeicherung und Serverlandschaft	Server Nord	Ausfall Kälte Nord	1	2	Ausfall EDV Netzwerk	100%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall Server Nord	10%	Redundanz zum Serverraum Süd; Kälteversrogung mit separatem Spliteinzelgerät: Ausfall Kälte => Ausfallwahrscheinlichkeit des gesamt Systems = sehr gering
	Serverraum Süd BT 3.2 Et. -1	Serverraum mit Core-Switch; Datenspeicherung und Serverlandschaft	Server Süd	Ausfall Kälte Süd	1	2	Ausfall Server Nord	100%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall Server Süd	10%	Redundanz zum Serverraum Süd; Kälteversrogung mit separatem Spliteinzelgerät: Cyberangriff => forcierter Shutdown
	Schwachstromsicherheitsanlagen BT 2.0 Et. -1	Technikraum mit allen Schwachstromsicherheitsanlagen: GMS, BMA, ZUKO, CCTV, Telekom,	Schwachstrom	Ausfall Kälte Süd	1	2	Ausfall Server Süd	10%	
				Cyberangriff - SD (Shutdown)	1	3	Ausfall Server Süd	100%	Redundanz zum Serverraum Süd; Kälteversrogung mit separatem Spliteinzelgerät: Cyberangriff => forcierter Shutdown
	Telekomanlage BT 2.0 Et. -1	Technikraum mit allen Schwachstromsicherheitsanlagen: GMS, BMA, ZUKO, CCTV, Telekom,	Schwachstrom	AV-SV Stromausfall	1	3	Ausfall Server Süd	100%	
				Ausfall EDV Netzwek	1	3	AV-SV Stromausfall	100%	keine Redundanzen; Ausfall AV & SV Stromversorgung => Ausfall der Anlage
	elektr. Zutrittskontrolle BT 2.0 Et. -1	Zutrittskontrolle für die verschiedenen Eingänge der AEMP	Zutrittstechnik	Cyberangriff - SD (Shutdown)	1	3	Ausfall EDV Netzwerk	100%	
				AV-SV Stromausfall	1	3	Cyberamgriff - SD	100%	Anlage ist nicht redundant, komplett redundant verkabelte Netzwerkstruktur (CoreSwitch, Glasfaserverkabelung, Etagenswitch...); Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Ausfall EDV Netzwek	1	3	AV-SV Stromausfall	100%	
				Ausfall EDV Netzwek	1	3	Ausfall EDV Netzwerk	100%	Anlage ist nicht redundant, komplett redundant verkabelte Netzwerkstruktur (CoreSwitch, Glasfaserverkabelung, Etagenswitch...); Ausfall AV & SV Stromversorgung => Ausfall der Anlage
				Cyberangriff - SD (Shutdown)	1	3	Cyberamgriff - SD	100%	
				AV-SV Stromausfall	1	3	Ausfall Zutrittsstechnik	100%	Eigenständige Anlage an SV-Versorgung angeschlossen; Ausfall SV => Ausfall der Anlage
				Ausfall EDV Netzwek	1	3	Ausfall Zutrittsstechnik	100%	

14.13 Ergebnisse der Risikoanalysen

14.13.1 Statische Risikoanalyse - Kritische Prozesse

Übersicht der einzelnen Prozesse mit den Angaben der Schadensklassen und der Verfügbarkeitszeiten.

Tabelle 17: Risikoanlage - Überblick der kritischen Prozesse

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit	
	Finanz	Regular	Image	Operate	RTO	RPO	MTPD	Integrität	Vertraulichkeit
SP 4.2-Aufbereitungseinheit für Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit	
	Finanz	Regular	Image	Operate	RTO	RPO	MTPD	Integrität	Vertraulichkeit
SP 4.2.1-Transport gebrauchte Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.2-Vorreinigung & Vorbereitung MP	Managebar	Managebar	Managebar	Signifikant	30 Minuten	1 Stunde	24 Stunden	Korrekt	öffentlich
SP 4.2.3-maschinelle Reinigung & Desinfektion MP	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.4-Sichtprüfung & manuelle Trocknung MP	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.5-Freigabe nach Prüfung Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.6-Funktionskontrolle & Pflege MP	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.7-Verpackung Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.8-Sterilisation Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	2 Stunden	24 Stunden	Korrekt	öffentlich
SP 4.2.9-Freigabe nach Sterilisation MP	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich
SP 4.2.10-Transport sterile Medizinprodukte	Managebar	Managebar	Managebar	Signifikant	30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich

Im Folgenden sind je untergeordnetem Prozess die Ressourcen-Abhängigkeiten nach Ressourcen-Kategorien aufgeteilt. Je Ressource wird die RTO-Verfügbarkeitszeit unterhalb der Zeitskala mit einer „1“ angegeben.

Tabelle 18: stat. Risikoanalyse - Übersicht der Abhängigkeiten pro Prozess

Prozess	Schadensklassen				Verfügbarkeit				Informationssicherheit		
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD		Integrität	Vertraulichkeit
SP 4.2.1-Transport gebrauchte Medizinprodukte	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden		Korrekt	öffentlich
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit				Informationssicherheit		
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD		Integrität	Vertraulichkeit
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Logistiker		1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Externer Transportunternehmer		1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software		1	1	1	1	1	1				Excel
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Aufzug A7 BT 3.1		1	1	1	1	1	1				
Aufzüge A4-A6 BT 2.0		1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit				Informationssicherheit		
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD		Integrität	Vertraulichkeit
SP 4.2.2-Vorreinigung & Vorbereitung MP	Managebar	Managebar	Managebar	Signifikant		30 Minuten	1 Stunde	24 Stunden		Korrekt	öffentlich
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit				Informationssicherheit		
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD		Integrität	Vertraulichkeit
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP			1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern			1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software			1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1			1	1	1	1	1				
Etagenverteiler BT 3.1 Et. 2			1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2			1	1	1	1	1				
Produktion Med. Druckluft 5 bar BT 1.1 Et. -1			1	1	1	1	1				
TR-W Enthärtung BT 1.1 Et. -1			1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
EDV Hardware (Desktop PC in der AEMP)			1	1	1	1	1				
Ultraschallbecken			1	1	1	1	1				
Waschbecken für Vorreinigung			1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.3-maschinelle Reinigung & Desinfektion MP	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP		1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern		1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software		1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2		1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2		1	1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
EDV Hardware (Desktop PC in der AEMP)		1	1	1	1	1	1				
Reinigungs- & Desinfektionsgeräte (RDG)		1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.4-Sichtprüfung & manuelle Trocknung MP	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP		1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern		1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software		1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2		1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2		1	1	1	1	1	1				
Produktion Med. Druckluft 5 bar BT 1.1 Et. -1		1	1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
EDV Hardware (Desktop PC in der AEMP)		1	1	1	1	1	1				
Packtsche		1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.5-Freigabe nach Prüfung Medizinprodukte	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP	1	1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern	1	1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software	1	1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2	1	1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2	1	1	1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
EDV Hardware (Desktop PC in der AEMP)	1	1	1	1	1	1	1				
Packtische	1	1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.6-Funktionskontrolle & Pflege MP	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
AEMP Stammdatenadministrator	1	1	1	1	1	1	1				
Fachkundige in der Aufbereitung von MP	1	1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern	1	1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software	1	1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2	1	1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2	1	1	1	1	1	1	1				
Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	1	1	1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Packtische	1	1	1	1	1	1	1				
unterstützende Geräte zur Funktionskontrolle	1	1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.7-Verpackung Medizinprodukte	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP		1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern		1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software		1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2		1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2		1	1	1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
EDV Hardware (Desktop PC in der AEMP)		1	1	1	1	1	1				
Einschweißgerät		1	1	1	1	1	1				
Packtische		1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.8-Sterilisation Medizinprodukte	Managebar	Managebar	Managebar	Signifikant		30 Minuten	2 Stunden	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP				1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern				1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software				1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2				1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2				1	1	1	1				
Prozessgeräte	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Sterilisatoren				1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.9-Freigabe nach Sterilisation MP	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Fachkundige in der Aufbereitung von MP	1	1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Ausfallkonzept mit 2 anderen Krankenhäusern	1	1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software	1	1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Etagenverteiler BT 3.1 Et. 2	1	1	1	1	1	1	1				
Lüftungsanlage 17A Südtrakt Et. 2	1	1	1	1	1	1	1				

Prozess	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
SP 4.2.10-Transport sterile Medizinprodukte	Managebar	Managebar	Managebar	Signifikant		30 Minuten	30 Minuten	24 Stunden	Korrekt	öffentlich	
Untergeordnete Prozesse	Schadensklassen				Verfügbarkeit			Informationssicherheit			
	Finanz	Regular	Image	Operate		RTO	RPO	MTPD	Integrität	Vertraulichkeit	
Rollen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Logistiker	1	1	1	1	1	1	1				
Juristische Personen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Externer Transportunternehmer	1	1	1	1	1	1	1				
IT Software	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Qualitätsmanagement Software	1	1	1	1	1	1	1				
Versorgung / techn. Anlagen	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
Aufzug A7 BT 3.1	1	1	1	1	1	1	1				
Aufzüge A4-A6 BT 2.0	1	1	1	1	1	1	1				

14.13.2 Statische Risikoanalyse - Kritische Ressourcen

Tabelle 19: stat. Risikoanalyse - kritische Ressourcen

AEMP Stammdatenadministrator												
SP 4.2.6 - Funktionskontrolle & Pflege MP												

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround		
	1	1	1	1	1	1						

Fachkundige in der Aufbereitung von MP												
SP 4.2.2 - Vorreinigung & Vorbereitung MP												
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP												
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP												
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte												
SP 4.2.6 - Funktionskontrolle & Pflege MP												
SP 4.2.7 - Verpackung Medizinprodukte												
SP 4.2.8 - Sterilisation Medizinprodukte												
SP 4.2.9 - Freigabe nach Sterilisation MP												

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround		
		1	1	1	1	1						
	1	1	1	1	1	1						
	1	1	1	1	1	1						
	1	1	1	1	1	1						
	1	1	1	1	1	1						
			1	1	1	1						
	1	1	1	1	1	1						

Logistiker												
SP 4.2.1 - Transport gebrauchte Medizinprodukte												
SP 4.2.10 - Transport sterile Medizinprodukte												

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround		
	1	1	1	1	1	1						
	1	1	1	1	1	1						

Ausfallkonzept mit 2 anderen Krankenhäusern												
SP 4.2.2 - Vorreinigung & Vorbereitung MP												
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP												

Verfügbarkeit												
RPO		10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
				1	1	1	1	1				
			1	1	1	1	1	1				

SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP			1	1	1	1	1	1				
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte			1	1	1	1	1	1				
SP 4.2.6 - Funktionskontrolle & Pflege MP			1	1	1	1	1	1				
SP 4.2.7 - Verpackung Medizinprodukte			1	1	1	1	1	1				
SP 4.2.8 - Sterilisation Medizinprodukte					1	1	1	1				
SP 4.2.9 - Freigabe nach Sterilisation MP			1	1	1	1	1	1				

Externer Transportunternehmer	Verfügbarkeit											
	RPO	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.1 - Transport gebrauchte Medizinprodukte			1	1	1	1	1	1				
SP 4.2.10 - Transport sterile Medizinprodukte			1	1	1	1	1	1				

Qualitätsmanagement Software											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.1 - Transport gebrauchte Medizinprodukte		1	1	1	1	1	1				
SP 4.2.10 - Transport sterile Medizinprodukte		1	1	1	1	1	1				
SP 4.2.2 - Vorreinigung & Vorbereitung MP			1	1	1	1	1				
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP		1	1	1	1	1	1				
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP		1	1	1	1	1	1				
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte		1	1	1	1	1	1				

SP 4.2.6 - Funktionskontrolle & Pflege MP
SP 4.2.7 - Verpackung Medizinprodukte
SP 4.2.8 - Sterilisation Medizinprodukte
SP 4.2.9 - Freigabe nach Sterilisation MP

	1	1	1	1	1	1				
	1	1	1	1	1	1				
			1	1	1	1				
	1	1	1	1	1	1				

EDV Hardware (Desktop PC in der AEMP)
SP 4.2.2 - Vorreinigung & Vorbereitung MP
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte
SP 4.2.7 - Verpackung Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				

Einschweissgerät
SP 4.2.7 - Verpackung Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
	1	1	1	1	1	1				

Packtische
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
	1	1	1	1	1	1				
	1	1	1	1	1	1				

SP 4.2.6 - Funktionskontrolle & Pflege MP		1	1	1	1	1	1				
SP 4.2.7 - Verpackung Medizinprodukte		1	1	1	1	1	1				

Reinigungs- & Desinfektionsgeräte (RDG)											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP		1	1	1	1	1	1				

Sterilisatoren											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.8 - Sterilisation Medizinprodukte				1	1	1	1				

Ultraschallbecken											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.2 - Vorreinigung & Vorbereitung MP			1	1	1	1	1				

unterstützende Geräte zur Funktionskontrolle											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.6 - Funktionskontrolle & Pflege MP		1	1	1	1	1	1				

Waschbecken für Vorreinigung											
	10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
SP 4.2.2 - Vorreinigung & Vorbereitung MP			1	1	1	1	1				

Aufzug A7 BT 3.1
SP 4.2.1 - Transport gebrauchte Medizinprodukte
SP 4.2.10 - Transport sterile Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
	1	1	1	1	1	1				
	1	1	1	1	1	1				

Aufzüge A4-A6 BT 2.0
SP 4.2.1 - Transport gebrauchte Medizinprodukte
SP 4.2.10 - Transport sterile Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
	1	1	1	1	1	1				
	1	1	1	1	1	1				

Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1
SP 4.2.2 - Vorreinigung & Vorbereitung MP

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				

Etagenverteiler BT 3.1 Et. 2
SP 4.2.2 - Vorreinigung & Vorbereitung MP
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				

SP 4.2.6 - Funktionskontrolle & Pflege MP
SP 4.2.7 - Verpackung Medizinprodukte
SP 4.2.8 - Sterilisation Medizinprodukte
SP 4.2.9 - Freigabe nach Sterilisation MP

	1	1	1	1	1	1				
	1	1	1	1	1	1				
			1	1	1	1				
	1	1	1	1	1	1				

Lüftungsanlage 17A Südtrakt Et. 2
SP 4.2.2 - Vorreinigung & Vorbereitung MP
SP 4.2.3 - maschinelle Reinigung & Desinfektion MP
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SP 4.2.5 - Freigabe nach Prüfung Medizinprodukte
SP 4.2.6 - Funktionskontrolle & Pflege MP
SP 4.2.7 - Verpackung Medizinprodukte
SP 4.2.8 - Sterilisation Medizinprodukte
SP 4.2.9 - Freigabe nach Sterilisation MP

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				
			1	1	1	1				
	1	1	1	1	1	1				

Produktion Med. Druckluft 5 bar BT 1.1 Et. -1
SP 4.2.2 - Vorreinigung & Vorbereitung MP
SP 4.2.4 - Sichtprüfung & manuelle Trocknung MP
SP 4.2.6 - Funktionskontrolle & Pflege MP

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				
	1	1	1	1	1	1				
	1	1	1	1	1	1				

TR-W Enthärtung BT 1.1 Et. -1
SP 4.2.2 - Vorreinigung & Vorbereitung MP

10min	30min	1h	2h	4h	8h	12h	24h	3d	7d	Workaround
		1	1	1	1	1				

14.13.3 Dynamische Risikoanalyse – Überschwemmung UG 2 > 1m

Auf den folgenden 3 Seiten sind die Ergebnisse dargestellt.

Nachstehend sind alle Knotenpunkte aufgelistet mit der Angabe wie stark der Knotenpunkt vom Anfangszustand abweicht. Mit der Standardabweichung wird die Widerstandsfähigkeit (Resilience) eines Knotenpunktes berechnet. Resilience = 1,0 bedeutet der Knotenpunkt ist gegenüber dem Szenario zu 100% widerstandsfähig, wo gegen Resilience = 0,0 bedeutet, dass der Knotenpunkte zu 0% widerstandsfähig ist.

Tabellenbeschreibung:

Eigenschaft	Beschreibung
Initial - Anfangszustand	Der Zustand des Knotens vor der Simulation.
Distribution - Verteilung	Zeigt an, wie oft der Knoten in welchem Zustand gelandet ist (wenn man mit dem Mauszeiger über den Balken fährt, wird der relative Anteil angezeigt).
Avg. - Mittelwert	Der durchschnittliche Endzustand des Knotens über alle Simulationsläufe.
Std. Dev. – Standardabweichung	Die relative durchschnittliche Abweichung vom Ausgangszustand über alle Simulationsläufe hinweg.
Max. Dev. - Max. Abweichung.	Die maximal mögliche Abweichung vom Ausgangszustand.
Vulnerability - Verwundbarkeit	Die relative Verwundbarkeit des Knotens gegenüber dem simulierten Szenario, die berechnet wird, indem die durchschnittliche relative Abweichung durch die maximal mögliche Abweichung geteilt wird (Std.Dev./Max.Dev.).
Resilience -Widerstandsfähigkeit	Die relative Resilienz des Knotens gegenüber dem simulierten Szenario, die als das Gegenteil der Verwundbarkeit dargestellt wird (1 - Verwundbarkeit).

Step 1: Select initially compromised asset(s)

Add initial trigger(s) for your network elements to the simulation. If no valid triggers for an element exist (i.e., the transition table does not have any transitions originating in the element's current state), it will be disabled in the list below.

Alert source

Schachtverteiler BT 3.1 Et. -2 ✓

Select where the alert is triggered

Trigger

Select what is triggered at Schachtverteiler BT 3.1 Et. -2

Step 2: Configure simulation scenario

Here you can find your constructed scenario of triggers initially affecting corresponding assets. You can disable triggers in order not to simulate them or remove them from the scenario by using the corresponding action buttons.

Scenario

3 / 3

Order	Asset Name	Trigger	Actions
1.	Schachtverteiler BT 1.1 Et. -2	Überschwemmung > 1m	✓ ⬆ ⬇ ⬆
2.	Schachtverteiler BT 2.0 Et.-2	Überschwemmung > 1m	✓ ⬆ ⬇ ⬆
3.	Schachtverteiler BT 3.1 Et. -2	Überschwemmung > 1m	✓ ⬆ ⬇ ⬆

Step 3: Set simulation parameters and simulate

Set how many simulation runs you want to execute and, if preferred, a time step limit. The latter restricts each simulation run to the given amount of logical time steps. In order to simulate, at least one trigger has to be enabled in the scenario!

Number of simulations

 ✓

Set how many simulations should be run

Time step limit

☐ ✓

Set how many simulation steps should be simulated per run or disable it

simulate

[Inspector](#) [Entity Analysis](#) [Network Cases](#) [Network Metrics](#) [Entity Prognosis](#)

Show simulation until

☐ ✓

Set how many simulation steps should be shown or disable it

The table below contains a quick summary about how often nodes ended up in what *final* state in those simulations and how much they deviate in average from the initial state of the corresponding node. Based on the standard deviation, a node's relative resilience is calculated where 1.0 means fully resilient and 0.0 not resilient at all to the simulated scenario. For more information about the properties displayed in the table take a look at the "Table Description". The shown node entities can be filtered and sorted by the given criteria in the collapsible menu of "Filter" and "Sort".

[Table Description](#) [Filter](#) [Sort](#)

By:

☐ Node name ☐ State distribution (ascending) ☒ State distribution (descending)

Entity	Initial	Distribution	Avg.	Std. Dev.	Max. Dev.	Vulnerability	Resilience
unterstützende Geräte zur Funktionskontrolle	1	1000	3.000	2.000	2	1.000	0.000
Ultraschallbecken	1	1000	3.000	2.000	2	1.000	0.000
TR-W UV Behandlung & Chlorierung BT 1.1 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
TR-W Enthärtung BT 1.1 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Telekomanlage BT 2.0 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Sterilisatoren	1	1000	3.000	2.000	2	1.000	0.000
Schwachstromsicherheitsanlagen BT 2.0 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Schachtverteiler BT 3.1 Et. -2	1	1000	3.000	2.000	2	1.000	0.000
Schachtverteiler BT 2.0 Et.-2	1	1000	3.000	2.000	2	1.000	0.000
Schachtverteiler BT 1.1 Et. -2	1	1000	3.000	2.000	2	1.000	0.000

Reinigungs- & Desinfektionsgeräte (RDG)	1		3.000	2.000	2	1.000	0.000
Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
Produktion Med. Druckluft 5 bar BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
Packtische	1		3.000	2.000	2	1.000	0.000
Osmoseanlage BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
Lüftungsanlage 17A Südtrakt Et. 2	1		3.000	2.000	2	1.000	0.000
Kälteübergabe Nord BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
Etagenverteiler BT 3.1 Technikzentrale 1A	1		3.000	2.000	2	1.000	0.000
Etagenverteiler BT 3.1 Et. 2	1		3.000	2.000	2	1.000	0.000
Etagenverteiler BT 2.0 Et.-1	1		3.000	2.000	2	1.000	0.000
Etagenverteiler BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
elektr. Zutrittskontrolle BT 2.0 Et. -1	1		3.000	2.000	2	1.000	0.000
Einschweisgerät	1		3.000	2.000	2	1.000	0.000
EDV-Netzwerk redundant	1		3.000	2.000	2	1.000	0.000
EDV-Netzwerk nicht redundant	1		3.000	2.000	2	1.000	0.000
EDV Hardware (Desktop PC in der AEMP)	1		3.000	2.000	2	1.000	0.000
Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1	1		3.000	2.000	2	1.000	0.000
Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2	1		3.000	2.000	2	1.000	0.000
Aufzüge A4-A6 BT 2.0	1		3.000	2.000	2	1.000	0.000
Aufzug A7 BT 3.1	1		3.000	2.000	2	1.000	0.000
Abwasserhebeanlage BT 2.0 Et. -2	1		3.000	2.000	2	1.000	0.000
2 Vorreinigung & Vorbereitung MP	1		2.970	1.980	2	0.990	0.010
6 Funktionskontrolle & Pflege MP	1		2.850	1.880	2	0.940	0.060
7 Verpackung Medizinprodukte	1		2.840	1.880	2	0.940	0.060
8 Sterilisation Medizinprodukte	1		2.730	1.800	2	0.900	0.100
5 Freigabe nach Prüfung Medizinprodukte	1		2.720	1.790	2	0.895	0.105
4 Sichtprüfung & manuelle Trocknung MP	1		2.690	1.770	2	0.885	0.115
3 maschinelle Reinigung & Desinfektion MP	1		2.650	1.710	2	0.855	0.145
9 Freigabe nach Sterilisation MP	1		2.560	1.680	2	0.840	0.160
1 Transport gebrauchte Medizinprodukte	1		1.420	0.650	1	0.650	0.350
10 Transport sterile Medizinprodukte	1		1.400	0.630	1	0.630	0.370
AEMP Stammdatenadministrator	1		1.360	0.600	1	0.600	0.400
Krankenhausinformationssystem	1		1.330	0.800	2	0.400	0.600
Verwaltung Leihsets	1		1.320	0.780	2	0.390	0.610
Qualitätsmanagement Software	1		1.320	0.780	2	0.390	0.610
klassische IT Office Software	1		1.310	0.780	2	0.390	0.610
Waschbecken für Vorreinigung	1		1.310	0.770	2	0.385	0.615
Fachkundige in der Aufbereitung von MP	1		1.310	0.550	1	0.550	0.450
Leitung der AEMP	1		1.300	0.550	1	0.550	0.450
Qualitätsmanager AEMP (Stellv. Leiter AEMP)	1		1.300	0.550	1	0.550	0.450
IT Hardwarespezialisten	1		1.200	0.540	1	0.540	0.460

IT Hardwarespezialisten

Technischer Dienst

IT Softwarespezialisten

Logistiker

Wartungsfirma Versorgungsanlagen

Wartungsfirma Sicherheitstechnische Anlagen

Wartungsfirma IT Hardware (Netz, DB, Server, ...)

Wartungsfirma IT Software

Wartungsfirma Sterilisator

Wartungsfirma RDG

Wartungsfirma Einschweisgerät

Gebäudeleittechnik

Etagenverteiler BT 3.2 Technikzentrale 1B

Etagenverteiler BT 3.1 Et. 1

anlagen spezifische Software

Ausfallkonzept mit 2 anderen Krankenhäusern

Serverraum Nord BT 1.3. Et. -1

Externer Transportunternehmer

Wärmeübergabe Süd BT 3.2 Et. -2

Versorgung durch Telekomanbieter BT 2.0 Et. -1

USV Stromversorgung Südtrakt Et. 2

Trinkwasserversorger

Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2

Telekomversorger

SV Übergabe & Etagenverteiler BT 3.2 Et.-1

Serverraum Süd BT 3.2 Et. -1

Schachtverteiler BT 1.3 Et. -1

Reindampfversorgung Süd BT 3.2 Et. 2

Kälteübergabe Süd BT 3.2 Et. -2

Hausdampfübergabe Süd BT 3.2 Et.2

Etagenverteiler BT 1.3 Et. -1

BHKW Wärmeversorgung

BHKW SV Stromversorgung

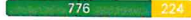
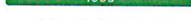
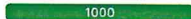
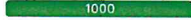
BHKW Kälteversorgung

BHKW Hausdampfversorgung

BHKW Betreiber

BHKW AV Stromversorgung

AV Übergabe & Etagenverteiler BT 3.2 Et.-1

1		1.300	0.340	1	0.340	0.400
1		1.290	0.540	1	0.540	0.460
1		1.280	0.530	1	0.530	0.470
1		1.260	0.510	1	0.510	0.490
1		1.240	0.490	1	0.490	0.510
1		1.230	0.480	1	0.480	0.520
1		1.230	0.480	1	0.480	0.520
1		1.230	0.480	1	0.480	0.520
1		1.220	0.470	1	0.470	0.530
1		1.220	0.470	1	0.470	0.530
1		1.210	0.460	1	0.460	0.540
1		1.190	0.590	2	0.295	0.705
1		1.170	0.590	2	0.295	0.705
1		1.170	0.590	2	0.295	0.705
1		1.150	0.550	2	0.275	0.725
1		1.140	0.370	1	0.370	0.630
1		1.100	0.320	2	0.160	0.840
1		1.030	0.160	1	0.160	0.840
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	1	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	1	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000

14.13.4 Dynamische Risikoanalyse - Cyberangriff

Auf den folgenden 3 Seiten sind die Ergebnisse dargestellt.

Nachstehend sind alle Knotenpunkte aufgelistet mit der Angabe wie stark der Knotenpunkt vom Anfangszustand abweicht. Mit der Standardabweichung wird die Widerstandsfähigkeit (Resilience) eines Knotenpunktes berechnet. Resilience = 1,0 bedeutet der Knotenpunkt ist gegenüber dem Szenario zu 100% widerstandsfähig, wo gegen Resilience = 0,0 bedeutet, dass der Knotenpunkte zu 0% widerstandsfähig ist.

Tabellenbeschreibung:

Eigenschaft	Beschreibung
Initial - Anfangszustand	Der Zustand des Knotens vor der Simulation.
Distribution - Verteilung	Zeigt an, wie oft der Knoten in welchem Zustand gelandet ist (wenn man mit dem Mauszeiger über den Balken fährt, wird der relative Anteil angezeigt).
Avg. - Mittelwert	Der durchschnittliche Endzustand des Knotens über alle Simulationsläufe.
Std. Dev. – Standardabweichung	Die relative durchschnittliche Abweichung vom Ausgangszustand über alle Simulationsläufe hinweg.
Max. Dev. - Max. Abweichung.	Die maximal mögliche Abweichung vom Ausgangszustand.
Vulnerability - Verwundbarkeit	Die relative Verwundbarkeit des Knotens gegenüber dem simulierten Szenario, die berechnet wird, indem die durchschnittliche relative Abweichung durch die maximal mögliche Abweichung geteilt wird (Std.Dev./Max.Dev.).
Resilience -Widerstandsfähigkeit	Die relative Resilienz des Knotens gegenüber dem simulierten Szenario, die als das Gegenteil der Verwundbarkeit dargestellt wird (1 - Verwundbarkeit).

Step 1: Select initially compromised asset(s)

Add initial trigger(s) for your network elements to the simulation. If no valid triggers for an element exist (i.e., the transition table does not have any transitions originating in the element's current state), it will be disabled in the list below.

Alert source

Serverraum Süd BT 3.2 Et. -1

Select where the alert is triggered

Trigger

Select what is triggered at Serverraum Süd BT 3.2 Et. -1

Step 2: Configure simulation scenario

Here you can find your constructed scenario of triggers initially affecting corresponding assets. You can disable triggers in order not to simulate them or remove them from the scenario by using the corresponding action buttons.

Scenario

4 / 4

Order	Asset Name	Trigger	Actions
1.	Serverraum Nord BT 1.3. Et. -1	Cyberangriff - SD	☒ ☐ ☐ ☐
2.	EDV-Netzwerk redundant	Cyberangriff - SD	☒ ☐ ☐ ☐
3.	EDV-Netzwerk nicht redundant	Cyberangriff - SD	☒ ☐ ☐ ☐

« < 1 2 > »

Step 3: Set simulation parameters and simulate

Set how many simulation runs you want to execute and, if preferred, a time step limit. The latter restricts each simulation run to the given amount of logical time steps. In order to simulate, at least one trigger has to be enabled in the scenario!

Number of simulations

-100 1000 ☒ +100

Set how many simulations should be run

Time step limit

☐ 1 ☒

Set how many simulation steps should be simulated per run or disable it

simulate

Inspector Entity Analysis Network Cases Network Metrics Entity Prognosis

Show simulation until

☐ 1 ☒

Set how many simulation steps should be shown or disable it

The table below contains a quick summary about how often nodes ended up in what *final* state in those simulations and how much they deviate in average from the initial state of the corresponding node. Based on the standard deviation, a node's relative resilience is calculated where 1.0 means fully resilient and 0.0 not resilient at all to the simulated scenario. For more information about the properties displayed in the table take a look at the "Table Description". The shown node entities can be filtered and sorted by the given criteria in the collapsible menu of "Filter" and "Sort".

Table Description

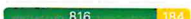
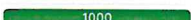
Filter

Sort

By:

☐ Node name ☐ State distribution (ascending) ☒ State distribution (descending)

Entity	Initial	Distribution	Avg.	Std. Dev.	Max. Dev.	Vulnerability	Resilience
Verwaltung Leihsets	1	1000	3.000	2.000	2	1.000	0.000
Telekomanlage BT 2.0 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Serverraum Süd BT 3.2 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Serverraum Nord BT 1.3. Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Schwachstromsicherheitsanlagen BT 2.0 Et. -1	1	1000	3.000	2.000	2	1.000	0.000
Qualitätsmanagement Software	1	1000	3.000	2.000	2	1.000	0.000
Krankenhausinformationssystem	1	1000	3.000	2.000	2	1.000	0.000
klassische IT Office Software	1	1000	3.000	2.000	2	1.000	0.000
Gebäudeleittechnik	1	1000	3.000	2.000	2	1.000	0.000
elektr. Zutrittskontrolle BT 2.0 Et. -1	1	1000	3.000	2.000	2	1.000	0.000

EDV-Netzwerk redundant	1		3.000	2.000	2	1.000	0.000
EDV-Netzwerk nicht redundant	1		3.000	2.000	2	1.000	0.000
7 Verpackung Medizinprodukte	1		2.350	1.570	2	0.785	0.215
6 Funktionskontrolle & Pflege MP	1		2.310	1.540	2	0.770	0.230
8 Sterilisation Medizinprodukte	1		2.300	1.530	2	0.765	0.235
4 Sichtprüfung & manuelle Trocknung MP	1		2.160	1.440	2	0.720	0.280
3 maschinelle Reinigung & Desinfektion MP	1		2.160	1.440	2	0.720	0.280
5 Freigabe nach Prüfung Medizinprodukte	1		2.120	1.430	2	0.715	0.285
9 Freigabe nach Sterilisation MP	1		2.100	1.390	2	0.695	0.305
EDV Hardware (Desktop PC in der AEMP)	1		2.020	1.300	2	0.650	0.350
2 Vorreinigung & Vorbereitung MP	1		1.910	1.260	2	0.630	0.370
Reinigungs- & Desinfektionsgeräte (RDG)	1		1.730	1.110	2	0.555	0.445
unterstützende Geräte zur Funktionskontrolle	1		1.710	1.090	2	0.545	0.455
Einschweisgerät	1		1.690	1.070	2	0.535	0.465
Sterilisatoren	1		1.680	1.070	2	0.535	0.465
Ultraschallbecken	1		1.280	0.530	2	0.265	0.735
Packtische	1		1.280	0.530	2	0.265	0.735
Fachkundige in der Aufbereitung von MP	1		1.280	0.530	1	0.530	0.470
Waschbecken für Vorreinigung	1		1.270	0.520	2	0.260	0.740
AEMP Stammdatenadministrator	1		1.270	0.520	1	0.520	0.480
Wartungsfirma IT Software	1		1.250	0.500	1	0.500	0.500
Wartungsfirma Sterilisator	1		1.230	0.480	1	0.480	0.520
Wartungsfirma IT Hardware (Netz, DB, Server, ...)	1		1.230	0.480	1	0.480	0.520
Wartungsfirma RDG	1		1.220	0.470	1	0.470	0.530
Qualitätsmanager AEMP (Stellv. Leiter AEMP)	1		1.220	0.470	1	0.470	0.530
Wartungsfirma Einschweisgerät	1		1.220	0.470	1	0.470	0.530
Wartungsfirma Sicherheitstechnische Anlagen	1		1.210	0.460	1	0.460	0.540
Wartungsfirma Versorgungsanlagen	1		1.210	0.460	1	0.460	0.540
IT Hardwarespezialisten	1		1.210	0.460	1	0.460	0.540
Logistiker	1		1.200	0.450	1	0.450	0.550
Technischer Dienst	1		1.200	0.440	1	0.440	0.560
Leitung der AEMP	1		1.180	0.430	1	0.430	0.570
IT Softwarespezialisten	1		1.180	0.430	1	0.430	0.570
Ausfallkonzept mit 2 anderen Krankenhäusern	1		1.160	0.400	1	0.400	0.600
Externer Transportunternehmer	1		1.030	0.180	1	0.180	0.820
Wärmeübergabe Süd BT 3.2 Et. -2	1		1.000	0.000	2	0.000	1.000
Versorgung durch Telekomanbieter BT 2.0 Et. -1	1		1.000	0.000	2	0.000	1.000
USV Stromversorgung Südtrakt Et. 2	1		1.000	0.000	0	0.000	1.000
Trinkwasserversorger	1		1.000	0.000	1	0.000	1.000
Trinkwassereinspeisung Wasserversorger BT 1.1 Et. -2	1		1.000	0.000	0	0.000	1.000
TP-W UV Behandlung & Chlorierung BT 1.1 Et. -1	1		1.000	0.000	2	0.000	1.000

TR-W Entthärtung BT 1.1 Et. -1

Telekomversorger

SV Übergabe & Etagenverteiler BT 3.2 Et.-1

Schachtverteiler BT 3.1 Et. -2

Schachtverteiler BT 2.0 Et.-2

Schachtverteiler BT 1.3 Et. -1

Schachtverteiler BT 1.1 Et. -2

Reindampfversorgung Süd BT 3.2 Et. 2

Produktion Techn. Druckluft 8 bar BT 1.1 Et. -1

Produktion Med. Druckluft 5 bar BT 1.1 Et. -1

Osmoseanlage BT 1.1 Et. -1

Lüftungsanlage 17A Südtrakt Et. 2

Kälteübergabe Süd BT 3.2 Et. -2

Kälteübergabe Nord BT 1.1 Et. -1

Hausdampfübergabe Süd BT 3.2 Et.2

Etagenverteiler BT 3.2 Technikzentrale 1B

Etagenverteiler BT 3.1 Technikzentrale 1A

Etagenverteiler BT 3.1 Et. 2

Etagenverteiler BT 3.1 Et. 1

Etagenverteiler BT 2.0 Et.-1

Etagenverteiler BT 1.3 Et. -1

Etagenverteiler BT 1.1 Et. -1

Druckerhöhungsanlage n. Osmose BT 1.1 Et. -1

Druckerhöhungsanlage für Reindampf BT 3.2 Et. -2

BHKW Wärmeversorgung

BHKW SV Stromversorgung

BHKW Kälteversorgung

BHKW Hausdampfversorgung

BHKW Betreiber

BHKW AV Stromversorgung

AV Übergabe & Etagenverteiler BT 3.2 Et.-1

Aufzüge A4-A6 BT 2.0

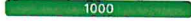
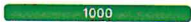
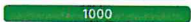
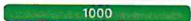
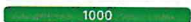
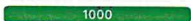
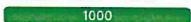
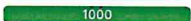
Aufzug A7 BT 3.1

anlagen spezifische Software

Abwasserhebeanlage BT 2.0 Et. -2

10 Transport sterile Medizinprodukte

1 Transport gebrauchte Medizinprodukte

		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	1	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	1	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	0	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	2	0.000	1.000
1		1.000	0.000	1	0.000	1.000
1		1.000	0.000	1	0.000	1.000

14.14 Mindmap der Literaturrecherche

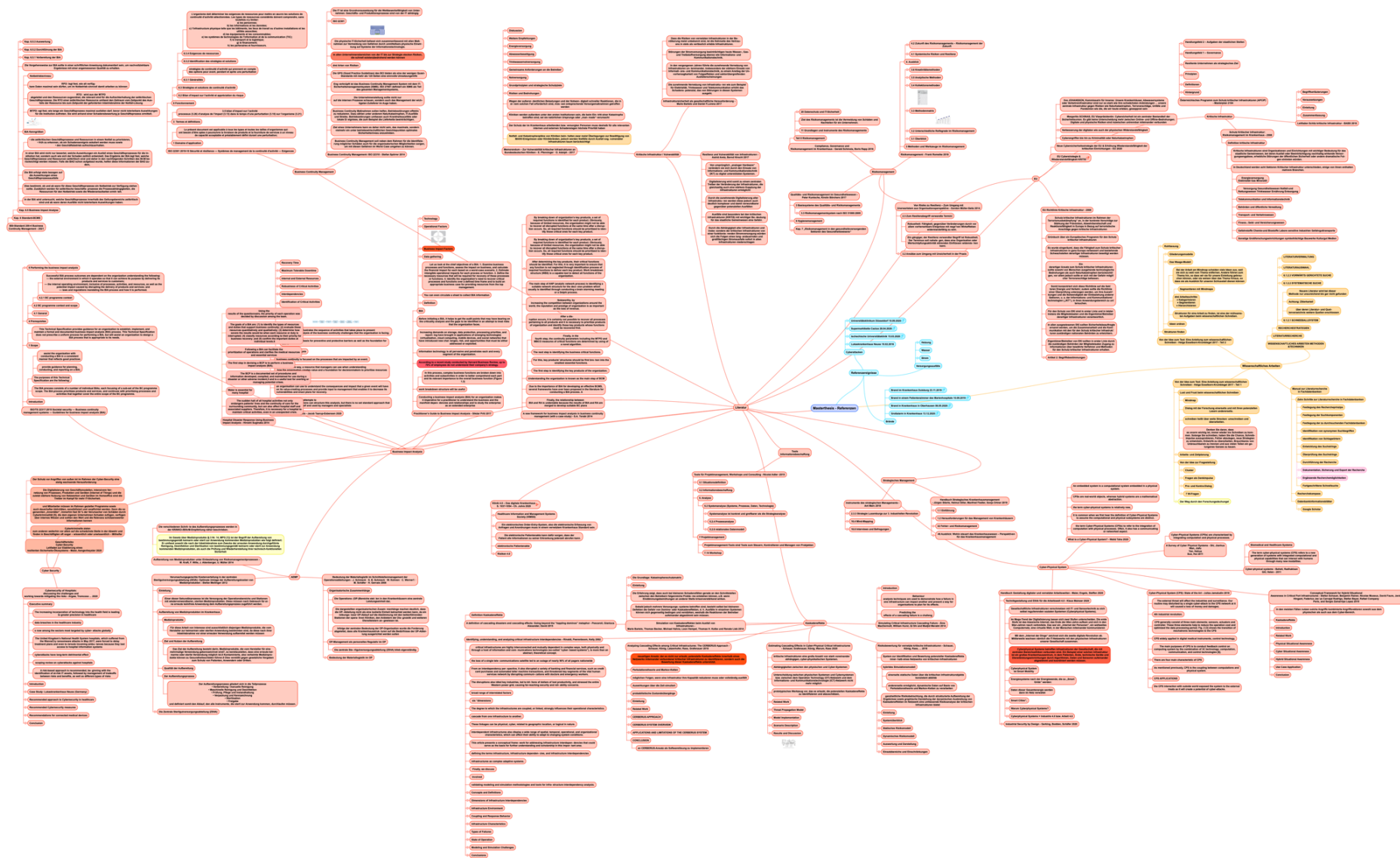


Abbildung 85: Mindmap der Literaturrecherche