



TECHNISCHE
UNIVERSITÄT
WIEN

Diplomarbeit

Design und Entwicklung eines Phasenmodells für die Zustandsüberwachung mittels Anomalieerkennung einer Industrieofenanlage

**Design and Development of a Phase Model for Condition Monitoring using Anomaly
Detection in the Use Case of Industrial Furnace Plant**

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

Diplom-Ingenieurs

unter der Leitung von

Priv.-Doz. Dr.-Ing. Fazel Ansari, MSc

(E330 Institut für Managementwissenschaften, Forschungsbereichs Betriebstechnik, Systemplanung,
Forschungsgruppe Smart and Knowledge-Based Maintenance)

Dipl.-Ing. Klaudia Kovacs

(E330 Institut für Managementwissenschaften, Forschungsbereichs Betriebstechnik, Systemplanung,
Fraunhofer Austria Research GmbH)

eingereicht an der Technischen Universität Wien

Fakultät für Maschinenwesen und Betriebswissenschaften

von

Thaddäus Paul Lechenauer, BSc

01325747

Wien, im Oktober 2021

Vorname Nachname



TECHNISCHE
UNIVERSITÄT
WIEN

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

Diplomarbeit

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Ich erkläre außerdem Eides statt, dass ich meine Diplomarbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen selbstständig ausgeführt habe und alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur, genannt habe.

Ferner erkläre ich, dass ich dieses Diplomarbeitsthema bisher weder im In- noch Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Wien, im Oktober 2021

Thaddäus Lechenauer

Danksagung

Zu Beginn dieser Diplomarbeit sei ein großer Dank an all diejenigen ausgesprochen, die mich bei der Erstellung der vorliegenden Arbeit unterstützt haben.

Allen voran gilt mein Dank meinem Hauptbetreuer der Diplomarbeit Herrn Priv.-Doz. Dr. Ing. Fazel Ansari, der durch seine Anregungen und konstruktive Kritik bei der Erstellung maßgeblich mitgewirkt hat. Darüber hinaus möchte ich mich besonders bei Frau DI Klaudia Kovacs bedanken, die mich durch ihre hilfsbereite sowie zielgerichtete Art und praktischen Anregungen optimal mitbetreut hat.

Ohne meine Unigruppe wäre das Studium an der TU Wien nicht das gleiche gewesen. Anna, Arthur, Christopher, Constanze, Eleonore, Konrad, Leona, Paul und Stanislaus ihr wart ein unverzichtbarer Rückhalt auch in harten Zeiten. Vielen lieben Dank euch allen für diese unvergessliche Zeit.

Ferner gilt auch meiner lieben Cousine Ulrike ein besonderer Dank. Mit ihrer strengen Korrektur der sprachlichen Umsetzung und ihren wertvollen Kommentaren zur wissenschaftlichen Aufbereitung hat sie die vorliegende Diplomarbeit verfeinert.

Mein größter Dank aber gilt meiner Familie. Ohne die ununterbrochene Unterstützung auf allen Ebenen und die motivierenden Worte meiner Eltern Hedwig und Paul sowie meiner lieben Schwester Hedwig wäre mein Studium nicht möglich gewesen.

Thaddäus Lechenauer

Wien, im Oktober 2021

Kurzfassung

Mit der Entwicklung von cyber-physischen Produktionssystemen (CPPS) als Schlüsseltechnologie in der Industrie 4.0 findet auch ein Paradigmenwechsel von deskriptiver hin zu präskriptiver Instandhaltung statt. Mit jener Entwicklung einhergehend gewinnen somit sensorbasierte bzw. datengetriebene Instandhaltungsstrategien zunehmend an Bedeutung im Instandhaltungsmanagement. Besondere Aufmerksamkeit wird hierbei kritischen und hochkomplexen Anlagen zuteil, wo ungeplante Stillstände unter anderem zu langen Ausfallzeiten und somit zu besonders hohen Ausfallkosten führen. Diese hochkomplexen Anlagen werden in den meisten Fällen mit einer zuverlässigkeitsorientierten Instandhaltungsstrategie betrieben. Für einen Umstieg aber auf eine datengetriebene Strategie fehlen im Umkehrschluss Ausfallsdaten, da Ausfälle stets weitestgehend vermieden werden. Somit kann eine gängige datengetriebene Zustandsüberwachung (Condition Monitoring, CM) erschwert angewendet werden, da eine entsprechende Datengrundlage fehlt. Durch bisherige Forschung konnte gezeigt werden, dass Anomalieerkennung in den Datensätzen einen möglichen Lösungsansatz für diese Aufgabestellung darstellt.

Ziel der Diplomarbeit ist es, mittels Anomalieerkennungsalgorithmen aus dem Bereich des maschinellen Lernens (ML) unter der gegebenen schwierigen Datenlage festzustellen, ob eine komplexe und hochkritische Anlage wie erwartet operiert oder nicht. Sollten Abweichungen sprich Anomalien in den Daten erkannt werden, muss das Anlagenpersonal entsprechend informiert werden, sodass in Folge die Ursache dieser ermittelt und behoben werden kann. Dazu werden die Forschungsschwerpunkte Zustandsüberwachung komplexer Anlagen, Informationsgewinnung unter schlechter Datenausgangslage bzw. fehlenden Ausfallsdaten und Anomalieerkennung für CM miteinander verknüpft.

Ergebnis der Diplomarbeit ist ein Phasenmodell für die Umsetzung eines CM mittels Anomalieerkennung, das eine Ablauflogik für diesen Zweck bereitstellt und als Grundlage für einen Softwareprototyp verwendet werden kann. Mit dem entwickelten Modell kann unter Zuhilfenahme passender ML-Algorithmen der Zustand einer komplexen Anlage ohne Daten über die Ground Truth oder zum jeweiligen Ausfallsverhalten überwacht werden. Mittels Anomalieerkennung in den Mess- und Maschinendaten kann ein abnormales Verhalten einer Anlage detektiert werden und so auf eventuellen Instandhaltungsbedarf geschlossen werden.

Eine Fallstudie aus dem Bereich industrieller Wärmebehandlungsanlagen zeigt die Anwendbarkeit des Phasenmodells für komplexe Industriemaschinen. Mit einer entsprechenden Visualisierung über ein Dashboard können dem Instandhaltungspersonal die Ergebnisse aus dem Anomalieerkennungsprozess verständlich kommuniziert werden.

Schlagwörter zur Arbeit: zustandsbasierte Instandhaltung, Condition Monitoring, Anomalieerkennung, Maschinelles Lernen, Phasenmodell, Indifferenter Datensatz

Abstract

With the emergence of cyber physical production systems (CPPS) as one of the enabling technologies for Industry 4.0, there is a fundamental shift from descriptive towards prescriptive maintenance. Along with this transformation, sensor-based and data-driven maintenance management strategies are becoming increasingly important. Significant attention is paid to critical and highly complex plants, where unplanned downtimes lead to overlong maintenance times and thus to particularly high downtime costs. In most cases, these highly complex plants are operated with a reliability-centered maintenance strategy. For a changeover to a data-driven condition-based strategy, however, there is a lack of failure data, as failures are always avoided as far as possible. Thus, a common data-driven condition monitoring (CM) cannot be applied, since a corresponding data basis is missing. Previous research has shown that anomaly detection in data is a possible solution to this problem.

Aim of this thesis is to apply machine learning (ML) methods, in particular anomaly detection algorithms under the given indifferent data situation to determine whether a complex and highly critical plant is operating as expected or not. If deviations, i.e. anomalies, are detected in the data, the plant personnel must be informed accordingly so that the root-cause of these can subsequently be determined and remedied. For this purpose, the research areas of CM, information extraction under a poor initial data situation or missing failure data and anomaly detection for CM are linked with each other.

The result of the thesis is a qualitative phase model for CM using anomaly detection, which provides a logic for the given purpose and can be used as a software prototype. Using suitable ML algorithms, the state of a complex plant can be assessed with the developed model without data on the ground truth or the respective failure behavior. By means of anomaly detection in the measurement and machine data, abnormal behavior of a plant can be detected and thus, a possible need for maintenance can be concluded.

A case study from the field of industrial heat treatment plants demonstrates the applicability of the phase model for complex industrial machines. With a corresponding visualization via a dashboard, the results from the anomaly detection process can be communicated to the maintenance staff in a comprehensible way.

Key words: condition-based maintenance, condition monitoring, anomaly detection, machine learning, phase model, indifferent data

Inhaltsverzeichnis

1	Einleitung.....	3
1.1	Problemstellung, Ziele und Forschungsfragen.....	3
1.2	Verwendete Methoden	6
1.2.1	Design Science Methode	6
1.2.2	Internet- und Literaturanalyse	8
1.2.3	Proof-of-Concept.....	10
1.3	Struktur der Arbeit	10
2	Theoretische Grundlagen	12
2.1	Instandhaltung und Instandhaltungsstrategien.....	12
2.1.1	Instandhaltungsmanagementstrategien	14
2.1.2	Strategien ohne Einsatz von Sensorik und Computertechnologie	14
2.1.3	Strategien mit Einsatz von Sensorik und Computertechnologie	15
2.1.4	Instandhaltung in Sinne von wissensbasierten Systemen	17
2.2	Condition Monitoring.....	19
2.2.1	Vor- und Nachteile von Condition Monitoring.....	20
2.2.2	Stufen des Condition Monitoring	21
2.2.3	Datenakquirierung	23
2.3	Data Mining und Maschinelles Lernen	24
2.3.1	Data Mining	25
2.3.2	Maschinelles Lernen (ML).....	26
2.4	Anomalieerkennung.....	28
2.4.1	Arten von Anomalien	29
2.4.2	Herausforderungen der Anomalieerkennung	30
2.4.3	Drei grundlegende Ansätze zur Anomalieerkennung.....	31
2.4.4	Anomalieerkennung mit Hilfe des Maschinellen Lernens	32
2.4.5	Exkurs: Statistische Techniken zur Anomalieerkennung	33
3	Stand der Technik.....	35
3.1	CM für kritische und hochkomplexe Anlagen	35
3.1.1	Aufbau des morphologischen Kastens für die Analyse.....	36
3.1.2	Einzelanalyse der Dimensionen.....	39
3.2	Informationsgewinnung unter fehlender bzw. begrenzter Ground-Truth- und Ausfallsdatenlage.....	44

3.2.1	Merkmalsextraktion für Zeitreihen	45
3.2.2	Aufbau des morphologischen Kastens für die Analyse	47
3.2.3	Analyse der Dimensionen	49
3.3	Anomalieerkennung für CM	53
3.3.1	Aufbau des morphologischen Kastens für die Analyse	54
3.3.2	Auswertung der Analyse	55
3.4	Zusammenfassung der Literaturanalyse	58
4	Phasenmodell für CM mittels AE	62
4.1	Überblick über das Phasenmodell	62
4.2	Datenebene	63
4.3	Verarbeitungs- und Analyseebene: Verarbeitung	63
4.3.1	Preprocessing	63
4.3.2	Datensplitting	64
4.3.3	Merkmalsextraktion	64
4.3.4	Normalisierung	65
4.4	Verarbeitungs- und Analyseebene: Analyse	66
4.4.1	Erstellung Datenmodell und Anomaliedetektion	66
4.4.2	Anomalie Scores (Anomaliefaktor)	74
4.4.3	Alarmlogik mit Falschalarmfilter	76
4.4.4	Ergebnisvisualisierung	77
4.5	Nutzerebene	77
4.5.1	Dashboard	77
4.5.2	Evaluierung und Ableitung Instandhaltungsmaßnahmen	78
5	Validierung	79
5.1	Datenebene	79
5.1.1	Einführung in den Anwendungsfall	79
5.1.2	Einblick in die Rohdaten	80
5.2	Verarbeitungs- und Analyseebene: Verarbeitung	84
5.2.1	Preprocessing und Informationsgewinnung	84
5.3	Verarbeitungs- und Analyseebene: Analyse	87
5.3.1	Erstellung Datenmodell und Anomaliedetektion	87
5.3.2	Anomalie Scores und Alarmlogik mit Falschalarmfilter	97
5.3.3	Ergebnisvisualisierung	98
5.4	Nutzerebene	100

5.4.1	Prototyp Dashboard	100
5.4.2	Evaluierung und Ableitung Instandhaltungsmaßnahmen.....	102
5.4.3	Auswahl der Algorithmen	103
5.4.4	Identifizierte anomale Signalverläufe	105
6	Zusammenfassung und Ausblick.....	107
6.1	Kritische Reflexion auf die Forschungsfragen	107
6.2	Abgleich der Ziele für die Bearbeitung der Fallstudie.....	109
6.3	Eingrenzung der Arbeit.....	112
6.4	Ausblick	112
7	Anhang	114
7.1	Informationen zu Software Prototyp	114
7.2	Zusätzliche Darstellung für PoC der unüberwachten Ansätze	114
7.2.1	Darstellung zum statistischen Ansatz.....	114
7.2.2	Darstellungen zum unüberwachten Ansatz.....	116
7.2.3	Darstellungen zu den halbüberwachten Ansätzen	119
7.2.4	Darstellungen zum signalgruppenbasierten Ansatz	122
7.2.5	Weitere Beispiele von Dashboards	123
7.2.6	Zusätzliche Darstellungen zu Kapitel 5.4.4	125
8	Literaturverzeichnis.....	127
9	Abbildungsverzeichnis	136
10	Formelverzeichnis	139
11	Tabellenverzeichnis	140
12	Abkürzungsverzeichnis	142

1 Einleitung

Unternehmen sind an mehreren Fronten mit massivem Druck und massiver Dynamik konfrontiert. Außerhalb des Unternehmens entwickeln sich Technologie, Markt und Konkurrenz stetig und auch mit zunehmender Geschwindigkeit weiter. Zusätzlich gestalten sich innerhalb der Unternehmen organisatorische Veränderungen, produkt- und produktionsspezifische Anforderungen sowie notwendige hohe Flexibilität sehr herausfordernd für die jeweiligen Firmen und deren Akteure. Daher ist es umso wichtiger, dass Unternehmen eine funktionierende und schlagkräftige Instandhaltung haben, um dadurch Produktionsstörungen zu vermeiden und in Folge dessen auch ein besseres Betriebsergebnis zu erwirtschaften.¹ Die Hauptaufgabe der Instandhaltung ist die Sicherstellung der Funktionstüchtigkeit von Werkzeugen, Maschinen und Anlagen, sodass diese ihre zugewiesenen Aufgaben erfüllen können. Mit der Entwicklung von cyberphysischen Produktionssystemen (CPPS) als Schlüsseltechnologie in der Industrie 4.0 findet ein Paradigmenwechsel von deskriptiver hin zu präskriptiver Instandhaltung statt. Ansätze für das Instandhaltungsmanagement verändern sich in zunehmenden Maß zu (halb-) automatischen wissensbasierten Unterstützungssystemen zur Entscheidungsfindung.² Mit jener Entwicklung einhergehend gewinnen im Instandhaltungsmanagement auch sensorbasierte bzw. datengetriebene Instandhaltungsstrategien zunehmend an Bedeutung (siehe Kapitel 2.1.3 auf S.15).

Die vorliegende Arbeit beschäftigt sich mit der Entwicklung eines Phasenmodells, mit dem ein theoretisches Fundament für die Zustandsüberwachung mittels Anomalieerkennung kritischer und hochkomplexer Anlagen geschaffen wird. Die Zustandsüberwachung zielt darauf ab, Informationen über das beobachtete System zu liefern.

1.1 Problemstellung, Ziele und Forschungsfragen

Besondere Aufmerksamkeit wird in der Instandhaltung kritischen und hochkomplexen Anlagen zuteil, bei denen ungeplante Stillstände unter anderem zu langen Ausfallzeiten und somit zu besonders hohen Ausfallkosten führen. Diese hochkomplexen Anlagen werden so betrieben, dass sie bis zur nächsten geplanten Wartung mit hoher Zuverlässigkeit fahren können (*Reliability Centered Maintenance*, RCM).

Im Umkehrschluss bedeutet dies für derart betriebene Anlagen aber, dass wenige oder gar keine Ausfalldaten vorliegen. Das führt dazu, dass gängige datengetriebene Zustandsüberwachungssysteme (*Condition Monitoring System*, CMS) erschwert angewendet werden können. Konventionell überwachende CMS lösen Instandhaltungsmaßnahmen basierend auf Grenz-/ Alarmwerten der einzelnen Parameter (z.B. Temperatur, Schwingungsausschlag) aus. Es werden sozusagen gesunde und fehlerhafte Zustände miteinander verglichen. Diese starren, regelbasierten Lösungen versagen aber bei komplexen dynamischen Systemen. Zusätzlich ist es schwieriger, mit jenen Daten zuverlässige (korrekte) Prognosemodelle über den zukünftigen Zustand der Maschine zu berechnen. Bei der RCM

¹ vgl. Schenk, 2010, S.VII

² vgl. Ansari et al., 2019, S.1; vgl. ebenda, S.9

Instandhaltungsstrategie werden gewisse Teile daher frühzeitig getauscht, obwohl diese eventuell noch für längere Zeit funktionstüchtig gewesen wären. Diese verfrühten Maßnahmen führen zu unnötig hohen Instandhaltungskosten, welche durch erhöhten Personal-, Zeit- und Materialaufwand bedingt sind.

Es konnte durch bisherige Forschung bereits gezeigt werden, dass Anomalieerkennung (AE) in den Datensätzen einen möglichen Lösungsansatz für diese Aufgabenstellung darstellt.³ Die Detektion von Abnormalitäten oder Anomalien ermöglicht die Aufklärung von unüblichen Werten oder Ausreißern, die nicht in den normalen (gesunden) Datensatz oder zu erwarteten Abfolgen (Pattern) passen. Diese erkannten Anomalien können als frühzeitige Anzeichen für Maschinen- oder Bauteilversagen gesehen werden.⁴ Auf Basis jener detektierten Abweichungen in den Sensordaten soll in Folge ein Alarm ausgelöst, Instandhaltungsmaßnahmen eingeleitet und somit eine kritische Abnutzung oder gar ein Stillstand vermieden werden.

Neben der fachlich richtigen Anwendung der verschiedenen Algorithmen stellt auch die Interpretation der Ergebnisse ein Problem dar. Eine geeignete (Input-) Datenqualität muss sichergestellt werden. Das *Ground Truth* Problem – aktuelle Daten reichen nicht aus um Fehlerklassen (*Cluster*) zu definieren – erschwert die Datenanalyse. Es fehlt die Definition (in den Parametern), was eine Anomalie ist und was nicht. Nur ein bedingter Einblick in das Verhalten der einzelnen Parameter ist vorhanden: so liegen keine beschreibenden Eigenschaften (Mittelwert, Verteilung etc.) zu den einzelnen Parametern vor und der Zusammenhang der Parameter untereinander (Multidimensionalität des Datensatzes) ist nicht bekannt. Dies spiegelt eine der Herausforderungen von CPPS wider, nämlich Wissen aus heterogenen Daten zu generieren.⁵

Für Anlagenbetreiber bergen diese Maschinendaten ein immenses Potenzial zur Optimierung der eigenen Produktions- und Wartungsprozesse. Für den Maschinenbauer (*Original Equipment Manufacturer*, OEM) liegen die Potenziale in höheren Serviceumsätzen, zufriedeneren Kunden, neuen Dienstleistungen und möglichen neuen Geschäftsmodellen.⁶ Eine weiteres Problemfeld, das in dieser Arbeit beleuchtet werden soll, ist die begrenzte Verfügbarkeit von wissenschaftlichen Arbeiten zum Thema CM mittels Anomalieerkennung von kritischen Anlagen. Hierzu werden Arbeiten untersucht, die sich mit Themengebieten der Wärmebehandlungs-, Prozessindustrie und kritischen Energieanlagen (Nukleare Anlagen) beschäftigen. Diese Industriefelder sind durch ähnliche Gegebenheiten gekennzeichnet.

Tabelle 1: Ausgangslage und Problemfelder

P1	Es werden große Datenmengen gesammelt, aber keine Informationen (oder in schlechter Qualität) über das Ausfallverhalten der Wärmebehandlungsanlage. Dies führt zum sogenannten Ground-Truth-Problem für die weiterführende Datenverarbeitung.
P2	Ein konventionelles CMS mit statischen Grenz-/ Alarmwerten lässt sich nicht umsetzen.
P21	Statische Alarmwerte erzeugen falsche Alarmer (False positives) oder lösen trotz kritischen Zustandes nicht aus.
P22	CM mit statischen Alarmwerten berücksichtigen weder das dynamische und komplexe Verhalten der Anlage noch saisonale Einflüsse.

³ vgl. Kamat & Sugandhi, 2020, S.2

⁴ vgl. ebenda, S.2

⁵ vgl. CPS-Week, 2008, S.10

⁶ vgl. Traphöner, 2018, S.2

P3	Es ist nur ein bedingter Einblick in das Verhalten der einzelnen Parameter vorhanden.	
	P31	Es liegen keine beschreibenden Eigenschaften (Mittelwert, Verteilung, etc.) zu den einzelnen Parametern vor.
	P32	Man kennt den Zusammenhang der Parameter untereinander nicht.
P4	Die Anwendung von Algorithmen für das CM und die darauffolgende Ergebnisinterpretation erfordert Expertenwissen.	
P5	Es liegen keine Datenanalysealgorithmen vor.	

Im Zuge dieser Diplomarbeit sollen Datenanalysealgorithmen aus dem Bereich des maschinellen Lernens für ein CMS analysiert und bewertet werden. Es soll geklärt werden, ob es möglich ist, ein CMS für hochkomplexe Anlagen unter jenen datentechnisch schwierigen Umständen einzuführen, sodass eine proaktive Instandhaltung für diese Art von Anlagen ermöglicht wird und Schäden frühzeitig erkannt und minimiert werden können. Die Anomalieerkennungsalgorithmen werden sodann an einem Industrie-Use-Case eines etablierten österreichischen Herstellers von Industrieöfen validiert. Hier wurde eine Wärmebehandlungsanlage mit Sensorik nachgerüstet (*Retrofitting*), um so Daten über den Zustand der Anlage sammeln zu können. Dadurch wurde die Anlage formal zu einem CPPS, weil eben die physikalische und die virtuelle Welt miteinander verschmolzen wurden.⁷

Basierend auf der identifizierten Problemstellung wurden Ziele der Diplomarbeit abgeleitet. Diese Ziele sind in Tabelle 2 zusammengefasst dargestellt.

Tabelle 2: Ziele der Diplomarbeit

Z1	Passende Merkmale (Features) zur Beschreibung des Zustandes finden
Z2	Passende Anomalieerkennungsalgorithmen finden (auch mit der Integration von mehrerer Entscheidungsvariablen)
Z3	Anomalien erkennen und in Kategorien einteilen
Z4	Anomaliebewertungsskala definieren
Z5	Einheitlichen Anomaliebericht entwickeln und Ergebnisse interpretieren
Z6	Intelligentes Alarmsystem entwickeln: Regeln definieren, wann Alarm ausgelöst werden sollte
Z7	Qualitatives Phasenmodell für das CM mittels Anomalieerkennung entwickeln, das als Grundlage für einen Software-Prototyp verwendet werden kann

Daraus ergeben sich Forschungsfragen und diese werden daher wie folgt formuliert: (Es gibt eine Hauptforschungsfrage (FF1) mit vier Unterpunkten (FF1.X).)

Tabelle 3: Hauptforschungsfrage mit vier Unterpunkten

FF1	Wie kann man für hochkritische Anlagen unter fehlender bzw. begrenzter Ground-Truth- und Ausfallsdatenlage ein CM System aufbauen?	
	FF11	Mit welcher Methode der AE können außergewöhnliche Zustände festgestellt werden? Wie kann tatsächlich ein Mehrwert für die zustandsbasierte Instandhaltung generiert werden?
	FF12	Wie können die Ergebnisse aus der Datenverarbeitung kommuniziert und sinnvoll interpretiert werden?
	FF13	Wie können detektierte Anomalien einheitlich quantitativ bewertet werden?
	FF14	Wie können die berechneten Ergebnisse in ein intelligentes Alarmsystem verpackt werden, sodass es für die Zustandsüberwachung der Anlage verwendet werden kann?

Bei der Formulierung der Forschungsfragen wird ein allgemein gültiger Ansatz verfolgt, sodass die Ergebnisse über den oben genannten Anwendungsfall hinaus von Nutzen sind. Der

⁷ vgl. Matyas, 2018, S.138

Zusammenhang zwischen den Problemfeldern, den Zielen und den daraus abgeleiteten Forschungsfragen lässt sich wie folgt skizzieren:

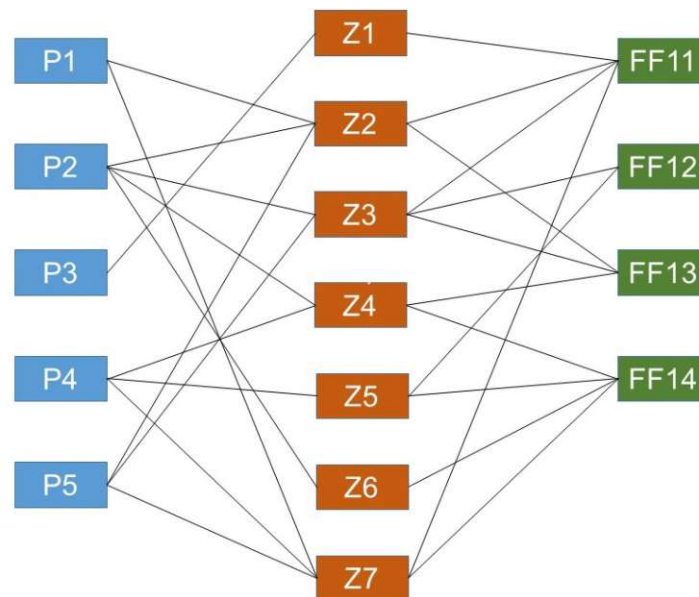


Abbildung 1: Zusammenhang Problemfelder, Ziele und den vier Unterpunkten der Hauptforschungsfrage

Abgrenzung: am Use Case der Industrieofenanlage soll keine Ursachendiagnose im Sinne einer Fehlermöglichkeitseinflussanalyse (FMEA) durchgeführt werden, sondern eventuelle Anomalien in den Daten erkannt und interpretiert werden. Es soll auch kein Prognosemodell erstellt werden. Es gilt, eine fundierte Datengrundlage für eventuelle weitere Prognosemodelle (*Predictive Maintenance*, siehe Kapitel 2.1.3 auf S.15) zu schaffen. Es sollten somit nur Abweichungen vom Gutzustand detektiert werden.

1.2 Verwendete Methoden

In diesem Unterkapitel werden die gewählten und verwendeten Methoden dargelegt. Die wichtigste Methode ist jene der Gestaltungswissenschaft (*Design Science*), da sie den konzeptionellen Rahmen für die Erstellung dieser wissenschaftlichen Arbeit darstellt. Zur Analyse der aktuell verfügbaren Information und zur Informationsgewinnung wird die Literatur- bzw. Internetrecherche verwendet. Um die Ergebnisse der Algorithmen beurteilen zu können, werden statistische Kennzahlen herangezogen.

1.2.1 Design Science Methode

Eines der Ziele dieser Diplomarbeit ist unter anderem die Entwicklung eines Phasenmodells, welches zukünftig als Grundlage für einen Software-Prototyp verwendet werden kann. Zur Erstellung dieses Modells wird die Design Science Methode von A. R. Hevner et al. (2004) verwendet, die für Informationssysteme (IS) entwickelt wurde. Dieser unterscheidet zwei komplementäre Forschungsparadigmen in der wissenschaftlichen Forschungsarbeit - Behaviorismus und Gestaltungswissenschaften:⁸

⁸ vgl. Hevner et al., 2004, S.76

Paradigma des Behaviorismus (der Verhaltenswissenschaften): Es wird versucht, Gesetze und Prinzipien zu entwickeln, „[...] um organisatorische Phänomene in Zusammenhang mit Analyse, Entwurf, Implementierung, oder Management von Informationssystemen zu erklären [...]“⁹ und vorauszusagen. Es wird dabei untersucht, wie bestehende Artefakte (Modell, Methoden, Konstrukte und Systeme) auf Menschen und Organisationen wirken.¹⁰

Paradigma der Gestaltungswissenschaften: Es werden Artefakte erschaffen und evaluiert, die identifizierte organisatorische Probleme behandeln und lösen sollen. „Die entwickelten Artefakte können indirekt menschliches oder organisatorisches Verhalten beeinflussen und somit Einfluss auf die Gesetze der Behavioral Science nehmen.“¹¹

Die Design Science Methode bietet Richtlinien für die Erfassung eines wissenschaftlichen Problems und zur Modellentwicklung für die Problemlösung. Es werden sieben Richtlinien angegeben:

1. **„Design als zielgerichtetes Artefakt:** Das Ergebnis von Designwissenschaft stellt ein innovatives, zielgerichtetes Artefakt dar, um ein Problem zu lösen.
2. **Problemrelevanz:** Das Ziel von Designwissenschaft ist die Entwicklung technischer Lösungen für wichtige aktuelle und zukünftige Probleme in Unternehmungen. Relevanz wird über den Nutzen definiert, den eine Lösung stiftet.
3. **Evaluierung:** Nutzen, Qualität und Effizienz eines Artefaktes müssen durch adäquate wissenschaftliche Methoden evaluiert werden.
4. **Beitrag der Forschung:** Designwissenschaft muss einen klar definierbaren Beitrag zur Problemlösung und/oder den Forschungsmethoden der Disziplin liefern. Die Innovationshöhe eines Beitrages kann in Bezug auf die Neuigkeit, die Allgemeingültigkeit und die Bedeutung eines Artefaktes für einen Anwendungsbereich gezeigt werden.
5. **Methodische Stringenz in den Forschungsmethoden:** Designwissenschaft erfordert die stringente Anwendung wissenschaftlicher Methoden in der Schaffung und in der Evaluierung von Artefakten.
6. **Design als Suchprozess:** Design stellt einen Suchprozess dar, in dem Lösungen vorgeschlagen, verfeinert und evaluiert werden, und damit schrittweise eine Wissensbasis aufbauen.
7. **Weitergabe von Forschungsergebnissen:** Die Ergebnisse von Designwissenschaft müssen sowohl technologieorientierten als auch managementorientierten Interessenten effektiv vermittelt werden können.“¹²

Am Ende des Designprozesses steht als Ergebnis ein nützliches Artefakt, das dazu verwendet wird, ein wichtiges Problem innerhalb des Verwendungsrahmens anzusprechen und zu lösen. Das Artefakt muss ausreichend dokumentiert sein, sodass eine Einführung und eine darauffolgende Anwendung möglich werden.

⁹ Bichler, 2006, S.133

¹⁰ vgl. Nemeth, 2020, S.11

¹¹ ebenda, S.11f

¹² Bichler, 2006, S.134

1.2.2 Internet- und Literaturanalyse

Die Methode der Literaturanalyse und insbesondere die der Internetliteraturanalyse erfüllt in der vorliegenden Arbeit zweierlei Aufgaben. Zum einen werden das Thema betreffende theoretische Grundlagen in Erfahrung gebracht und zum anderen wird damit der aktuelle Forschungsstand in jenem Forschungsgebiet erhoben. Beim letzteren geht es auch unter anderem darum, die Grenzen der vorliegenden Literatur zu identifizieren und Forschungsbedarf/ -lücken aufzuzeigen.

Eine Literaturanalyse kombiniert eine Zusammenfassung sowie kritische Betrachtung von wichtiger Information aus verschiedenen Quellen und eine Reorganisation der gesammelten Information. Zum Sammeln der Information werden wissenschaftliche Artikel, (Fach-)Bücher und andere Quellen zu einem gewissen Thema oder Themenbereich durchsucht. Folgende Fragen sollten danach beantwortet sein:

- Was wurde zu einem Thema veröffentlicht?
- Wer sind die relevanten Autoren?
- Was sind die vorherrschenden Theorien und Hypothesen?
- Welche Forschungsfragen werden gestellt?
- Welche Methode und Methodologie hat sich als adäquat und zielführend herausgestellt?¹³

Um für LeserInnen der Arbeit die Zuverlässigkeit und Validität der Literaturanalyse beurteilbar zu machen, muss der Verfasser der Analyse die benutzten Kriterien offenlegen:

- Forschungsfragen formulieren
- Aufnahme- und Ausschlusskriterien festlegen
- Literatur vorauswählen
- Qualität der Literatur beurteilen und Literatur in Analyse aufnehmen
- aufgenommene Literatur analysieren, Kernaussagen zusammenfassen und aufbereiten¹⁴

An die eben genannte Vorgehensweise und an Nemeth (2020) angelehnt soll nun der Gang der Untersuchung für die State-of-the-Art-Analyse hier dargestellt werden:

Tabelle 4: Gang der Untersuchung

Nr.	Prozessschritt	Beschreibung
1	Forschungsfragen formulieren	<p>Folgende Themengebiete werden untersucht:</p> <ol style="list-style-type: none"> 1. CM für hochkomplexe Anlagen 2. Informationsgewinnung unter fehlender bzw. begrenzter Ground-Truth- und Ausfallsdatenlage 3. Anomalieerkennung für CM <p>Daraus werden für die Literatursuche und -selektion Literaturfragen abgeleitet:</p> <ol style="list-style-type: none"> 1. Was charakterisiert hochkomplexe kritische Anlagen und wie wird deren Zustand überwacht? 2. Welche Techniken und Algorithmen werden angewendet, um das Problem der schwierigen Ground-Truth-Datenlage zu überwinden?

¹³ vgl. Ramdhani et al., 2014, S.48

¹⁴ vgl. ebenda, S.49

Nr.	Prozessschritt	Beschreibung
		3. Welche Möglichkeiten gibt es zur AE im CM mit besonderem Bezug zur Instandhaltung?
2	Aufnahme- und Ausschlusskriterien festlegen	Die hier angeführten Kriterien sind Anhaltspunkte dafür, ob eine Publikation in die weitere Literaturanalyse aufgenommen wird oder nicht: <ul style="list-style-type: none"> • Stichwörter: Condition Monitoring, Health Monitoring, Fault Detection, Diagnostics; Critical Plants (Machinery, Assets, Infrastructure, Power Plants, Nuclear Plants, Thermal Plants); Industrial Furnace (Oven), Thermal Treatment, Thermal Processing; Data Driven (Based) Maintenance; Ground-Truth-Problem, Missing Value, Imbalanced Data Set, Data Imputation; Feature Extraction (Selection); Anomaly (Novelty, Outlier) Detection; Anomaly Detection in Maintenance; Industrial Analytics • Zeitraum: 2010-2020 • Sprache: Deutsch und Englisch • Vorwiegend betrachtete Literaturarten: akademische Artikel, Bücher und Buchkapitel, Konferenz- und Journalschriften
3	Literatur vorauswählen	Anhand der oben gewählten Kriterien werden potentielle Publikationen ausgewählt und in den „Kandidatenkanon“ aufgenommen. Im Fokus stehen dabei primäre und sekundäre Literaturquellen, die über Online Bibliothekskataloge und Literaturdatenbanken gesucht und bezogen wurden. Beispiele für Datenbanken sind: <ul style="list-style-type: none"> • Google Scholar • ResearchGate • Science Direct • IEEE Xplore • Springer Über den Titel der Publikation, die Stichwörter (Keywords) und durch das Lesen des Abstracts (und sonstigem Anlesen, Querlesen) wird eine Vorauswahl und eine Aussage über die generelle Relevanz für die Arbeit getroffen. Dieser Prozessschritt stellt somit in der literarischen Materialauswahl die Beschaffung dar. ¹⁵
4	Qualität der Literatur beurteilen und in Analyse aufnehmen	Hat die Publikation den ersten Filter (Prozessschritt Nr. 3) passiert, muss diese nun bewertet und auf Eignung für die Weiterverwendung in der Literaturanalyse geprüft werden. Auch in diesem Schritt kann eine Publikation noch ausscheiden. <ul style="list-style-type: none"> • Die verwendete Quelle muss „<i>seriös im Sinne von ernst zu nehmen, redlich, kompetent und verlässlich sein.</i>“¹⁶ • Der Use Case im Paper muss ins geforderte Anwendungsgebiet passen
5	Aufgenommene Literatur analysieren, Kernaussagen zusammenfassen und aufbereiten	Die Publikationen werden vollständig aufgearbeitet und die Kernaussagen notiert. Mittels morphologischer Analyse wird eine kompakte Übersicht realisiert. Die tatsächliche Umsetzung der morphologischen Analyse erfolgt für jede drei Forschungsfragen ähnlich, aber mit durchaus unterschiedlicher Ausprägung.

Für die (erste) Beurteilung von Internetquellen soll folgende Checkliste herangezogen werden:

- „Institutionelle, kommerzielle oder private Website
- Ziel der Publikation: Information, Werbung oder Selbstdarstellung
- Inhaltliche Vollständigkeit: Quellennachweis, Grafiken
- Aktuelle oder aktualisierte Version des Textes und der Links
- Qualität der angebotenen bzw. aufgenommenen Links
- Verantwortliche Organisation, Autorennachweis
- Verfassernachweis und Verfasserumfeld

¹⁵vgl. Theisen, 2017, S.89

¹⁶Bänsch & Alewell, 2013, S.7

- *Weiterführende Hinweise und zusätzliches Material*¹⁷

1.2.3 Proof-of-Concept

Ein Proof-of-Concept (PoC) oder Proof-of-Principle (zu Deutsch: Machbarkeitsstudie) wird erbracht, um zu zeigen, dass ein Vorhaben (oder z.B. die Anwendung eines Modells) durchführbar ist. Als ein dem Projektmanagement entspringender Begriff gilt der PoC auch als ein Meilenstein, an dem dann feststeht, ob der Machbarkeitsnachweis positiv oder negativ ausfällt – also das Vorhaben durchführbar ist oder nicht. Mit einem PoC geht in vielen Fällen auch die Entwicklung eines Prototyps einher, der bereits die geforderten Kernfunktionen enthält.¹⁸ Das Konzept dahinter ist: *„If it works here, it will also work in all cases like this.“*¹⁹

Aus den folgenden Gründen wird ein PoC durchgeführt:

- *„Risikominimierung für Entscheidungsgrundlagen und Budget*
- *Validierung kritischer Anforderungen an die Anwendung*
- *Akzeptanztest der Anwendung in Zusammenarbeit mit Herstellern und Partnern*²⁰

Der PoC ist in dieser Arbeit Teil der in Kapitel 1.2.1 vorgestellten Design Science Methode. Es ist sodann Teil der Evaluierung (Punkt 3), wo Nutzen, Qualität und Effizienz des Artefaktes festgestellt wird.

1.3 Struktur der Arbeit

In diesem letzten Teil des Einleitungskapitels wird der Gang der Untersuchung der vorliegenden Arbeit dargestellt. In Bezug auf die Forschungsmethodik der Gestaltungswissenschaften (Kapitel 1.2.1 auf S.6) wird für diese Arbeit daher der gestaltungswissenschaftliche Ansatz gewählt, zumal dieser Ansatz seine Wurzeln in den Ingenieurwissenschaften hat.²¹ Die Struktur der Forschungsarbeit orientiert sich an der nominellen Herangehensweise der Gestaltungswissenschaft. Als Einstiegspunkt für die Forschungsarbeit wird der *problemzentrierte Ansatz* gewählt, da eine industrielle und angewandte Problemstellung die Forschungsaktivitäten angestoßen hat.²²

Nachdem der Leserin/ dem Leser eine kompakte Einleitung in das Thema Instandhaltung gegeben sowie die identifizierte Problemstellung, die Ziele und die sich daraus ergebenden Forschungsfragen dargelegt wurden, wird nun in Kapitel 2 auf das nötige theoretische Hintergrundwissen zu Instandhaltungsmanagement, CM und Anomalieerkennung eingegangen. Im Anschluss wird in Kapitel 3 der Stand der Technik mittels einer Literaturanalyse erhoben, um allgemeine und angewandte Konzepte für die drei verschiedenen Problemfelder und eventuell bestehende Forschungslücken zu eruieren. Das erste Problemfeld bezieht sich auf das CM von hochkomplexen und kritischen Anlagen, das

¹⁷ Theisen, 2017, S.98

¹⁸ vgl. o. V., 2013, S.2

¹⁹ Kendig, 2016, S.741

²⁰ o. V., 2013, S.2

²¹ vgl. Hevner et al., 2004, S.76

²² vgl. Peffers et al., 2007, S.54

zweite auf die Informationsgewinnung bei einer schlechten Ausgangslage bzgl. der Daten und das dritte Gebiet auf das CM mittels Anomalieerkennung. Kapitel 3.4 liefert dazu eine überschaubare Zusammenfassung der Analyse. In Kapitel 4 wird das Design und die Entwicklung des Artefaktes dieser Arbeit erklärt, welches in Form eines Phasenmodells realisiert wird. Dazu werden auch die in Frage kommenden Kandidatenalgorithmen und Ansätze zur Anomalieerkennung dargelegt. Im selben Kapitel erfolgt auch die Formulierung des Postprocessings, bei dem die Verwendung und Interpretation der Ergebnisse (Output) der Algorithmen definiert wird. Kapitel 5 widmet sich der Validierung des Phasenmodells und somit dem der Arbeit zugrundeliegenden Anwendungsfall. Um die Anwendbarkeit des Artefaktes zu demonstrieren wird der Anwendungsfall mit eben jenem Phasenmodell bearbeitet. Zur Evaluierung des Modells steht nur Expertenwissen zur Verfügung und somit können keine Metriken, die Aufschluss über die Performance geben, berechnet werden. In Kapitel 6 werden die Ergebnisse aufbereitet, zusammengefasst und kritisch betrachtet. Zum Abschluss wird es noch eine Eingrenzung der vorliegenden Forschungsarbeit und ein Ausblick auf zukünftige Forschungsaktivitäten in Bezug auf dieses Gebiet geben. Mit der vorliegenden Diplomarbeit wird somit der identifizierte Forschungsbedarf, das designte Artefakt und die Ergebnisse der Arbeit kommuniziert.

2 Theoretische Grundlagen

Dieses Kapitel behandelt die theoretischen Grundlagen, die für das Verständnis dieser Arbeit unabdingbar sind. Zuerst wird ein Überblick über die Instandhaltung im Allgemeinen und deren Strategien gegeben, damit im Anschluss detailliert auf die Zustandsüberwachung (*Condition Monitoring*, CM) von Maschinen und Anlagen eingegangen werden kann. Da Algorithmen der Anomalieerkennung unter anderem auch für CM verwendet werden und dies im Speziellen auch mit Hilfe des maschinellen Lernens bewerkstelligt werden soll, werden auch für jenes Themengebiet die wichtigsten Begrifflichkeiten besprochen. Im Anschluss wird dann genauer auf mögliche Anomalien in Daten und deren Erkennung eingegangen.

2.1 Instandhaltung und Instandhaltungsstrategien

Die Instandhaltung stellt also die Funktionstüchtigkeit von Werkzeugen, Maschinen und Anlagen, sodass diese ihre zugewiesenen Aufgaben erfüllen können. Gerade im komplexen und vernetzten industriellen Umfeld reicht ein bloßes Erfüllen der Aufgaben nicht aus: Arbeitsaufträge müssen auch in der geplanten Zeit und Qualität sowie zu den veranschlagten Kosten vollbracht werden (klassisches Zieldreieck). Wird die Instandhaltung jedoch vernachlässigt, resultieren bei aufkommenden Schäden daraus unzumutbare Kosten. Diese Mehrkosten entstehen beispielsweise aufgrund einer Produktionsunterbrechung und einer nötigen Erneuerung von Maschinenteilen.²³ „Die Instandhaltung verfolgt darüber hinaus auch humane Ziele, die durch die Vermeidung von Unfallrisiken, die Erhöhung der Arbeits- und Anlagensicherheit sowie die Verhinderung von Umweltbelastungen oder -schäden charakterisiert sind.“²⁴ Darüber hinaus kann ein gut funktionierendes bzw. optimiertes Instandhaltungssystem auch die Wandlungsfähigkeit eines Unternehmens positiv beeinflussen. Wandlungsfähigkeit wird als Summe von Flexibilität, Effizienz und Reaktionsfähigkeit gesehen (erweitertes Zieldreieck).

In der DIN 31051 wird Instandhaltung im Allgemeinen folgendermaßen definiert:

„Kombination aller technischen und administrativen Maßnahmen sowie Maßnahmen des Managements während des Lebenszyklus eines Objektes zur Erhaltung des funktionsfähigen Zustandes oder der Rückführung in diesen, sodass sie die geforderte Funktion erfüllen kann“.²⁵

Als Objekt wird ein Teil, Bauelement, System oder Ähnliches gesehen, welches für sich allein beschrieben werden kann.²⁶ Die Formulierung aus der obigen Definition „zur Erhaltung des funktionsfähigen Zustandes oder der Rückführung in diesen“ impliziert eine Möglichkeit der Einteilung der Instandhaltung. So kann zwischen einer planmäßigen vorbeugenden Instandhaltung und einer Ausfallbehebung (wie in Abbildung 2 dargestellt) unterschieden werden. Die vorbeugende Strategie kann dann weiter unterteilt werden – siehe 2.1.2 und 2.1.3.

²³ vgl. Chebel-Morello et al., 2017, S.IX

²⁴ Schenk, 2019, S.VII

²⁵ Deutsches Institut für Normung, DIN/31051, S.4

²⁶ vgl. ebenda, S.7

Für diese beiden grundlegenden Strategien werden laut DIN 31051 vier operative Prozesse definiert.

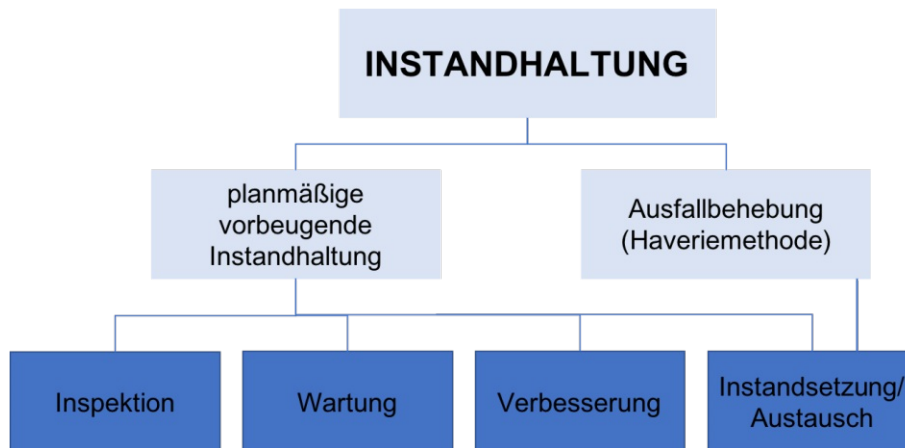


Abbildung 2: Maßnahmen der Instandhaltung²⁷

Bei einer Inspektion wird der Ist-Zustand festgestellt und beurteilt. Wird eine Wartung durchgeführt, reinigt oder schmiert man z.B. bewegliche Teile einer Maschine, sodass deren Lebensdauer verlängert und ein Austausch hinausgezögert werden (Erhaltung des Soll-Zustandes²⁸). Bei Verbesserungsmaßnahmen werden Tätigkeiten am Objekt durchgeführt, sodass es zu einer Steigerung der Funktionssicherheit kommt.²⁹ „Manchmal wird dabei übersehen, dass das Versagen oder der vorzeitige Verschleiß eines Betriebsmittels möglicherweise ein Indiz dafür ist, dass die derzeitige Ausführung nicht optimal geeignet ist. In solch einem Fall ist die Instandsetzung eine gute Gelegenheit für eine qualitative Aufwertung durch Umbau und Modernisierung.“³⁰ Um also bei einem fehlerhaften Objekt wieder die ursprüngliche Funktion herzustellen, muss dieses instandgesetzt oder ausgetauscht werden.³¹

Wie jeder andere Industriezweig unterliegt auch die Instandhaltung einem ständigen Wandel und einer fortlaufenden Veränderung. So herrschte im frühen Industrialisierungszeitalter (19. Jh.) die ausfallorientierte Instandhaltung vor. Ausfallorientierte Instandhaltung meint, erst auf eingetretene Ausfälle zu reagieren. Heute wird in den meisten Branchen und Anwendungsfällen, wo es auch technisch möglich und wirtschaftlich sinnvoll ist, eine Veränderung hin zur proaktiven Instandhaltung angestrebt.³² So hat mittlerweile auch ein Paradigmenwechsel bzgl. der Kosten und der damit verbundenen Wichtigkeit der Instandhaltung in den Unternehmen stattgefunden:

Tabelle 5: Paradigmenwechsel in der Instandhaltung³³

Früher	Welche Kosten verursacht die Instandhaltung?
Heute	Welche Kosten verhindert die Instandhaltung?
Zukunft	Welchen Wert erzielt/ schafft die Instandhaltung?

²⁷ vgl. Matyas, 2018, S.33

²⁸ vgl. Schenk, 2010, S.19

²⁹ vgl. Matyas, 2018, S.33

³⁰ Steck-Winter, 2008, S.6

³¹ vgl. Deutsches Institut für Normung, DIN/31051, S.6

³² vgl. Abbildung 1.1 in Schenk, 2010, S.2

³³ vgl. Matyas, 2018, S.28

Die Instandhaltung ist also nicht mehr nur ein Kostenfaktor oder ein *notwendiges Übel* im Unternehmen. Eine zentrale Frage im Instandhaltungsmanagement ist, wie man zur richtigen Instandhaltungsstrategie kommt. Diese regelt, zu welchem Zeitpunkt welche Maßnahme wie oft an welchem Objekt angewendet wird.³⁴ Das Finden der richtigen Methode stellt ein komplexes Unterfangen dar, bei der einige Kriterien wie z.B. Verkettung und Redundanz der Anlagen, Arbeitszeitvereinbarungen, Qualitäts- und Sicherheitsnormen und Ersatzteilverfügbarkeit die Wahl beeinflussen.³⁵ Deshalb muss eine Analyse des betrachteten Instandhaltungsobjektes und dessen Umgebung gemacht werden, um eine profunde Basis für eine diesbezügliche Entscheidung zu schaffen. Es können die Instandhaltungsstrategien in drei Hauptgruppen eingeteilt werden, wobei die in Abbildung 2 (zweite Ebene) gemachte Einteilung verfeinert bzw. ausgebaut wird in: Managementstrategien, Strategien ohne den Einsatz und Strategien mit Einsatz von Sensorik und Computertechnologie.³⁶

Bevor im Folgenden ein kompakter Überblick über diese grundlegendsten Strategien gegeben wird, muss der Begriff Ausfall definiert sein. Ein Ausfall, der ein Ereignis darstellt, ist der „[...] Verlust der Fähigkeit eines Objektes, eine geforderte Funktion zu erfüllen.“³⁷ Im Gegensatz dazu stellt ein Fehler einen Zustand dar, in dem das Objekt die geforderte Funktion nicht erfüllt. Ein Fehler ist normalerweise das Ergebnis eines vorhergehenden Ausfalls.³⁸

2.1.1 Instandhaltungsmanagementstrategien

Managementstrategien im Bereich der Instandhaltung erfassen organisatorische Ansätze wie z.B. *Reliability-Centered Maintenance* (RCM) und *Total Productive Maintenance* (TPM). In dieser Arbeit wird diesbezüglich nur auf RCM eingegangen, da diese Strategie später beim Anwendungsfall im Fokus steht. Man spricht dabei von einer zuverlässigkeitsorientierten Instandhaltungsstrategie, die einen optimalen Mix aus Ausfallbehebung, vorbeugender Instandhaltung, zustandsorientierter Instandhaltung und vorausschauender Instandhaltung darstellt.³⁹ Für weitere Details bzgl. RCM wird auf Moubray (1996) und Mehairjan (2017) verwiesen.

Ein weiteres Managementkonzept, das besonders durch die Einführung von CPPS relevant geworden ist, stellt die wissensbasierte Instandhaltung dar. Dieses wird in Kapitel 2.1.4 auf S.17 näher erklärt.

2.1.2 Strategien ohne Einsatz von Sensorik und Computertechnologie

In der Instandhaltung werden auch Strategien, welche ohne Einsatz von Sensorik und Computertechnologie auskommen, gebündelt. Hierbei wird in reaktive, präventive und proaktive Instandhaltung unterteilt.

³⁴ vgl. Schenk, 2010, S.26

³⁵ vgl. Matyas, 2018, S.120

³⁶ vgl. ebenda, S.320

³⁷ Deutsches Institut für Normung, DIN/31051, S.10

³⁸ vgl. ebenda, S.9

³⁹ vgl. Matyas, 2018, S.144

Reaktive Instandhaltung: Das betrachtete Objekt wird so lange betrieben, bis ein Ausfall eintritt und ein weiterer Betrieb nicht mehr möglich ist. Erst dann wird das Objekt wieder in den funktionstüchtigen Zustand zurückgebracht. Andere Bezeichnungen dafür sind störungsbedingte oder ausfallsorientierte Instandhaltung, *run-to-failure*-Strategie oder Feuerwehrstrategie.⁴⁰ Ein plakatives Beispiel ist der Wechsel einer Glühbirne. Diese wird, nach dem Verlust der Fähigkeit zu leuchten, einfach durch ein neues funktionierendes Leuchtmittel ersetzt. Jene Strategie eignet sich aber wenig für komplexe und verkettete Maschinen bzw. Anlagen, da hier weitere Schäden, Prozessunterbrechungen oder gar Sicherheitsprobleme riskiert werden. Dem relativ niedrigen Aufwand für die Organisation stehen als Kostentreiber bei dieser Strategie die hohen Ersatzteillager- und Überstundenkosten, Maschinenstillstandszeiten und die niedrige Verfügbarkeit gegenüber.⁴¹

Präventive Instandhaltung: Bei dieser Strategie wird möglichen Ausfällen durch periodisch durchgeführte Instandhaltungsmaßnahmen vorgebeugt. Es ist eine Herangehensweise, bei der Maßnahmen wie kleinere geplante Reparaturen/ Bauteilwechsel, Schmierarbeiten, Inspektionen und Adjustierungen der Maschineneinstellungen zeit- oder intervallabhängig durchgeführt werden. Im Vergleich zum reaktiven Ansatz ist es kostengünstiger, ein noch intaktes Bauteil zeitgerecht zu tauschen als ein bereits ausgefallenes zu reparieren und eine Betriebsunterbrechung zu riskieren. Dabei wird aber in Kauf genommen, dass jenes Bauteil eventuell noch einige Zeit verwendbar gewesen wäre (*Remaining Useful Life*, RUL) und bei präventiven Eingriffen im noch intakten System Beschädigungen durch das Personal verursacht werden können.⁴² Die Maßnahmen zur präventiven Instandhaltung können zeitabhängig, zyklusgesteuert oder anwenderspezifisch eingeleitet werden. Dadurch wird die Ausfallswahrscheinlichkeit des Gesamtsystems oder einzelner Komponenten verringert, was aber mit erhöhtem Aufwand einhergeht.⁴³

Proaktive Instandhaltung: Diese „[...] setzt sich die Bestimmung der Ursachen von Maschinenausfällen durch das Setzen von Maßnahmen und korrektiven Handlungen zum Ziel, um somit Anlagenausfälle zu vermeiden.“⁴⁴ Es ist ein ganzheitlicher Ansatz, bei dem die Instandhaltung nicht isoliert von anderen Abteilungen gesehen wird. Mobley (2002) beschreibt dafür die fünf Grundsätze für eine Weltklasse-Instandhaltung: Verbesserung der Geräteeffektivität, Einbeziehung der Werker in die tägliche Instandhaltungsarbeit, Verbesserung der Instandhaltungseffektivität und -effizienz, Ausbildung und Training der Mitarbeiter und Konstruktion und Management von Anlagen und Maschinen, um Instandhaltungsprävention zu erreichen.⁴⁵

2.1.3 Strategien mit Einsatz von Sensorik und Computertechnologie

Für die sensorbasierten Strategien gilt folgende entscheidende Annahme: in der zustandsorientierten Instandhaltung und folglich in ihren Weiterentwicklungen wird (prädiktive

⁴⁰ vgl. Schenk, 2010, S.27

⁴¹ vgl. Mobley, 2002, S.2

⁴² vgl. Matyas, 2018, S.124

⁴³ vgl. ebenda, S.320

⁴⁴ ebenda

⁴⁵ vgl. Mobley, 2002, S.395f

und präskriptive Instandhaltung) nämlich vorausgesetzt, dass Fehler oder Störungen nicht schlagartig eintreten, sondern sich durch Warnsignale (Änderungen in den Parametern) bemerkbar machen. Es sind also in den gemessenen Signalen eine potentielle Störung (*Potential Failure*, P) und der Ausfall (*Failure*, F) selber erkennbar. Jener Zusammenhang kann in einer sogenannten P-F-Kurve dargestellt werden.⁴⁶

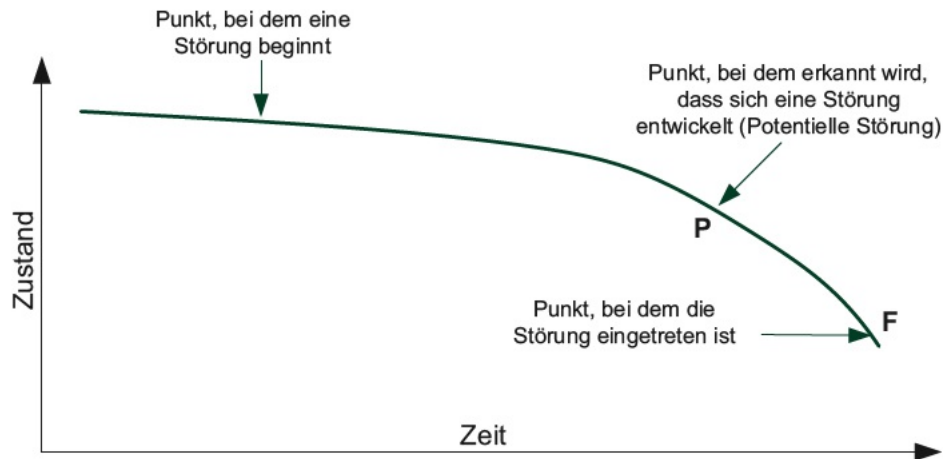


Abbildung 3: P-F-Kurve zeigt den Verlauf des Zustandes⁴⁷

Zustandsorientierte Instandhaltung (Condition-based Maintenance, CBM): Auch diese Strategie ist vorbeugend, die allerdings erst Maßnahmen veranlasst, wenn sich gewisse beobachtete Parameter einer Maschine oder Anlage in einem nicht mehr akzeptablen Bereich befinden oder im Begriff sind, sich dort hinzubewegen. Diese Strategie ist somit zustandsbasiert. Man versucht also, die Zeit zwischen P und F (siehe Abbildung 3) optimal auszunutzen. Hier wird eine ständige Zustandsüberwachung (*Condition Monitoring*, CM) benötigt, welche die nötigen Maschinen- oder Anlagendaten akquiriert – näheres dazu in Kapitel 2.2 auf S.19. Für die weitere Auswertung müssen im Vorhinein Soll-Zustände definiert worden sein, sodass diese mit den festgestellten/ gemessenen Ist-Zuständen verglichen und Abweichungen festgestellt werden können.⁴⁸ „Der Einsatz von CBM Ansätzen und Technologien (Handheld- oder Mobil-Devices oder integrierte Sensorik) führt zur Identifikation und Auflösung von Anomalien bevor funktionale Fehler eintreten.“⁴⁹ In der Literatur wird von einigen Autoren der CBM Strategie auch noch der Prognoseschritt zugeschrieben, hier wird aber die Definition von Matyas (2018) verwendet und somit werden keine prädikativen Aussagen (Prognosen) über das Verhalten der Anlage getroffen.

Prädiktive Instandhaltung (Predictive Maintenance, PdM): Basierend auf den mit CM gesammelten Daten wird mittels fortgeschrittenen Prognosetechniken versucht, die RUL des betrachteten Objektes vorherzusagen. Durch die Anwendung von Advanced Industrial Analytics versucht man also die Frage *Was wird wann passieren?* zu beantworten. Die Beantwortung erfolgt auf Basis von historischen und in Echtzeit verfügbaren

⁴⁶ vgl. Matyas, 2018, S.125

⁴⁷ ebenda

⁴⁸ vgl. Schenk, 2010, S.127f

⁴⁹ Matyas, 2018, S.320

Instandhaltungsdaten.⁵⁰ Die Analyse bzw. Prognose kann rein datengetrieben, physikalisch-modellbasiert, wissensbasiert oder auf einen hybriden (der vorher genannten) Ansatz basierend durchgeführt werden. Anhand dieser Schätzungen oder Prognosen werden dann entsprechende Instandhaltungsmaßnahmen eingeleitet.

Präskriptive Instandhaltung (Prescriptive Maintenance, PresM): Zusätzlich zur Information, welches Objekt wann zu bearbeiten sein wird, gibt diese Instandhaltungsstrategie Empfehlungen zur optimalen Durchführung von Maßnahmen und zur Strategie ab, sodass der Arbeitsfluss und der Prozess der Entscheidungsfindung verbessert werden können.⁵¹ Hier bedient man sich also der präskriptiven Analytik, die mehrere Handlungsempfehlungen abgibt und so auch mehrere Handlungsoptionen miteinander vergleichbar macht.⁵² Es wird auch erwartet, dass diese Strategie im Rahmen von CPPS ermöglicht, eine Selbstdiagnose der Maschinen und eigenständige (automatisierte) Instandhaltungsplanung umzusetzen. Jenen Systemen wird es dann machbar sein, sich auf bestimmte Umstände einzustellen und in dieser neuen Adaption optimal zu arbeiten.⁵³ Es wird auch von selbstheilenden Maschinen gesprochen.⁵⁴

2.1.4 Instandhaltung in Sinne von wissensbasierten Systemen

Das Konzept der wissensbasierten Instandhaltung (*Knowledge-based Maintenance*, KBM) basiert auf der Annahme, dass Wettbewerbsvorteile für das Unternehmen durch Kostensenkung in der Instandhaltung über eine holistische Betrachtungsweise derselben erreicht werden. Die Instandhaltung wird nicht mehr isoliert, sondern in den Wertschöpfungsprozess integriert betrachtet.⁵⁵ In diesem systemorientierten Ansatz werden nicht nur die Auswirkungen von Maßnahmen auf einzelne Systemkomponenten betrachtet, sondern auch auf Effekte andere Elemente bzw. auf das Gesamtsystem geachtet. Damit jene Wechselwirkungen sichtbar gemacht werden können, werden neben den vorliegenden EDV-Daten auch das im Unternehmen verfügbare MitarbeiterInnenwissen und die Erfahrung der MitarbeiterInnen genutzt. In diesem ganzheitlichen Konzept wird vor allem den langfristigen Auswirkungen von Instandhaltungsentscheidungen auf die Wirtschaftlichkeit besondere Aufmerksamkeit zu Teil.⁵⁶ Jene Wechselwirkungen und Abhängigkeiten sind in der Konzeptdarstellung in Abbildung 4 zu sehen.

Dem Instandhaltungsmanagement stehen durch die digitale Transformation und CPPS eine große Menge an Daten aus den unterschiedlichen Unternehmensbereichen zur Verfügung. Diese Informationen werden nicht nur aus der Instandhaltungsabteilung und der Produktion gewonnen. Aus diesen Daten und dem zusammengefassten Wissen kann neues Wissen (Exploration) und neuer Wert generiert werden. KBM wird im Zusammenhang mit CPPS „[...]“

⁵⁰ vgl. Ansari et al., 2019, S.9

⁵¹ vgl. Matyas, 2018, S.321

⁵² vgl. Weber, 2020, S.11f

⁵³ vgl. Ansari et al., 2019, S.4

⁵⁴ vgl. o.V.: Selbstheilende Maschinen (27.03.2017)

https://www.sps-magazin.de/?inc=artikel/article_show&nr=123168 (gelesen am: 04.12.2020)

⁵⁵ vgl. Pawallek, 2016, S.10

⁵⁶ vgl. ebenda, S.9

durch seine erweiterten funktionalen Fähigkeiten zur Wissensentdeckung, -vorhersage, -optimierung und automatischen Adaptierung charakterisiert.“⁵⁷

„Die Vorgehensweise ist ergebnisorientiert und umfasst folgende drei Einflussbereiche:

1. Die Organisation bzw. Abläufe ergeben sich durch die gewählten Instandhaltungsstrategien, die wissensbasiert ermittelt werden.
2. Da sich der Anlagenzustand immer auf ein konkretes Instandhaltungsobjekt bezieht, ist eine detaillierte Betrachtung bis zur Objektebene notwendig.
3. Die Auswirkungen bzw. Folgen durchgeführter bzw. unterlassener Maßnahmen werden untersucht, um Risiken abschätzen zu können.“⁵⁸

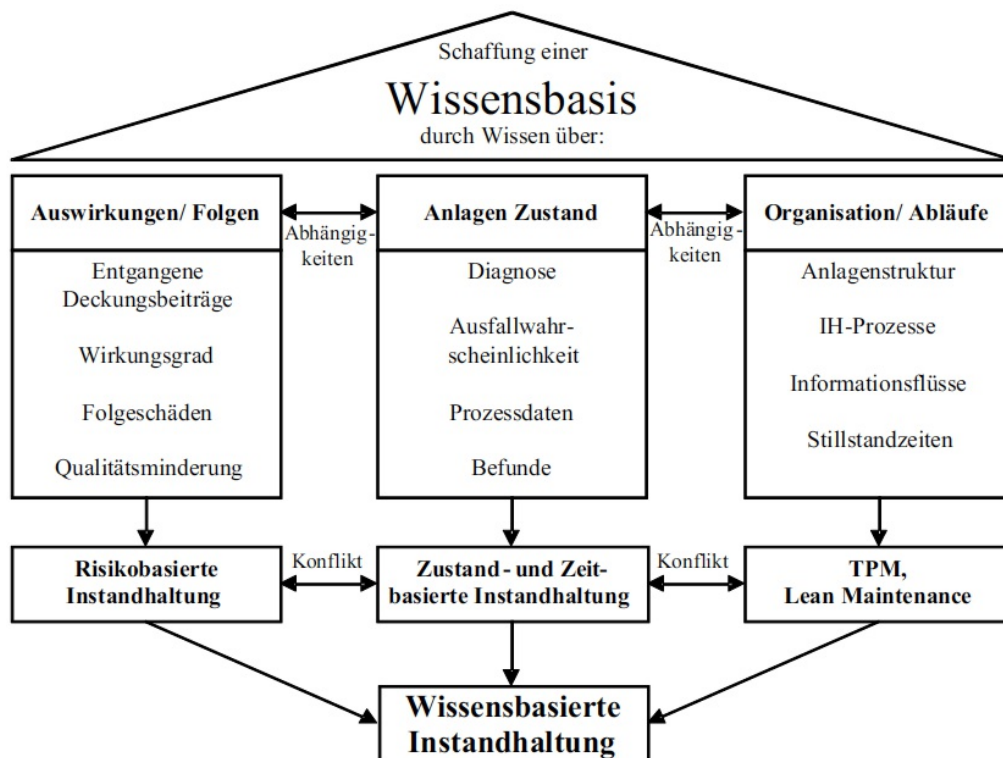


Abbildung 4: Konzept der wissensbasierten Instandhaltung⁵⁹

KBM ist kategorisiert in vier Stufen (Typ I bis IV) bzgl. Reifegrad und Komplexität ihrer funktionalen Fähigkeiten.⁶⁰ Diese werden im Folgenden kurz beschrieben und sind in der daran anschließenden Abbildung 5 ersichtlich:⁶¹

- Typ I - *Deskriptive Instandhaltung (Descriptive Maintenance)*: Geringe Komplexität und geringer Reifegrad des KBM. Es wird die Frage beantwortet *Was ist passiert?*, um so Informationen über vorausgegangene Instandhaltungsmaßnahmen und andere Geschehnisse zu erhalten. Die Strategie unterstützt also die Informationssammlung

⁵⁷ Nemeth, 2020, S.23

⁵⁸ Pawallek, 2016, S.9

⁵⁹ ebenda, S.10

⁶⁰ vgl. Ansari et al., 2019, S.4

⁶¹ ebenda

und -analyse und dadurch kann auch das (historische) Verhalten der Anlage sichtbar gemacht werden.

- Typ II – *Diagnostische Instandhaltung (Diagnostic Maintenance)*: Mittlere Komplexität und geringer Reifegrad des KBM. Es wird die Frage beantwortet *Warum ist es passiert?*. Es werden Ursachenanalysen angestellt und dadurch werden Gründe für Ausfälle ermittelt. Diese Strategie unterstützt die Wissensgenerierung und erhöht die Transparenz der Wissensbasis für die Instandhaltung.
- Typ III – *Prädiktive Instandhaltung (Predictive Maintenance)*: Hohe Komplexität und mittlerer Reifegrad des KBM. Diese Strategie liefert eine Antwort auf die Frage *Was wird wann passieren?*.
- Typ IV – *Präskriptive Instandhaltung (Prescriptive Maintenance)*: Hohe Komplexität und hoher Reifegrad des KBM. Es wird die Frage beantwortet *Was sollte getan werden, damit ein bestimmtes Ereignis eintritt?*.

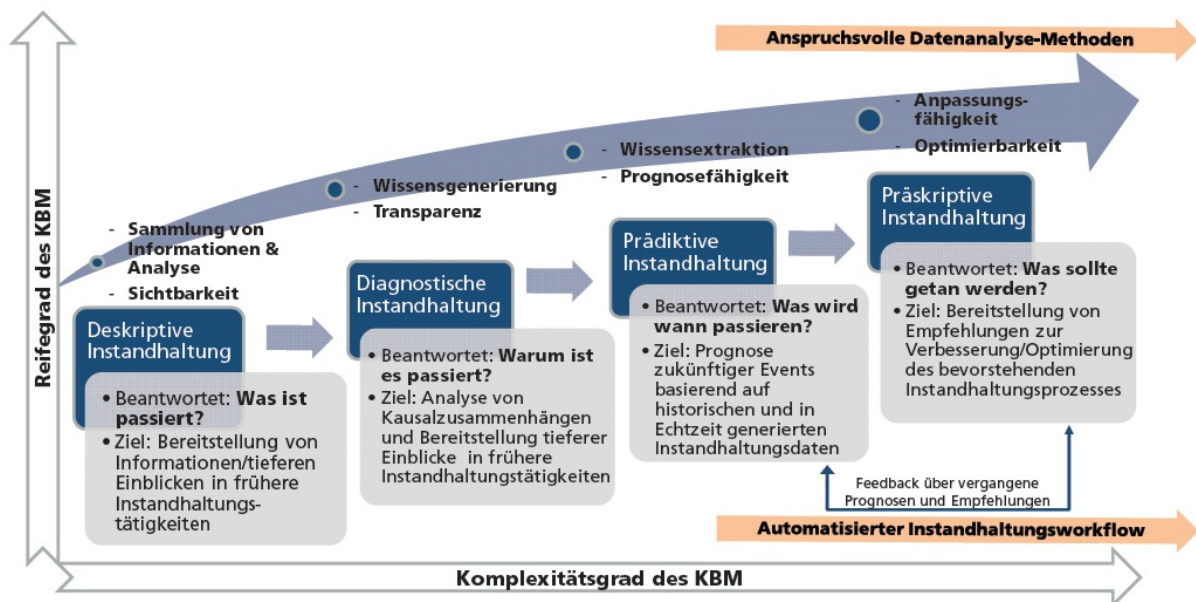


Abbildung 5: Die Reifegrad- und Komplexitätsstufen der wissensbasierten Instandhaltungsstrategien (KBM)⁶²

2.2 Condition Monitoring

Wie in Kapitel 2.1.2 erwähnt, bildet eine Zustandsüberwachung (CM) die Grundlage für alle proaktiven Instandhaltungsstrategien. Dazu muss der aktuelle Zustand der Maschine oder Anlage bekannt sein und die Daten dazu liefert das CM. Die Datenerhebung kann einerseits durch den Menschen (z.B. Sichtprüfung bei Inspektionsroutinen) erfolgen und andererseits automatisiert durch an der Maschine oder Anlage angebrachte oder integrierte Sensoren – mehr dazu in Kapitel 2.2.3 auf S.23. Man spricht hier also von einer Anlagenüberwachung und Anlagendiagnose, welche auch als Technische Diagnostik bezeichnet werden.⁶³ Schenk (2010) sieht als wichtigste Aufgaben der technischen Diagnostik in der Instandhaltung die Beanspruchungs-, Abnutzungs- und Schadensüberwachung. Bei Einführung eines

⁶² Nemeth, 2020, S.24 in Anlehnung an Ansari et al., 2019, S.9

⁶³ vgl. Matyas, 2018, S.126

entsprechenden CM-Systems können dann Schädigungsverläufe diagnostiziert, Grenzwerte überwacht sowie proaktiv potentielle Schäden erkannt werden.⁶⁴

Isermann (2011) sieht im Allgemeinen als Grundaufgaben der Überwachung (*Supervision*) von technischen Prozessen die Fehlererkennung und das Fehlermanagement.⁶⁵ Erst wenn fortgeschrittene Methoden (mathematische Modelle für das Signal Processing und die zugrundeliegenden Prozesse) auf die Fehlererkennung und -diagnose angewendet werden, wird die (Zustands-)überwachung als *Condition Monitoring* bezeichnet. Diese Methoden sind auch in der Lage, kleine Fehler und Abweichungen bereits im frühen Stadium zu entdecken.⁶⁶

Das CM, auch als *Health Monitoring* bezeichnet, von Maschinen und Anlagen beruht auf der Annahme, dass Fehler bzw. Ausfälle nicht schlagartig ohne vorherige Anzeichen eintreten. Der Bediener kennt zu Beginn des Betriebes (*Lifecycle*) der Anlage, die überwacht wird, ihren Normalzustand. Bezieht man sich auf die Bezeichnung *Health Monitoring* kennt der Bediener sozusagen ihren *gesunden* Zustand. Zusätzlich werden auch noch in Normen, Qualitäts- oder Sicherheitsanforderungen Grenzwerte für bestimmte Anlagen- oder Maschinenparameter definiert. Diese Grenzwerte geben den Bereich vor, worin ein akzeptabler und sicherer Betrieb möglich ist. Betrachtete Parameter können unter anderem Öltemperatur, Motordrehzahl oder Pumpendruck sein. Aufgrund der eingangs erwähnten Annahme bietet CM keinen Schutz vor plötzlichen Ausfällen oder Bauteildefekten.

Pawallek (2016) teilt der technischen Diagnostik die Aufgabe der Zustandsermittlung einer Anlagenkomponente zu, während er Condition Monitoring als „[...] die computergestützte Erfassung und Überwachung des gesamten Anlagenzustands mit Hilfe des Online-Systems“⁶⁷ sieht. Ein CM-System führt dabei nach der Datenerfassung unterschiedliche Messgrößen, beispielsweise aus der Vibrationsanalyse, Stromaufnahme- und Öltemperaturmessung, zusammen und analysiert diese, sodass ein Zustandsschaubild der Anlage erstellt werden kann.⁶⁸ Ein CM-System führt grundsätzlich drei Schritte aus: Datenakquise, Datenverarbeitung und Datennutzung.⁶⁹

2.2.1 Vor- und Nachteile von Condition Monitoring

Die Gründe, warum CM im Maschinen- bzw. Anlagenbetrieb integriert werden sind zahlreich. Nachfolgend findet sich eine tabellarische Zusammenfassung jener Gründe, die für bzw. gegen die Einführung von CM im Unternehmen sprechen:⁷⁰

Tabelle 6: Gründe für die Einführung von CM

Kosten	Senkung der Betriebs-, Anlagen-, Instandsetzungs- und Ausfallkosten <ul style="list-style-type: none"> • Erkennung und Diagnose von Fehlern in Aktuatoren, Prozessen, Komponenten und Sensoren • Reduktion des manuellen Inspektionsaufwandes (bei automatisierten Systemen) • Senkung der Fehlereintrittswahrscheinlichkeit
--------	---

⁶⁴ vgl. Schenk, 2010, S.132

⁶⁵ vgl. Isermann, 2011, S.11

⁶⁶ vgl. ebenda, S.3

⁶⁷ Pawallek, 2016, S.160

⁶⁸ vgl. ebenda, S.161

⁶⁹ vgl. Karner, 2019, S.26

⁷⁰ vgl. Matyas, 2018, S.127/130; Mehairjan, 2017, S.109/124; Isermann, 2011, S.3; Schenk, 2010, S.31

	<ul style="list-style-type: none"> • Verhindern von Beschädigungen an noch intaktem Equipment bzw. gefährlichen und kostenintensiven Totalausfällen • Verhindern von Produktionsausfällen und Strafzahlungen
Wirtschaftlichkeit	Sicherstellung der Verfügbarkeit und Zuverlässigkeit (Basis für betriebsweites Asset Management)
Technik	<ul style="list-style-type: none"> • Basis für fehlertolerante und rekonfigurierbare Systeme • Basis für alle proaktiven Instandhaltungsstrategien • Fernfehlererkennung und -diagnose möglich
Qualität	Normgerechter Betrieb stellt geforderte Produktqualität sicher
Gesetze	Gewährleisten eines sicheren Betriebes (wichtig für kritische Infrastruktur) <ul style="list-style-type: none"> • Verhindern von Schäden am Menschen und umliegender Infrastruktur • Verhindern von Schäden an der Umwelt • Sicherstellen der Versorgungssicherheit

Tabelle 7: Gründe gegen die Einführung von CM

Kosten	<ul style="list-style-type: none"> • Hohe Investitions- und Set-Up-Kosten • Aufwand und Nutzen bei großen und komplexen Anlagen schwer abschätzbar • Laufendes MitarbeiterInnentraining notwendig
Technik	<ul style="list-style-type: none"> • ExpertenInnenwissen notwendig – fehlende Erfahrung der MitarbeiterInnen • Durch Einbau von neuen Sensoren entsteht neue Fehlerquelle • Wechselwirkungen bei komplexen Anlagen oft nicht bekannt • Ausfallverhalten (<i>failure mode</i>) oft nicht bekannt • Ansammlung einer großen Datenmenge bei unklarer IT-Organisation – Schwierigkeiten in der Datenverarbeitung

Anmerkung: in Tabelle 6 und Tabelle 7 wird nicht unterschieden, ob CM nur auf ein Bauteil, eine gesamte Maschine oder Anlage angewendet wird.

2.2.2 Stufen des Condition Monitoring

In der Literatur sind zahlreiche Definitionen für CM zu finden und somit auch für die Ausbaustufen von CM-(Systemen). Hier wird jene von Jardine et al. (2006) verwendet. Dieser unterscheidet zwischen zwei verschiedenen Ausbaustufen:⁷¹

1. *Diagnosesysteme*: konzentrieren sich darauf, Fehler zu entdecken, zu isolieren und zu identifizieren. Dabei ist der Fehler aber bereits aufgetreten und die geforderte Funktionsweise kann nicht sichergestellt werden.
2. *Prognosesysteme*: versuchen Fehler und Ausfälle anhand von historischen und aktuellen Daten vorherzusagen bevor diese auftreten. Jene Fehler können dann durch entsprechende präventive Maßnahmen verhindert werden.

Die Ausbaustufen eines CM-(Systems) reichen vom reinen beobachtenden Reporting bis hin zur *Prognose*. Abbildung 6 zeigt eine Synthese aus der Einteilung von Jardine (2006) mit den Spezifikationen von Isermann (2011). CM-Systeme mit Prognosefähigkeit wird in der Literatur auch oft als *Prognostics and Health Management (PHM)* geführt. Auf das Prognosesystem wird nicht genauer eingegangen, da es nicht im Fokus dieser Arbeit liegt.

Die einfachste Variante des CM ist die Grenzwertüberwachung (*Limit Checking*). Dabei wird eine gewisse Messvariable $Y(t)$ beobachtet. Sobald diese einen Grenzwert über- oder unterschreitet, wird ein Alarm ausgelöst (getriggert). Der Anlagenbetreiber muss nun

⁷¹ vgl. Jardine et al., 2006, S.1491

Maßnahmen ergreifen, sodass die Anlage wieder im Toleranzbereich $Y_{min} < Y(t) < Y_{max}$ arbeitet. Aus Systemsicht stellt dies einen offenen Regelkreis dar.⁷²

Das System kann dann auch dahingehend erweitert werden, sodass es sich von selbst beim Verlassen des Toleranzbereiches schützt – Automatischer Eingriff (*Automatic Protection*). Dies verlangt aber eine Rückkopplung (Feedback), sodass der aktuelle Zustand und der Soll-Zustand verglichen werden können. Demzufolge muss also ein geschlossener Regelkreis vorliegen. Dann kann das System regelnd eingreifen und gefährliche Anlagenzustände verhindern. Die vorher und eben genannte Ausprägung von CM gehen aber nicht über eine Überwachung hinaus und können damit im Sinne von KBM kein neues Wissen generieren. Hierfür werden fortschrittliche Fehlererkennungs- und Fehlerdiagnosemethoden benötigt.⁷³

Dementsprechend ergibt sich also ein Überwachungssystem mit Fehlerdiagnose und -management. Aus den Signalen werden Kennwerte (*Features*) generiert, z.B. Abweichungsmaße, die dann wiederum von der Fehlererkennung als relevante Abweichungen eingestuft werden (oder nicht). Hier kommt Anomalieerkennung zum Einsatz, welche in Kapitel 2.4 auf S.28 behandelt wird. Es folgen eine Diagnose und eine mögliche Zuordnung/Einstufung der Fehler. Das daraus generierte Wissen über den Zustand der Maschine wird in Handlungsempfehlungen übergeleitet, sodass der Fehler behoben oder verhindert werden kann.⁷⁴ Hier ist die Grenzziehung zwischen Diagnose- und Prognosesystem nicht eindeutig.

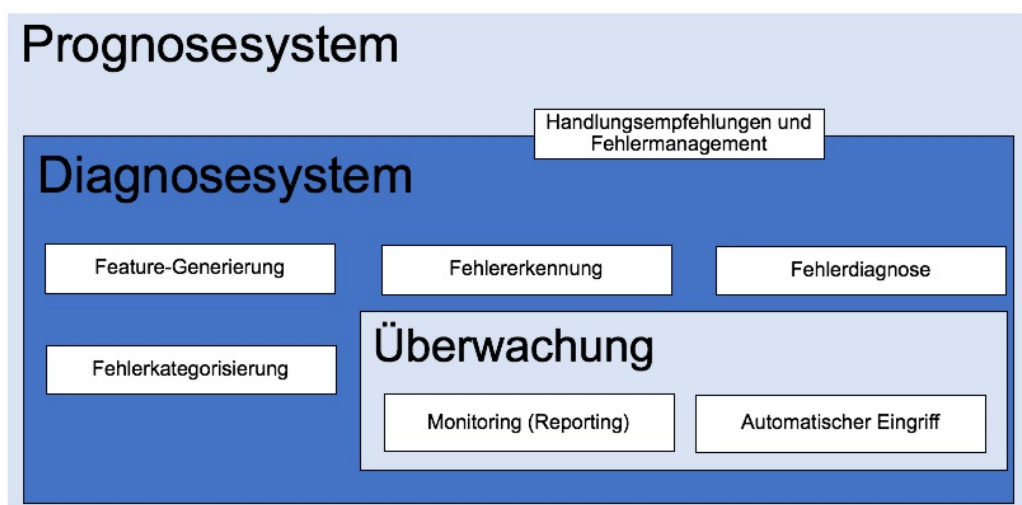


Abbildung 6: Ausbaustufen des CM⁷⁵

Im Zuge dieser Forschungsarbeit werden für die Diagnose folgende Modelle betrachtet (bei der State-of-the-Art-Analyse in Kapitel 3 auf S.35):

- **Physikalische Modelle:** White-Box Ansatz (z.B. Zustandsraummodelle), bei dem die physikalischen und mathematischen Zusammenhänge bekannt sind.

⁷² vgl. Isermann, 2011, S.12

⁷³ vgl. ebenda, S.13f

⁷⁴ vgl. ebenda, S.15f

⁷⁵ Eigene Darstellung

- **Datengetriebene Modelle:** Hier werden nicht nur CM-Daten, sondern auch Maschinendaten, Log-Daten etc. genutzt, um das Anlagenverhalten/ den Anlagenzustand abzubilden. Beispiele sind künstliche neuronale Netze.
- **Wissensbasierte Modelle:** Eine Kombination aus Erfahrung und KI-Techniken wird auf gespeicherte Informationen bestehend aus Expertenwissen und hinterlegtem Regelwerk angewendet (*Fuzzy Logic* und *Expert Systems*).⁷⁶
- **Hybride Modelle:** Kombination aus den oben genannten Ansätzen.

2.2.3 Datenakquirierung

Mit der Datenakquise, also der Datensammlung und -speicherung, wird das Fundament für CM geschaffen. Die dabei erfassten Informationen werden in *Eventdaten* und *Condition Monitoring Daten* eingeteilt. Eventdaten beinhalten z.B. Informationen über Instandhaltungsaktivitäten oder Anlagenausfälle. CM-Daten hingegen reichen von Vibrationsmessungen bis hin zu Wetter- und Umweltdaten.⁷⁷ Jene Einteilung wird später in der Literaturanalyse im Kapitel 3.1 auf S.35 präzisiert. Nun stellt sich die Frage, auf welche Weise Daten für die Zustandsüberwachung gesammelt werden, sodass diese dann weiterverarbeitet und genutzt werden können. Es bestehen zwei Möglichkeiten: entweder erfolgt die Zustandsüberwachung durch den Menschen oder mittels Sensoren.

Zustandsüberwachung durch den Menschen: Die einfachste Form der Überwachung wird über eine akustische Kontrolle der Anlage durch den Mitarbeiter im Rahmen einer Inspektion realisiert. Das menschliche Ohr eines/einer erfahrenen und geschulten Mitarbeiters/ einer Mitarbeiterin ist fähig, bereits marginale Abweichungen vom normalen (Anlagen-)Klang zu erkennen. Diese Methode ist schnell umsetzbar und benötigt kein Equipment, ist aber subjektiv und liefert keine Information über die Ursache des Fehlers.⁷⁸ Im Zuge der Inspektion besteht auch die Möglichkeit den Zustand der Anlage über eine Sichtprüfung (visuelle Inspektion) zu beurteilen. *„Hierbei wird auf sichtbare geometrische Veränderungen, Korrosion, Flüssigkeitsstände, Dichtigkeiten, Temperaturen, Geräusche oder Vibrationen geachtet.“*⁷⁹ Eine weitere Option zur Inspektion besteht auch durch die Verwendung von mobilen technischen Prüfgeräten (*Temporäre Diagnosesysteme*⁸⁰), wie z.B. einem Endoskop oder durch andere Prüfverfahren, wie z.B. Schweißnahtprüfung durch Farbeindringverfahren (*Penetration Testing*, PT).

Die Zustandsüberwachung durch den Menschen kann nur diskontinuierlich erfolgen und garantiert somit keine lückenlose Datensammlung. Zusätzlich werden die Ergebnisse/ Beobachtungen in unstrukturierten Textdateien und eventuell nicht standardisiert dokumentiert. Die automatisierte Auswertung dieser und die Wissensexploration im Sinne von KBM stellt ein weiteres Problemfeld für Instandhaltungsmanager dar (→ *Text Mining* im Kontext von CPPS⁸¹).

⁷⁶ vgl. Pecht & Kang, 2018, S.597

⁷⁷ vgl. Karner, 2019, S.27

⁷⁸ vgl. Matyas, 2018, S.128

⁷⁹ Schenk, 2010, S.132

⁸⁰ vgl. ebenda

⁸¹ vgl. Ansari et al., 2019, S.15, Breitschopf, 2020 und Madreiter, 2020

Dem Trend der Automatisierung und der Digitalisierung der Instandhaltung folgend versucht man zunehmend die Fähigkeiten des *traditionellen Maschinenflüsterers* durch digitale Pendants wie integrierte Sensoren (im weiteren Sinne dann auch durch fortgeschrittene Simulations- und Analysemodelle) zu ersetzen.⁸² Damit gelangt man zum CM durch Sensoren.

CM mit Sensoren: Zusätzlich zu Sensoren, die akustische Effekte nutzen, sind auch noch mechanische, thermische und elektrische Sensoren verfügbar. Diese können entweder einzeln oder kombiniert eingesetzt werden.⁸³ Mit den Sensoren versucht man die fünf menschlichen Sinne zu ersetzen. Im Allgemeinen sind bei der verbauten Sensortechnologie die Entwicklungstrends extreme Miniaturisierung, sehr sparsame oder gar batterie lose Sensoren und Zusammenschluss bzw. Anbindung in Wireless-Netzwerke.⁸⁴

Während moderne (State-of-the-Art) Maschinen oder Anlagen bereits serienmäßig vollständig mit Sensorik ausgestattet sind, ist bei älteren Maschinen Retrofitting nötig. Das Nachrüsten mit Sensorik ermöglicht die Anbindung an ein CM-System, wie es auch der Fall im später behandelten Use-Case ist – siehe Beschreibung Kapitel 4. Es kann dann eine kontinuierliche Überwachung und Diagnose (Online) der Anlage oder Maschine etabliert werden. Eine weitere Möglichkeit der Verwendung von CM-System ist im Gegensatz zur Online-Überwachung die Datensammlung mit anschließender Offline-Datenauswertung und -Diagnose.

Eine direkte Datenerfassung, egal ob durch Sensoren oder durch den Menschen, setzt den Zugang zur messenden Größe voraus. In komplexen Anlagen oder Maschinen ist dies jedoch aus verschiedenen Gründen (z.B. konstruktions- oder sicherheitsbedingt) oft nicht realisierbar, sodass dieser Parameter oft nur indirekt über andere Größen geschätzt werden kann.

Da in obigen Ausführungen vom frühen Erkennen von Fehlern und Abweichungen in den Daten (bzw. an der Maschine oder Anlage) gesprochen wurde, braucht man offensichtlich Anomalieerkennung (AE) für das CM. Da AE unter anderem auch mit Methoden des maschinellen Lernens (ML) durchgeführt werden kann, werden zuerst Grundbegrifflichkeiten aus dem Bereich ML und *Data Mining* erklärt.

2.3 Data Mining und Maschinelles Lernen

Bevor die Begriffe *Data Mining* und *Maschinelles Lernen* erläutert werden, gilt es, das Feld dieser Begrifflichkeiten abzustecken. Beide Begriffe entstammen dem Bereich der Künstlichen Intelligenz (KI), im Englischen *Artificial Intelligence (AI)*, die oft auch als Schlüsseltechnologie für die Industrie 4.0 angeführt wird. Es wird dabei versucht Computersystemen menschenähnliche Intelligenz anzutrainieren. Die Systeme sollten nicht nur menschlich, sondern vor allem auch rational, denken und handeln.⁸⁵ „Im Kern ist das Ziel dort, Probleme zu lösen, die dem Menschen leicht fallen, für die eine gewisse Form an Intelligenz notwendig zu sein scheint.“⁸⁶ Künstliche Intelligenz wird als Überbegriff für die Verarbeitung von Informationen und Daten geführt, gemeint sind meistens sehr spezielle Anwendungen, die

⁸² vgl. Güntner et al., 2015, S.20

⁸³ vgl. Matyas, 2018, S.128

⁸⁴ vgl. Pecht & Kang, 2018, S.565

⁸⁵ vgl. Russel & Norvig, 2010, S.2

⁸⁶ Schacht & Lanquillon, 2019, S.90

durch Algorithmen aus den Unterbereichen des Maschinellen Lernens, Deep Learning (tiefen Neuronale Netze) oder der Neuronale Netze realisiert werden. Daraus lässt sich ableiten, dass *Maschinelles Lernen* ein Teilgebiet der KI, *Deep Learning* ein Teilgebiet des *Maschinellen Lernens*, und Neuronale Netze wiederum eine Teildisziplin des *Deep Learning* darstellen – siehe Abbildung 7. Dabei stellen Neuronale Netze die einfachste Form dar.

Ein weiterer wichtiger Begriff, der gerne im selben Atemzug mit KI, Industrie 4.0 und CPPS genannt wird, ist *Big Data*. Das sind jene Daten, „[...] die sich bezüglich der „3 V“ (*Volume, Variety, Velocity*), also hinsichtlich der Datenmenge, der Heterogenität der Daten und der Frequenz des Datenanfalls, bzw. der Anforderung an die Verarbeitungsgeschwindigkeit über das normale Maß hinaus auszeichnen.“⁸⁷

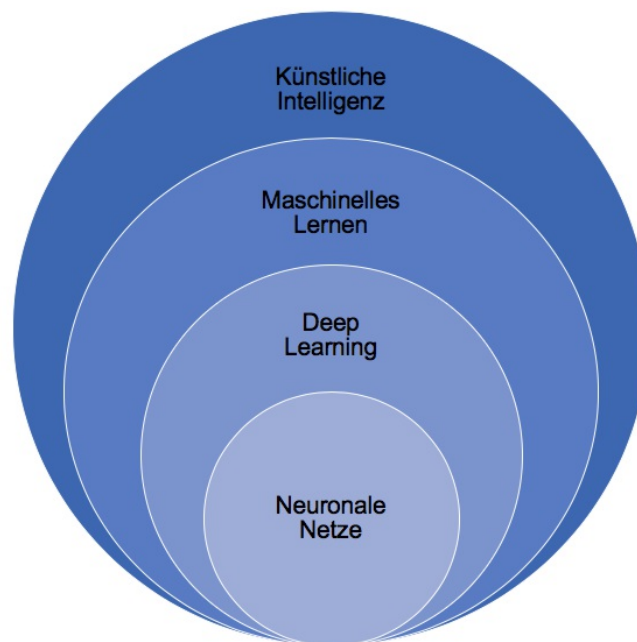


Abbildung 7: Einteilung und Bezug der verschiedenen Begrifflichkeiten der Künstlichen Intelligenz⁸⁸

2.3.1 Data Mining

Auch *Data Mining* ist ein sehr weit gefasster Begriff, der unterschiedlichste Ausformungen der Datenverarbeitung beschreibt. Der Fokus aber liegt in den meisten Anwendungen auf der Datensammlung, -bereinigung, -verarbeitung und -analyse, um daraus neue Informationen bzw. Erkenntnisse erlangen zu können. Dafür wurde ein weithin akzeptiertes Rahmenwerk (Quasi-Standard) geschaffen, nämlich der *Cross-industry standard process for data mining* (CRISP-DM). Es ist ein branchenübergreifendes Vorgehensmodell – in Abbildung 8 dargestellt.⁸⁹ Es forciert „[...] die Wiederholbarkeit und Nachvollziehbarkeit aller tatsächlich durchgeführten Verarbeitungsschritte und Entscheidungen, erleichtert so die Dokumentation und auch die Wiederverwendung von Erfahrungen.“⁹⁰ Beim *Data Mining* werden z.B. neben Verfahren aus der multivariaten Statistik auch welche aus dem Bereich des *Maschinellen*

⁸⁷ Dorchain & Schöning, 2017, S.463

⁸⁸ Eigene Darstellung

⁸⁹ vgl. Weber, 2020, S.22f

⁹⁰ Schacht & Lanquillon, 2019, S.112

Lernens verwendet. So stellt das *Maschinelle Lernen* einen Teil des mathematischen Unterbaus von *Data Mining* dar.

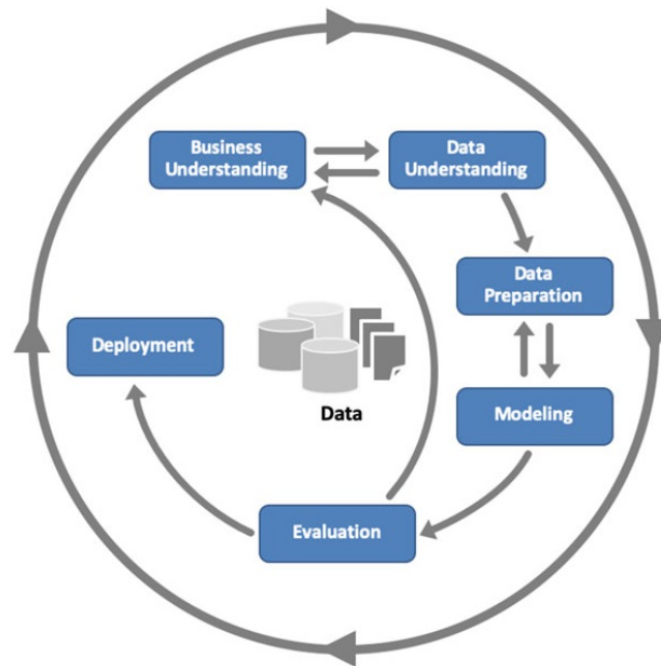


Abbildung 8: Prozessmodell CRISP-DM⁹¹

2.3.2 Maschinelles Lernen (ML)

Im Fokus beim ML steht das Bilden oder Finden von Modellen, die die Beziehung von Eingangs- und Ausgangssignalen (Input/ Output) optimal beschreiben. Das durch eine mathematische Funktion repräsentierte Modell legt Regeln fest, wodurch ein gewisses Verhalten beschrieben oder vorhergesagt werden kann. Was nun tatsächlich das *Maschinelle Lernen* ausmacht, ist, dass das Prinzip der Input- bzw. Outputverarbeitung umgedreht wird: „Aus einer Eingabe und der gewünschten Ausgabe als gemeinsame Eingabe eines Lernverfahrens erstellt dieses ein Programm, das die Eingabe in die gewünschte Ausgabe überführen kann.“⁹² Abbildung 9 zeigt diesen Unterschied der klassischen Modellbildung durch den Menschen und durch ein computergestütztes Lernverfahren. Das Modell kann also eine Induktion durchführen, indem anhand von einigen spezifischen Beispielen (Input-Output-Paaren) generelle Zusammenhänge und Regeln erlernt werden.⁹³

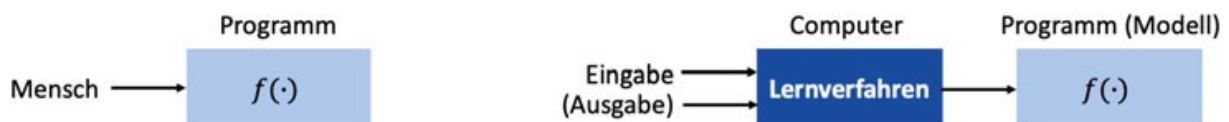


Abbildung 9: Modellierung auf klassische Weise (links) und durch ML (rechts)⁹⁴

Im Weiteren wird kompakt dargelegt welche unterschiedlichen Verfahren für das Lernen bzw. Trainieren des Modells (Lernformen) verwendet werden können. Die Einteilung bezieht sich

⁹¹ ebenda

⁹² ebenda, S.91

⁹³ vgl. Russel & Norvig, 2010, S.694

⁹⁴ Schacht & Lanquillon, 2019, S.91

auf die Erscheinungsform des Trainingsdatensatzes. Es werden vier Lernverfahren unterschieden⁹⁵:

Überwachtes Lernen/ Supervised Learning: Der Algorithmus bildet in der Trainingsphase aus bekannten Input-/ Output-Paaren (gelabelte Daten) ein Modell, das dann im Betrieb fähig ist, unbekannte Inputdaten bekannten Zielwerten zuzuordnen. Das Modell überträgt sozusagen die Eingabewerte an eine oder mehrere gewünschte Ausgabewerte. Dies wird auch Mapping genannt. *„Das Ziel ist es, die Funktion so aufzubauen, dass über die initialen Daten hinaus eine Verallgemeinerung der Funktion möglich wird, also unbekannte Daten zum richtigen Ergebnis zuzuordnen.“*⁹⁶ Es müssen also markierte Datensätze vorliegen, das ist in der Praxis aber oft nur sehr schwer zu realisieren. Sollte mit dem eingelernten Modell in der Anwendung dann der Eingabewert in eine Kategorie, also einen diskreten Wert, eingeordnet (vorhergesagt) werden, spricht man von einer Klassifikation (z.B. der Spam-Ordner beim Email-Posteingang). Sollte mit dem Modell ein stetiger/ kontinuierlicher Wert vorhergesagt werden, spricht man von einer Regression. Folgende Algorithmen und Methoden können als Beispiel genannt werden: Regression, Entscheidungsbaum, Naive Bayes, Vector Machines, Random Forest und Neuronale Netze.

Unüberwachtes Lernen/ Unsupervised Learning: Im vorhergenannten Lernverfahren wird vom *Lernen aus Beispielen* gesprochen, beim unüberwachten Lernen allerdings vom *Lernen aus Beobachtungen*.⁹⁷ Es liegen nur Daten ohne Markierungen (ungelabelt) vor. Daher versucht der Algorithmus über verborgene Merkmale in den Daten Ähnlichkeiten und somit eine Struktur zu finden. Wird versucht, anhand von Mustern Gruppen oder Klassen in den Daten zu definieren, spricht man vom *Clustering* – z.B. Einteilung der Kunden nach Kaufverhalten. Wird versucht, Regeln für den Datensatz und dessen Struktur zu definieren, spricht man von der Assoziationsanalyse – z.B. zusammenhängendes Kaufinteresse (Personen, die A oder B gekauft haben, könnten eventuell auch M und N Gefallen finden). Folgende Algorithmen und Methoden können als Beispiel genannt werden: k-Means, Recommender Systems, Hierarchical Clustering

Halbüberwachtes Lernen/ Semi-supervised Learning: Es stellt eine Mischform der beiden oben genannten Extremformen dar und kommt dann zum Einsatz, wenn ein kleiner Teil des Datensatzes gekennzeichnet ist. Zumindest von einer Klasse ist Information vorhanden und dadurch kann eine Verallgemeinerung für andere Fälle erreicht werden. Für die praktische Anwendung gilt das also als eine attraktive Lösung. Als Beispiel kann hier der One-Class-SVM Algorithmus angeführt werden.

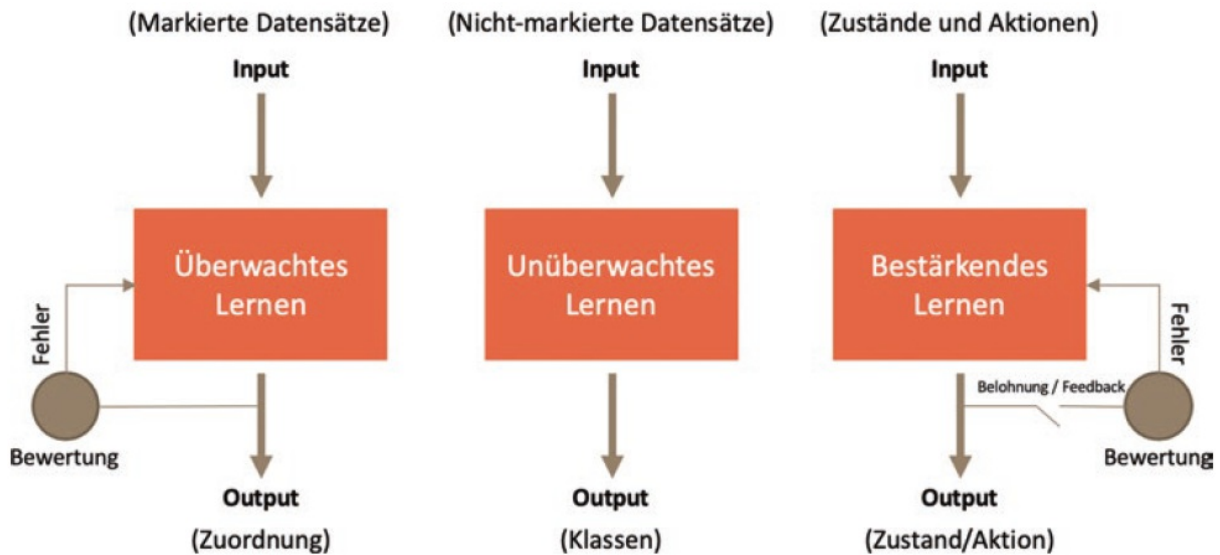
Bestärkendes Lernen/ Reinforcement: Diese Art des Lernens wird eingesetzt, *„[...] wenn es kaum Trainingsdaten gibt und der ideale Zielzustand nicht definiert werden kann oder erst durch Interaktion mit der Umwelt erschlossen werden muss.“*⁹⁸ Als Beispiele für Algorithmen und Methoden können folgende genannt werden: Q-Learning, Temporal Difference (TD), Deep Adversarial Networks oder auch der State-Action-Reward-State-Action (SARSA) Algorithmus.

⁹⁵ vgl. Weber, 2020, S.40ff

⁹⁶ ebenda, S.40

⁹⁷ vgl. Schacht & Lanquillon, 2019, S.96f

⁹⁸ Weber, 2020, S.44

Abbildung 10: Die drei Hauptgruppen des Maschinellen Lernens⁹⁹

2.4 Anomalieerkennung

Die Erkennung von Anomalien stellt einen sehr wichtigen Problemtyp der *Künstlichen Intelligenz* und deren Algorithmen dar. Die Anwendungsgebiete der Anomalieerkennung sind vielfältig und ein Auszug derer ist in Folge dargestellt. Bevor genauer auf die Ausprägungen von Anomalien und die Techniken der Anomaliedetektion eingegangen wird, sollten die Begriffe *Anomalie* und *Anomalieerkennung* definiert werden.¹⁰⁰

- **Anomalie:** nicht mit dem Großteil der anderen Datenpunkte übereinstimmender Datenpunkt oder nicht übereinstimmende Abfolge (*non-conforming pattern*) von Datenpunkten
- **Anomalieerkennung:** Aufgabenstellung, bei der versucht wird, eben diese Abfolgen (Pattern) in den Daten zu finden, die nicht mit dem erwarteten Muster/ Verhalten der Daten, also dem Großteil der Datenmenge, übereinstimmen.

Anomalien entstehen aufgrund von menschlichen Fehlern, Fehlfunktionen in Messinstrumenten, natürlichen Abweichungen/ Veränderungen in Populationen, betrügerischem Verhalten und Veränderungen im Verhalten oder Fehlern in Systemen. Der Ursprung der Anomalie und auch das Einsatzgebiet bestimmen den Umgang mit der entdeckten Anomalie.¹⁰¹ Für die Literaturrecherche werden zur besseren Übersicht Synonyme zu Anomalie und andere damit verbundene Begriffe angeführt:

Tabelle 8: Synonyme und Nicht-Synonym von Anomalie¹⁰²

<i>Anomalie (engl. anomaly)</i>	Englisch	Deutsch
Synonyme	abnormalities	Abnormalitäten
	rare events	Ereignisse, die in geringer Häufigkeit (selten) auftreten
	outliers	Ausreißer
	exceptions	Ausnahmen
	aberrations	Abweichung, Deviation
	surprises	Überraschungen

⁹⁹ ebenda, S.39¹⁰⁰ vgl. Chandola et al., 2009, S.1f¹⁰¹ vgl. Hodge & Austin, 2004, S.4¹⁰² vgl. Chandola et al., 2009, S.1ff

	peculiarities	Eigenarten
	contaminants	Verunreinigungen
Verwandt bzw. Nicht-Synonym	novelties	Neuheiten im Sinne von: unbeobachtete Abfolgen, die aber dann in das Modell aufgenommen werden, also es zukünftig beeinflussen
Nicht-Synonym	noise	Rauschen (in den Daten)

Weber (2020) findet zwei entscheidende Gründe, eine Ausreißeranalyse durchzuführen:¹⁰³

- Entfernen störender Ausreißer: Aufgrund von Fehlern in den Daten kann der Modellbau (für datengetriebene Modelle) gestört werden. Die Ausreißer müssen korrigiert oder entfernt werden. Für die Algorithmusauswahl bzw. den Modellaufbau ist auch zu berücksichtigen, dass manche Algorithmen sensibler auf Ausreißer reagieren als andere.
- Generieren von neuer Information: In eben genau den sich von der Vielzahl der anderen Daten unterscheidenden Datenpunkten liegt eine gesuchte oder entscheidende Information.

Als Beispiele für Einsatzbereiche der Anomaliedetektion seien folgende angeführt:¹⁰⁴

- Intrusion Detection: Einbrüche/ Eindringen feindlich gesinnter Nutzer (Hacker) in Netzwerke, sogenannte Netzwerk- und Systemattaken
- Betrugserkennung: z.B. Kreditkartenbetrug
- Medizinische Anwendungen mit Patientendaten
- **Industrielle Schadensdetektion:** Erkennen von Schäden an aktiven Komponenten und an passiven physischen Strukturen - Fokus dieser Arbeit (Kapitel 3.3 auf S.53 und folgende).
- Bildverarbeitung: Bewegungs- und Ereigniserkennung, in der Medizintechnik zur Erkennung von Krebsgewebe
- Anomalieerkennung in Textdaten
- Überwachung von Sensornetzwerke

2.4.1 Arten von Anomalien

Es gibt unterschiedliche Erscheinungsformen oder Ausprägungen von Anomalien in Daten. Diese beeinflussen die Wahl des Erkennungsalgorithmus. Chandola et al. (2009) gliedern Anomalien in folgende drei Kategorien:¹⁰⁵

Punktuelle Anomalien: Eine Dateninstanz wird als punktuelle oder univariate Anomalie bezeichnet, wenn diese anomal im Vergleich zu den anderen Daten ist. Als Beispiel kann Kreditkartenbetrug genannt werden: Es liegt ein Betrugsverdacht vor, wenn die Karte normalerweise in der Region A verwendet wird, dann aber plötzlich Abbuchungen in Region X gemeldet werden.

Kontextuelle Anomalien: Ist eine Dateninstanz in einem speziellen Kontext - aber sonst nicht - anomal, so kann diese als kontextuelle Anomalie kategorisiert werden. Als Beispiel kann ein plötzlicher Temperaturabfall an einem Sommertag angeführt werden (Saisonalität). Das Problem der Saisonalität wird vor allem bei Zeitreihen schlagend.

¹⁰³ vgl. Weber, 2020, S.61f

¹⁰⁴ vgl. Chandola et al., 2009, S.11ff

¹⁰⁵ vgl. ebenda, S.7ff

Kollektive Anomalien: Ist eine Ansammlung/ Anhäufung an ähnlichen Dateninstanzen anomal relativ zum gesamten Datensatz, so kann diese Ansammlung als kollektive Anomalie bezeichnet werden. Innerhalb dieser und in Bezug auf diese Häufung sind die einzelnen Dateninstanzen folglich nicht anomal – ein Beispiel ist in Abbildung 11 ersichtlich:

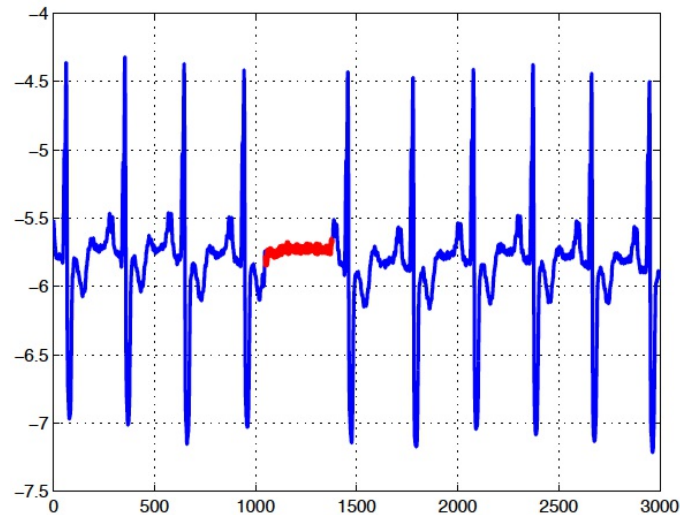


Abbildung 11: Kollektive Anomalie (rot markiert) im Verlauf eines menschlichen Elektrokardiogramms¹⁰⁶

In Bezug auf den gesamten Datensatz liegen in diesem Beispiel über eine längere Zeitdauer anomale Werte vor.

2.4.2 Herausforderungen der Anomalieerkennung

Oft lassen sich Ausreißer bereits nach einer simplen Datenvisualisierung erkennen – durch den Menschen sozusagen *mit freiem Auge*. Bei großen und multidimensionalen Datensätzen aber wird das Sichtbarmachen der Ausreißer schwierig, sodass es notwendig wird, automatisierte Erkennungsalgorithmen zu verwenden.¹⁰⁷ Es muss also definiert werden, was normales und was anomales Verhalten repräsentiert, sodass der angewendete Algorithmus danach entscheiden kann. Dabei ergeben sich aber einige Herausforderungen:¹⁰⁸

Definition des normalen Verhaltens/ der normalen (Daten-)Region: Es ist oft nicht eindeutig, wo die Grenzlinie zwischen normal und anomal gezogen werden soll, oder welche Maße dafür verwendet werden sollen.

Veränderung des normalen Verhaltens: Was im aktuellen Betrachtungszeitraum als normal bezeichnet wird, ist gegebenenfalls in einem zukünftigen Zeitraum nicht mehr als normal anzusehen.

Veränderung der Anomalien: Anomalien ändern ihre Erscheinungsform z.B. im Kontext der Betrugsdetektion. Daher muss man sich auch auf einen dynamischen, sich adaptierenden Betrüger einstellen, der dem System normales Verhalten vormacht, sodass er nicht als Betrüger erkannt wird.

¹⁰⁶ Chandola et al., 2009, S.9

¹⁰⁷ vgl. Weber, 2020, S.61f

¹⁰⁸ vgl. Chandola et al., 2009, S.3

Keine einheitliche Anwendbarkeit der Algorithmen: Ein Modell bzw. eine Technik entwickelt für eine Domäne lässt sich nicht einfach für andere übertragen und dort anwenden. Kleine Abweichungen z.B. der Körpertemperatur sind wichtige Informationen in der Medizin, die entdeckt werden müssen, während Schwankungen im Aktienkurs als normal und erwartet angesehen werden.

Verfügbarkeit von gelabelten Daten: Für Training, Test und Validierung der Detektionsalgorithmen muss die Grundwahrheit - das sogenannte *Label* - vorliegen. Das Label kennzeichnet in den Daten die Zugehörigkeit entweder zur normalen oder zur anomalen Datenmenge. In realen Anwendungen fehlt meistens jene Information, die nötig wäre entsprechende Klassen zu definieren.¹⁰⁹ In der Literatur wird dieser Sachverhalt auch als *Ground Truth-Problem* erwähnt.¹¹⁰

Rauschen in den Daten: Mess- und Prozessrauschen (*Noise*), also zufällige Einflüsse, in den Daten kann mit tatsächlichen Anomalien verwechselt werden und ist somit schwer zu entfernen (Problem des *Data Cleansing*).

„Abweichungen zwischen Ausreißern und den normalen Datenpunkten können sich durch extreme Werte bei einem Merkmal zeigen (univariat), was vergleichsweise leicht zu entdecken ist. Eine deutlich größere Herausforderung stellt dagegen das Entdecken von Ausreißern dar, bei denen die Werte jedes einzelnen Attributes unauffällig sind, jedoch eine ungewöhnliche Kombination mehrere Attribute (Muster) vorliegt (multivariate Betrachtung).“¹¹¹

2.4.3 Drei grundlegende Ansätze zur Anomalieerkennung

Es können grundsätzlich drei verschiedene Herangehensweisen für die Anomaliedetektion unterschieden werden, bei denen man sich unter anderem der Techniken des Maschinellen Lernens und der Statistik bedient.¹¹²

Bei **Typ 1**, dem **unüberwachten Clustering**, wird versucht Ausreißer in ungelabelten Daten, also ohne Vorwissen, zu finden. Dieser Ansatz verarbeitet die Dateninstanzen im Sinne einer statischen Verteilung und beurteilt anhand von verschiedenen Abstandsmaßen, ob jene Dateninstanzen Ausreißer sind. *„Die Clusteranalyse befasst sich mit der Organisation von Daten in Gruppen mit ähnlichen Merkmalen. Im Idealfall sind die Daten innerhalb einer Gruppe eng aufeinander abgestimmt, während die Gruppen selbst sehr unterschiedlich sind.“¹¹³* Es sei angemerkt, dass dafür der gesamte Datensatz verfügbar sein muss.

Liegt Vorwissen anhand von gelabelten Daten vor, kann der **Typ 2** Ansatz angewandt werden. Dieser Ansatz gleicht der **überwachten Klassifikation** und es werden beide Klassen, nämlich normal und anomal, aus den gelabelten Daten modelliert. Somit kann jede Dateninstanz entweder der normalen oder anomalen Klasse zugeordnet werden. *„Klassifikation ist der*

¹⁰⁹ vgl. Kamat & Sugandhi, 2020, S.2

¹¹⁰ vgl. Krig, 2014, S.284

¹¹¹ Schacht & Lanquillon, 2019, S.109

¹¹² vgl. Hodge & Austin, 2004, S.4ff

¹¹³ Weber, 2020, S.54

Prozess der Vorhersage der Klasse der gegebenen Datenpunkte. [...] Die prädiktive Modellierung der Klassifizierung ist die Aufgabe, eine Abbildungsfunktion (f) von Eingangsvariablen (X) auf diskrete Ausgangsvariablen (y) zu approximieren.¹¹⁴ Durch das Vorwissen wird auch eine Online-Klassifizierung von Daten möglich.

In den meisten realen Anwendungsfällen liegt die Information über anomale und normale Zustände nur selten angemessen gleichverteilt vor, was in Folge die Modellbildung (z.B. für überwachte Klassifikation) erschwert oder gar unmöglich macht. Oft liegt z.B. nur die Information über den guten/ gesunden Zustand eines Systems vor, die aber dann natürlich dahin genutzt werden kann, nur den Gut-Zustand zu modellieren. In diesem Fall eignet sich der **Typ 3** Ansatz, dem **halb-überwachten Erkennen**, für die Anomalieerkennung. Einige Autoren bezeichnen diesen Ansatz auch als *Novelty Detection*, da bisher unbeobachtete Dateninstanzen beurteilt werden müssen. Es besteht auch die Möglichkeit, dass das Modell aus den neu beobachteten Daten lernt und sich so den Umständen anpasst.

2.4.4 Anomalieerkennung mit Hilfe des Maschinellen Lernens

In die vorher getätigte Einteilung der drei verschiedenen Ansätze werden nun Erkennungsmethoden des Maschinellen Lernens eingegliedert. Diese werden jedoch nur überblicksmäßig gelistet, weil die detaillierte Erklärung ausgewählter Algorithmen in Kapitel 4.4.1 auf S.66 erfolgt.¹¹⁵

Auf Klassifikation basierend: Das Modell (Der *Classifier*) muss anhand der gelabelten Daten eingelernt werden, sodass es im nächsten Schritt normale von anomalen Dateninstanzen unterscheiden kann. Es besteht die Möglichkeit auch mehrere normale Klassen einzulernen, wenn man z.B. von einer Maschine mehrere Betriebszustände kennt und zwischen diesen gewechselt wird. In diesem Fall wird von einem *multi-class-classifier* (Mehrklassenproblem) gesprochen. Das Gegenteil dazu ist der *one-class-classifier*. Diese Methoden werden dem Typ 2 bzw. Typ 3 zugeordnet. Folgende Algorithmen können als Beispiele genannt werden:

- Auf Neuronalen Netzwerken basierend: Multilayer Perceptron (MLP), Replikator neuronales Netzwerk (RNN)
- Auf Bayes Netzwerken basierend: Naiver Bayes-Klassifikator
- Auf Support Vector Machines (SVM) basierend: SVM, one-class-SVM
- Regelbasiert: Entscheidungsbaum, Bezeichnungen für Algorithmen dieser Art sind ID3 und C4.5¹¹⁶

Auf Nächster-Nachbar-Ansatz basierend: Die Methode des nächsten Nachbarn beruht auf der Annahme, dass normale Dateninstanzen einer Gruppe in enger Nachbarschaft angehäuft auftreten. Anomale Dateninstanzen hingegen sind weiter entfernt von ihren nächstgelegenen Nachbar-Dateninstanzen. Das Kriterium, ob normal oder anomal, wird entweder dichte- oder distanzbasiert formuliert. Diese Methoden werden dem Typ 1 zugeordnet. Folgende Algorithmen können als Beispiele genannt werden:

¹¹⁴ ebenda, S.47

¹¹⁵ vgl. Chandola et al., 2009, S.20ff

¹¹⁶ vgl. Agrawal & Agrawal, 2015, S.710

- Distanzbasiert: k-Nearest-Neighbor (kNN)
- Dichtebasiert: Local Outlier Factor (LOF), Connectivity-bases Outlier Factor (COF),

Auf Clustering basierend: hier werden Dateninstanzen, die in gewisser Weise Ähnlichkeiten aufweisen, gruppiert. Auch jene Methoden entsprechen dem Typ 1. Folgende Algorithmen gelten hierfür als Beispiele:

- k-Means
- k-Medoids
- Self-Organizing Maps (SOM)

Hofmockel (2019) führt auch noch als eigene Kategorie der Anomalieerkennung den Algorithmus des *Isolation Forest* an. Auch diese Methode ist dem Typ 1 zuzuordnen, weil hier keinerlei Vorinformation benötigt wird.

Aufgrund der unüberschaubaren Menge an Algorithmen, Variationen derer und anderen Techniken erhebt die vorangegangene Auflistung keinen Anspruch auf Vollständigkeit.

2.4.5 Exkurs: Statistische Techniken zur Anomalieerkennung

Im Folgenden wird nur ein kompakter Überblick zu statistischen Techniken zur Anomalieerkennung gegeben, da der Fokus dieser Forschungsarbeit auf den Techniken des maschinellen Lernens liegt. Die zentrale Annahme bei der Anomalieerkennung mittels statistischer Techniken ist:¹¹⁷ Normale Dateninstanzen treten in jenen Bereichen des stochastischen Modells (z.B. der Normalverteilung) mit hoher Wahrscheinlichkeit auf, während sich Anomalien außerhalb dieser Bereiche, also in Bereichen mit niedriger Wahrscheinlichkeit, wiederfinden.

Es wird ein sogenannter Anpassungstest (*Goodness-of-Fit*) durchgeführt, mit dem überprüft wird, ob die vorliegende Dateninstanz (Stichprobe) dem formulierten statistischen Modell entspricht. Mittels Modellannahmen wird aus den Daten der Normalzustand (möglicher Weise auch anomaler Zustand) modelliert und im Anschluss ein statistischer Interferenztest abgehalten, sodass die beobachtete Dateninstanz in Folge als normal oder anomal klassifiziert werden kann.¹¹⁸ Als Kriterien für die Kategorisierung als Anomalie oder Normalwert werden statistische Kennwerte oder gewisse Signal-Metriken herangezogen. Der wesentliche Unterschied zwischen statistischer Anomalieerkennung und Anomalieerkennung mittels ML ist, dass eine Modellstruktur angenommen wird, also der Zusammenhang zwischen Input und Output gewissen Modellvorstellungen entspricht. Es wird bei der statistischen Anomalieerkennung zwischen parametrischen und parameterfreien Detektionstechniken unterschieden:¹¹⁹

Parametrische Modelle: es wird angenommen, dass normale Dateninstanzen aus einem Modell, das aus den Daten konstruiert wurde, hervorgehen. Es wird *a priori* eine Modellannahme über die Verteilung (z.B. Gauß-Verteilung, Gamma-Verteilung) und daher

¹¹⁷ vgl. Chandola et al., 2009, S.33

¹¹⁸ vgl. Chandola et al., 2009, S.33

¹¹⁹ vgl. ebenda, S.33ff

über die Anzahl der zu ermittelnden Parameter getroffen. Demzufolge müssen jene Modellparameter aus den Daten geschätzt werden. Für die eindeutige Bestimmung z.B. der Gaußverteilung sind dies Mittelwert und Standardabweichung. Beispiele für Methoden:

- Auf Gauss Modell basierend: Six-Sigma, Box-Plot, Z-Score (Modified Z-Score¹²⁰) und Inter Quartile Range (IQR, Tukey-Test¹²¹)
- Auf Regressionsmodell basierend: hier werden Abweichungen der aktuell vorliegenden Dateninstanzen vom trainierten Prognosemodell (Residual) beurteilt. Beispiele für Modelle: ARIMA, ARMAX
- Auf einer Kombination von parametrischen Verteilungen basierend: z.B. Gaussian Mixture Model (GMM)

Parameterfreie Modelle: hier werden *a priori* keine Modellannahmen über die vorliegende Wahrscheinlichkeitsverteilung getroffen. Erst durch die Auswertung der Daten kann ein Modell gebildet und die Anzahl der nötigen Parameter bestimmt werden. Beispiele dafür sind:

- Auf Histogramm basierend: Histogram-based Outlier Score (HBOS)
- Auf einer Kernel-Funktion (Kerndichteschätzer) basierend

Mit dem nötigen Theoriewissen aus Instandhaltung, CM und Anomalieerkennung kann nun der Stand der Technik in drei verschiedenen Gebieten mittels einer ausführlichen Literaturanalyse erhoben werden. Die Ergebnisse der Literaturanalyse bilden die Grundlage für die Entwicklung des Phasenmodells für CM mittels Anomalieerkennung.

¹²⁰ vgl. Alam, M.: Statistical techniques for anomaly detection (15.09.2020) <https://towardsdatascience.com/statistical-techniques-for-anomaly-detection-6ac89e32d17a> (gelesen am: 10.01.2021)

¹²¹ vgl. Weber, 2020, S.62

3 Stand der Technik

In diesem Kapitel wird eine ausführliche Literaturanalyse zum Stand der Technik (SdT) der Zustandsüberwachung von kritischen und hochkomplexen Anlagen, der Informationsgewinnung unter schwieriger Datenlage und der Anomalieerkennung für die Zustandsüberwachung durchgeführt. Die Vorgehensweise richtet sich nach den Ausführungen aus Kapitel 1.2.2 auf S.8. Nach jedem Unterkapitel wird eine eventuell bestehende Forschungslücke ausgewiesen.

3.1 CM für kritische und hochkomplexe Anlagen

Durch die durchgeführte Literaturrecherche in diesem Forschungsfeld konnte ein Einblick in das CM von hochkomplexen und kritischen Anlagen und Maschinen erlangt werden. Bevor aber auf die Auswertung eingegangen werden kann, wird der Aufbau des morphologischen Kastens, der für die Literaturanalyse herangezogen wurde, erklärt.

Die Suche nach Literatur im Umfeld von *kritischen und hochkomplexen Anlagen* ist nötig, da nur sehr wenig Fachliteratur bzgl. CM von Industrieöfen verfügbar ist. Dadurch muss der Suchradius auf Anlagen wie Nuklear-, Heiz- oder Wasserkraftwerke und Anlagen aus der Prozess- und Produktionsindustrie erweitert werden. Diese (Kraftwerks-)Anlagen sind von zentraler Bedeutung für die Gesellschaft und das alltägliche Zusammenleben, da z.B. eine große Abhängigkeit zur elektrischen Energieversorgung, Wasserversorgung und zu Telekommunikationsnetzwerken besteht. Eine Störung dieser oder gar ein Ausfall hätte katastrophale Auswirkungen auf die betroffenen und abhängigen Personen und Institutionen. Gleichzeitig wird aber auch die Überwachung und Steuerung dieser Anlagen aufgrund der steigenden Komplexität und Vernetzung immer schwieriger.¹²² Diese Eigenschaften der Komplexität, Vernetzung und Verkettung zeichnen auch im Mikrokosmos einer Fabrikhalle eine Thermoprozessanlage aus. Zur Beurteilung der Komplexität der Anlage kann folgendes Klassifikationsschema in Abbildung 12 herangezogen werden.

	Komplexität		
	Gering	Mittel	Hoch
Transparenz	Gut zugänglicher Fehler	Versteckter Fehler	Zusätzlich komplizierte Funktionsprüfungen erforderlich
Informationsvielfalt	Einfaches Messgerät erforderlich	Zusätzlich Programmiergerät und Listings erforderlich	Zusätzlich komplizierte Messapparaturen erforderliche
Vernetztheit	Eindeutige Symptomatik	Nicht eindeutige Symptomatik	Vollkommen unklare Symptomatik
Fach- und Anlagenwissen (Diagnosekompetenz)	Nur begrenzter Wissensausschnitt erforderlich	Kenntnis komplizierter Zusammenhänge erforderlich	Zusätzlich besonders Spezialwissen erforderlich

Abbildung 12: Klassifikationsschema für komplexe Anlagen¹²³

¹²² vgl. Polycarpou et al., 2010, S.18

¹²³ Pawallek, 2016, S.160

3.1.1 Aufbau des morphologischen Kastens für die Analyse

Das folgende Analysekonstrukt dient dazu die selektierte Literatur auf strukturierte Weise und reproduzierbar zu analysieren und relevante Information zu extrahieren. Es ermöglicht ein Zerlegen des komplexen Themengebietes in überschaubare, leichter zu erfassende Teilbereiche. Das dabei verwendete Hilfsmittel *Morphologischer Kasten* wird auch im Produktentstehungsprozess sehr verbreitet verwendet, um eine Gesamtlösung aus vielen verschiedenen möglichen Teillösungen zu erarbeiten. Die Methode wurde vom Schweizer Fritz Zwicky (1971) entwickelt.¹²⁴ Dieselbe Intention liegt natürlich auch den Analysen in Kapitel 3.2.2 und 3.3.1 zugrunde. Die Beschreibung des Aufbaus speziell für das Thema CM bei kritischen und hochkomplexen Anlagen ist in Tabelle 9 zu sehen.

Tabelle 9: Aufbau des morphologischen Kastens für die Analyse von CM bei kritischen und hochkomplexen Anlagen

Dimension	Inhalt
Datensammlung	Die Sammlung der Daten und Informationen den Anlagenzustand betreffend geschieht entweder durch den Menschen oder durch fest angebaute Sensoren – siehe Kapitel 2.2.3 auf S.23.
Diagnose-Modelle	Diagnose-Modelle für CM wie in Kapitel 2.2.2 auf S.21 beschrieben. <u>Physikalische Modelle:</u> White-Box Ansatz wie z.B. Zustandsraummodelle <u>Datengetriebene Modelle:</u> Beispiele sind u.a. KNN und SVM; aber auch signalbasierte Techniken wie Fast Fourier Transformation (FFT) <u>Wissensbasierte Modelle:</u> Eine Kombination aus Erfahrung und ML-Techniken wird auf gespeicherte Informationen bestehend aus Expertenwissen und hinterlegtem Regelwerk angewendet (Fuzzy Logic und Expert Systems) <u>Hybride Modelle:</u> Kombination aus den oben genannten Ansätzen
Datenquellen	<u>Fehler-/ Ausfalldaten:</u> Informationen zu erfassten Betriebsstörungen bzw. -unterbrechungen <u>Produktqualität-Daten:</u> Erfassung der Output-Qualität der Anlage wie z.B. die Oberflächengüte eines Werkstückes <u>CM-Daten:</u> den Zustand der Maschine beschreibende Daten wie z.B. Drehzahl oder Schwingungsausschlag <u>Prozessdaten:</u> Daten, die den Prozess charakterisieren; z.B. Chargennummer oder Werkzeugdaten <u>Umwelt-Daten:</u> die Umgebung beschreibende Daten wie z.B. die Umgebungstemperatur oder -feuchtigkeit, Erschütterungen <u>IH-Daten:</u> Informationen zu Instandhaltungsaktivitäten, die durch ein entsprechendes System erfasst wurden
Anwendungsgebiet	Bezeichnet das Forschungsfeld, aus dem die Publikation stammt
Überwachte Komponente	Es können entweder aktive oder passive Anlagenkomponenten überwacht werden. <u>Aktive Komponenten:</u> sind sich bewegende Bauteile wie z.B. eine Kaplan turbine eines Wasserkraftwerks. In diesem Zusammenhang spricht man von Condition Monitoring (CM) <u>Passive Komponenten:</u> z.B. Dammmauer eines Speicherkraftwerks oder die Rohrleitungen eines Reaktorbehälters in einem Kernkraftwerk. In diesem Zusammenhang spricht man daher auch von Structural Health Monitoring (SHM)

Im Folgenden werden nun die Ergebnisse der morphologischen Analyse von ausgewählter Literatur über CM für hochkomplexe und kritische Anlagen aufgelistet. Für eine übersichtliche Darstellung muss die Gesamttabelle in drei Subtabellen aufgeteilt werden – siehe Tabelle 10, Tabelle 11 und Tabelle 12. Die ausgewählte Literatur wird mit Hilfe der oben genannten Systematik untersucht und bewertet. Trifft ein Merkmal einer Dimension auf eine Publikation zu, so wird an dieser Stelle ein Kreuz gesetzt. Der Fokus liegt auf Publikationen, die ab 2010 zu diesem Thema veröffentlicht wurden. Der Beitrag von Steck-Winter (2008) wird zusätzlich

¹²⁴ vgl. Feldhusen & Grote, 2013, S.373

in den Kanon aufgenommen, da er dem Anwendungsgebiet Industrieofen zuzuordnen ist und daher Relevanz für die Forschungsarbeit hat.

Tabelle 10: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (1/3)

SdT-Analyse			Datensammlung		Diagnose-Modelle			
Nr.	Jahr	Autor(en)	Mensch	Sensor	Physikalische	Datengetriebene	Wissensbasierte	Hybride
CM1	2017	Antonovskaya et al.		X		x		
CM2	2011	Baraldi et al.		X		x		
CM3	2014	Bonaldi et al.		X		x		
CM4	2015	Coble et al.		X	x	x	x	x
CM5	2012	Coble et al.		X	x	x	x	
CM6	2020	Demin et al.		X		x		
CM7	2018	Egusquiza et al.		X	x		x	
CM8	2010	Fast & Palmé		X		x		
CM9	2014	Gofuku		X	x	x	x	x
CM10	2011	Granjon		X	x			
CM11	2013	Shameer & Shameer		X		x		
CM12	2011	Jin et al.		X		x		
CM13	2019	Klun et al.		X		x		
CM14	2020	Monkova et al.		X		x		
CM15	2015	Lahdelma & Juuso		X		x		
CM16	2013	J. Liu et al.		X		x		
CM17	2011	Ma & Jiang		X	x	x		
CM18	2016	Marais et al.		X	x			
CM19	2016	Papaelias et al.	x		Nur Inspektion			
CM20	2010	Polycarpou et al.			Allgemein über kritische Infrastruktur			
CM21	2012	Shumaker et al.	x		Inspektion durch mobile Geräte			
CM22	2017	Steck-Winter et al.	x	X	x	x	x	
CM23	2020	Steck-Winter & Unger		X				
CM24	2017	Valero et al.		X	x			
CM25	2018	Xiao et al.		X		x		
CM26	2008	Steck-Winter	x	x				

Tabelle 11: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (2/3)

SdT-Analyse			Datenquellen				Anwendungsgebiet			
Nr.	Jahr	Autor(en)	Fehler/Ausfall	CM-Daten	Prozessdaten	Umwelt	IH-Daten	Industrieofen/Ofenanlage	Atomkraft-werk	Solarkraft-werk
CM1	2017	Antonovskaya et al.		x		x				
CM2	2011	Baraldi et al.		x					x	
CM3	2014	Bonaldi et al.		x						
CM4	2015	Coble et al.	x	x	X	x	x		x	
CM5	2012	Coble et al.	x	x	X	x	x		x	
CM6	2020	Demin et al.		x			x			
CM7	2018	Egusquiza et al.	x	x	X		x			
CM8	2010	Fast & Palmé		x	X					
CM9	2014	Gofuku		x	X				x	
CM10	2011	Granjon		x					x	

SdT-Analyse			Datenquellen					Anwendungsgebiet		
Nr.	Jahr	Autor(en)	Fehler/ Ausfall	CM- Daten	Prozess- daten	Umwelt	IH- Daten	Industrieofen/ Ofenanlage	Atomkraft- werk	Solarkraft- werk
CM11	2013	Shameer & Shameer		x						
CM12	2011	Jin et al.		x					x	
CM13	2019	Klun et al.		x		x				
CM14	2020	Monkova et al.		x						
CM15	2015	Lahdelma & Juuso		x						
CM16	2013	J. Liu et al.		x					x	
CM17	2011	Ma & Jiang		x					x	
CM18	2016	Marais et al.		x						
CM19	2016	Papaelias et al.					x			x
CM20	2010	Polycapou et al.						Allgemein über kritische Infrastruktur		
CM21	2012	Shumaker et al.					x		x	
CM22	2017	Steck-Winter et al.	x	x	X	x	x	x		
CM23	2020	Steck-Winter & Unger		x	X			x		
CM24	2017	Valero et al.		x						
CM25	2018	Xiao et al.	x	x	X	x	x			
CM26	2008	Steck-Winter	x	x	X	x	x	x		

Tabelle 12: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (3/3)

SdT-Analyse			Anwendungsgebiet				Überwachte Komponente		
Nr.	Jahr	Autor(en)	Heizkraftwerk	Wasserkraftwerk	Prozessindustrie	Produktion	Aktiv (CM)	Passiv (SHM)	
CM1	2017	Antonovskaya et al.		X			x	x	
CM2	2011	Baraldi et al.					x	x	
CM3	2014	Bonaldi et al.	x				x		
CM4	2015	Coble et al.					x	x	
CM5	2012	Coble et al.					x	x	
CM6	2020	Demin et al.			x		x		
CM7	2018	Egusquiza et al.		X			x		
CM8	2010	Fast & Palmé	x				x		
CM9	2014	Gofuku					x		
CM10	2011	Granjon					x		
CM11	2013	Shameer & Shameer		X			x		
CM12	2011	Jin et al.					x	x	
CM13	2019	Klun et al.	x					x	
CM14	2020	Monkova et al.		X			x		
CM15	2015	Lahdelma & Juuso				x	x		
CM16	2013	J. Liu et al.					x		
CM17	2011	Ma & Jiang					x	x	
CM18	2016	Marais et al.			x		x		
CM19	2016	Papaelias et al.						x	
CM20	2010	Polycapou et al.	Allgemein über kritische Infrastruktur						
CM21	2012	Shumaker et al.						x	
CM22	2017	Steck-Winter et al.					x	x	
CM23	2020	Steck-Winter & Unger					x		

SdT-Analyse			Anwendungsgebiet				Überwachte Komponente	
Nr.	Jahr	Autor(en)	Heizkraftwerk	Wasserkraftwerk	Prozessindustrie	Produktion	Aktiv (CM)	Passiv (SHM)
CM24	2017	Valero et al.		X			x	
CM25	2018	Xiao et al.		X				
CM26	2008	Steck-Winter					x	x

3.1.2 Einzelanalyse der Dimensionen

3.1.2.1 Datensammlung

Nachfolgend wird beschrieben welche Möglichkeiten es gibt, Daten für die Zustandsüberwachung zu erheben. Ein Großteil der analysierten Publikationen beschreibt die Datensammlung für das CM mittels Sensoren, einige wenige der analysierten Arbeiten beinhalten aber auch die Datensammlung bzw. Zustandserhebung durch den Menschen. Der Fokus dieser Arbeit liegt auf der Datenerhebung mittels Sensoren.

So werden bei Papaelias et al. (2016) die Vor- und Nachteile der verschiedenen State-of-the-Art zerstörungsfreien Prüfverfahren beschrieben mit denen passive Komponenten (z.B. isolierte Rohrleitungen oder Speichertanks) eines Solarwärmekraftwerks bei einer Inspektion überprüft werden können. Dabei werden Verfahren wie die Farbeindringprüfung (*Liquid Penetrant Inspection*, LPI) für das Erkennen von Oberflächendefekten oder die Ultraschalltestung (UT) vorgestellt. Die Autoren erwähnen auch bei gewissen Verfahren eventuelles Automatisierungspotential. Shumaker et al. (2012) betonen die Wichtigkeit von Kabelmonitoring und Kabelalterungsmanagement in Nuklearkraftwerken, da Kabel als passive Elemente für den Datenaustausch (Signalleitungen) fundamental wichtig sind. Das Problem bei Datenleitungen ist, dass diese selbst zur Fehlerquelle werden können und dadurch eventuelle Signale, die Fehlerinformationen beinhalten (z.B. Sensor im Reaktordruckbehälter misst kritische Temperaturen), nicht ordnungsgemäß weitergegeben werden können und kritische Zustände somit unentdeckt bleiben oder falsche Alarme ausgelöst werden. Es werden u.a. Lösungen für mobile Geräte vorgeschlagen, als auch ein integriertes Kabeltest- und Kabelmonitoringsystem. Steck-Winter et al. (2017) betonen, dass eine automatisierte Zustandsüberwachung von kritischen und hochkomplexen Anlagen – in deren Fall eine Industrieofenanlage – zusätzlich immer noch durch Inspektionen begleitet werden sollte. Die Forschungsbemühungen bei dieser Art von Anlagen zielen natürlich darauf ab, dieses menschliche Zutun auf ein Minimum zu reduzieren und das Personal optimal zu unterstützen. Gerade, weil z.B. in Atomkraftwerken die Strahlenbelastung für IH-Personal bestmöglich reduziert bzw. vermieden werden sollte.

Für die Zustandsüberwachung werden bei den angebrachten Sensoren unterschiedliche Effekte ausgenutzt: dynamische, chemische, physikalische, elektrische, Temperatur- und Partikeleffekte.¹²⁵ So wird z.B. die Beobachtung der Vibration der Kategorie der dynamischen Effekte zugeordnet - wie es auch bei Monkova et al. (2020) beim CM der Lagerung einer Kaplan-Turbine angewandt wird. Die Überwachung einer Pumpenmotoreinheit mittels

¹²⁵ vgl. Matyas, 2018, S.133f

Strommessung (Current Signature Analysis, CSA), wie dies bei Bonaldi et al. (2014) im Anwendungsfall eines Heizkraftwerks genutzt wird, wird der Kategorie der elektrischen Effekte zugezählt. Coble et al. (2015) machen darauf aufmerksam, dass auch die Sensoren (wie auch andere Instrumente) selbst als aktive Komponente überwacht und immer wieder einer Rekalibrierung unterzogen werden müssen, sodass ein sicherer Betrieb gewährleistet werden kann. Dieselben Autoren sehen weiteren Forschungsbedarf in Bezug auf die Platzierung der Sensoren vor allem bei passiven Komponenten von Nuklearkraftwerken (z.B. Wärmetauscher, Transformatoren, Kabel/ Leitungen). Hier gilt es aus Kostengründen zwischen der Anzahl der platzierten Sensoren und der nötigen Abdeckung/ Ausmaß der Überwachung abzuwiegen.

3.1.2.2 Diagnose-Modelle

Das Monitoring einer Anlage und auch die Fehlerdiagnose bei erkanntem Fehler kann auf unterschiedliche Weise, wie in Kapitel 2.2.2 auf S.21 beschrieben, realisiert werden. Bei den Diagnose-Modellen wird also zwischen datengetriebenen, physikalischen, wissensbasierten und hybriden Ansätzen unterschieden. Diese Modelle bestimmen, wie ein möglicher Instandhaltungsbedarf festgestellt werden kann. Aufgrund der Komplexität der Anlagen und dem daraus resultierenden unbekanntem Zusammenspiel einzelner Parameter wird im Großteil der untersuchten Publikationen auf datengetriebene Modelle für das CM gebaut. Doch bei datengetriebenen Modellen entsteht daraufhin ein neues Problem - ein Datenproblem. Die Nützlichkeit und Verlässlichkeit des trainierten Modells hängen nämlich direkt mit der Qualität der vorhandenen Daten zusammen, sodass sich z.B. fehlende Daten oder ungleichmäßig verteilte Daten (Problem in Kapitel 3.2 auf S.44 behandelt) negativ darauf auswirken.

Datengetriebene Modelle: Steck-Winter & Unger (2020) und Steck-Winter et al. (2017) stellen ein smartes CM für eine industrielle Thermoprozessanlage vor, das über die Zustandserfassung und das Monitoring hinaus auch Anomalien erkennt und Prognosen erstellt. Den Zeitverlauf einer Zustandsvariable kann das IH-Personal über ein Ampelchart verfolgen, über das der/die BedienerIn auch bei Abweichungen von der identifizierten Normkurve gewarnt wird. Das verwendete CM-System kann auch eine Kurvenverlaufsanalyse durchführen, bei der mittels Mustererkennung Kurvenmerkmale (z.B. Kontur und Volatilität) extrahiert und klassifiziert werden können.

Aus dem Bereich der Nuklearkraftwerküberwachung werden bei dieser Analyse fast nur datengetriebene Modelle untersucht. Jin et al. (2011) untersuchen eine datengetriebene Methode zum CM mittels Anomalieerkennung, die bei Sensoren unter der Annahme unterschiedlicher Rauschbelastung an einem Druckwasserreaktor-Simulator getestet wird. Mit *Symbolic Dynamic Filtering* (SDF) wird ein echtzeitfähiges Mustererkennungs-Tool an verschiedenen Bauteilen des Reaktors angewendet. Baraldi et al. (2011) zeigen am Fallbeispiel einer Reaktorkühlpumpe eines Druckwasserreaktors eine Methode, eine große Anzahl an unterschiedlichen Messsignalen nach zwei verschiedenen Gesichtspunkten zu gruppieren. Diese werden entweder anhand von deren Sensorplatzierung oder Signalkorrelation gruppiert. Daraus entstehen danach wieder Untergruppen. Für diese Untergruppen werden Auto-Assoziative Kernel Regressionsmodelle erstellt (AAKR), die in Folge Abweichungen feststellen können. Bei Ma & Jiang (2011) wird zwischen modellbasierter (in dieser Analyse gleichgesetzt den physikalischen Modellen, siehe im Folgeabsatz) und modellfreier (datengetriebene und signalbasierte Modelle) Fehlererkennung und -diagnose bei Komponenten von

Nuklearanlagen unterschieden. Für das datengetriebene CM von Instrumentierung, Anlagenequipment oder dem Reaktorkern werden unter anderem Künstliche Neuronale Netze (KNN), die *Multivariate State Estimation Technique* (MSET) oder *Principal Component Analysis* (PCA) vorgeschlagen. Bei der Analyse von z.B. Vibrationssignalen von Equipment, Motorstrom oder eventuellen losen Teilen (Loose Part Monitoring), also signalbasiertes CM, werden Methoden wie Fast Fourier Transformation (FFT), Autoregressive Modelle (AR), Zeit-Frequenz Analyse oder Wavelet Transform (WT) empfohlen. Klun et al. (2019) verwenden ein (berührungsloses) Laser-Doppler Vibrometer für die Vibrationsmessung von nicht-stationären Zuständen in einer Maschinenhalle eines Wasserkraftwerks. Diese Messungen sollen das SHM mittels seismischer Sensoren der Dammmauer unterstützen – dies stellt auch signalbasiertes CM dar, weil zur Signalverarbeitung FFT verwendet wird. Es werden auch Methoden zur Filterung von störenden Signaleinflüssen diskutiert.

Physikalische Modelle: Bei physikalischen Modellen wird das normale Verhalten der Anlage anhand von bekannten physikalischen Zusammenhängen modelliert. Dabei bedient man sich z.B. an Modellen der Strömungsmechanik oder Thermodynamik. Um Abweichungen zu detektieren, werden die analytisch errechneten Werte einer Zustandsvariable mit den tatsächlichen Messwerten verglichen, also Residuen gebildet, und so ein Alarm ausgelöst, wenn der zulässige Grenzwert überschritten wird. Da der Prozess selbst und auch die Messung durch gewisse Unsicherheiten verrauscht werden, müssen statistische Tests mit den Residuen durchgeführt werden, um valide Aussagen über den Zustand zu bekommen. Ma & Jiang (2011) zählen dazu z.B. den Luenberger-Beobachter (*Diagnostic Observer*), Kalman Filter, Zustandsraum-Modelle oder andere Methoden der Parameterschätzung. Sie sehen aber nur eine sehr geringe Bedeutung der physikalischen Modellierung (vor allem für Komponenten von Atomkraftwerken), da diese in der Anwendung nur sehr speziell und limitiert möglich ist. Marais et al. (2016) nützen den thermodynamischen Zusammenhang zwischen Entropie und Enthalpie für die Fehlerdetektion bei einem Reaktor für die autothermale Reformierung (ATR) in der Prozessindustrie. Die genaue Modellierung ermöglicht nicht nur die Erkennung von Fehlern, sondern auch die Unterscheidung von verschiedenen Fehlern (Fehlerisolation). Egusquiza et al. (2018) entwickeln ein numerisches Modell für den Betrieb einer Peltonturbine über ein FEM Modell für die Turbine und ein CFD Modell für den antreibenden Wasserstrahl. Über das FEM Modell der Turbine können somit Verformungen und Spannungen in Abhängigkeit vom Wasserstrahl berechnet werden. Diese Berechnungen werden mit Daten von 28 verschiedenen Peltonturbinen aus 25 Jahren Betrieb gegengeprüft. Die Zustandsüberwachung geschieht dadurch, dass gesammelte Echtzeitdaten in einem Diagnosezentrum (hohe Rechenleistung verfügbar) ausgewertet werden und so über strömungsmechanische und strukturmechanische Berechnungen die RUL ermittelt werden kann. Zusätzlich werden auch noch Vibrationsmessungen durchgeführt und mit einer umfangreichen Datenbank verglichen.

Wissensbasierte Modelle: Gofuku (2014) verwendet in seinem Paper die Technik *Cased-based Reasoning* (CBR), bei der mehrere Attribute der Messsignale beobachtet werden und so aufgrund von Änderung in diesen Attributen auf Anomalien der betrachteten Anlage geschlossen werden kann. Für diese Technik werden Referenzdaten benötigt, mit denen dann die aktuell gemessenen Daten verglichen und dadurch auf Ähnlichkeiten überprüft werden können. Es wird also die Ähnlichkeit zu einem normalen oder anomalen Zustand geprüft. Wenn

eine Abweichung festgestellt wird, erfolgt die Ermittlung, ob diese Anomalie bereits bekannt oder bisher unbekannt ist. Die Ähnlichkeit wird über eine exponentielle Verteilung ausgedrückt und kann Werte zwischen 0 und 1 annehmen, wobei 1 einer Übereinstimmung gleichbedeutend ist. Coble et al. (2015) argumentieren, dass Experten Systeme (Wissensbasierte Systeme) für umfangreiche und komplexe Systeme, wie ein Atomkraftwerk es darstellt, unübersichtlich werden können. Als Beispiele werden regelbasierte und fuzzy regelbasierte (*fuzzy rule-based*) Systeme genannt. Bei komplexen Systemen, wo viele Parameter überwacht werden, kann es im Falle einer Betriebsstörung oder eines Ausfalls zur Auslösung vieler Alarme bei Überschreitung der Grenzwerte kommen. In diesem Fall wird von einer Alarmflut (*Alarm Shower*) gesprochen. Sie ruft als Folge Überforderung beim IH-Personal hervor. Das Personal kann der geforderten Ausfallsbehebung und Ursachenanalyse nicht mehr zeitgerecht nachkommen.¹²⁶

Hybride Modelle: Es sei auch erwähnt, dass Steck-Winter et al. (2017) eine weitere Herangehensweise für die Zustandsüberwachung von Thermoprozessanlagen darlegen: sensorbasierende Zustandsüberwachungsmethoden ohne CM-System. Hier bedient man sich z.B. der Prozessdatenvalidierung bei der die Messdaten mit einem Funktionsmodell aus Bilanz- oder Massenstromgleichungen verglichen werden und so Abweichungen festgestellt werden können. Eine weitere Möglichkeit stellt das Control Performance Monitoring dar. Hierbei können anhand von der beobachteten Reglerperformance Rückschlüsse auf den Zustand der Anlage gemacht werden. Gofuku (2014) beschreibt in seiner Review ein hybrides Diagnosesystem, bei dem ein sogenannter Integrationsagent die Diagnoseergebnisse von verschiedenen Diagnoseagenten sammelt und auswertet. Die Diagnoseagenten verarbeiten die Signale aus dem Kernreaktor nach den oben genannten Modellen, also nach einem physikalischen, datengetriebenen, signalbasierten und wissensbasierten Modell.

3.1.2.3 Datenquellen

Egusquiza et al. (2018) nutzen für die numerische Modellierung der Peltonturbine Schadens- und Ausfallsdaten und analysieren diese, um fehlertypische Symptome zu ermitteln. Für einige repräsentative Schadensarten kann man auch typische Vibrationssignaturen, bzw. die Evolution dieser, vor und nach einer Reparatur identifizieren und in einer Datenbank hinterlegen. Steck-Winter & Unger (2020) und Steck-Winter et al. (2017) nutzen ebenfalls das Wissen über durchgeführte Reparaturen, um die Normalkurven, welche als Referenz für den Gutzustand bestehen, bestimmter Zustandsparameter zu aktualisieren. Dieselben Autoren verwenden auch Umgebungsmessungen (Umweltdaten) für eine ganzheitliche Zustandsbeobachtung. Daher erfassen Umfeldsensoren unter anderem Abgastemperatur, Erschütterungen (Beschleunigungen), Luftdruck und Ähnliches. Als Beispiel für das Verwenden von CM-Daten kann akustische Emission von Maschinenlagern herangezogen werden, so wie das Shameer & Shameer (2013) für ein proaktives CM eines Kraftwerks anwenden. Fast & Palmé (2010) verwenden für das *Online Condition Monitoring* eines Heizkraftwerkes zusätzlich auch Prozessdaten. Neben der Umgebungstemperatur und dem Umgebungsdruck dienen der Betriebsmodus und die Information, ob der *Anti-Icing* Modus gewählt ist, als Input für die KNN-Modelle von Gasturbine und Abhitzedampferzeuger.

¹²⁶ vgl. Isermann, 2011, S.11

3.1.2.4 Anwendungsgebiete

Hierzu werden zwei der betrachteten Anwendungsgebiete mit Fokus auf Instandhaltung kompakt beschreiben. Auf das Anwendungsgebiet von Industrieöfen wird aufgrund der direkten Relevanz zum Use Case dieser Arbeit eingegangen. Darüber hinaus werden Atomkraftwerke behandelt, da bestimmte Komponenten dieser Anlagen ähnliche Komplexitätsmerkmale aufweisen wie jene vom Use Case.

Industrieofen/ Thermoprozessanlage: Steck-Winter (2008) schreibt im Fachbericht über Thermoprozessanlagen, dass bei diesen eine Anlagenverfügbarkeit von mindestens 93% gefordert ist. Ein weiterer Faktor, der die Instandsetzung von Thermoprozessanlagen äußerst kostenintensiv macht, ist Zeit: bevor überhaupt Instandsetzungsarbeiten an der Anlage durchgeführt werden können, muss diese abgeheizt und im Anschluss an die fertiggestellten Instandsetzungsarbeiten wieder bereitgestellt (Aufheizen und Konditionierung der Ofenatmosphäre) werden. Jene Zeit beträgt in den meisten Fällen ein Vielfaches der eigentlichen Instandsetzungszeit. Steck-Winter & Unger (2020) argumentieren, dass industrielle Thermoprozessanlagen deshalb so schwierig zu warten und zu überwachen sind, weil alle ausfallkritischen Teile innerhalb des Ofens eingebaut sind. Es kann aber keine Sensorik wegen der hohen Temperaturen im Inneren des Ofens angebracht werden. Zusätzlich wird üblicherweise nur einmal jährlich eine Zustandsinspektion bei kaltem Ofen durchgeführt. Diese Ofenanlagen werden grundsätzlich als Blackbox angesehen, wodurch ein datengetriebener CM-Ansatz vorteilig ist.

Atomkraftwerk: Als sicherheitskritisches System, so Ma & Jiang (2011), steht die Erhaltung der Sicherheit bei Atomkraftwerken an oberster Stelle. Dazu trägt auch ein funktionierendes Überwachungs- und Instandhaltungssystem bei. Ein automatisiertes CM-System oder ein System zur automatisierten Fehlererkennung- und -diagnose (*Fault detection and diagnosis, FDD*) reduzieren die Strahlenbelastung für das IH-Personal, erhöhen die Equipmentzuverlässigkeit, verhindern das Einsetzen von Sicherheitsmechanismen (was zu Abschaltungen führen kann), helfen bei der korrekten Entscheidungsfindung und verringern Unsicherheiten bei der Reaktorkernüberwachung. Für das CM und vor allem das PHM von Atomkraftwerken bieten Coble et al. (2015), J. B. Coble et al. (2012) und Gofuku (2014) einen detaillierten Überblick.

3.1.2.5 Überwachte Komponente

Bei kritischen Anlagen (z.B. Speicherkraftwerk) werden neben der sich drehenden und stromerzeugenden Turbine zusätzlich auch nichtbewegliche Teile der Anlage überwacht. Sich bewegende Komponenten werden als aktive Teile bezeichnet und mittels CM überwacht. Durch *Structural Health Monitoring (SHM)* werden hingegen passive Komponenten wie eine Dammmauer beobachtet, wie Klun et al. (2019) zeigen. Bei passiven Komponenten treten Schäden unter anderem in Form von Rissen und Korrosion auf und resultieren typischerweise in lokalen Änderungen der Materialeigenschaften (elektrische und thermische Leitfähigkeit, magnetische Permeabilität etc.).¹²⁷

Durch die Vielzahl der überwachten Komponenten und die sich daraus ergebende heterogene Datenstruktur steht das Instandhaltungsmanagement vor einer weiteren Herausforderung

¹²⁷ vgl. Coble et al., 2012, S.3 (Kapitel 4)

diese Daten so aufzubereiten und verfügbar zu machen, dass diese für das CM genutzt werden können (*Sensor Fusion*) und verlässliche Diagnosen zulassen. Xiao et al. (2018) stellen zu diesem Thema ein *Fog-Computing* Rahmenwerk für das PHM eines Wasserkraftwerks vor. Dieses unterstützt bei geringer Latenz die Vernetzung von physischen Komponenten mit der Netzwerkinfrastruktur. Es ermöglicht zusätzlich Remote-Zugriff und Datensicherheit.

Tabelle 13: Fazit zum Forschungsbedarf bei komplexen Anlagen

Fazit Forschungsbedarf	
Synergien in der Datensammlung werden nicht genutzt	Im Großteil der Publikationen werden Daten nur über Sensoren gesammelt. Auch wenn Daten in einigen wenigen Fällen durch den Menschen gesammelt werden, werden diese selten mit Sensordaten kombiniert. Hier könnte aber neues Wissen generiert und z.B. auch detektiertes anomales Verhalten erklärt werden.
Datengetriebene Modelle stehen im Fokus der Publikationen	Die meisten analysierten Publikationen beschäftigen sich mit ML-basiertem und signalbasiertem CM. Dabei gerät die Einbeziehung von Expertenwissen ins Hintertreffen, sodass wissenschaftliche Diagnosemodelle nur selten vorkommen. Gerade bei komplexen Anlagen ist aber humanes Wissen oft unverzichtbar in der Modellierung und Interpretation.
Vorhandene Datenquellen bleiben ungenutzt	Für die Modellierung werden mehrheitlich nur CM-Daten herangezogen. Auch wenn dabei oft mehrere Parameter gemessen werden, bleiben Ausfalls-, Umgebungs-, Prozess- und IH-Daten ungenutzt. Auch hier liegt ein offensichtliches Ausbaupotenzial vor. Aber die Verarbeitung von heterogenen Datensätzen eröffnet völlig neue Forschungspfade – siehe Ansari et al. (2019).
Untersuchte Datensätze für ML-Modelle sind bereits gelabelt	Den Autoren stehen aufwendig präparierte und gelabelte Datensätze (oder Forschungsdatensätze) zur Verfügung, an denen die Diagnosemodelle für das CM validiert werden können. Es wird kaum auf Datensätze mit fehlender Ground Truth eingegangen.

In einigen der vorher genannten Publikationen wird zwar auf das Problem der Informationsgewinnung unter fehlender bzw. begrenzter Ausfallsdatenlage für das Training von datengetriebenen Diagnosemodellen hingewiesen, die meisten Autoren aber bleiben eine genaue Ausführung zur Problemlösung schuldig. Daher wird auch zu diesem Themenbereich eine Literaturanalyse durchgeführt.

3.2 Informationsgewinnung unter fehlender bzw. begrenzter Ground-Truth- und Ausfallsdatenlage

In diesem Abschnitt wird das Problem einer möglichen schlechten Datenlage für das Trainieren von Modellen bearbeitet. Neben fehlenden Dateneinträgen (*Missing Values*) kann auch ein unbalancierter Datensatz (Fokus dieser Arbeit) Probleme bereiten: Sollte eine Klassifikation für das Erkennen von guten und schlechten Anlagenzuständen durchgeführt werden müssen dafür genügend repräsentative Daten für den guten wie auch den schlechten/fehlerhaften Anlagenzustand vorhanden sein. Nur so gelingt ein Einlernen eines aussagekräftigen Modells, das innerhalb eines CM-Systems verwendet werden kann. Abbildung 13 visualisiert das Problem mit Hilfe eines Schachbrettmusters.

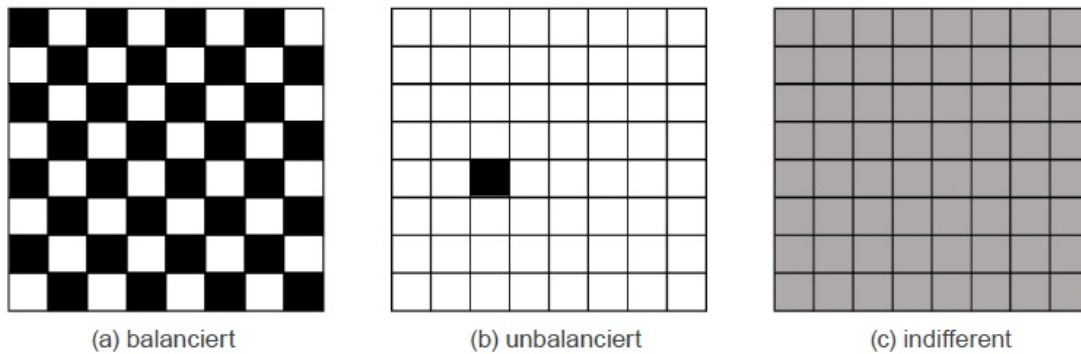


Abbildung 13: Qualität des Trainingsdatensatzes¹²⁸

Die weißen Quadrate repräsentieren die Daten z.B. des Gutzustandes und die schwarzen die des Schlechtzustandes. Beide Zustände sind bei der Instandhaltung von Interesse. Beispiel (a) liegt eine ausgeglichene Verteilung beider Zustände vor – optimale Voraussetzungen für ein Modell-Training. In (b) hingegen ist nur ein Datenbeispiel des Schlechtzustandes verfügbar. Er herrscht also ein unbalancierter Datensatz vor, aber immerhin sind die Label (*gut*, *schlecht*) bekannt. Um die schlechte Balance der Daten in einem binären Problem zahlenmäßig auszudrücken, eignet sich die *Imbalance Ratio* (IR), bei der die Anzahl der Negativbeispiele (schwarz) durch die Anzahl der Positivbeispiele (weiß) dividiert wird.¹²⁹ In der Praxis ist meistens letzteres Beispiel (c) vorzufinden, wo weder Informationen über den Zustand und schon gar keine über die Verteilung vorhanden sind. Das beschreibt eine schlechte *Ground-Truth*. Hier bedarf es *Data Engineering*, „[...] d. h. das Bereinigen der Daten von Fehlern, Rauschen und vor allem das Entwickeln von Strategien, gut von schlecht unterscheiden zu können.“¹³⁰

Den Use Case betreffend: Aufgrund von der bisher gewählten Ofen-Instandhaltungsstrategie (siehe Problemdefinition Kapitel 1.1 auf S.3) liegen nur sehr wenige Datenbeispiele für einen Schlechtzustand der Anlage vor bzw. wurden jene Beispiele nicht als solche gelabelt, sodass sie für den Algorithmus weder als gut noch schlecht klassifizierbar sind. Man spricht also von einem unbalancierten (*imbalanced/ skewed data*) bzw. von einem indifferenten Datensatz. Es gibt für dieses Problem unterschiedlichste Ansätze zur Problemlösung. Bevor aber über Merkmale und deren Kennzeichnung diskutiert werden kann, müssen diese erst aus den Datensätzen erzeugt werden.

Hier geschieht eine Eingrenzung für diese Literaturanalyse bzgl. Informationsgewinnung: es werden nur Zeitreihen (*Time Series*) betrachtet. Das entspricht dem Datensatz der zur Verfügung gestellten Messungen vom Use Case.

3.2.1 Merkmalsextraktion für Zeitreihen

Eine Zeitreihe setzt sich aus endlich vielen, zeitlich nacheinander angeordneten Messwerten zusammen

¹²⁸ Traphöner, 2018, S.4

¹²⁹ vgl. Fernández et al., 2018, S.20

¹³⁰ Traphöner, 2018, S.4

Formel 1: Mathematische Darstellung einer Zeitreihe

$$x(t_1), x(t_2), \dots, x(t_T) \in \mathbb{R}^n, k = 1, \dots, T$$

wobei $t_1 < t_2 < \dots < t_T$ gilt. Eine Zeitreihe wird als skalar oder univariat bezeichnet, wenn $n=1$ gilt, also zu jedem Zeitpunkt nur eine Beobachtung vorliegt. Liegen zu jedem Zeitpunkt mehrere Beobachtungen vor, also $n > 1$, dann nennt man die Zeitreihe multivariat.¹³¹ Beispiele für Zeitreihen sind unter anderem Wetterbeobachtungen oder Aktienkurse.

Bei der Analyse von Zeitreihen versucht man diese in ihre Anteile zu zerlegen. So besteht ein Interesse an eventuellen Trends, besonderen Formen oder Mustern in den Zeitreihen.¹³² Es können z.B. auch Mittelwert, Offset (konstantes Niveau), Saisonalität oder Ähnliches in den Beobachtungen ermittelt werden. Auch so können wiederum neue Informationen über die Zeitreihe generiert werden.

Ratanamahatana et al. (2010) argumentieren, dass für die Analyse der Zeitreihen mittels Data Mining bzw. ML- Techniken eine höher dimensionale Repräsentation notwendig ist und rohe Zeitreihendaten nicht ausreichend sind. Die neue Repräsentation der Daten fungiert einerseits als Merkmalsextraktionsschritt (*Feature Extraction*) und andererseits auch als Optimierung der Speicherbelastung bei der computerbasierten Datenverarbeitung. So wird die Ähnlichkeit mehrerer Zeitreihen mittels Euklidischem Abstandsmaßes, Dynamic Time Wrapping (DTW), Longest Common Subsequence Similarity (LCSS), stochastischer Methoden oder Formähnlichkeitsanalyse untersucht. Höherwertige Repräsentationen stellen Ergebnisse aus der Discret Fourier Transformation (DFT), Discrete Wavelet Transform (DWT), Piecewise linear oder Piecewise Constant Models (PAA), Adaptive Piecewise Constant Approximation (APCA) und die Single Value Decomposition (SVD) dar. Mit diesen Datentransformationen ausgerüstet können auch klassische Data Mining Ansätze für Zeitreihen wie Clustering, Klassifikation etc. angewendet werden. Besondere Erwähnung gilt der Verdichtung (*Summarization*) einzelner Merkmale, wie z.B. des Mittelwertes, mit der auf einfache Weise Informationen sichtbar gemacht werden können. In Abbildung 15 ist ein roher Zeitreihendatensatz zu sehen: Hier wurden einzelne Strommesswerte tageweise aufsummiert. Die Darstellung ist übersichtlicher als jene in Abbildung 14.

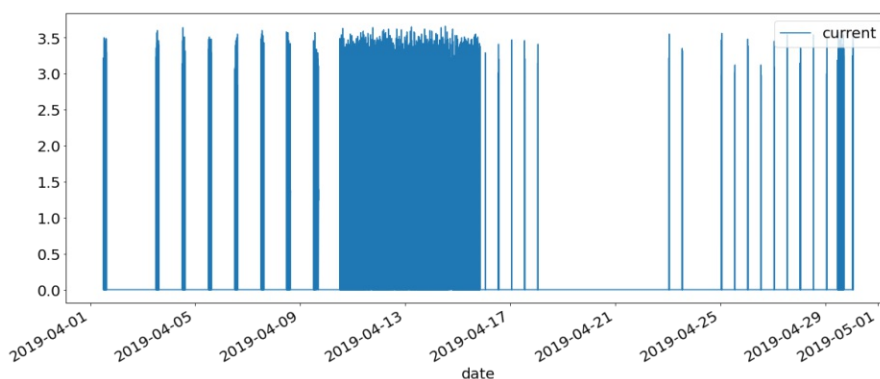


Abbildung 14: Rohes Zeitreihendatensatz über Strommessung im Monat April 2019¹³³

¹³¹ vgl. Deistler & Scherrer, 2018, S.1

¹³² vgl. Ratanamahatana et al., 2010, S.1065

¹³³ Eigene Darstellung

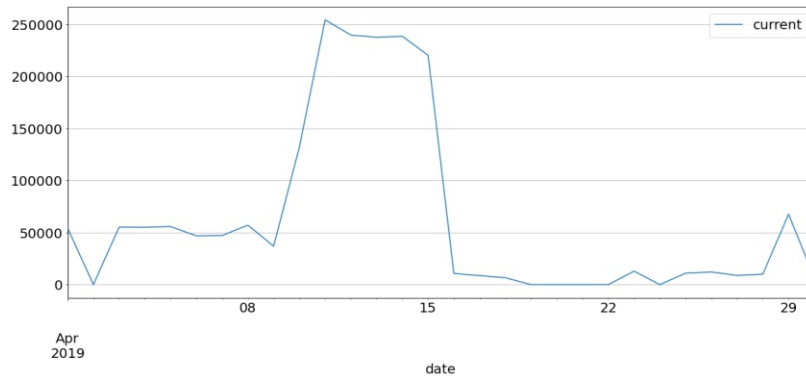


Abbildung 15: Beispiel für Verdichtung einer Zeitreihe¹³⁴

Nach dem eine Merkmalsrepräsentation (*Feature Space*) der Zeitreihen erstellt wurde und sehr wahrscheinlich ein unbalancierter oder gar indifferenter Datensatz entstanden ist, müssen auch für jenes Problem Techniken gefunden werden. Hierzu wird vorher die Methode zur Literaturanalyse dargelegt.

3.2.2 Aufbau des morphologischen Kastens für die Analyse

In Tabelle 14 wird der Zusammensetzung des morphologischen Kastens für die Analyse der Publikationen zum Thema unbalancierte Datensätze aufbereitet.

Tabelle 14: Aufbau des morphologischen Kastens für die Informationsgewinnung bei unbalancierten Daten

Dimension	Inhalt
Ansatz zur Lösung	Das Problem des unbalancierten Datensatzes kann entweder auf Daten- oder Algorithmusebene angegangen werden. Hier werden genauer vier verschiedene Arten betrachtet: <u>Pre-Processing</u> : beim Aufbereiten der Daten werden unterschiedliche Resampling-Techniken betrachtet. Z.B.: SMOTE, undersampling <u>Algorithmus-fokussiert</u> : bekannte Lernalgorithmen werden um Techniken des Imbalanced Learning erweitert. Z.B.: Bagging, Boosting <u>Kostensensitives Lernen</u> : einer falschen Klassifikation werden Kosten zugerechnet. Z.B.: Universum-SVM <u>Ensemble</u> : Parallelschaltung mehrerer Klassifikatoren und Kombinationstechnik aus den oben genannten. Z.B.: Weighted Minority Oversampling Technique (MWMOTE)
Lernmodell	Hier wird der verwendete Lernalgorithmus angeführt. Sollte der Ansatz zur Lösung des Datenproblems algorithmusbasiert sein, wird hier im Speziellen der erweiterte Algorithmus genannt. Beispiele: KNN, SVM, Random Forest
IB-Methode	In dieser Dimension wird der verwendete Lösungsansatz genannt. Wird z.B. ein Pre-Processing Ansatz in der Publikation verwendet, könnte hier stehen: SMOTE
Performance-Metriken	Zur Evaluation der Leistung der angewandten Datentechniken werden verschiedene Kennzahlen herangezogen, wie z.B. G-mean, ACC
Anwendungsgebiet	Bezeichnet das Forschungsfeld, aus dem die Publikation stammt

In Tabelle 15 und Tabelle 16 sind die Ergebnisse der morphologischen Analyse aufgelistet. Auch hier musste die Gesamttabelle aus Gründen der Übersichtlichkeit in zwei Subtabellen aufgeteilt werden.

¹³⁴ Eigene Darstellung

Tabelle 15: Informationsgewinnung unter schlechter Ausgangsdatenlagen: Ergebnisse der morphologischen Analyse (1/2)

SotA-Analyse			Ansatz zur Lösung				Lernmodell
Nr.	Jahr	Autor(en)	Pre-Process-ing	Algorithmus-fokussiert	Kosten-sensitives Lernen	Ensemble	
IB1	2016	Birla et al.	x	x	x		CART; Logistic Regression
IB2	2010	Chawla	x			x	
IB3	2017	Douzas & Bacao	x				Logistic Regression; Gradient Boosting Machine
IB4	2020	Feng et al.				x	Random Forest, Adaboost
IB5	2018	Fernández et al.	x				Diverse
IB6	2017	Haixiang et al.	x	x	x	x	Diverse
IB7	2019	Kaur et al.	x	x	x	x	Diverse
IB8	2016	Krawczyk	x	x	x	x	Diverse
IB9	2017	Lin et al.	x				C4.5, SVM, MLP, NN, NB, alle auch mit AdaBoost; andere Benchmark Algorithmen
IB10	2017	Lu et al.				x	C.4.5, Adaboost
IB11	2015	Mahdiyah et al.		x			ELM; IDELM; BPNN; SVM
IB12	2019	Parsa et al.	x				SVM, PNN
IB13	2018	Picek et al.	x				Radial Kernel SVM, RF
IB14	2015	Santos et al.	x	x	x	x	Diverse
IB15	2015	Sanz et al.		x			IVTURS (RRW_I), basierend auf FARC-HD
IB16	2019	Tang et al.			x		LDM
IB17	2018	B. Wang & Mao				x	Cw-SVDD
IB18	2015	Yan et al.		x			CNN

Tabelle 16: Informationsgewinnung unter schlechter Ausgangsdatenlagen: Ergebnisse der morphologischen Analyse (2/2)

SotA-Analyse			IB-Methode	Performance Metriken	Anwendungsfall
Nr.	Jahr	Autor(en)			
IB1	2016	Birla et al.	Prior Probabilities; Under-sampling; Loss-Matrix	AUC/ ROC; auch ACC	Risikobewertung in Kreditvergabe
IB2	2010	Chawla	SMOTE; SMOTEBoost	AUC/ ROC; auch ACC	
IB3	2017	Douzas & Bacao	SOM Oversampling (SOMO)	AUC; G-mean; F-measure	Diverse
IB4	2020	Feng et al.	SMOTE-Adaboost	AUC; Specificity, G-mean; ACC, recall	Prognose der Montagequalität
IB5	2018	Fernández et al.	SMOTE und Erweiterungen		Diverse
IB6	2017	Haixiang et al.	Diverse	Diverse	Diverse
IB7	2019	Kaur et al.	Diverse	Diverse	Diverse
IB8	2016	Krawczyk	Diverse		Diverse
IB9	2017	Lin et al.	Clustering-based und under-sampling	AUC/ ROC; auch ACC	Diverse Datensätze (auch large-scale)
IB10	2017	Lu et al.	Ensemble Undersampling	Sensitivität; Spezifität; FPC-rate; F-measure; G-Mean;	Medizin: Erkennung von Krebsgewebe in MRI Bildern
IB11	2015	Mahdiyah et al.	Integrating Data Selection mittels MSE	ACC, Precision, Recall; Specificity, G-Mean	Diverse Benchmark Datensätze
IB12	2019	Parsa et al.	Regular SMOTE; Borderline SMOTE; SVM SMOTE	ACC, DR, FAR	Echtzeit Verkehrsunfalldetektion

SotA-Analyse			IB-Methode	Performance Metriken	Anwendungsfall
Nr.	Jahr	Autor(en)			
IB13	2018	Picek et al.	SMOTE; SMOTE+ENN	Unterschiedl. aus ML und SCA-Analyse; werden verglichen	Side-Channel Attacks (SCA): Versuch kryptographische Verschlüsselungen mittels ML zu brechen
IB14	2015	Santos et al.	Diverse	MacroF	Testdaten von Windturbinenteststand
IB15	2015	Sanz et al.		Statistische Tests	Diverse Benchmark Datensätze aus der Finanzbranche
IB16	2019	Tang et al.		Sensitivität; G-Mean; AMC	Windturbinenmonitoring
IB17	2018	B. Wang & Mao		G-mean; F-measure; AUC	Lichtbogenofen
IB18	2015	Yan et al.	Bootstrapping	Recall, F-score	TRECVID Benchmark Video Datensatz

3.2.3 Analyse der Dimensionen

In diesem Abschnitt werden Techniken präsentiert, die ein Lernen von einem unbalancierten Datensatz ermöglichen. Es wird gezeigt, dass Klassifikation auch bei einer suboptimalen Datenausgangslage möglich ist. In der Literatur wird zwischen binärer (zwei mögliche Klassen) und multipler (mehrere Klassen möglich) Klassifikation unterschieden. Hier liegt Fokus auf binärer Klassifikation wegen des konkreten Anwendungsfalles. Konventionelle Klassifikationsalgorithmen bevorzugen beim Lernen jene Klasse, die zahlenmäßig stärker im Datensatz vertreten ist. Es entsteht also ein Bias hin zur Mehrheitsklasse (Majoritätsklasse). Das Resultat davon ist eine schlechtere Erkennung der unterrepräsentierten Minderheitsklasse (Minoritätsklasse).¹³⁵ Wie im vorliegenden Anwendungsfall dieser Arbeit steht aber gerade jene Minoritätsklasse im Fokus der Analyse.

Trotz der gesonderten Auflistung der Dimensionen in der Literatur wird die Folgende Auswertung nach den *Ansätzen zur Lösung* eingeteilt. Es werden also die anderen Dimensionen gleich miteinbezogen, mit Ausnahme der Dimension Performance-Metriken, die gesondert betrachtet wird.

3.2.3.1 Ansatz zur Lösung

Dabei wird versucht das Problem des unbalancierten Datensatzes entweder auf Datenebene (extern), also bevor ein ML-Algorithmus die Daten verarbeitet, oder auf Algorithmusebene (intern) zu lösen. In der Fachliteratur werden zusätzlich noch zwei weitere Kategorien unterschieden: kostensensitive und hybride Ansätze.

Pre-Processing: Es werden die Daten in der Vorbereitung entsprechend manipuliert, sodass keine Adaptionen am Lernalgorithmus vorgenommen werden müssen. Der Datensatz wird also davor durch verschiedene *Resampling*-Techniken ausbalanciert.

¹³⁵ vgl. Vluymans, 2019, S.81

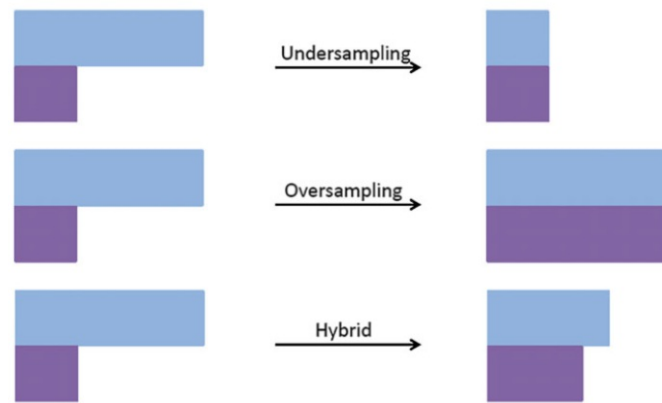


Abbildung 16: Ansätze für die Manipulation der Daten im Pre-Processing für den binären Fall: Mehrheitsklasse (hellblau) und Minderheitsklasse (violett)¹³⁶

In Abbildung 16 sind die drei möglichen Datenmanipulationen dargestellt. Beim *Undersampling*, so Fernández et al. (2018), wird einer Subset erstellt indem von der Mehrheitsklasse Instanzen eliminiert werden. Beim *Oversampling* wird die Minderheitsklasse mehrfach repliziert, sodass ein Gleichgewicht in der Anzahl der Dateninstanzen vorherrscht. Beim hybriden Ansatz des Pre-Processings wird eine Kombination von Undersampling und Oversampling angewandt. Pre-Processing Ansätze sind im Gegensatz zu den anderen Ansätzen in der Literatur am weitesten verbreitet.

Picek et al. (2019) testen als einfache Technik *Random Undersampling* für die Vorbereitung eines unbalancierten Datensatzes. Es ergeben sich dabei aber zwei Nachteile: 1) die Mehrheitsklasse wird zahlenmäßig massiv reduziert, um mit der Minoritätsklasse ausgeglichen zu sein, und daher besteht 2) die Möglichkeit, dass wichtige Informationen verloren gehen. Lin et al. (2017) verwenden ein Cluster-basiertes Undersampling. Dabei werden zwei verschiedene Strategien verfolgt: In der ersten Herangehensweise werden gleichviele Cluster k erzeugt, wie Dateninstanzen N in der Minderheitenklasse vorliegen, also $k=N$. Mit dem k-Means Algorithmus wird nun die Mehrheitsklasse geclustert, sodass N Cluster-Mittelpunkte vorliegen, die dann die Datenpunkte der Mehrheitklasse ersetzen. Weil in der ersten Strategie durch die Cluster-Mittelpunkte sozusagen neue synthetische Punkte eingeführt wurden, sucht die zweite Strategie den nächsten Nachbarn des in der ersten Strategie gefundenen Mittelpunktes und legt diesen Punkt als Vertreter der Mehrheitsklasse fest. Auch so kann wieder ein Gleichgewicht hergestellt werden.

Parsa et al. (2019) nützen die Oversampling-Technik SMOTE (*Synthetic Minority Oversampling Technique*), um die zwei überwachten Lernalgorithmen SVM und Probabilistic Neural Network (PNN) mit einem balancierten Datensatz zu trainieren. Das System sollte für die Echtzeit-Erkennung von Verkehrsunfällen verwendet werden, indem Merkmale des zu- und abfließenden Verkehrs und andere Parameter beobachtet werden. Es wurden drei Varianten getestet, nämlich Regular SMOTE, Boderline SMOTE und SVM SMOTE. Der reguläre SMOTE-Algorithmus setzte sich mit seiner Performance durch. Anstatt den vorhandenen Minderheitsdatensatz zu replizieren werden bei SMOTE zwischen den Datenpunkten der Minderheitsklasse in der Nachbarschaft (zufällig) interpoliert, sodass synthetisch mehr

¹³⁶ Vluymans, 2019, S.83

Datenpunkte der Minderheitsklasse entstehen. Dabei kann es unter anderem zu Überlappungen kommen, die aber durch Erweiterungen der Technik (Boderline SMOTE etc.) verhindert oder minimiert werden können.¹³⁷ Auch Picek et al. (2019) testen SMOTE und zusätzlich auch Random Undersampling, Random Oversampling with Replacement und eine Erweiterung von SMOTE (SMOTE+ENN) für die Datenvorbereitung. Oversampling-Techniken neigen grundsätzlich dazu ein Overfitting zu erzielen - d.h. der ML-Algorithmus passt sich zu sehr dem Trainingsdatensatz an und verliert die Fähigkeit zu generalisieren. Erweiterungen wie SMOTE Edited Nearest Neighbour (SMOTE+ENN) schaffen Abhilfe. Zuerst wird der gebräuchliche SMOTE-Algorithmus ausgeführt. Dann werden überlappende Datenpunkte in der Nachbarschaft durch die ENN-Methode entfernt, wodurch klar definierbare Klassen entstehen. Douzas & Bacao (2017) nützen Self-Organizing Map Oversampling (SOMO) um die Datensätze für Logistic Regression und Gradient Boosting Machine Klassifikatoren zu präparieren. Der ursprüngliche höherdimensionale Datensatz wird zuerst durch den SOM Algorithmus geclustert und dadurch in einen diskreten zweidimensionalen Datenraum gemappt. Danach wird innerhalb der Minderheitencluster (*intra cluster*) Oversampling durchgeführt. Im letzten Schritt werden bei Vorhandensein mehrerer Minderheitencluster zwischen den einzelnen Minderheitenclustern (*inter cluster*) auch noch neue synthetische Datenpunkte generiert.

Algorithmus-fokussiert: bei diesem *internen* Ansatz werden bestehende Klassifikationsalgorithmen so angepasst, dass auch die Minderheitenklasse entsprechend miteinbeziehen bzw. ein gewisser Bias zur Minderheitenklasse aufgebaut wird. Dazu muss natürlich die Funktionsweise des verwendeten Klassifikators bekannt und Wissen über das Anwendungsgebiet vorhanden sein.¹³⁸

Yan et al. (2016) verwenden für die Klassifikation von Multimedia Daten ein Convolutional Neural Network (CNN), eine Deep Learning Methode. In das CNN integriert ist ein Bootstrapping Schritt, mit dem die schiefe Datenverteilung ausgeglichen werden soll. Die Daten entstammen dem TRECVID Benchmark Datensatz. Die Bootstrapping Methode unterteilt den ursprünglichen Datensatz in gleich große Unterdatensätze (Batches). Diese haben wiederum die gleiche Imbalance Ratio wie der Ausgangsdatsatz. Mit diesen Batches kann dann das CNN trainiert werden. Bei Sanz et al. (2015) wird ein auf Fuzzy-Rules basiertes Klassifikationssystem präsentiert, mit dem unbalancierte Finanzdaten auf Algorithmusebene verarbeitet werden können. Mit dem *Internal-valued fuzzy rule-based classification system with tuning and rule selection* (IVTURS_{FARC-HD}) können Finanzmarkt-Abläufe auch unter dem Einfluss von hohem unerwartetem Risiko modelliert oder vorhergesagt werden, ohne dass die Daten gesampelt oder mittels Pre-Processing vorbereitet werden müssen.

Kosten-sensitiv: Kosten-sensitives Lernen fällt als Ansatz zwischen die Pre-Processing und Algrithmus-fokussierten Ansätze. Es werden Modifikationen auf Datenebene (spezifische Dateninstanzen stärker gewichtet) und auf Algorithmusebene (Gewichtungen im Lernprozess) vorgenommen, sodass ein Bias in Richtung der Minoritätsklasse entsteht.¹³⁹

¹³⁷ vgl. Fernández et al., 2018, S.98ff

¹³⁸ vgl. ebenda, S.22

¹³⁹ vgl. Fernández et al., 2018, S.22

Tang et al. (2019) nutzen einen Kosten-sensitiven Ansatz für die Schadenserkenkung bei Windturbinen. Der entwickelte Algorithmus ist eine *Cost-sensitive Large Margin Distribution Machine* (CLDM). Dessen Performance ist entweder gleich gut oder besser im Vergleich mit den Vergleichsalgorithmen SVM, w-SVM und LDM. Birla et al. (2016) versuchen mit Classification and Regression Tree (CART) und einer Logistic Regression (spezielle Aktivierungsfunktion eines Neuronalen Netzwerkes) das Kreditausfallsrisiko vorherzusagen. Da Ausfälle selten vorkommen, liegt ein unbalancierter Datensatz für das Training vor. Für den CART Algorithmus im Speziellen werden neben Ausgangswahrscheinlichkeiten (Ausfall oder nicht) und einer Undersampling Technik auch eine Verlust- und Gewichtungsmatrix getestet. Dabei werden entweder Falschklassifikationen bestraft oder richtige Klassifikationen belohnt und daher stärker beim Einlernen berücksichtigt.

Ensemble: Durch die Kombination mehrerer Klassifikatoren wird eine Verbesserung in der Präzision der Klassifikationsergebnisse erzielt. Dies geschieht meistens in Kombination mit Pre-Processing und kosten-sensitiven Methoden aus den oberen Kategorien, wodurch sich ein hybrider Ansatz ergibt.¹⁴⁰

Wang & Mao (2018) untersuchen in ihrer Arbeit die Prozessdaten eines Lichtbogenofens. Um datengetriebene Reglermethoden implementieren und deren ordnungsgemäßes Funktionieren gewährleisten zu können, müssen in den Daten Ausreißer in Echtzeit detektiert werden. Dies ist ein herausforderndes Unterfangen, da die vorliegenden Daten als indifferent, nicht-stationär und verrauscht charakterisiert sind. Dafür wird ein Dreiphasenmodell entwickelt, das sich aus einem Online-Modelltraining, einer Online-Anomaliedetektion und einem Updateschritt zusammensetzt. Im Online-Training wird der Datensatz in k Cluster mittels k-Means Clustering aufgeteilt und in jedem Cluster wird ein gewichtetes Support Vector Data Description Modell erstellt (w-SVDD). Jedes dieser gut trainierten Modelle stellt einen Ein-Klassen-Klassifikator dar, der eben nur den Gutzustand des Ofens kennt. Dadurch wird gleichzeitig das Problem der nicht-gelabelten und unbalancierten Daten gelöst. Aufgrund der Kombination von Clustering und dem verbesserten SVDD Algorithmus wird die Methode Cw-SVDD genannt. Nach dem Training liegt ein Referenzmodell vor (alle Untermodelle in Kombination), das dann in Echtzeit Datenpunkte auf Ausreißer untersucht. Können alle gut trainierten Untermodelle einen Datenpunkt verwerfen/ ablehnen, wird der Datenpunkt als Ausreißer gelabelt. Zusätzlich kann das Modell auch immer wieder aktualisiert werden, sodass es sich auf Arbeitspunktwechsel einstellen kann.

Feng et al. (2020) untersuchen eine Methode für höherdimensionale und unbalancierte Datensätze aus einem Montageprozess von Radlagern. Ziel war es, ein Vorhersagemodell für die Qualität der Montage zu erstellen. Jenes Modell basiert auf dem SMOTE-Adaboost Algorithmus. Adaboost ist ein Ensemble Lernalgorithmus, der auf ein Boosting Rahmenwerk aufbaut, das iterativ Bias und Varianz der Vorhersage reduziert, indem besonders die Missklassifikationen berücksichtigt werden. Auch Lu et al. (2017) verwenden für die Früherkennung von Brustkrebs einen Ensemble Lernalgorithmus. Dieser stellt das Fundament für die Untersuchung von MRI-Bildern und automatisierte computergestützte Diagnose dar. Die Methode kombiniert Ensemble Undersampling (EUS) mit Adaboost.

¹⁴⁰ vgl. ebenda

3.2.3.2 Performance-Metriken

Für die Bewertung der Leistung der Klassifikationsalgorithmen werden Performance-Metriken herangezogen. Doch nicht jedes Maß ist passend dafür, wenn unbalancierte Datensätze vorliegen, daher auch die gesonderte Betrachtung. Parsa et al. (2019) nützen als Metriken Accuracy (ACC), also die Anzahl der richtigen Klassifizierungen (Unfall – kein Unfall) bezogen auf die Gesamtanzahl der Beobachtungen, Detection Rate (DR), die Anzahl der entdeckten Unfälle bezogen auf die Gesamtanzahl der Beobachtungen, und die False Alarm Rate (FAR), die Anzahl der falsch berichteten Unfälle bezogen auf die Gesamtanzahl der Beobachtungen. Picek et al. (2019) untersuchen in ihrem Paper, ob gebräuchliche ML-Metriken genau so viel Aussagekraft bieten wie die domänenspezifischen Metriken Guessing Entropy (GE) und Success Rate (SR) für die Detektion von sogenannte Seitenkanalattacken (Side Channel Attacks, SCA; Domäne: Cybersicherheit). Es wird gezeigt, dass diese kein verlässlicher Indikator für die Detektion von SCAs sind bzw. kein offensichtlicher Zusammenhang zwischen Accuracy und GE/SR besteht. Lin et al. (2017) verwenden, wie sehr viele andere auch, die Fläche unter der Receiver Operating Characteristic (ROC) Kurve für die Evaluation ihres Cluster-basierten Undersampling Ansatzes bei verschiedenen Benchmark-Datensätzen. Diese Metrik wird mit AUC/ROC abgekürzt. Wang & Mao (2018) gebrauchen für die Bewertung ihres oben erwähnten Dreiphasenmodells ebenfalls AUC und berechnen zusätzlich auch die Metriken G-mean und F-measure. Auch Douzas & Bacao (2017) verwenden diese Metriken.

Chawla (2010) bemerkt, wenn die Verteilung der Testdaten unterschiedlich zu jenen der Trainingsdaten ist, kommt es bereits in der Trainingsphase zu Falschklassifikationen.

Tabelle 17: Fazit zum Forschungsbedarf über Informationsgewinnung unter schlechter Ausgangslage

Fazit Forschungsbedarf	
Es gibt keine Performance-Metriken für ungelabelte Datensätze	Die Beurteilung, ob ein Modell oder z.B. ein Resamplingalgorithmus akkurat arbeitet, passiert über Performance-Metriken, auch wenn das Imbalance-Problem in der Algorithmebene gelöst wird. Wenn die Ground Truth nicht bekannt ist, können diese auch nicht berechnet werden. Hier gilt es, Wege für eine Leistungsbewertung zu finden.

3.3 Anomalieerkennung für CM

Wie eingangs in der Problembeschreibung (Kapitel 1.1 auf S.3) dargelegt, stellt CM mittels Anomalieerkennung einen Lösungsansatz für die Zustandsüberwachung von komplexen und dynamischen Anlagen dar. Dieser Ansatz funktioniert aufgrund der Annahme, dass ein Fehler/ eine Störung die Daten einer Anlage, die von ihr erzeugt werden, ändert.¹⁴¹ Die Abweichung vom Normalzustand muss also in den Daten sichtbar werden. Zusammen mit der in Kapitel 2.2 auf S.19 getroffenen Annahme, dass hier nur Fehler/ Störungen betrachtet werden können, die nicht schlagartig auftreten, wird CM möglich.

¹⁴¹ vgl. Hendrickx et al., 2020, S.3

3.3.1 Aufbau des morphologischen Kastens für die Analyse

In Tabelle 18 wird in kompakter Weise der Aufbau und Inhalt des morphologischen Kastens erklärt, der für die Analyse von Publikationen zum Thema Anomalieerkennung für CM herangezogen wird.

Tabelle 18: Aufbau des morphologischen Kastens für die Analyse von Publikationen zum Thema AE für CM

Dimension	Inhalt
Detektionsverfahren	Einteilung siehe Kapitel 2.4 auf S.28: <ul style="list-style-type: none"> • Klassifikation • Nächster-Nachbar-Ansatz • Clustering • Isolation Forest • Statistisch
Lernmodell	Hier wird der verwendete Lernalgorithmus angeführt, wenn die Anomalieerkennung auf ML beruht. Beispiele: kNN, SVM, Random Forest
Was wird beobachtet	Hier wird angeführt, welche Parameter beobachtet und weiterverarbeitet werden.
Anwendungsgebiet	Bezeichnet das Forschungsfeld, aus dem die Publikation stammt.

In Tabelle 19 und Tabelle 20 werden die Ergebnisse der morphologischen Analyse über die Anomalieerkennung für CM angeführt. Für eine bessere Übersicht wurde auch hier eine Zweiteilung der Gesamttabelle vollzogen.

Tabelle 19: Anomalieerkennung für CM: Ergebnisse der morphologischen Analyse (1/2)

SotA-Analyse			Anomaliedetektion					Lernmodell
Nr.	Jahr	Autor(en)	Klassifikation	Nächster-Nachbar-Ansatz	Clustering	Isolation Forest	Statistisch	
AE1	2018	Baasch et al.				x		Isolation Forest
AE2	2016	Carino et al.	x					OC- SVM; NN
AE3	2015	Ge et al.	x					Least Squares SVM
AE4	2019	Genge et al.					x	PCA; Hotelling's T2
AE5	2020	Hendrickx et al.			X			Hierarchical Clustering
AE6	2020	Kamat & Sugandhi	x					Autoencoder in Kombination mit LSTM (Deep Learning)
AE7	2019	Kammerer et al.					x	MASS
AE8	2012	Lapira et al.	x					SOM; GMM; NN
AE9	2020	Liu et al.	x				x	Gaussian Process Regression; Kernel-PCA
AE10	2020	Q. Lu et al.					x	Bayesian Change Point detection
AE11	2020	Mao et al.	x					DAE, RDA
AE12	2018	Pourpanah et al.	x		X			Fuzzy ART NN; QFAM-GA NN
AE13	2020	Quatrini et al.	x					Random Forest; Decision Jungle
AE14	2020	Renström et al.	x					Autoencoder
AE15	2014	Suzuki et al.		x	X			VQC; LSC

SotA-Analyse			Anomaliedetektion					Lernmodell
Nr.	Jahr	Autor(en)	Klassifikation	Nächster-Nachbar-Ansatz	Clustering	Isolation Forest	Statistisch	
AE16	2020	Wang	x					Autoencoder
AE17	2020	Zeng et al.					x	Sparse Bayesian Learning
AE18	2020	Zhang et al.			X		x	Gaussian Process Ensemble Model
AE19	2018	Zhao et al.	x		X			RBM; Deep Autoencoder
AE20	2016	Zhong et al.					x	LCPM
AE21	2019	Zope et al.	x	x	X	x		Diverse

Tabelle 20: Anomalieerkennung für CM: Ergebnisse der morphologischen Analyse (2/2)

SotA-Analyse			Was wird beobachtet	Anwendungsfall
Nr.	Jahr	Autor(en)		
AE1	2018	Baasch et al.	CM-Daten	Zuginfrastruktur
AE2	2016	Carino et al.	CM-Daten	End-of-Line Test Machine
AE3	2015	Ge et al.	Monitoring Data	Satelliten
AE4	2019	Genge et al.	CM-Daten	CSTR, Sicherheit in alternder IIOT
AE5	2020	Hendrickx et al.	CM-und Prozessdaten	Flotte von elektr. Antrieben
AE6	2020	Kamat & Sugandhi	CM-und Prozessdaten	Fräsmaschine; Mantelstromtriebwerk
AE7	2019	Kammerer et al.	CM-Daten	Pharma: Blistermaschine
AE8	2012	Lapira et al.	Leistung (SCADA)	Windkraftanlage
AE9	2020	Liu et al.	EGT Daten von On-wing APU	Flugzeugtechnik
AE10	2020	Q. Lu et al.	Building Information Data	Pumpen von HVAC
AE11	2020	Mao et al.	Diverse Lagerdatensätze	Lagerteststand
AE12	2018	Pourpanah et al.	Motorstrom und Propellervibration	Unmanned Aerial Vehicle (UAV)
AE13	2020	Quatrini et al.	Diverse CM- und Prozessdaten	Pharma-Industrie
AE14	2020	Renström et al.	SCADA Daten	Windkraftanlage
AE15	2014	Suzuki et al.	CM-Daten	Gas Generatoren
AE16	2020	Wang	CM-Daten	Zuginfrastruktur, Oberleitungen
AE17	2020	Zeng et al.	Getriebeöltemperatur	Windkraftanlage
AE18	2020	Zhang et al.	Diverse	Kohleheizkraftwerk
AE19	2018	Zhao et al.	SCADA Daten	Windkraftanlage
AE20	2016	Zhong et al.	Simulierte Datensätze, Echte Flugdaten	Flugzeugtechnik
AE21	2019	Zope et al.	CM-Daten	IQT, CSTR

3.3.2 Auswertung der Analyse

Ein Großteil der Publikationen verwendet eine auf Klassifikation basierende Anomaliedetektion. Für das Training eines Klassifikationsmodells, welches eine Kategorisierung der anfallenden Maschinendaten in Gut- und Schlechtzustand durchführt, werden Ground-Truth-Daten benötigt. Es werden somit gelabelte Daten für das Einlernen des Klassifikationsalgorithmus benötigt. Dies stellt den größten Nachteil dieses Ansatzes dar. Gelabelte Daten sind nur in geringen Mengen oder gar nicht verfügbar bzw. nur sehr kostspielig und personalintensiv zu generieren. Ge et al. (2015) verwenden eine datengetriebene Anomaliedetektionsmethode für Punktanomalien, die auf der Prädiktion von Zeitreihen beruht. Aus der Vorhersage, wo eine Least Squares SVM verwendet wird, wird der erwartete Wert berechnet. Aber es wird nicht nur ein einzelner Punkt prädiziert, sondern es ist auch zusätzlich möglich, das erwartete Intervall, in dem die Vorhersage gültig ist, ausgegeben.

Liegt der beobachtete Wert dann nicht in jenem Intervall, kann er als Anomalie klassifiziert werden. Ein vielversprechender Algorithmus, der unter anderem auch für die Klassifikation verwendet werden kann, ist der Autoencoder. Ein Autoencoder ist ein Neuronales Netzwerk, das die Eingabe rekonstruiert. So wird der Autoencoder z.B. nur auf den Gutzustand der Maschine eintrainiert und „[...] dabei lernt das Netz über mehrere Stufen aus der Eingabe eine komprimierte Repräsentation, Code genannt, aus der es dann als Ausgabe die Eingabe rekonstruiert.“¹⁴² Würde etwas Anderes vorliegen als der eintrainierte Zustand, würde das als Abweichung oder Anomalie markiert werden. H. Wang (2020) verwendet Autoencoder für das CM von Oberleitungen des chinesischen Hochgeschwindigkeitseisenbahnnetzes. Zwischen Eingabe und Ausgabe, also der rekonstruierten Eingabe, wird der Mean Squared Error (MSE) berechnet und dann werden anhand von einem spezifizierten Perzentil die Anomalien bestimmt. Im eben genannten Beispiel besteht der Autoencoder aus der Eingabeschicht aus einer versteckten Schicht (Hidden Layer, in diesem Fall Code genannt) und aus der Ausgabeschicht. Werden zusätzliche Hidden Layers hinzugefügt, also die Netzwerkarchitektur komplexer gestaltet, spricht man von Deep Autoencoder, so wie das auch Mao et al. (2020), Renström et al. (2020) und Zhao et al. (2018) anwenden. Kamat & Sugandhi (2020) nutzen ebenfalls einen Deep Autoencoder, diesen verwenden sie, unter anderem für die Überwachung einer Fräsmaschine, aber in Kombination mit einem Long Short Term Memory (LSTM) Deep Learning Modell. Es besteht auch die Möglichkeit der Multi-Class-Klassifikation. So können verschiedene bekannte Fehlerklassen aus den Daten erkannt werden. Carino et al. (2016) realisieren für eine Lenksystem-Testanlage eine Multi-Fehler-Klassifikation und parallel dazu eine Novelty Detection für unbekannte Lenk- oder Fehlerszenarios. Für die Klassifikation bzw. für Systemzustandsbeurteilung wird ein Neuronales Netz und für die Novelty Detection eine One-Class-SVM verwendet. In der nächsten Referenz werden unterschiedliche Prozessphasen und Systemzustände klassifiziert. Quatrini et al. (2020) wenden eine Zwei-Schritte-Methode zur Anomalieerkennung in einem Herstellungsprozess der Pharmaindustrie an. Zuerst werden unterschiedliche Prozessphasen identifiziert und im zweiten Schritt dann mit der zusätzlichen Information aus dem ersten Schritt drei verschiedene Systemzustände (*Expected*, *Warning* und *Critical*) klassifiziert. Dabei werden der Random Forest Algorithmus und der Decision Jungle Algorithmus verwendet. Diese Publikation beschreibt sehr genau, wie das Data Pre-Processing erfolgt und welche Experten dazu innerhalb des Unternehmens eingebunden werden müssen. Pourpanah et al. (2018) entwickeln ein Monitoring System für ein Unmanned Aerial Vehicle (UAV, Drohne), das für die Merkmalsgenerierung beim Motorstrom eine Motor Current Signature Analysis (MCSA) und beim Propeller eine Vibration Signature Analysis (VSA) verwendet. Die Signale der MCSA werden über ein Fuzzy Adaptive Resonance Neural Network geclustert. Es wird also über ein unüberwachtes Lernen versucht zu entscheiden, ob ein normaler oder anormaler Systemzustand vorliegt. Für die Signale der Propeller wird ein Q-learning-based Fuzzy ARTMAP Neural Network verwendet, um Gut- oder Schlechtzustand zu klassifizieren. Hier liegt also eine auf bestärkendem Lernen basierende Klassifikation vor.

Suzuki et al. (2014) verwenden bei Gasmotorenanlagen zusätzlich zur Fernzustandsüberwachung mit festen Grenzwerten für jeden Sensor auch einen Data Mining Ansatz, um auch saisonale Schwankungen und andere Dynamiken in die Anomaliedetektion

¹⁴² Traphöner, 2018, S.13

miteinzubeziehen. Dazu werden gleichzeitig eine Clustering- und eine Nächster-Nachbar-Methode (Diagnosis Engines) für die kontinuierliche Anomaliedetektion angewandt. Für das Clustering wird Vector Quantization Clustering (VQC) und für die auf den nächsten Nachbar basierende Klassifikation ein Local Subspace Classifier (LSC) verwendet. Beide Algorithmen werden zuerst auf die Normalzustandsdaten eintrainiert.

Hendrickx et al. (2020) zeigen ein Anomalieerkennung-Rahmenwerk für ein flottenbasiertes CM. Das Online CM mehrerer Elektromotoren gleichzeitig ermöglicht ein CM ohne historische Daten und ohne Vorwissen zu möglichen Fehlererscheinungsformen. Dieser Ansatz wird möglich, da angenommen wird, dass der Großteil der überwachten Anlagen normal funktioniert. So werden einzelne Anlagen miteinander verglichen und dadurch können dann Abweichungen detektiert werden. Mittels Hierarchical Clustering Algorithmus werden alle ähnlich laufenden Maschinen gruppiert.

Baasch et al. (2018) verwenden einen Isolation Forest Algorithmus für die sensorgestützte Anomaliedetektion zur Zustandsbewertung einer Gleisanlage. Mit den fahrzeugseitig montierten Sensoren, die die Achslagerbeschleunigung aufzeichnen, können frühzeitig Gleisauffälligkeiten erkannt werden.

Ein großer Teil der analysierten Referenzen verwendet einen statistischen Ansatz zur Anomalieerkennung. Liu et al. (2020) verbessern das CM eines Hilfstriebwerkes (Auxiliary Power Unit, APU) eines Flugzeuges mittels datengetriebener Anomaliedetektion. Es wird die Abgastemperatur als repräsentativer Parameter beobachtet. Um bessere Detektionsergebnisse zu erzielen, werden zwei Methoden gleichzeitig angewendet und deren Ergebnisse fusioniert. In der ersten Methode wird ein einzelner Input mit einer Gaußprozess-Regression verarbeitet und daraus mit den Trainingsdaten ein Konfidenzintervall für die Detektion errechnet. Liegen die Testdaten außerhalb dieses Intervalls wird eine Anomalie erkannt. Die zweite Methode klassifiziert einen mehrdimensionalen Input mittels ML-Technik Kernel Principal Component Analysis (KPCA) und unterscheidet zwischen normal/ anomal anhand von von Squared Prediction Error (SPE). Auch Zhang et al. (2020) nützen für das CM von Komponenten in einem Blockheizkraftwerk Gaußprozesse – allerdings als Ensemble-ML Modell. Diese Modellierung kommt sehr gut mit dynamischen Veränderungen zurecht und es lässt sich wiederum ein (dynamisches) Intervall berechnen, mit dem anomales Verhalten erkannt werden kann. Genge et al. (2019) beschäftigen sich mit dem Aspekt der Alterung von physischen Prozessen und Cyberattacken im Kontext von Industrial Internet of Things (IIoT). Das angewandte Modell kann so unter Berücksichtigung von der Altersstufe, statistisch definiert durch Mittelwert und Standardabweichung, des betrachteten Prozesses bereits kleinste Abweichungen feststellen, welche auch von verschiedenartigen Attacken auf die Anlagensteuerung des Prozesses hervorgerufen werden können. Die Wirkung der Methode wird am Beispiel eines Rührkessels (Continuous Stirred-Tank Reactor, CSTR) und dessen Prozess- und Steuerungsvariablen gezeigt. Kammerer et al. (2019) finden Anomalien über die Anzahl von Musterteilen (Patterns) in einer Zeitreihe unter anderem für eine Blistermaschine (Verpackungsmaschine) der Pharmaindustrie. Über den Mueen's Algorithm for Similarity Search (MASS) können über ein Abstandsmaß verschiedene Muster in den gemessenen Zeitreihen gefunden werden. Je mehr unterschiedliche Muster vorliegen, desto mehr weicht der aktuelle Zustand vom Normalzustand ab. Zeng et al. (2020) überwachen die Öltemperatur

eines Getriebegehäuses einer Windkraftanlage. Die gesammelten SCADA-Daten werden mit einem Sparse Bayesian Learning Model (SBL) zu einem probabilistischen Vorhersage- (oder Schätz-) Modell verarbeitet, sodass daraus wiederum ein Konfidenzintervall für eine normale Öltemperatur berechnet werden kann. Mit einem Bernoulli Hypothesentest wird für ein bestimmtes gefordertes Konfidenzniveau bestimmt, ob die vorliegende Temperatur normal oder anomal ist.

Tabelle 21: Fazit zum Forschungsbedarf über Anomalieerkennung für CM

Fazit Forschungsbedarf	
In den Publikationen überwiegt die Anwendung von Klassifikatoren	Auch bei der Analyse der wissenschaftlichen Arbeiten aus diesem Bereich wird größtenteils mit gelabelten (Forschungs-) Datensätzen gearbeitet und dadurch werden vorwiegend Klassifikationsalgorithmen verwendet. So können natürlich auch Performance-Metriken berechnet werden. Das stellt eine Ausgangssituation dar, die in der industriellen Praxis selten anzutreffen ist. Es braucht eine Anwendbarkeit auf praktische Problemstellungen.
Bei der Einführung von ML-Systemen für die Anomalieerkennung bleibt die Kostenfrage oft unbeachtet	Bei all den hochentwickelten ML-Algorithmen bleibt die Frage nach einer wirtschaftlichen Realisierbarkeit unbeachtet. Die Erstellung der Datenmodelle, deren Training und tatsächliche Anwendung im Betrieb erfordern immense Rechnerleistungen. Es muss immer abgewogen werden, ob nicht (einfachere) statistische Ansätze trotzdem noch immer eine valide Alternative darstellen – so wie das Braei & Wagner (2020) in deren Studie über Anomaliedetektion in univariaten Zeitreihen zeigen. Stattdessen wird der untersuchte ML-Algorithmus mit anderen ML-Ansätzen verglichen.
In den vorliegenden Arbeiten wird nur sehr selten über die (personellen) Rahmenbedingungen geschrieben, die es benötigt, um ein CMS mit Anomalieerkennung einzuführen	Es bedarf einer ausführlichen Beschreibung, welche Abteilungen bzw. Schlüsselpositionen für die Umsetzung von industriellen Data Science Projekten im Speziellen in Bezug auf CM mittels Anomalieerkennung nötig sind - so wie das Quatrini et al. (2020) skizzieren.

3.4 Zusammenfassung der Literaturanalyse

Um die Literaturanalyse nun zu konsolidieren, werden die anfangs gestellten Literaturfragen nochmals angeführt:

1. Was charakterisiert hochkomplexe kritische Anlagen und wie wird deren Zustand überwacht?
2. Welche Techniken und Algorithmen werden angewendet, um das Problem der schwierigen Ground-Truth-Datenlage zu überwinden?
3. Welche Möglichkeiten gibt es zur AE im CM mit besonderem Bezug zur Instandhaltung?

Nach einer zusammenfassenden Beantwortung der Literaturfragen, werden auch die identifizierten Forschungslücken angeführt.

Was charakterisiert hochkomplexe kritische Anlagen und wie wird deren Zustand überwacht?

Hochkomplexe und kritische Anlagen sind von zentraler Bedeutung für die Gesellschaft und das alltägliche Zusammenleben. Es ist also unabdinglich jene Anlagen ständig zu überwachen und über deren Zustand Bescheid zu wissen. Die moderne Gesellschaft ist sehr stark von der

Energie- und Wasserversorgung und von Telekommunikationsnetzwerken abhängig. Deshalb sowie aufgrund der vorherrschenden Vernetzung muss eine mögliche Störung oder gar ein Ausfall von der Versorgungsinfrastruktur frühzeitig erkannt bzw. verhindert werden. Die Tragweite dessen erschließt sich vor allem bei Atomkraftwerken, wo bei Reaktorunfällen schwerwiegende gesundheitliche Schäden einer großen Bevölkerungsgruppe und katastrophale Auswirkungen auf die Umwelt zu erwarten wären. Durch die Komplexität im Aufbau der Anlagen liegt nur eine sehr geringe Transparenz bei der Diagnose von Fehlern und deren Ausgangspunkten vor. Aus der Perspektive des Monitorings ist es schwer oder gar nicht möglich, alle beteiligten Komponenten bzw. deren Parameter zu überwachen, sodass man einige kritische Komponenten bzw. Parameter identifizieren muss, die repräsentativ für den Zustand der betrachteten Anlage stehen. Die unterschiedlichen Erscheinungsformen der Anlagen, der verbauten Komponenten und der verwendeten Sensoren ergeben eine enorme Informationsvielfalt, wodurch zusätzliche eventuell komplizierte Messapparaturen notwendig und größere Datenmengen (Big Data) verarbeitet werden. Die Vernetztheit jener Anlagen lassen auch bei erkanntem (detektiertem) Fehler keine einfache Diagnose zu, da bei den vielen oft unbekanntem Abhängigkeiten, die Anlagen teilweise als Blackbox angesehen werden und eine vollkommen unklare Fehlersymptomatik vorliegt. Nach eingängiger Literaturanalyse ist festzustellen, dass ein erhebliches Prozessverständnis sowie Fach- und Anlagenwissen gepaart mit ausgeprägter Diagnosekompetenz für die Zustandsüberwachung jener Anlagen notwendig sind. Dies beginnt bei der richtigen Sensorauswahl und -applikation, der adäquaten Datensammlung und -aufbereitung, der optimalen Auswahl von Detektionsalgorithmen und zieht sich hin bis zur Verwendung von passenden Diagnosemodellen.

Wie bereits erwähnt werden jene kritischen und hochkomplexen Anlagen zum Großteil als Blackboxes gesehen, wo keine physikalischen Zusammenhänge bekannt oder nur unter erheblichem Aufwand modellierbar sind. Diesem Umstand geschuldet überwiegen die datengetriebenen Diagnosemodelle, zu denen bei dieser Analyse auch signalbasierte Modelle gezählt werden. Das sind unter anderem Modelle des ML wie z.B. KNN, PCA oder Clustering, die auf bestimmte Komponenten eingelernt werden. Hier sind die Modellierung und die Performance der Algorithmen primär abhängig von der Qualität und dem Umfang der verfügbaren Daten, was in den meisten realen Anwendungsfällen ein Problem darstellt. Klassifikatoren brauchen für das Einlernen z.B. Daten vom Schlecht- und Gutzustand. Die Herbeiführung gefährlicher Betriebszustände, nur um eine Datenrepräsentation eines Schlechtzustandes aufnehmen zu können, sind mit der Aussicht auf gesundheitliche oder infrastrukturelle Schäden nicht vertretbar. Hier müssen alternative Methoden herangezogen werden. Ebenfalls zu den datengetriebenen Modellen gezählt werden jene Modelle des signalbasierten CM, wo die gemessenen Signale z.B. via FFT oder WT weiterverarbeitet und mit Grenzwerten (statisch oder dynamisch) verglichen werden. Physikalische Modelle (Whitebox) finden nur sehr selten Anwendung, da diese nur unter kostenintensivem Aufwand realisierbar sind. Die Analyse würde aber durch diese Art der Modellierung transparenter werden, weil die Eingabe- und Ausgabewerte eine konkrete und interpretierbare physikalische Bedeutung haben. In diese Kategorie fallen auch Digital-Twin-Modellierungen, so wie diese z.B. in Egusquiza et al. (2018) gezeigt werden. Wissensbasierte Modelle, die z.B. WENN-DANN Regeln verwenden werden bei großen Anlagen sehr schnell undurchsichtig und unüberschaubar. Grundsätzlich muss unterschieden werden, ob das Monitoring aktive oder

passive Anlagenkomponenten erfasst. Weiterhin bedeutsam, nicht nur als Verifikation der sensorbasierten Überwachung und Diagnose, bleibt die Inspektion durch das geschulte und erfahrende Instandhaltungspersonal.

Welche Techniken und Algorithmen werden angewendet, um das Problem der schwierigen Ground-Truth-Datenlage zu überwinden?

Ein indifferenter Datensatz, eventuell wenig verfügbare, fehlende oder verrauschte Daten, ein unbalancierter Datensatz etc. stellen eine äußerst schlechte Ausgangslage für das Training von ML Modellen dar. Das ist das *Ground Truth* Problem. Jener Umstand ist in der Realität der Zustandsüberwachung aber fast die Regel, sodass dafür Lösungen bereitgestellt werden müssen. Bei all den fortgeschrittenen Algorithmen kommt man aber nicht ohne menschliches Zutun eines gut ausgebildeten Personals aus, weil erkannte Unregelmäßigkeiten diagnostiziert und bestimmten Ereignissen (z.B. Ausfällen, Störungen etc.) zugeordnet werden müssen, sodass eine Ground Truth aufgebaut werden kann. Nur gut ausgebildetes Personal hat das nötige Prozess- und Fehlerwissen. Hier werden auch Techniken der Anomalieerkennung verwendet, sodass Unregelmäßigkeiten im ersten Schritt erkannt werden. Auch gilt es, aussagekräftige Repräsentationen des erfassten Signals mittels zeitintensiven Feature Engineerings zu finden (siehe 3.2.1). Wenn nun bekannt sein sollte welche Daten den Gut- oder Schlechtzustand repräsentieren, kommt in den meisten Fällen das Problem des unbalancierten Datensatzes auf. Hier liegt ein Ungleichgewicht in den Datenbeispielen vor, sodass ein Zustand – meistens jener von besonderem Interesse – zahlenmäßig in den Daten unterrepräsentiert ist (siehe Abbildung 13). Dieses Problem kann grob gegliedert auf Daten- oder Algorithmusebene angegangen werden.

Auf Datenebene kann das mittels Pre-Processing durch Oversampling, Undersampling oder hybriden Ansätzen passieren, wo unter anderem der SMOTE Algorithmus als bekanntester Vertreter genannt wird. Bei der Verwendung dieser Methoden muss darauf geachtet werden, dass entweder nicht zu viel der Information verloren geht oder umgekehrt Overfitting auftritt. Auf Algorithmusebene wird dieses Problem entweder durch die Verwendung von Algorithmen, die weniger anfällig sind, einen Bias hin zur Mehrklasse zu entwickeln, oder durch die Modifikation von bestehenden ML Algorithmen gelöst. Es werden auch noch zwei weitere Ansätze angeführt, nämlich kosten-sensitives Lernen und Ensemble-Lernen. In der analysierten Literatur findet neben dem Pre-Processing Ansatz das Ensemble-Lernen verbreitet Anwendung, als Beispiel sei hier SMOTE-Adaboost angeführt. Es gilt zu bedenken, dass die Performance-Metriken an den Umstand des Lernens/ Trainierens mit unbalancierten Datensätzen angepasst werden müssen. G-mean, F-measure und die AUC/ROC sind hier zu bevorzugen.

Welche Möglichkeiten gibt es zur AE im CM mit besonderem Bezug zur Instandhaltung?

Vor allem für komplexe und umfangreiche Prozesse und Anlagen stellt eine anspruchsvolle Anomalieerkennung die Grundlage für ein erfolgreiches CM und im weiteren Sinne für CBM dar. Der Fokus bei der Anomalieerkennung in Bezug auf Instandhaltung liegt auf dem frühen Erkennen von Abweichungen vom geforderten Normalzustand, sodass dem Instandhaltungspersonal genügend Zeit bleibt, die notwendigen Instandhaltungsmaßnahmen optimal zu planen und auszuführen.

Die Auswahl der verwendeten Methoden zur Anomalieerkennung hängen direkt mit den verfügbaren Daten zusammen. Dies gilt insbesondere für die Methoden des ML, da diese vor der Online-Anwendung am zu überwachenden Prozess eingelernt werden müssen. Weil in den realen Fällen meistens eine herausfordernde Datenlage vorherrscht, finden vor allem Algorithmen, die nur auf eine Klasse (z.B. den Gutzustand) eintrainiert werden, verbreitet Anwendung. Hier sind besonders Autoencoder und One-Class-SVM zu erwähnen. Im speziellen Fall von Zeitreihen erweisen sich auch Modelle mit Zeitreihenprädiktion als erfolgreich. Hier wird aus einem trainierten Vorhersagemodell der nächste Zeitschritt prädiziert und dessen Wert mit dem tatsächlich gemessenen Wert verglichen, wodurch Abweichungen festgestellt werden können – meistens ausgedrückt durch Fehlermaße wie MSE. Die zweite wichtige Gruppe der Ansätze ist jene der statistischen Anomalieerkennung, die nach wie vor und trotz der immer besser werdenden ML-Ansätze weit verbreitet ist. Dabei können Unsicherheiten modelliert und Konfidenzintervalle berechnet werden. Gaußprozess Regression und Hypothesentests sind hier zwei der vorgeschlagenen Ansätze. Für Zeitreihen im Speziellen gelingt die Anomaliedetektion auch über Zeitreihenvergleiche, also der Untersuchung auf Ähnlichkeiten z.B. über DTW. Ein weiterer Ansatz ist Clustering, bei dem keine gelabelten Daten notwendig sind und somit unüberwachte Lernalgorithmen zum Einsatz kommen können. Die Daten normal (ähnlich) laufender Anlagen erzeugen große (dichte) Cluster mit den meisten Datenpunkten innerhalb dieser, während anomale Datenpunkte sich in anderen vom großen Cluster unterscheidbaren Clustern zusammenfinden. Das stellt den Idealfall dar. Im Realfall kommt es zu Überlappungen, sodass eine Differenzierung teilweise schwierig wird. Dieser Ansatz funktioniert z.B. sehr gut bei einem Flotten-CM. Dies wurde bereits dargelegt. Im Zuge der Analyse wurden auch noch die Anomalieerkennung über den Algorithmus Isolation Forest und über den Nächster-Nachbar Ansatz betrachtet. Zusammenfassend muss gesagt werden, dass es nicht genau die eine Lösungsmöglichkeit (Verfahren) für das eine Problem gibt. In Bezug auf Abbildung 13 empfiehlt Traphöner (2018) folgende Faustregel: sollte ein balancierter Datensatz (a) vorliegen werden Detektion und Klassifikation mit datengetriebenen (empirischen) Methoden des ML gelöst. Liegt allerdings ein unbalancierter Datensatz (b) vor, empfiehlt sich eine Kombination aus wissensgetriebenen (analytischen) und datengetriebenen Ansätzen. Bei einem indifferenten Datensatz (c) gilt es, diesen zuerst wissensgetrieben in einen Datensatz der Art (b) zu transformieren. Dies z.B. auch unter Zuhilfenahme von empirischen Methoden wie Clustering.

Mit dem theoretischen Wissen aus Kapitel 2 und auf Basis der Ansätze aus der Literaturanalyse wird nun in Kapitel 4 ein Phasenmodell für CM mittels Anomalieerkennung entwickelt. Es soll damit ein Beitrag zur Schließung der identifizierten Forschungslücken geleistet werden.

4 Phasenmodell für CM mittels AE

In diesem Kapitel wird das Artefakt des Design Science Prozesses, nämlich das Phasenmodell für das CM mittels Anomalieerkennung vollumfänglich dargestellt. Das Modell ist das Ergebnis der ausführlichen Literaturrecherche aus dem vorigen Kapitel, berücksichtigt das CRISP-DM Rahmenwerk und ist konkret an das von Ansari et al. (2019) formulierte Rahmenwerk für die präskriptive Instandhaltung cyberphysischer Produktionssysteme angelehnt dargestellt. Zuerst wird ein Überblick über die Architektur des Modells gegeben und danach werden die Ebenen bzw. die einzelnen darin enthaltenen Phasen genauer beschrieben. Im Anschluss an dieses Kapitel wird das Phasenmodell anhand einer industriellen Fallstudie in Kapitel 5 validiert.

4.1 Überblick über das Phasenmodell

Im Kontext der vorliegenden Forschungsarbeit wird eine Phase als Input-Output Transformation¹⁴³ verstanden. Jede Phase baut auf den Output der vorhergehenden auf. In Abbildung 17 ist die Architektur des Phasenmodells ersichtlich. Das Modell besteht aus drei Ebenen, nämlich aus 1) der Datenebene, 2) der Verarbeitungs- und Analyseebene und 3) der Nutzerebene. Jede Ebene besteht aus mehreren Phasen.

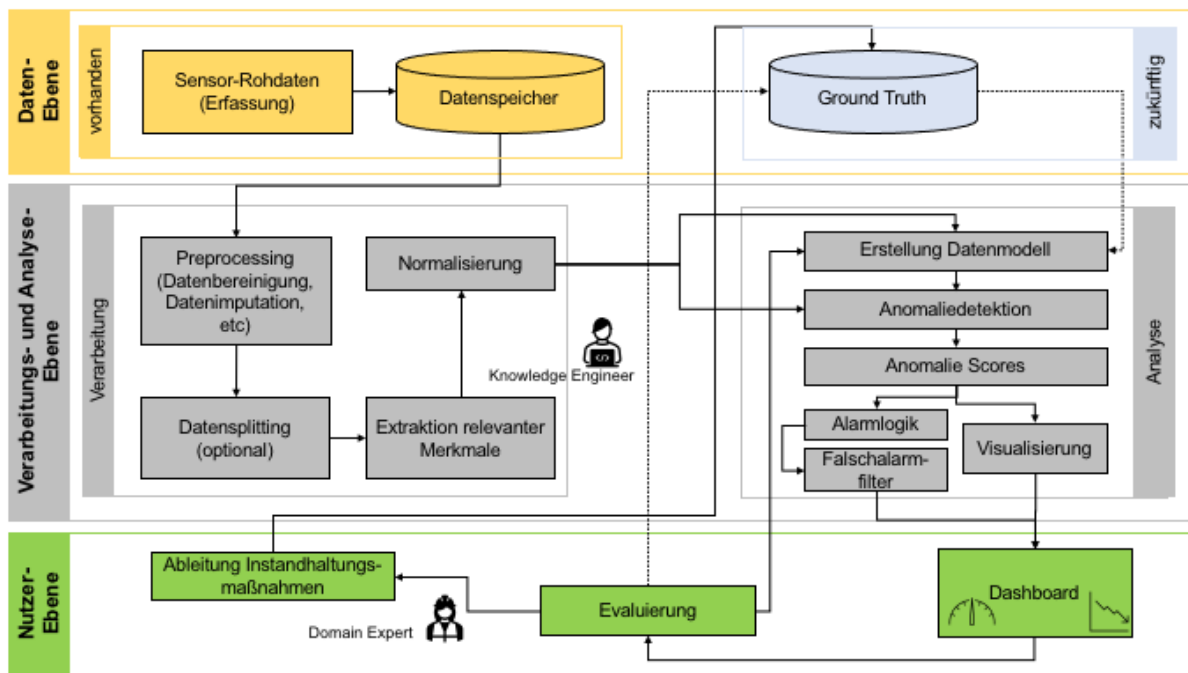


Abbildung 17: Phasenmodell für CM mittels Anomalieerkennung¹⁴⁴

Im Nachfolgenden wird der grundsätzliche Ablauf in den drei Ebenen und in den einzelnen Phasen genauer erklärt.

¹⁴³ vgl. Goeken, 2006, S.51

¹⁴⁴ Eigene Darstellung, in Anlehnung an Ansari et al. (2019)

4.2 Datenebene

In der obersten (chronologisch ersten) Ebene, der Datenebene, werden zuerst die Zustandsdaten der betrachteten Anlage erfasst und gesammelt. Diese Messungen werden als Sensor-Rohdaten an einen Datenspeicher weitergegeben. Eine einfache Datenerfassung und Speicherung der Rohdaten (oft als Nebenprodukt der Automatisierung) stellt eine typische Ausgangssituation für den Großteil der industriellen Anwendungsfälle dar und so sind auch die Gegebenheiten der vorliegenden Industriefallstudie (Kapitel 5) im Hinblick auf die vorhandene Dateninfrastruktur. In der gleichen Ebene befindet sich (zukünftig) auch die Ground Truth Datenbank, die weiter unten in Kapitel 4.5.2 auf S.78 erläutert wird. Aus dem Datenspeicher werden die Daten dann an die Datenverarbeitung in der Verarbeitungs- und Analyseebene weitergeleitet.

4.3 Verarbeitungs- und Analyseebene: Verarbeitung

In der zweiten Ebene werden die Daten aus dem Speicher nach einem Preprocessing sowie einer optionalen Aufteilung in Trainings- und Testdaten (Datensplitting) einer Transformation in statistische Merkmale unterzogen. Dabei werden statistisch relevante Merkmale aus den Rohdatensätzen (z.B. Zeitreihen) extrahiert, die dazu verwendet werden, um datengetriebene Modelle für die Anomaliedetektion zu erstellen. Bevor die Daten aber zur Modellierung oder direkt zur Anomalieerkennung weitergereicht werden können, werden diese noch normalisiert. Auch dieser Schritt ist optional, da einige Algorithmen dadurch nicht beeinflusst werden. Grundsätzlich aber sichert es die Vergleichbarkeit der unterschiedlich skalierten Datenpunkte in den Merkmalsdimensionen. Jene Schritte werden von einem *Knowledge Engineer* ausgelegt und ausgeführt. Dieser wählt auch das passende Modell für die darauffolgende Anomaliedetektion aus.

4.3.1 Preprocessing

Da die Messdaten in roher Form vorliegen und so nur suboptimal für die Detektionsalgorithmen verwendbar sind, müssen diese vorbereitet werden. Es findet also die Datenvorbereitung statt. Es gilt eine Datenbereinigung (*Data Cleansing*) unter größter Vorsicht durchzuführen, damit nicht Anomalien, die in dieser Anwendung im Fokus stehen, aus dem Datensatz entfernt werden.¹⁴⁵ Die zu entfernenden Ausreißer (*Outlier Detection/ Removal*) können unterschiedlichsten Ursprungs sein, wie z.B. Sensor- oder Prozessrauschen. Es sei angemerkt, dass jene später dargelegten Anomalieerkennungsalgorithmen auch zum Aufspüren von Ausreißern in dieser Phase verwendet werden können. Außerdem müssen fehlende Werte (*Missing Values, #NV*) mittels spezieller Techniken (*Data Imputation*) ergänzt werden.¹⁴⁶

¹⁴⁵ vgl. Strauß et al., 2018, S.1478

¹⁴⁶ vgl. Cernuda, 2019, S.67

4.3.2 Datensplitting

Nach diesem Schritt folgt das optionale Aufteilen der Daten in einen Trainings- und Testdatensatz, wenn denn Training notwendig ist. Dabei wird eine anwenderspezifische Zeitspanne zum Trainieren der Algorithmen ausgewählt, um auf der einen Seite die Datenmenge zu reduzieren, da der Trainingsprozess sehr rechen- und damit zeitintensiv ist. Auf der anderen Seite ist die Auswahl der Trainingsdaten ein zentraler Schritt für die halbüberwachten Algorithmen, da dadurch die Detektionsperformance maßgeblich beeinflusst werden kann. Hier wird auf die Zusammenarbeit von Knowledge Engineer und Domain Expert gebaut. Der Domain Expert kennt unter anderem jene Zeitspannen, in denen der Betrieb ohne Auffälligkeiten/ Ausfälle gelaufen ist, und so kann der Knowledge Engineer entsprechende Datensätze für das Training auswählen.

4.3.3 Merkmalsextraktion

Im Anschluss an das *Splitting* werden jeweils sowohl für den Trainings- als auch für den Testdatensatz Merkmale berechnet. Für die Datenmodellierung mit statistischen und ML-Ansätzen werden gewisse statistische Merkmale (siehe Tabelle 23) der Zeitreihendaten (Messdaten liegen meistens als Zeitreihendatensätze vor) unter anderem mittels **Sliding Rolling Window Ansatz** extrahiert. Da die Berechnung eines Merkmals über die gesamte Zeitreihe (siehe Formel 1) hinweg keine brauchbare Aussage liefern würde und dadurch maximal globale Ausreißer festgestellt werden könnten, wird der eben genannte Ansatz mit bewegtem/ fortschreitendem Fenster angewandt. Dadurch wird es möglich, Veränderungen in Relation zu vorhergehenden Datenpunkten sichtbar zu machen (in der Nachbarschaft) und eine feingranulare Detektion umzusetzen. Bei einer angenommenen Fensterlänge von $p=5$ werden sozusagen für jene 5 zurückliegenden Datenpunkte innerhalb dieses Bereiches die Merkmale wie Mittelwert oder Standardabweichung berechnet. Im Anschluss schiebt sich das Fenster um einen Datenpunkt weiter und wieder werden für diesen neuen Bereich die Merkmale retrospektiv formuliert.

Tabelle 22: Fortschreitendes Fenster für Berechnung der Merkmale

1	2	3	4	5	6	7	8	9	10	...
1	2	3	4	5	6	7	8	9	10	...
1	2	3	4	5	6	7	8	9	10	...
1	2	3	4	5	6	7	8	9	10	...
1	2	3	4	5	6	7	8	9	10	...

Wie in Tabelle 22 zu sehen, ergibt sich beispielsweise dann für Punkt 5 und 6 (fett gedruckt) folgende Berechnung des Mittelwertes x :

Formel 2: Beispielhafte Berechnung des Mittelwertes

$$\bar{x}_5 = \text{mean}(1,2,3,4,5) = 3$$

$$\bar{x}_6 = \text{mean}(2,3,4,5,6) = 4$$

Die gesamte Zeitreihe ist somit in zahlreiche Subsequenzen mit fester Fensterlänge p unterteilt worden. Python z.B. stellt hier über *Pandas* Funktionen zur Implementierung zur Verfügung.

Im Folgenden werden angewandte statistische Merkmale, die aus den einzelnen Zeitreihen extrahiert werden (*Feature Extraction*), beschrieben:

Tabelle 23: Beschreibung der verwendeten statistischen Merkmale¹⁴⁷

Merkmals	Beschreibung	Mathematische Formulierung
Mean	Durschnitt aller betrachteten Werte innerhalb des Datensatzes (Mittelwert)	$\mu = \frac{1}{n} \sum_{i=1}^n x_i$
Median	Wert genau in der Mitte der Verteilung - Zentralwert	Diskreter Wert aus Datenmenge
Std	Maß für die Streubreite um den Mittelwert (Standardabweichung)	$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2}$
Varianz	Maß für die Breite der Verteilung – quadratische Abweichung	σ^2
Max	Maximalwert innerhalb des Datensatzes	$x_{max} = \max(\{x_1, x_2, \dots, x_n\})$
Skewness	Maß für die Asymmetrie des Datensatzes (der Verteilung)	$Sk = \frac{\mu_3}{\sigma^3} \text{ mit } \mu_3 = \frac{1}{n} \sum_{i=1}^n (x_i - \mu)^3$
Kurtosis	Maß für die Wölbung der Verteilung; gibt an, wie weit die vorliegende Verteilung von einer Normalverteilung abweicht	$Ku = \frac{\mu_4}{\sigma^4} \text{ mit } \mu_4 = \frac{1}{n} \sum_{i=1}^n (x_i - \mu)^4$
RMS	Maß für die Größenordnung der betrachteten Werte - Quadratisches Mittel, Effektivwert	$RMS = \sqrt{\frac{\sum_{i=1}^n x_i^2}{n}}$
Perzentil	Wert einer Variablen, unter diesen eine bestimmte Prozentzahl der Beobachtungen fällt.	Bsp.: p10 = 1.37A → 10% der gemessenen Werte sind kleiner als 1.37A
IQR	Berechnet sich aus der Differenz dem 25%- und 75%-Perzentil	$IQR = p_{75} - p_{25}$ Interquartil Range
Entropy	Maß für die „Verunreinigung“ des Datensatzes – also auch eine Art Streuungsmaß	$H(X) = - \sum_{i=1}^n P(x_i) * \log_2 P(x_i) \text{ mit}$ $P(x_i) \dots \text{relative Häufigkeit}$
Approx. Integral	Speziell für den Anwendungsfall: Näherungsweise Berechnung der Fläche unter dem Signalverlauf – Einheit [A*s]. Schrittweite für das numerische Integral gleich dem Samplingintervall	$\text{Approx. Int} \approx \sum_{i=1}^n x_i * h \text{ mit}$ $h = 0.004 \text{ s} \dots \text{Schrittweite}$

4.3.4 Normalisierung

In den nach der Merkmalsextraktion entstandenen Datensätzen herrschen skalenmäßige Unterschiede in den einzelnen Dimensionen vor. Um hier ein Bias bei der Weiterverwendung zu vermeiden und die Daten vergleichbar zu machen, können die Daten durch Berücksichtigung der Informationen über Minimal- und Maximalwerte skaliert bzw. normalisiert werden. Dieser Schritt ist optional, weil nicht jeder Algorithmus vom *Feature Scaling* beeinflusst wird. Als Beispiel ist hier der *MinMaxScaler* (Python) angeführt. Dabei wird vom betrachteten Merkmalswert x das Minimum subtrahiert und dann durch die Spanne (Minimum und Maximum) dividiert.

¹⁴⁷ vgl. Esmael et al., 2013, S.457f

Formel 3: Normalisierung von Variablen

$$x_{norm} = \frac{(x - \min(x))}{\max(x) - \min(x)}$$

Es wird sozusagen ein neuer Wert x_{norm} konstruiert. Somit sind alle Dimensionen/ Merkmale auf eine Skala im Bereich [0,1] normalisiert. Die relative Distanz zwischen den Punkten bleibt aber erhalten.

4.4 Verarbeitungs- und Analyseebene: Analyse

Nun kann der Knowledge Engineer mit dem präparierten Datensatz einen Algorithmus zur Anomalieerkennung einlernen und auf die zu untersuchenden Daten loslassen. Die Auswertung der Anomalieerkennung erfolgt über Anomalie Scores, die über eine Visualisierung am Dashboard (Teil der Nutzerebene) angezeigt werden. Die Anomalie Scores werden auch dazu verwendet, um eine Bewertung der detektierten Anomalien vorzunehmen. Parallel dazu überwacht eine implementierte Alarmlogik den Zustand der Maschine und meldet kritische Zustände an den *Domain Expert*. Die für die Verarbeitung und Analyse der Daten benötigte Zeit variiert stark und ist abhängig vom untersuchten Datenvolumen und vom ausgewählten Modell. Ferner ist auch die Analysequalität direkt abhängig von der zur Verfügung stehenden Datenqualität.

4.4.1 Erstellung Datenmodell und Anomaliedetektion

In diesem Kapitel werden jene ausgewählten Algorithmen erklärt, die als Kandidaten für die Anomalieerkennung in der beschriebenen Datenausgangslage in Frage kommen.¹⁴⁸ Dabei wird überblicksmäßig ein grundlegendes Verständnis über die Funktionsweise der Algorithmen hergestellt. Es sollen auch die Voraussetzungen und Gründe für die Anwendung erläutert werden. Die Auswahl der Algorithmen basiert auf der ausführlichen Literaturanalyse aus Kapitel 3 ab S.35 und zusätzlich werden auch Bemerkungen zur prototypischen Implementierung gemacht.

4.4.1.1 Statistische Anomalieerkennung

Es wird ein parameterfreier statistischer Ansatz von Goldstein & Dengel (2012) angewendet und getestet. Der **HBOS-Algorithmus** (*Histogram-based Outlier Score*) stellt eine Möglichkeit dar Anomalien ohne vorhergehende Modellannahmen und ohne vorhergehendes Training (Parameterschätzen) zu erkennen. Es wird für jedes Feature (jede Featurespalte) im Datensatz ein Histogramm erstellt und angenommen, dass jedes Feature (jede Dimension d) unabhängig von den anderen Features im Datensatz ist. Jedes erstellte Histogramm wird sodann auf 1 normiert, sodass jedes Feature gleich gewichtet wird. Danach wird für jede Instanz/ jede Messung (Reihe im Datensatz) p ein Ausreißerwert/ Anomaliewert (*Outlier Score*) anhand von d Histogrammen berechnet:

¹⁴⁸ Es besteht kein Anspruch auf Vollständigkeit. Jene Algorithmen stellen sozusagen den empfohlenen Inhalt der Werkzeugkiste für die Datenmodellierung dar, aus der der Knowledge Engineer auswählen kann.

Formel 4: Berechnung des Histogramm-basierten Anomaliefaktors HBOS

$$HBOS(p) = \sum_{i=0}^d \log\left(\frac{1}{hist_i(p)}\right)$$

Es wird also die Dichteverteilung mittels Histogramme modelliert. Vorteile dieser Methode sind ihre Effizienz und ihr geringer Rechenaufwand, was besonders wichtig für große Datensätze ist. Der Algorithmus ist um einiges schneller als vergleichbare multivariate Ansätze, dies aber auf Kosten der Präzision. Die Autoren stellten fest, dass der Algorithmus 5-mal bzw. 7-mal schneller arbeitet als auf Clustering bzw. Nächster Nachbar basierende Ansätze. Der Ansatz eignet sich somit sehr gut für die Anwendung am Fallbeispiel, da auch hier keine oder nur wenige Informationen über die Verteilung der Daten vorliegen und weil mit Blick auf eine eventuelle Online-Anwendung (CM in Echtzeit) eine kurze Rechenzeit gefragt ist. Die Implementierung basiert auf der Python Bibliothek *PyOD*, die speziell für die Anomalieerkennung entwickelt wurde. Es wird nur die erwartete Kontamination mit Anomalien als Parameter angegeben in der Grundeinstellung.

4.4.1.2 Nächster Nachbar Ansatz (Dichtebasiert)

Breunig et al. (2000) schlagen für die Ausreißererkennung den **LOF-Algorithmus** (*Local Outlier Factor*) vor. Dieser weist jedem Datenpunkt einen Faktor zu, der darauf hinweist, wie sehr der Punkt sich von benachbarten Punkten unterscheidet. Man geht also davon weg, das Problem binär zu betrachten (Ausreißer/ kein Ausreißer), da dies für komplexe Probleme oft weniger zielführend ist. Das *local* bezieht sich auf die Umgebung des betrachteten Punktes. Der Anomaliefaktor setzt sich aus dem Verhältnis von durchschnittlicher lokaler Dichte der k nächsten Punkte in Nachbarschaft des betrachteten Datenpunktes und dessen eigener Dichte zusammen. Die Nachbarschaft wird anwenderspezifisch durch den Parameter *MinPts*, also wieviele Punkte sich in der Nachbarschaft des betrachteten Punktes befinden sollen, definiert. „Die lokale Dichte eines Datenpunktes ist der Kehrwert der durchschnittlichen Erreichbarkeitsdistanz zu seinen nächsten Nachbarn. Unter der Erreichbarkeitsdistanz von Punkt x_A zu x_B wiederum wird das Maximum des Abstandes zwischen den Punkten und des Abstandes von Datenpunkt x_B zu dem k -nächsten Nachbarn verstanden.“¹⁴⁹

Als Vorteile dieser Methode können genannt werden, dass es eine unüberwachte ML-Methode ist und dass nur ein Parameter (*Contamination*) vorgegeben werden muss, was das Tuning des Algorithmus erleichtert. Mit *Contamination* schätzt der Anwender wieviel Prozent der Daten anomal sind (wie kontaminiert der Datensatz mit Ausreißern ist). Zum Berechnen des LOF muss aber jeder Datenpunkt mit jedem benachbarten verglichen werden. Dies wiederum mündet in einem hohen Rechenaufwand und das wirkt sich daher nachteilig auf die Leistung aus. Es wird zum einen ein unüberwachter Ansatz und zum anderen ein *Novelty detection* Ansatz über die *scikit-learn* Bibliothek implementiert.

4.4.1.3 Nächster Nachbar Ansatz (Distanzbasiert)

Als Vertreter der distanzbasierten Nächsten Nachbar Ansätze wird hier der **kNN-Algorithmus** (*k-nearest Neighbor*) am Fallbeispiel eingesetzt. Der einfache Algorithmus findet breite

¹⁴⁹ Hofmockel, 2019, S.57

Anwendung in den verschiedensten Bereichen der Klassifikation, aber dieser kann auch für unüberwachte Anomalieerkennung eingesetzt werden. Die Kategorisierung der betrachteten Datenpunkte passiert distanzbasiert. Dazu können verschiedene Abstandsmetriken (Mahalanobis, Manhattan etc.) eingesetzt werden. Das hier angeführte Beispiel zeigt das euklidische Abstandsmaß d .

Formel 5: Berechnung des euklidischen Abstandsmaßes

$$d(\mathbf{x}_i, \mathbf{x}_j) = \sqrt{(x_{i1} - x_{j1})^2 + \dots + (x_{iM} - x_{jM})^2}$$

worin \mathbf{x}_i und \mathbf{x}_j zwei Samples mit M Merkmalen (*Features*) sind.¹⁵⁰ Der Algorithmus lernt also über die Abstände die Datenpunkte nach dem Training in verschiedene Klassen einzuteilen. „Wenn unbekannte diskrete Daten empfangen werden, analysiert es die nächstgelegene k Anzahl von gespeicherten Instanzen (nächstgelegene Nachbarn) und gibt die gebräuchlichste Klasse als Vorhersage zurück und gibt für reale Daten den Mittelwert von dem k nächstgelegenen Nachbarn zurück.“¹⁵¹ Über eine Mehrheitsentscheidung wird somit ein Datenpunkt einer Klasse zugeordnet und um bei dieser Entscheidung ein Unentschieden zu vermeiden, wird k immer ungerade gewählt.¹⁵² Der kNN-Algorithmus findet also den Abstand des betrachteten Punktes zu den k nächsten Nachbarn, der kMeans-Algorithmus (siehe Kapitel 4.4.1.4 auf S.68) stellt allerdings den Abstand vom betrachteten Punkt zum Mittelpunkt des nächsten Clusters dar. Wird jene Distanz zu den k Nachbarn anomal groß, kann davon ausgegangen werden, dass es sich um einen Ausreißer handelt. Auch bei diesem Algorithmus ist kein Vorwissen über die Verteilung der Daten notwendig (unüberwachtes Lernen), was diesen Ansatz attraktiv für die Anwendung am Use Case macht. Ähnlich wie beim oben genannten LOF-Algorithmus entsteht auch bei diesem Ansatz ein hoher Rechenaufwand. In der Python-Umsetzung wird der Algorithmus über die freie Software-Bibliothek *scikit-learn* bezogen.

4.4.1.4 Clustering Ansatz

Der Clustering Ansatz wird vor allem dafür verwendet, Licht in das Daten-Dickicht zu bringen und Klassen zu erkennen. So ergeben sich besonders bei großen räumlichen (bzw. höherdimensionalen) Datensätzen folgende Anforderungen und Vorteile für Clustering-Algorithmus:¹⁵³

- Es ist nur geringes Domänenwissen für die (Algorithmus-) Inputparameter erforderlich, da adäquate Werte ja auch im Vorhinein nicht bekannt sind – gerade bei großen Datensätzen.
- Es sollten Cluster von unterschiedlicher Form vom Algorithmus erkannt werden. Die Erscheinungsformen von Clustern in räumlichen Datensätzen sind z.B. sphärisch, linear oder gezogen.
- Der Algorithmus sollte große Datenmengen effizient verarbeiten können.

¹⁵⁰ vgl. J. Zhao et al., 2018, S.16

¹⁵¹ Weber, 2020, S.50

¹⁵² vgl. Russel & Norvig, 2010, S.738

¹⁵³ vgl. Ester et al., 1996, S.231

Als bekanntester Vertreter der Clustering-Algorithmen wird der **kMeans-Algorithmus** angeführt. Der Anwender schätzt, idealerweise über eine vorher durchgeführte visuelle Inspektion des Datensatzes, eine Anzahl von k Mitteln (*Means*) – sprich die erwartete Anzahl von k Clustern in den Daten. Der Algorithmus erzeugt k zufällige Clusterzentren (Mittel) in den Daten und ordnet sodann die anderen Datenpunkte über Abstandsmaße den nächstgelegenen Clusterzentren zu. Im Anschluss werden die Schwerpunkte der entstandenen Cluster zum neuen Mittel, sodass die Clusterzuweisung neu iteriert werden kann – solange bis Konvergenz eintritt, also nur mehr geringe Verschiebungen der Mittel passieren oder eine festgelegte Anzahl an Iterationen durchgeführt wurde. Die Vorteile von kMeans-Clustering sind die Effizienz und Schnelligkeit. Als Nachteil wird die geschätzte Anzahl von Mitteln und zufällige Initiierung durch den Algorithmus gesehen, da hier bei wiederholter Anwendung des Algorithmus auf den gleichen Datensatz unterschiedliche Ergebnisse resultieren.¹⁵⁴ Ein weiterer Nachteil in Bezug auf die vorliegende Anwendung der Anomalieerkennung ist, dass der Algorithmus jeden Datenpunkt einem Cluster zuordnet. Als Lösung dieses Problems wird zuerst ein Model gefittet und im Anschluss werden Anomalien in den Daten über ein Abstands- bzw. Fehlermaß in Kombination mit einem festgelegten Grenzwert bestimmt.

4.4.1.5 Klassifikationsansatz

Da keine bzw. eine nur sehr schwache Repräsentation der anomalen Klasse gegeben ist, wird ein Algorithmus angewandt, der nur mit normalen Daten (nur mit einer Klasse) trainiert wird – die **One-Class SVM** (*One-Class Support Vector Machine*) vorgeschlagen von Schölkopf et al. (1999). Dieser halbüberwachte Lernalgorithmus erkennt also, ob die betrachtete Dateninstanz der einen eintrainierten (normalen) Klasse angehört oder von dieser signifikant abweicht, sodass diese als Anomalie markiert werden muss. Der Einsatz dieses Algorithmus für den vorliegenden Anwendungsfall ist gerechtfertigt, weil über vorhandenes Expertenwissen zumindest einige Messperioden als *anomaliefrei* (fehlerfrei) identifiziert wurden, wodurch ein zuverlässiges Training möglich wird. Aus Sicht der Anomalieerkennung stellt dieser Ansatz eine Novelty detection dar, weil noch ungesehene bzw. neue Datenpunkte (Dateninstanzen) als zur trainierten Klasse zugehörig oder nicht zugehörig kategorisiert werden müssen. Der One-Class SVM Algorithmus lernt mit den Trainingsdaten eine Entscheidungsgrenze (eine sphärische Hülle, *Hyperplane*) ein, sodass sich der Großteil der Datenpunkte innerhalb dieser Grenze bzw. dieses Bereiches befindet. Alle Punkte außerhalb dieser werden als Anomalien klassifiziert. Grundsätzlich ist der Output des Algorithmus binär, es lässt sich aber auch hier ein Ausreißerfaktor (*Outlier Score*) berechnen. Der Anwender kann eine implizite Transformationsfunktion wählen, die über Kernelfunktionen wie z.B. RBF (Radiale Basisfunktion), den Eingabevektor in eine höhere Dimension überführt.¹⁵⁵ Als Parameter wird die Regressionsgenauigkeit Nu vorgegeben, die vom Verhältnis von Fehlern im Training und Unterstützungsvektoren (SV, *Support Vectors*) anhängig ist und das Verhalten der quadratischen Programmierung beeinflusst. Der Algorithmus arbeitet mit einer beherrschbaren Rechenkomplexität (quadratische Optimierung), allerdings gestaltet sich eine passende Wahl der Kernelfunktion als schwierig.¹⁵⁶

¹⁵⁴ vgl. Weber, 2020, S.54f

¹⁵⁵ vgl. Amer et al., 2013, S.9f

¹⁵⁶ vgl. Schölkopf et al., 1999, S.583f

Autoencoder, auch Replikator Neuronale Netzwerke¹⁵⁷, werden ebenfalls mit historischen Daten einer Klasse trainiert – im Anwendungsfall des Industrieofens auch nur mit Daten des gesunden Maschinenzustandes. Ein Autoencoder ist ein künstliches neuronales Netz mit einer feedforward Architektur: Der Signalfuss im Netz läuft nur in eine Richtung – vom *Inputlayer* (Eingangsschicht) durch ein *hidden Layer* (verborgen, kein direkter Netzausgang) hin zum *Outputlayer* (Ausgangsschicht). Abbildung 18 zeigt die Grundstruktur eines Autoencoders:

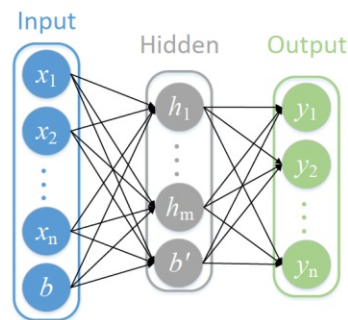


Abbildung 18: Grundlegende feedforward Struktur eines Autoencoders¹⁵⁸

Der Autoencoder kann auch mit ungelabelten Daten Zusammenhänge vom zugrundeliegenden System lernen. Dazu wird das Inputdaten-Trainingset \mathbf{x} in die verborgene Darstellung \mathbf{h} (hidden representation) mit einer nicht-linearen Aktivierungsfunktion $\varphi(\cdot)$ übergeführt

Formel 6: Zusammenhang zwischen Input Layer und Hidden Layer mit nicht-linearer Aktivierungsfunktion

$$\mathbf{h} = \varphi(\mathbf{W}\mathbf{x} + \mathbf{b}).$$

Jener Schritt wird *encoding* genannt. Hier wird ein höherdimensionaler Raum auf einen niedrigerdimensionalen Raum abgebildet. Danach wird die verborgene Darstellung vom Eingang (also der Vektor \mathbf{h}) in der Art auf den Ausgang \mathbf{y} projiziert, dass dieser ähnlich dem Eingang \mathbf{x} ist

Formel 7: Zusammenhang zwischen Hidden Layer und Output Layer mit nicht-linearer Aktivierungsfunktion

$$\mathbf{y} = \varphi(\mathbf{W}'\mathbf{x} + \mathbf{b}').$$

Dieser Schritt wird *decoding* genannt und danach wird wieder ein höherdimensionaler Raum abgebildet. Durch das encoding und decoding lernt der Autoencoder dann die notwendigen Modellparameter $\theta = [\mathbf{W}, \mathbf{b}, \mathbf{W}', \mathbf{b}']$. Die Parameter \mathbf{W} und \mathbf{W}' sind die Gewichte der einzelnen Knotenpunkte (*nodes*), \mathbf{b} und \mathbf{b}' stellen ein Bias dar. Mit diesen eingelernten Parametern kann der Output aus dem Input rekonstruiert/ repliziert werden, sodass gilt

Formel 8: Rekonstruktion des Eingangs über die gelernte Funktion

$$\mathbf{y} = f_{\theta}(\mathbf{x}) \cong \mathbf{x}$$

Für das Training/ Einlernen des Modells wird also versucht, den Rekonstruktionsfehler zu minimieren. Anomalien in den Daten werden dadurch erkannt, dass bei gewissen

¹⁵⁷ vgl. Hofmockel, 2019, S.84

¹⁵⁸ H. Wang, 2020, S.2

Dateninstanzen hohe Rekonstruktionsfehler auftreten. Überschreitet das Fehlermaß einen festgelegten Wert, wird die dazugehörige Dateninstanz als Anomalie kategorisiert.¹⁵⁹ Vorteile dieser Methode sind unter anderem, dass ein Anomalie Score ausgegeben wird und sie auch für höherdimensionale Datensätze geeignet ist. Als Nachteile können eine fehlende Robustheit gegenüber Ausreißern in Trainingsdaten und die schwierige Bestimmung der Rechenkomplexität (auch Trainingsdauer) aufgrund der variablen Architektur angeführt werden.¹⁶⁰

4.4.1.6 Isolation Forest

Diese Methode wurde das erste Mal von F. T. Liu et al. (2008) vorgestellt. Bei diesem Ansatz wird nicht versucht, wie vorher oft dargestellt, ein Profil von normalen Dateninstanzen zu erstellen, mit denen dann andere Dateninstanzen verglichen und dadurch gegebenenfalls als anomal eingestuft werden. Der Isolation Forest (auch iForest) Algorithmus stellt fest, wie schnell sich ein Datenpunkt von anderen Punkten der Datenmenge isolieren lässt – siehe Abbildung 19. Dabei werden zwei quantitative Eigenschaften von Anomalien ausgenutzt: 1) Anomalien sind immer als Minderheit repräsentiert und 2) ihre Attribute (Features, Merkmale) sind meistens gut unterscheidbar von den normalen Dateninstanzen. Führt man sich die binäre Baumstruktur aus Abbildung 20 vor Augen, werden Anomalien aufgrund ihrer Anfälligkeit zur schnellen Absonderung bereits nach wenigen Iterationen, also nahe an der Baumwurzel, isoliert (kurze Pfadlänge). Normale Dateninstanzen hingegen werden weiter unten eher am Ende der Baumstruktur (große Pfadlänge) isoliert. Mehrere iTrees im Ensemble ergeben eben einen iForest. Anomale Punkte sind dann jene, die eine kurze durchschnittliche Pfadlänge aufweisen.¹⁶¹ „Jeder Baum besteht aus einem zufälligen Subset des Datensatzes mit einer festgelegten Größe. Der Datensatz wird solange partitioniert, bis entweder jeder Datenpunkt isoliert dargestellt wird oder eine durchschnittliche Tiefe erreicht wird.“¹⁶²

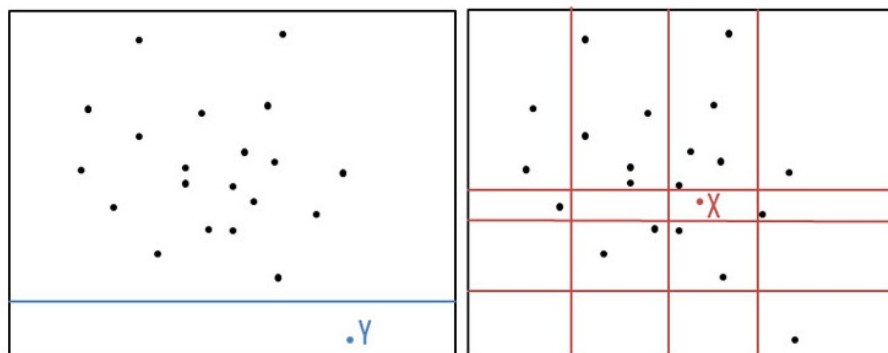


Abbildung 19: Isolation Forest – Darstellung des Unterschiedes zwischen schneller Absonderung (Y) und langsamer Absonderung (X)¹⁶³

¹⁵⁹ vgl. H. Wang, 2020, S.2f

¹⁶⁰ vgl. Hofmockel, 2019, S.53

¹⁶¹ vgl. F. T. Liu et al., 2008, S.413

¹⁶² Köhne, F.: Anomalien mit H2O.AI – Isolation Forest finden und erklären (26.04.2019), <https://blog.viadee.de/isolation-forests-anomalien-mit-h2o-ai> (Gelesen am 23.03.2021)

¹⁶³ Köhne, F.: Anomalien mit H2O.AI – Isolation Forest finden und erklären (26.04.2019), <https://blog.viadee.de/isolation-forests-anomalien-mit-h2o-ai> (Gelesen am 23.03.2021)

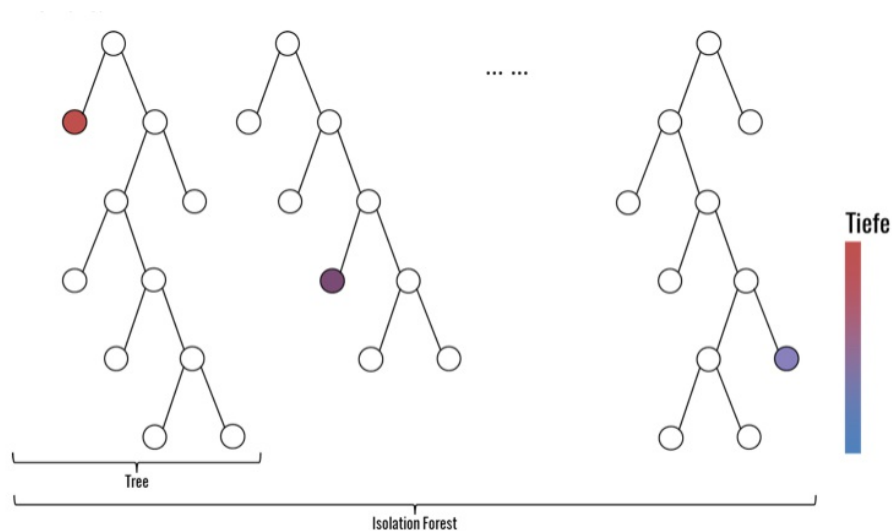


Abbildung 20: Isolation Forest – Darstellung der Baumstruktur und unterschiedliche Pfadlängen (Strukturtiefe)¹⁶⁴

Als Vorteile dieses Algorithmus führen Baasch et al. (2018) an, dass der Algorithmus einmal trainiert ohne wiederkehrende Kalibrierung auf neue Daten angewendet werden und die Stärke/ den Grad der Anomalie (engl. anomaly score) ausgeben kann. F. T. Liu et al. (2008) betonen, dass der iForest auch höherdimensionale Datensätze adäquat verarbeitet (bzgl. Rechenaufwand/ -zeit) und sich daher auch für Online Anomaliedetektions-Anwendungen eignet. Der Algorithmus erkennt Anomalien ungeachtet davon, ob sich Anomalien im Trainingsdatensatz befinden oder nicht. Als Tuning-Parameter für den Algorithmus dienen die maximale Subsample-Größe, die Anzahl der iTrees im iForest, die maximale iTree-Tiefe und Pfadlänge. In der Python-Umsetzung wird der Algorithmus über die freie Software-Bibliothek *scikit-learn* bezogen.

Es sei hier im allgemeinen Teil auch ein Ansatz erwähnt, der speziell für den vorliegenden Anwendungsfall des Industrieofens entwickelt wird: ein signalgruppenbasierter Ansatz, wo Öffnungs- und Schließsignale als Gesamtheit durch Features charakterisiert und mit Hilfe des Isolation Forest Algorithmus' auf Anomalien untersucht werden. Die Erklärung dazu wird direkt in der Fallstudienbearbeitung angeführt (siehe Kapitel 5.3.1.4 auf S.94).

Abschließend soll eine Zusammenstellung der verwendeten Methoden gegeben werden. Eine diesbezügliche Übersicht findet sich in Abbildung 21. Tabelle 24 vergleicht zusammenfassend relevante Eigenschaften der empfohlenen Detektionsalgorithmen. Jene Tabelle kann dem Knowledge Engineer bei der Auswahl des passenden Modells helfen. Grundsätzlich zeigt aber die Erfahrung, dass die Anwendung von mehreren verschiedenen Algorithmen und Ansätzen mit anschließender Bewertung von Vorteil ist.

Es entscheiden die Algorithmen also auf unterschiedliche Art und Weise über die Normalität bzw. Anomalität einer Dateninstanz. Dies geschieht entweder algorithmusintern direkt über die Ausgabe eines Anomalie Scores oder über errechnete Abstandsmaße. Den Messwerten in den einzelnen Dataframes (Python-Spezifikum) wird nicht nur eine Spalte mit den Anomalie

¹⁶⁴ ebenda

Scores zugeordnet, sondern auch eine Spalte bestehend aus der binären Information über die Anomalie (z.B. Normaler Punkt dargestellt durch 1, anomaler Punkt durch -1).

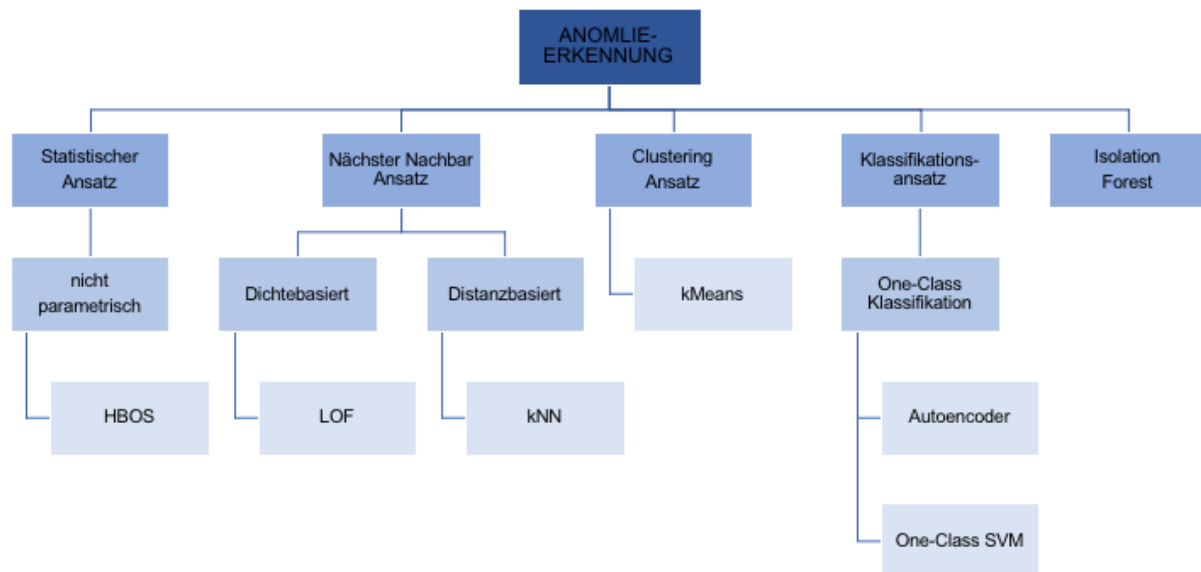


Abbildung 21: Verwendete Methoden der Anomalieerkennung¹⁶⁵

Tabelle 24: Vergleich der Kandidatenalgorithmen auf Basis der Literatur

Algorithmus	Effizienz bei großen Datensätzen	Ausgabe Anomalie-score	Algorithmus-interner Grenzwert	Trainingsdauer	Parameter
HBOS	Ja	Ja	Ja	-	1
LOF	Nein	Ja	Ja	Wenn als halbüberwacht angewandt: lange	1
kNN	Ja	Nein	Nein	-	1
kMeans	Ja	Nein	Nein	-	1
Autoencoder	Wenn einmal trainiert, ja	Nein	Nein	Variabel; abhängig von Netzwerkstruktur	
OC-SVM	Nein	Ja	Ja	Wenn als halbüberwacht angewandt: lange	1
Isolation Forest	Ja	Ja	Ja	kurz	1

Das Postprocessing, das Nachbereiten der Ausgaben der angewandten Algorithmen, bildet nicht nur die Grundlage für Entscheidungen bzgl. Instandhaltungsmaßnahmen, sondern auch für die Interpretation der Ergebnisse. Zusätzlich kann eine „[...] Robustheit gegen Anomalien in den Trainingsdaten [...] nachträglich erfüllt werden. Durch eine datenbasierte Bestimmung des Grenzwertes anhand der Trainingscores können die außergewöhnlichsten Trainingspunkte ignoriert werden, was eine Robustheit gewährleistet.“¹⁶⁶ Es gilt, ein verlässliches und effizientes Arbeiten der Anomalieerkennung sicherzustellen und brauchbare Ergebnisse für den Anwendungsfall zu erhalten. Mögliche Anomalien werden einerseits über

¹⁶⁵ Eigene Darstellung

¹⁶⁶ Hofmockel, 2019, S.94

einen Anomalie Score und andererseits über Abstandsmaße in Kombination mit statischen Grenzwerten bestimmt.

4.4.2 Anomalie Scores (Anomaliefaktor)

Einige der Algorithmen geben, wie bereits erwähnt, nicht nur binäre Aussagen (Anomal/Normal) über Dateninstanzen zurück, sondern kontinuierliche Werte über den Grad der Anomalität (Anomaliefaktor). Der Anomalie Score zeigt an, wie sehr sich die betrachtete Dateninstanz vom Großteil der Daten unterscheidet oder diesem ähnlich ist. Die verwendeten Algorithmen berechnen die Scores intern und entscheiden somit auch automatisch, welche Punkte als Anomalien ausgegeben werden und welche nicht. Für ein tieferes Verständnis bieten jene Algorithmen Funktionen, mit denen für jede einzelne Dateninstanz der Score ausgegeben und visualisiert werden kann. Abbildung 22 zeigt einen Dataframe (Python-spezifisches Ausgabeformat), der den gemessenen Strom (*current*), sämtliche statistische Merkmale (*rollingMean* etc.), die kategorische Variable (*anomalies*) und den Anomaliefaktor (*neg outlier factor*) darstellt, und zwar mit dem Zeitstempel als Index (*date*). Hier ist zu sehen, dass der letzte sichtbare Eintrag z.B. mit einem Faktor von ca. -9.7 deutlich von den vorhergehenden abweicht und der Algorithmus diese Dateninstanz als anomal (*anomalies* = -1) einstuft.

Folgende der angewandten Algorithmen geben direkt Anomaliefaktoren aus:

- HBOS
- LOF
- One-Class SVM
- Isolation Forest

date	current	rollingMean	rollingMedian	rollingDev	rollingVar	rollingSkew	rollingMax	anomalies	neg outlier factor
2019-04-29 11:40:06.087	1.38	1.372	1.370	0.004216	0.000018	1.778781e+00	1.38	1	-0.998997
2019-04-29 11:40:06.093	1.38	1.373	1.370	0.004830	0.000023	1.035098e+00	1.38	1	-1.199181
2019-04-29 11:40:06.099	1.38	1.374	1.370	0.005164	0.000027	4.841229e-01	1.38	1	-1.127160
2019-04-29 11:40:06.106	1.38	1.375	1.375	0.005270	0.000028	4.213012e-09	1.38	1	-1.154339
2019-04-29 11:40:06.112	1.36	1.374	1.375	0.006992	0.000049	-7.801058e-01	1.38	-1	-9.713268
...

Abbildung 22: Beispiel eines Dataframes mit Messwerten, Features und Anomaliefaktor (Ergebnisse einer Analyse mit LOF)¹⁶⁷

Im Folgenden wird darauf eingegangen, wie für jene Algorithmen ohne direkten und internen Scoreoutput Entscheidungsgrenzen gewählt und berechnet werden.

4.4.2.1 Bestimmen von Grenzwerten für Abstandsmaße

Es muss also geklärt werden, bei welchen Werten eine beobachtete Dateninstanz als anomal oder normal eingestuft wird, wenn die Daten mit einem kNN- oder kMeans-Algorithmus oder einem Autoencoder analysiert werden. Für diese Entscheidung können bei kNN und kMeans eben das Abstandmaß und beim Autoencoder der Rekonstruktionsfehler herangezogen

¹⁶⁷ Eigene Darstellung

werden. Es wird eine statische Grenzwertberechnung angewandt, was heißt, dass sich der Grenzwert über den Beobachtungszeitraum nicht ändert. Über eine empirische Regel (*Rule of Thumb*), nämlich der *3-Sigma-Regel*, wird ein Grenzwert τ festgelegt.

Formel 9: Berechnung des unteren (lower) und oberen (upper) Grenzwertes (τ)

$$\tau_{L,U} = \mu \pm 3 * \sigma$$

μ ist der Mittelwert der berechneten Abstandsmaße d und σ die Standardabweichung der beobachteten Abstandsmaße d (bzw. der Rekonstruktionsfehler). Am Beispiel des Abstandsmaßes wird somit die betrachtete Dateninstanz \mathbf{x}_t als normal gekennzeichnet, wenn für das berechnete Abstandsmaß $d(t, \mathbf{x}_t)$, das als Output der Algorithmen zum Zeitpunkt t ausgegeben wird, gilt:

Formel 10: Formulierung des normalen Bereiches für d

$$\tau_L < d(t, \mathbf{x}_t) < \tau_U$$

Liegt der errechnete Wert aber außerhalb dieses Bereichs, wird die Dateninstanz als Anomalie erkannt. Der statische Ansatz ist gerechtfertigt, da keine saisonalen Änderungen und Arbeitspunktwechsel im konkreten Anwendungsfall zu erwarten sind.

Für beide Ansätze, Anomalie Score oder Abstandsmaß, wird für eine übersichtliche Darstellung später deren Entwicklung im Zeitverlauf dargestellt. Der Verlauf kann in weiterer Folge auch auf einem *Dashboard* (Darstellung der Verläufe wesentlicher Parameter in der Nutzerebene) für das Instandhaltungspersonal visualisiert werden. So erhält anomales Verhalten des Systems einen zeitlichen Bezug. Die berechneten Grenzwerte sind auch Ausgangspunkt für die Einteilung der identifizierten Anomalien in Kategorien nach Kritikalität. Es wird im weiteren Verlauf nur mehr von einem Grenzwert τ gesprochen, ohne die Unterscheidungs- bzgl. der Berechnungsart zu berücksichtigen.

4.4.2.2 Bestimmung Kritikalitätslevel

Nachdem die einzelnen Algorithmen etwaige anomale Datenpunkte in den Zeitreihen detektiert haben, gilt es die Kritikalität (*Severity Level, SV*) dieser Anomalien zu bewerten. Dies geschieht über den Anomalie Score. Dazu wird eine vierstufige Bewertungsskala eingeführt, siehe Tabelle 25.

Tabelle 25: Beschreibung der Kritikalitätskategorien (Severity Levels) mit Übergangsgrenzwerten

Kritikalität	Beschreibung	Farbcode
sv ₀	Normalwertbereich, in dem die Werte im erwarteten Bereich liegen und somit kein anomales Verhalten vorliegt. Anomalie Score liegt unterhalb des Grenzwertes.	Grün
SV ₀₁		
sv ₁	<i>Sonstige</i> Anomalie festgestellt, bei der der Grenzwert durch den Anomalie Score nur leicht überschritten wird. Mögliche Gründe sind z.B. Mess- oder Prozessrauschen oder ungünstige Grenzwertwahl.	Gelb
SV ₁₂		
sv ₂	<i>Mäßige</i> Anomalie festgestellt, bei der die Grenzwertüberschreitung durch den Anomalie Score instandhaltungstechnische Relevanz hat. Eine Häufung von Anomalien dieser Art sind ein klares Warnsignal für das Anlagenpersonal.	Orange
SV ₂₃		
sv ₃	<i>Kritische</i> Anomalie festgestellt, bei der der Grenzwert durch den Anomalie Score massiv überschritten wird. Eine Häufung von Anomalien dieser Art können umgehende Maßnahmen erfordern.	Rot

Nun wird geklärt, wie diese Einteilung aus dem vorhandenen Anomalie Score (AS) berechnet wird, also wie die Kritikalitätsbereiche (sv_0 - sv_3) numerisch unterteilt werden. Für diese drei Übergangswerte (sv_{01} , sv_{12} , sv_{23}) wird im ersten Schritt der algorithmusinterne oder über die 3-Sigma-Regel ausgegebene Grenzwert τ herangezogen. Die erste Grenze also zwischen sv_0 und sv_1 bildet der Grenzwert τ , sodass gilt

Formel 11: Bestimmung von sv_{01}

$$sv_{01} = \tau$$

Für die anderen Übergänge muss eine Spanne (*Range*) des Anomalie Scores betrachtet werden. Dazu wird der Bereich zwischen Grenzwert τ und dem Maximum des Anomalie Scores betrachtet

Formel 12: Bestimmung der Spanne des anomalen Bereiches

$$range = \max(AS_a) - \tau$$

wobei gilt, dass $\max(AS_a) = \max(AS)$. AS_a bezeichnet den anomalen Bereich des Anomalie Scores. In dieser *range* befinden sich eben die drei Kritikalitätsbereiche sv_1 - sv_3 . Die Spanne wird nun dreigeteilt, sodass die zwei fehlenden Übergangswerte ermittelt werden können.

Formel 13: Bestimmung von sv_{12}

$$sv_{12} = sv_{01} + \frac{1}{3} * range$$

Formel 14: Bestimmung von sv_{23}

$$sv_{23} = sv_{01} + \frac{2}{3} * range$$

sodass gilt

Formel 15: Zusammenhang der Übergangswerte

$$sv_{01} < sv_{12} < sv_{23}$$

Durch einen einfachen Vergleich des vorliegenden Anomalie Scores mit den bestimmten Übergangswerten kann damit ein Messpunkt entsprechend seiner Kritikalität kategorisiert werden. Liegt z.B. ein Anomalie Score eines Messwertes zwischen sv_{01} und sv_{12} , kann dieser als *sonstige* Anomalie eingestuft werden. Offensichtlich ist die Spanne alleinig vom Anomalie Score abhängig, was wiederum bedeutet, dass bei einem kleinen AS_a die Spanne nur sehr eng wird. Infolgedessen können die Übergangswerte sehr nah beieinanderliegen und somit auch die einzelnen Kritikalitätsbereiche nur sehr schmal sein. Der Grenzwert τ für die Anomalieentscheidung und die Übergangswerte (sv_{01} , sv_{12} , sv_{23}) werden, wie später zu sehen ist, im Schaubild des Anomalie Scores visualisiert.

4.4.3 Alarmlogik mit Falschalarmfilter

Nun wird eine Alarmlogik eingeführt, die verhindert, dass bei jeder detektierten Anomalie ein Alarm getriggert wird. Wenn die Daten feingranular auf Anomalien untersucht werden, kommt

es vor, dass auch nur kleine aber eigentlich harmlose Ausschläge oder Abweichungen bereits als anomal erkannt werden (Bereich sv_1). Würde hier bei jedem anomalen Punkt ein Alarm an das IH-Personal gesendet werden, würde es abstumpfen und das Vertrauen in das CM-System verlieren. Es würde wie in der Literaturanalyse erwähnt zu einem *Alarm Shower* kommen. Somit wird erst ein Alarm ausgelöst, wenn mehrere anomale Punkte in einem vordefinierten Zeitfenster erkannt werden, aber nur jene mit der Kritikalität sv_2 und darüber. Die Logik wirkt sozusagen wie ein Falschalarmfilter. Es wird vorgeschlagen, über einen Sliding Window Ansatz die Anzahl der Überschreitungen des errechneten Grenzwertes (sv_{12}) in einem vordefinierten Zeitfenster aufzusummieren. Je größer das Zeitfenster wird, desto glatter wird der Verlauf der Summe. Übersteigt jene Summe/ Anzahl einen durch den Domain Expert festgelegten Grenzwert, wird ein Alarm ausgelöst. Einen angemessenen Wert zu finden gestaltet sich als äußerst schwierig und kann z.B. über *Trial and Error* bewerkstelligt werden. Eine andere Möglichkeit stellt auch die Berechnung eines Grenzwertes über die 3-Sigma-Regel dar.

4.4.4 Ergebnisvisualisierung

Die Darstellungen der Ergebnisvisualisierung bilden die Grundlage für die Zusammensetzung eines Dashboards, von dem das Instandhaltungspersonal Zustandsinformationen abliest. Das Dashboard soll eine Übersicht über den Zustand der Anlage in einem bestimmten Betrachtungszeitraum geben. Aus den Ergebnissen der Anomalieerkennung können der Verlauf der Messsignale (Zeitreihen) gemeinsam mit markierten Anomalien und der Verlauf des Anomaly Scores mit den Übergangswerten der Kritikalitätsbereiche dargestellt werden. Außerdem wird die Anzahl der Grenzwertüberschreitungen in einem bestimmten Zeitfenster überwacht. Für die zusätzliche Diagnose kann auch die Anzahl der Messpunkte in den einzelnen Bereichen (sv_0 - sv_3) aufgeschlüsselt werden.

4.5 Nutzerebene

In dieser letzten Ebene kann das Personal direkt mit der Anlage/ dem System interagieren. Es können Informationen abgelesen werden und bei Bedarf auch Instandhaltungsmaßnahmen initiiert werden. Hauptakteur in dieser Ebene ist der Domain Expert.

4.5.1 Dashboard

In der dritten Ebene ist als zentrale Einheit das Dashboard angebracht, welches eine übersichtliche grafische Benutzeroberfläche ist, auf der Messwerte sowie der zeitliche Verlauf des Anomalie Scores angezeigt werden. Zusätzlich kann der Verlauf der relevanten Grenzwertüberschreitungen (Alarmlogik) mitverfolgt werden. Die genaue Ausgestaltung der Ergebnisvisualisierung im Zuge des Dashboards ist abhängig vom Anwendungsfall und den gegebenen Präferenzen des Betreiberpersonals. Jene Benutzeroberfläche ist zentral in der Nutzerebene eingebettet, da hier die Interaktion mit dem Domain Expert passiert. Der Domain Expert kennt die betrachtete Anlage und das Umfeld dergleichen.

Eine prototypische Ausgestaltung des Dashboards wird im Zuge der Bearbeitung des Anwendungsfalles in Kapitel 5.4.1 auf S.100 entworfen.

4.5.2 Evaluierung und Ableitung Instandhaltungsmaßnahmen

Der Domain Expert kann durch die grafische Aufbereitung und durch seine Erfahrung Ergebnisse aus der Anomaliedetektion evaluieren und gegebenenfalls Instandhaltungsmaßnahmen einleiten. Das Dashboard dient zur Unterstützung bei der Entscheidungsfindung durch das Instandhaltungspersonal. Werden tatsächlich anomale Stromverläufe detektiert, beurteilt der Mitarbeiter/ die Mitarbeiterin jene Meldung, veranlasst entsprechende Maßnahmen und speichert das Gelernte und die Aktion dann in Form einer Ground Truth in der Ground Truth Datenbank ab. Wird aber bei der Evaluierung durch den Domain Expert festgestellt, dass das Datenmodell auffällig viele Falschmeldungen erzeugt, muss das angewandte Datenmodell vom Knowledge Engineer überarbeitet werden.

In der Nutzerebene können also zwei Fälle auftreten: 1) Es wird tatsächlich anomales Verhalten festgestellt (Alarmlogik schlägt richtig an) und dann darauffolgend eine Instandhaltungsaktivität eingeleitet. Jene Informationen einerseits die Instandhaltungsaktion (wer hat was wann wo warum durchgeführt) und andererseits die anomale Dateninstanz (Anomalie bekommt zeitlichen Kontext) betreffend werden in der Ground Truth abgespeichert. Oder 2) es kommt zu einer Falschmeldung bzw. es ist nicht erklärbar, warum die Alarmlogik anschlägt. Hier muss evaluiert werden, ob nicht eben der Algorithmus durch den Knowledge Engineer adaptiert werden muss. Diese letzten Schritte bestehend aus dem Abspeichern der Instandhaltungsaktivitäten und dem Erklären sowie Markieren von Anomalien (*Reasoning and Labelling*) wird auch *Ground Truth Building* genannt und ist Teil zukünftiger Entwicklungen. Dies bildet die Grundlage für das zukünftige Einlernen von überwachten Klassifikatoren und einer möglichen Schadenskategorisierung, ist aber nicht Teil dieser Untersuchungen.

Aufgrund der zugrundeliegenden Datenlage, ungelabelte Messungen mit erwartungsgemäß wenigen Anomalieerscheinungen, kann keine automatisierte Algorithmevaluierung implementiert werden. D.h. es können keine Performance-Metriken wie F-measure, Precision oder AUC berechnet werden. An die Stelle der softwaretechnischen Evaluierung tritt die Evaluierung durch ExpertInnen.

Nachdem das Phasenmodell mit den einzelnen Ebenen entwickelt und erklärt wurde, wird im folgenden Kapitel der Anwendungsfall des Industrieofens bearbeitet. Es sollen Anomalien im Stromkurvenverlauf einer Einlauffüre eines Industrieofens entdeckt werden, sodass eine datenbasierte Zustandsüberwachung realisiert werden kann. Die Bearbeitung des Anwendungsfalles basiert auf dem entwickelten Phasenmodell, das die nötigen Schritte zur Realisierung der Zustandsüberwachung transparent offenlegt.

5 Validierung

Das entwickelte Phasenmodell wird in Form einer Proof-of-Concept Studie an einem konkreten Industrieanwendungsfall angewendet. So werden zuerst der Anwendungsfall und die vorhandenen Daten erklärt und untersucht (*Datenebene*). Im Anschluss daran werden jene Daten aufbereitet, sodass diese für die tatsächliche Modellierung brauchbar eingesetzt werden können (*Verarbeitungs- und Analyseebene*). Eine umfassende Evaluierung der Ergebnisse (bis auf wenige Ausnahmen) ist mit der vorliegenden Informationslage bei diesem Anwendungsfall nur eingeschränkt möglich. Das Kapitel der Validierung beinhaltet auch die Visualisierung der Ergebnisse mit Hilfe einer Skizze eines Dashboards. Grundlage für die folgenden Ausführungen ist das in Python implementierte und auf den Anwendungsfall angewandte Phasenmodell. Es wird also die Anwendung der drei Ebenen des entwickelten Phasenmodells erläutert.

Nach der Literaturanalyse kann folgendes für den vorliegenden Anwendungsfall angemerkt werden:

- ExpertInnenwissen ist für das CM der hochkomplexen Industrieofenanlage unbedingt notwendig, damit die richtigen bzw. repräsentativen Bauteile überwacht werden.
- Gemessene Daten müssen mit großem Aufwand präpariert werden, bevor ML-Algorithmen darauf angewendet werden können. Dies sollte ca. 80% der Arbeit ausmachen. Besonderes Augenmerk muss dabei auf das Feature Engineering gelegt werden.
- Es liegt ein binäres Klassifikationsproblem vor. Das Ungleichgewicht im indifferenten Datensatz kann nur auf Algorithmusebene behandelt werden, da keine Label oder sonstige dafür relevante Informationen vorliegen.
- Aufgrund der fehlenden Label (Ground Truth) können keine Performance-Metriken berechnet werden.
- Kandidatenalgorithmen sind Isolation Forest, One-Class-Classifier, Autoencoder und andere unüberwachte bzw. halbüberwachte Ansätze. Jene Algorithmen wurden bereits im Kapitel 4.4.1 auf S.66 dargelegt.

Die gesamte softwaretechnische Umsetzung der Datenverarbeitung bzw. des Phasenmodells passiert in einer Jupyter Notebook Umgebung und basiert auf unterschiedlichen Python Software Bibliotheken.

5.1 Datenebene

Zuerst wird ein Geschäftsverständnis für den Anwendungsfall hergestellt und danach ein Verständnis für die vorhandenen Sensorrohdaten.

5.1.1 Einführung in den Anwendungsfall

Die betrachtete Industrieofenanlage wurde von einem österreichischen Hersteller industrieller Wärmebehandlungsanlagen entwickelt und hergestellt. Thermische Prozessmaschinen werden im Allgemeinen bei Temperaturen zwischen 400°C und 950°C betrieben und sind

nahtlos in den Produktionsablauf integriert, wodurch sich eine kritische Verkettung mit nachfolgenden Prozessen ergibt. Die betrachtete Anlage ist eine sogenannte Durchstoßanlage und diese wird im industriellen Umfeld besonders dort für die Gasaufkohlung eingesetzt, wo große Stückzahlen einer Wärmebehandlung unterzogen werden müssen. Die Anlage besteht aus mehreren Einzelaggregaten mit unterschiedlichen Verwendungen. Im Zuge dieser Diplomarbeit wird ein Vorwärmofen betrachtet. Vorwärmöfen im Allgemeinen erwärmen einzelne Chargen, sodass bei der anschließenden Wärmebehandlung der Bauteilverzug verringert und die Aufkohlungsgleichmäßigkeit verbessert wird. Als eine der kritischen Komponenten der Vorwärmanlage wurde durch ExpertInnen unter anderem die Einlauftüre, welche eine lineare Öffnungs- und Schließbewegung beim Chargiervorgang (Auf/Zu) ausführt, identifiziert.

Grundsätzlich werden jene hochkomplexen und für den Fertigungsablauf kritischen Anlagen mittels RCM-Strategie instandgehalten, sodass es mit hoher Wahrscheinlichkeit zu keinen unerwarteten Ausfällen während des laufenden Betriebes (also vor der einmaligen jährlichen Wartung) kommt. Das Ziel der Forschungsarbeit ist es aber, zu untersuchen, ob eine Zustandsüberwachung möglich ist. „An Thermoprozessanlagen wird CM zur Anomalieerkennung hauptsächlich eingesetzt, weil die Inspektionsintervalle einer Jahreswartung typischerweise zu lange sind, um sich anbahnende Zustandsverschlechterungen rechtzeitig zu erkennen.“¹⁶⁸ Da dazu kontinuierlich Daten notwendig sind, wurde eine bestehende Anlage ohne Sensorik nachgerüstet, sodass Zustandsdaten der Maschine erhoben werden können. Bei der retrogefitteten Anlage ist es nun möglich, dass z.B. wie im vorliegenden Anwendungsfall die Stromaufnahme des Türmechanismus gemessen wird. Mit dem Einführen einer Zustandsüberwachung soll die Grundlage für eine (proaktive) zustandsbasierte Instandhaltungsstrategie geschaffen werden. Der Vorteil der Messung der Stromaufnahme ist ihre gute nachträgliche Modernisierbarkeit (*Retrofitting*) und das bei einer kostengünstigen Umsetzung. Außerdem gewinnt die Messung des Stromverbrauchs an Bedeutung, da Nachhaltigkeit in der Produktion zunehmend in den Fokus rückt. Als Nachteile werden das nötige ExpertenInnen- und Fachwissen für die Umsetzung und eine aufwendige Ergebnisanalyse genannt. Oft fehlt das Wissen über Grenzwerte, die gute oder schlechte Maschinenzustände charakterisieren, und es wird auch die geringe Vorwarnzeit als nachteilig angeführt.¹⁶⁹

5.1.2 Einblick in die Rohdaten

Für den Anwendungsfall stehen Messungen über mehrere Monate aus den Jahren 2019, 2020 und 2021 zur Verfügung – siehe Tabelle 26 bis Tabelle 28. Die Messdaten wurden, wie vorher erwähnt, an der nachgerüsteten Anlage an der Einlauftüre aufgenommen. *Count* gibt die Anzahl der enthaltenen Datenpunkte an, *Mean* den Mittelwert über alle Datenpunkte, *Std* die Standardabweichung des Datensatzes und zusätzlich werden noch die Maximalwerte angegeben (Minimum ist immer 0 A). Die Messungen von September, Oktober und November 2019 sind fehlerhaft, sodass diese nicht verwendet werden können. Es sind univariate Zeitreihen, welche den Stromverlauf (Einheit: Ampere, A) der Einlauftüre des Vorwärmofens

¹⁶⁸ Steck-Winter & Unger, 2020, S.40

¹⁶⁹ vgl. Pawallek, 2016, S.159

abbilden. Aus einer Vorarbeit¹⁷⁰ und zusätzlich verfügbarem ExpertInnenwissen ist das zu beobachtende Signal bereits wohl definiert. Die Daten können grundsätzlich als stationär betrachtet werden, weil sich der Arbeitspunkt der Türbewegung über die Zeit nicht ändert. Der Bewegungsablauf bleibt immer der gleiche und es treten eben nur Änderungen im Falle von Störungen/ Anomalien auf.

Tabelle 26: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2019

2019					
Monat	Count	Mean	Std	Max	Dateigröße
April	1484384	1.266 A	0.191 A	3.66 A	44.5 MB
September	Fehlerhaft				362.7 MB
Oktober	Fehlerhaft				1.65 GB
November	Fehlerhaft				1.63 GB
Dezember	6586382	1.266 A	0.190 A	3.65 A	197.6 MB

Tabelle 27: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2020

2020					
Monat	Count	Mean	Std	Max	Dateigröße
Jänner	8465334	1.208 A	0.199 A	3.68 A	254 MB
Februar	9154196	1.195 A	0.204 A	3.67 A	275.6 MB
März	5053925	1.270 A	0.194 A	3.68 A	151.6 MB
April	5216697	1.279 A	0.195 A	3.67 A	156.6 MB
Mai	8748228	1.205 A	0.203 A	3.69 A	262.7 MB
Juni	9180704	1.198 A	0.204 A	3.72 A	275.4 MB
Juli	9178236	1.194 A	0.202 A	3.66 A	275.3 MB
August	3228323	1.299 A	0.198 A	4.09 A	98.8 MB
September	9493147	1.189 A	0.208 A	3.68 A	284.8 MB
Oktober	343856	1.273 A	0.190 A	3.64 A	10.3 MB
November	8887468	1.203 A	0.203 A	3.69 A	266.6 MB
Dezember	4219177	1.277 A	0.191 A	3.66 A	126.6 MB

Tabelle 28: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2021

2021					
Monat	Count	Mean	Std	Max	Dateigröße
Jänner	7432381	1.244 A	0.195 A	3.70 A	223 MB
Februar	8021962	1.226 A	0.198 A	3.69 A	240.7 MB
März	5897222	1.273 A	0.193 A	3.72 A	176.9 MB

Abbildung 23 zeigt die Stromaufnahmemessung des gesamten Monats September 2020. Es bedarf aber einer Vergrößerung, sodass man den charakteristischen Stromverlauf erkennen. So ist in Abbildung 24 der normale Stromverlauf eines Zirkels mit Öffnungs- und Schließbewegung aus dem Monat April 2019 zusehen. In Abbildung 25 ist hingegen ein Verlauf mit seltenen Anomalien aus dem Monat April 2019 zu sehen, deren Ursprung bekannt ist: es wurden zu Testzwecken Gewichte an der bewegten Tür angebracht.

¹⁷⁰ vgl. Fürst, 2020, S.1f

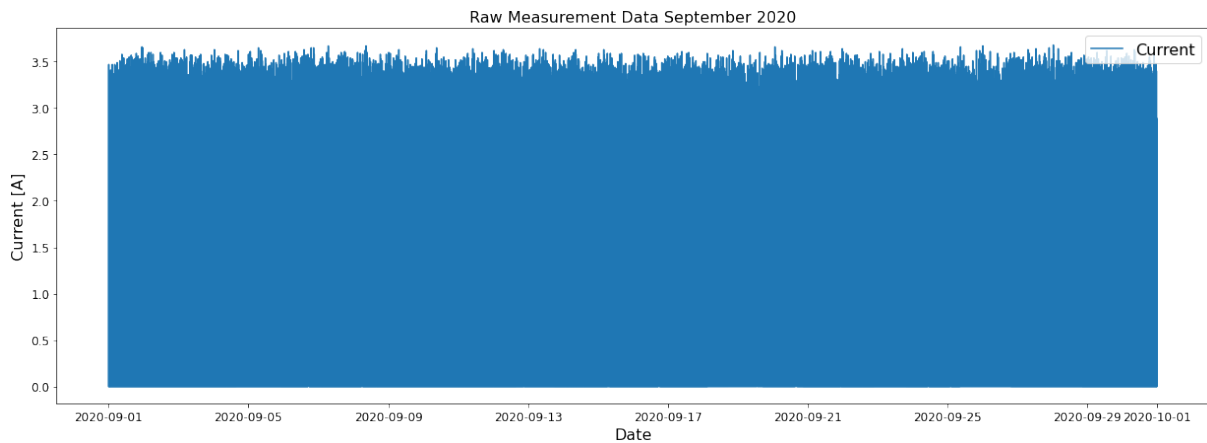


Abbildung 23: Darstellung eines gesamten Monats (September 2020)

Die für die später folgende Untersuchung entscheidende Phase ist nicht der Einschwingvorgang zu Beginn des Signals mit Spitzenwerten über 3 A, sondern das Plateau bei ca. 1.4 A (Öffnen) bzw. 1.2 A (Schließen). Daher kommt es auch zum Kappen der Signale – mehr dazu später.

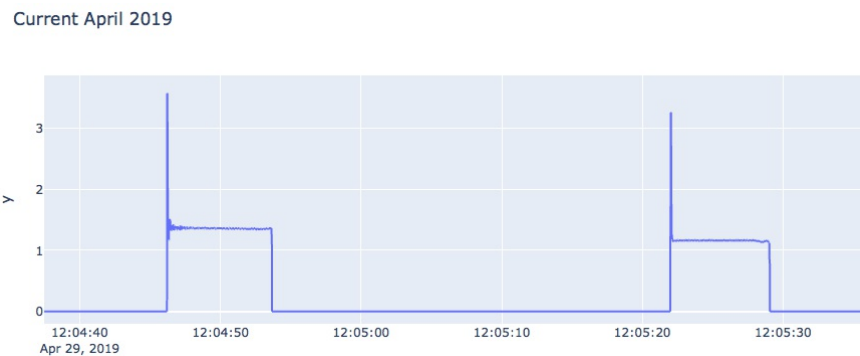


Abbildung 24: Stromstärkenverlauf (y-Achse) unter normalen Umständen



Abbildung 25: Stromstärkenverlauf (y-Achse) mit deutlich sichtbarem anomalem Verhalten beim Öffnen

Ferner wurde durch ExpertInnenwissen in Erfahrung gebracht, dass der Betrieb unter anderem in den Monaten Februar und März 2020 frei von Störungen gewesen ist. Daher können beispielsweise in dieser Zeitspanne Daten ohne Anomalien erwartet und sogenannte Normkurven/ Standardkurven berechnet werden, deren Kennzahlen in Tabelle 29 zusammengefasst sind.

Tabelle 29: Merkmale der Normkurven für Februar und März 2020 (beispielhaft)

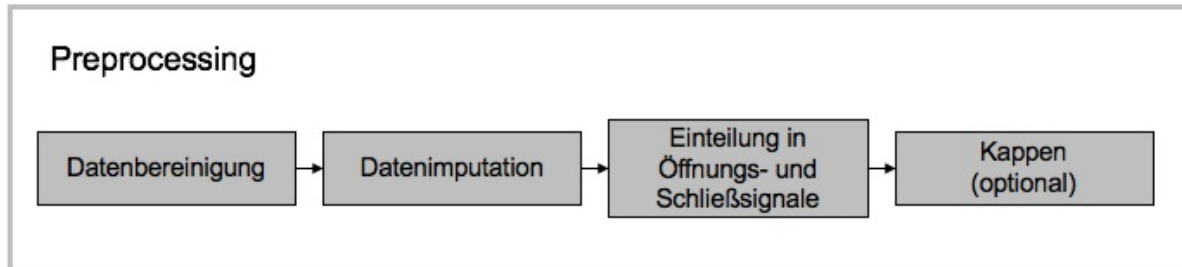
Februar 2020	
Dauer Öffnen	7.48 s
Dauer Schließen	7.06 s
Strom Öffnungssignal (1 s bis 7 s)	1.36 A (+/- 0.04 A)
Strom Schließsignal (1 s bis 6.9 s)	1.16 A (+/- 0.031 A)
März 2020	
Dauer Öffnen	7.48 s
Dauer Schließen	7.06 s
Strom Öffnungssignal (1 s bis 7 s)	1.37 A (+/- 0.039 A)
Strom Schließsignal (1 s bis 6.9 s)	1.16 A (+/- 0.032 A)

Außerdem ist bekannt, dass die Monate Juli und August 2020 Wartungsmonate sind. In dieser Zeit wird der Betrieb heruntergefahren, um Revisionsarbeiten an der Anlage durchzuführen. Im August kommt es somit auch vollständig zum Stillstand bzw. in der zweiten Monatshälfte zum Hochfahren und Konditionieren der Anlage. Ende Dezember bzw. Anfang Jänner (Feiertage und Jahreswechsel, 2019/ 2020 und 2020/ 2021) wird ebenfalls der Betrieb eingestellt, was dann wieder ein Hochfahren und Konditionieren im Monat Jänner nach sich zieht. Im Monat April 2020 ist ein Rückgang des Betriebes zu erkennen, da sich hier die COVID19 Krise auf die Produktion ausgewirkt hat. Somit stehen Daten aus jenen Monaten nicht im Fokus der Untersuchungen.

Die Stromaufnahme an der Einlaufftüre wurde mit eine Samplingrate von ca. 4 ms gemessen. Es besteht die Vorgabe, dass in der gleichen Granularität etwaige Anomalien detektiert werden sollen. Aufgrund der durch den Betreiber gewählten RCM Instandhaltungsstrategie kommt es nur äußerst selten zu anomalem Verhalten der Anlage, was in einer niedrigen Fehlerrate resultiert. Dadurch enthalten die Datensätze wenig bis gar keine Anomaliepunkte. Für die weitere Analyse stehen also zwei Datentypen zur Verfügung: Zeitstempel (*timestamp data*) und gepaart mit diskreten numerischen Strommesswerten. Beide unabhängigen Variablen (*predictor variables*) sind die Grundlage für die Berechnung von statistischen Merkmalen (*Features*), die als Input für die Anomaliedetektionsmethoden bzw. für die Operationen der Zeitreihentransformation dienen. Als Ausgabevariablen der Algorithmen (*target variables*) werden entweder binäre kategorische Variablen (Anomalie Ja/ Nein) ausgegeben oder kontinuierliche Anomaliefaktoren/ Anomalie Scores. In der tatsächlichen Ausführung werden kategorische Variablen binärisiert, also wird z.B. einer Anomalie die Ziffer -1 und einem normalen Wert die Ziffer 1 zugeordnet.

5.2 Verarbeitungs- und Analyseebene: Verarbeitung

5.2.1 Preprocessing und Informationsgewinnung



Durch das Unternehmen wird bereits ein bereinigter Datensatz zur Verfügung gestellt. Der bereinigte Datensatz wird nun in Öffnungs- und Schließsignale getrennt. Dies ist ein aufgrund der unterschiedlichen Charakteristiken (siehe Tabelle 29 auf S.83) wichtiger Schritt für die Anomalieerkennung, mit dem die Detektionsleistung verbessert wird. Die Öffnungs- und Schließsignale treten immer in der gleichen Sequenz auf: zuerst wird die Einlaufftüre geöffnet, danach geschlossen und diese Abfolge dauert ca. 45 s. Aufgrund der unterschiedlichen Merkmale (z.B. Mittelwert) können beim Clustering Öffnungs- und Schließsignale auch als klar trennbare Cluster wahrgenommen werden – siehe Abbildung 26.

Danach können die Signale optional am Anfang und Ende abgeschnitten werden. Durch das Kappen wird zu Beginn das Aufschwingen zum Spitzenwert über 3 A sowie das folgende kurze Einschwingen entfernt. Am Ende des Signals wird das Abfallen auf 0 A abgetrennt, sodass nach dem Kappen nur das Plateausignal erhalten bleibt. Diese Vorgehensweise wird für alle Ansätze angewendet mit Ausnahme des signalgruppenbasierten Ansatzes (siehe Kapitel 5.3.1.4 auf S.94), da ja hier als weiteres Feature das Flächenintegral des gesamten Signales errechnet wird. Das Beschneiden (*Truncating*, Kappen) des Stromsignals wird durchgeführt, da durch ExpertInnenwissen festgestellt wurde, dass die Aufschwing- und Abfallphasen nicht sachdienlich für die Anomaliedetektion sind. Werden jene Phasen nicht weggeschnitten, werden die dazugehörigen Datensamples hier fälschlicherweise immer als Anomalien erkannt.

In Abbildung 26 sind die zwei Cluster vom gekappten Öffnungs- bzw. Schließsignal zu sehen. Es werden Daten (ca. 265000 Dateninstanzen) einer Zeitspanne von ca. 10 Tagen im März 2020 mittels kMeans ($k=2$) geclustert. Der Algorithmus erhält als Input den fortschreitenden Mittelwert und die fortschreitende Standardabweichung (siehe Kapitel 4.3.3 auf S.64). Das grüne Cluster repräsentiert den Schließvorgang und das blaue den Öffnungsvorgang. Die zwei schwarzen Kreuze markieren die Zentren (Means) der Cluster.

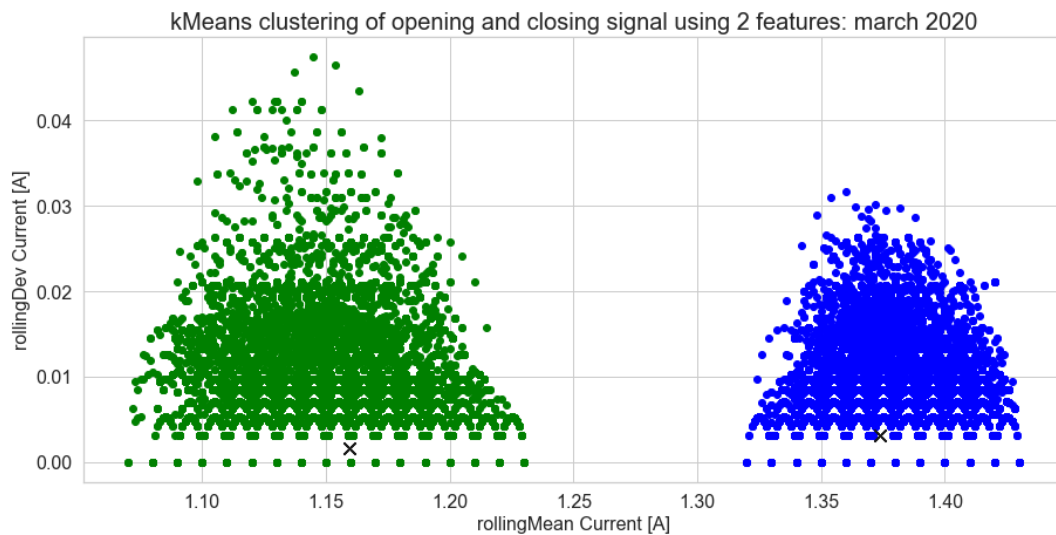


Abbildung 26: kMeans (inkl. Center) geclustertes Öffnungs- und Schließsignal März 2020

Je nachdem, welche Anomalieerkennungsalgorithmen im Anschluss verwendet werden, wird an dieser Stelle ein Datensplitting durchgeführt. Es findet nur bei der Novelty Detection ein Datensplitting statt, da hier zuerst das Modell auf die normalen (fehlerfreien) Daten trainiert werden muss. Daran anschließend folgt die Merkmalsextraktion gemäß Kapitel 4.3.3 auf S.64. Softwaretechnisch werden jene Features über die freie Python Software-Bibliothek *scipy* mittels Built-In Funktionen berechnet, mit Ausnahme des approximierten Integrals. Aufgrund der überschaubaren Anzahl an Features wird auf *Feature Ranking* bzw. *Feature Selection* verzichtet. Im Anschluss an die Feature Extraction wird die Normalisierung durchgeführt. Dazu wird, wie im theoretischen Teil erwähnt, der *MinMaxScaler* (eine Built-In Funktion des *sklearn*-Packages) verwendet. Bei den halbüberwachten Ansätzen wird der *Scaler* mit Trainingsdaten gefittet, dann abgespeichert und später auch auf die Testdaten angewendet.

Da im Analyseteil alle Kandidatenalgorithmen auf den Anwendungsfall angewandt und danach auch für das PoC bewertet werden, werden drei bestimmte Zeitspannen aus dem verfügbaren Daten (siehe Tabelle 30) untersucht:

Tabelle 30: Verwendete Daten (Öffnungssignale) für das PoC

Jahr	Monat	Zeitspanne	Zweck	Abkürzung
2019	April	29.04 09:30 – 14:30	Test	DS1
2020	September	07.09 (10:01) – 10.09	Training	DS2
2020	September	05.09 – 07.09 (10:00)	Test	DS3

Für die folgenden Ausführungen werden 6 Merkmale aus der Stromaufnahme mit einer Fensterlänge von $p=10$ extrahiert (siehe Tabelle 23) *rollingMean*, *rollingMedian*, *rollingDev* (standard deviation), *rollingVar*, *rollingSkew* und *rollingMax*. Abbildung 27 zeigt den verwendeten Dataframe (Ausgangsform, noch nicht normalisiert).

date	current	rollingMean	rollingMedian	rollingDev	rollingVar	rollingSkew	rollingMax
2020-09-05 00:11:45.602	1.34	1.356	1.34	2.065589e-02	4.266659e-04	0.408248	1.38
2020-09-05 00:11:45.607	1.34	1.352	1.34	1.932182e-02	3.733326e-04	0.872872	1.38
2020-09-05 00:11:45.611	1.38	1.352	1.34	1.932182e-02	3.733326e-04	0.872872	1.38
2020-09-05 00:11:45.616	1.38	1.352	1.34	1.932182e-02	3.733326e-04	0.872872	1.38
2020-09-05 00:11:45.620	1.38	1.352	1.34	1.932182e-02	3.733326e-04	0.872872	1.38
...

Abbildung 27: Anfang des zu analysierenden Dataframes mit 6 Merkmalen inklusive der ursprünglichen Messung der Stromstärke (*current*)

In den folgenden Abbildungen sind Zeitverläufe der Datensätze DS1, DS2 und DS3 aus Tabelle 30 ersichtlich. Hier sind das gekappte Stromsignal und zusätzliche zwei statistische Merkmale, *rollingMean* und *rollingDev* in einem Plot abgebildet. Bei einer rein visuellen Betrachtung der Zeitreihendarstellungen der drei verschiedenen Datensätze sind im DS2 keine bis nur sehr wenige Anomalien zu erwarten, da hier keine sichtbaren Unregelmäßigkeiten zu beobachten sind. In DS1 (am 29.04.2019 zwischen 11:30 und 13:00 Uhr) und DS3 (am 06.09.2020 um kurz von 18:00 Uhr) hingegen sollten die Algorithmen Anomalien identifizieren. Diese Betrachtungen sind die Grundlage für die Einschätzung der Performances der Algorithmen. Durch die fehlende Ground Truth kann hier nur abgeschätzt werden.

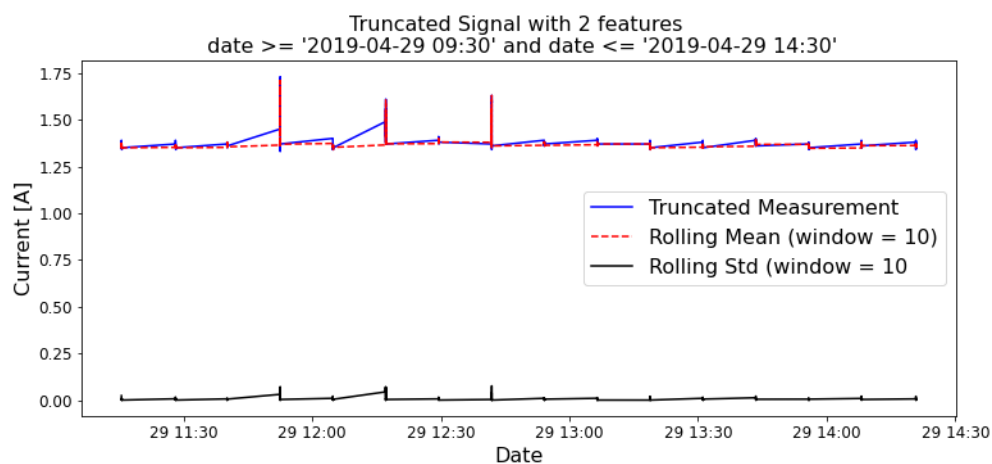


Abbildung 28: Gekapptes Signal mit 2 Features (DS1) mit drei auffälligen Ausschlägen

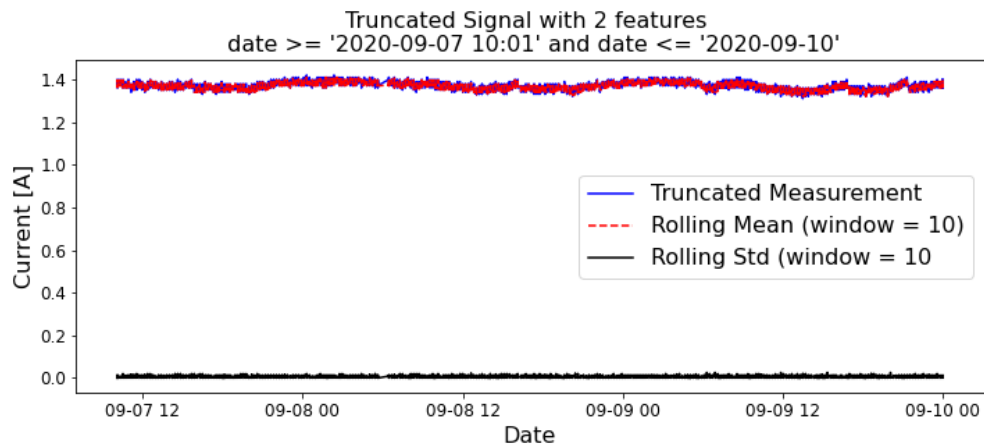


Abbildung 29: Gekapptes Signal mit 2 Features (DS2) ohne sichtbare Auffälligkeiten

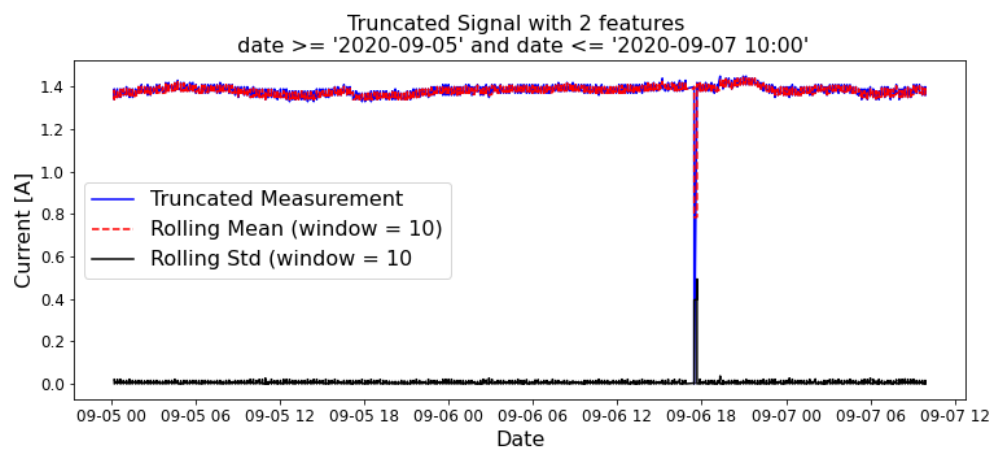


Abbildung 30: Gekapptes Signal mit 2 Features (DS3) mit einem auffälligen Stromabfall

Für das PoC des signalgruppenbasierten Ansatzes werden sowohl der gesamte Monat April 2019 (DS4), Mai und Juni 2020 kombiniert (DS5) als auch einmal September und Oktober 2020 kombiniert (DS6) untersucht. Unter anderem soll untersucht werden, ob Unterschiede in den Daten vor (DS5) und nach der Jahreswartung (DS6) bemerkbar sind. Durch die grobgranulare Analyse (statistische Merkmale nur für gesamte Signalgruppen und nicht einzelne Messpunkte) können größere Zeitspannen und somit größere Datenmengen effizient untersucht werden. Es werden hier sowohl Öffnungs- als auch Schließsignale untersucht.

5.3 Verarbeitungs- und Analyseebene: Analyse

Dieses Unterkapitel knüpft direkt an die Vorverarbeitung an und beschäftigt sich mit der tatsächlichen Anomalieerkennung in den zur Verfügung stehenden Daten.

5.3.1 Erstellung Datenmodell und Anomaliedetektion

Es sollen nun die Kandidatalgorithmen aus Kapitel 4.4.1 auf S.66 auf die vorbereiteten Datensätze angewandt werden. Dabei gibt es grundsätzlich vier verschiedene Herangehensweisen:

- Statistische Anomalieerkennung mit HBOS

- Unüberwachte Anomalieerkennung mit LOF, kNN, kMeans
- Novelty Detection (halbüberwachte Anomalieerkennung) mit LOF, OC-SVM, Autoencoder und iForest
- Signalgruppenbasierter Ansatz mit dem iForest

Nach jedem Unterkapitel werden die verwendeten Methoden anhand der **geforderten Eigenschaften bewertet**: es muss ein Anomalie Score ausgegeben werden, woraus auch ein Grenzwert eindeutig bestimmbar sein muss. Für einen algorithmusinternen Anomalie Score erhält der Ansatz volle 10 Punkte, bei einer gesonderten Berechnung nur 5 Punkte. Die Berechnungen bei der Anomaliedetektion müssen effizient durchgeführt werden und zusätzlich wird auch bewertet, ob zu viele oder zu wenige Anomalien detektiert werden. Diese Anforderung kann nur im Vergleich mit den anderen Algorithmen und durch Betrachtung der Zeitreihendarstellungen beurteilt werden, da ja keine Ground Truth zur Verfügung steht. Daraus ergibt sich in Folge eine Gesamtwertung für den jeweiligen Algorithmus. Tabelle 42 im Anhang dokumentiert die softwaretechnische Umsetzung für alle Ansätze.

5.3.1.1 Statistische Anomalieerkennung mit HBOS

Mit dem HBOS-Algorithmus wird ein sehr effizienter aber teilweise unpräziser Ansatz implementiert. Da es sich um einen (unüberwachten) statistischen Ansatz handelt, ist hier kein Aufteilen in Trainings- und Testdaten notwendig. Die untersuchten Datensätze werden wie bei den anderen Ansätzen durch 6 Merkmale/ Dimensionen repräsentiert analysiert. Aufgrund der Tatsache, dass dieser Algorithmus abstandsunabhängig ist, wird bei diesem Ansatz keine Normalisierung durchgeführt. Die Kontamination der Datensätze mit Anomalien wird auf 0.005 geschätzt, weil eben anomales Verhalten äußerst selten vorliegt. Hier wird der Kontaminationsparameter als einzige Stellgröße vorgegeben, was das Tuning des Algorithmus sehr vereinfacht. Die Detektionsleistung (wieviele Punkte werden als anomal identifiziert) ist aber direkt von diesem Parameter abhängig. Das wird ersichtlich, wenn die Anzahl der anomalen Punkte durch die der normalen Punkte dividiert wird. Es ergibt sich wieder die geschätzte Kontamination. Diese Vorgehensweise ist sowohl für die Diagnose der Öffnungs- als auch Schließsignale gleich. Darstellungen über den zeitlichen Verlauf der Detektion sind aus Gründen der Lesbarkeit im Anhang (Kapitel 7.2.1 auf S.114) ersichtlich.

In Tabelle 31 ist zu sehen, in welchen Datensätzen der HBOS-Algorithmus wie viele Anomalien detektiert hat. Wie erwartet, arbeitet der Algorithmus im Vergleich zu den anderen Methoden sehr effizient. Die Detektionsleistung des HBOS-Algorithmus' stellt sich aber als ungenau dar. In Tabelle 32 ist die Gesamtbewertung des HBOS-Algorithmus' zusammengefasst.

Tabelle 31: Detektierte Anomalien in den Datensätzen (DSx) mit HBOS

Datensatz	Normale Punkte	Anomale Punkte
DS1	10630	54
DS2	345262	1725
DS3	317014	1507

Bei Betrachtung der Zeitreihendarstellungen mit markierten Anomalien in Kapitel 7.2.1 auf S.114 wird die ungenaue Detektionsleistung des HBOS-Algorithmus' sichtbar. Im DS1 erkennt der Algorithmus (mit dem gewählten Parameter) zu wenige Anomalien – siehe in der vergrößerten Darstellung in Abbildung 31. Im DS2 können viele Falschklassifikationen

festgestellt werden. Dieser Umstand ist aber der Arbeitsweise des Algorithmus' geschuldet, der eben eine gewisse Anzahl (durch die Kontamination vorgegeben) als anomal detektiert (detektieren muss). Im DS3 liegt eine annehmbare Detektionsleistung vor. In diesem Fall und im Falle des DS2 wird der Falschalarmfilter schlagend werden (Kapitel 4.4.3 auf S.76).

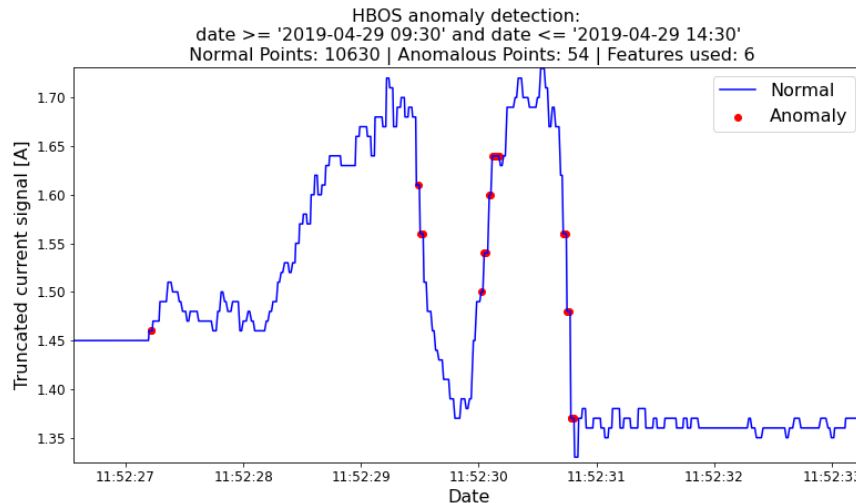


Abbildung 31: Zoom in ein einzelnes Öffnungssignal (DS1)

Tabelle 32: Zusammenfassende Bewertung der Leistung des statistischen Ansatzes (Anforderungen sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0)

Algorithmus	Anomalie Score	Effizienz	Grenzwertbestimmung	Anomalie-detektion	Gesamtwertung
HBOS	10	10	10	5	35

5.3.1.2 Unüberwachte Anomalieerkennung

Wie auch im vorher erläuterten Ansatz ist hier kein Datensplitting notwendig, da beim unüberwachten Lernen kein Training stattfindet – der Algorithmus wird also auch hier unvoreingenommen auf den vorbereiteten Datensatz losgelassen. Für das PoC werden Datenausschnitte der Öffnungssignale aus den Monaten April 2019 und September 2020 betrachtet. Anhand dieser Datensätze kann das nun dargelegte Softwarekonzept, bei dem durch eine nötige manuelle Grenzwertbestimmung bei kNN und kMeans mehr manuelles Zutun wie beim HBOS Ansatz gefordert ist, erläutert werden. Am Ende dieses Unterkapitels ist in Tabelle 33 zu sehen, welcher Algorithmus wie viele normale und anomale Datenpunkte identifiziert hat. Darstellungen über den zeitlichen Verlauf der Detektion sind aus Gründen der Lesbarkeit im Anhang (Kapitel 7.2.2 auf S.116) ersichtlich.

Für den **LOF-Algorithmus** wird wie beim HBOS-Algorithmus eine Kontamination von 0.005 als Parameter vorgegeben (siehe Kapitel 4.4.1.2 auf S.67). Die Wahl einer so niedrigen Kontamination beruht eben auf der Tatsache, dass von nur wenigen anomalen Datenpunkten ausgegangen werden kann. Wie erwartet ergeben sich bei größeren Datenmengen lange Rechenzeiten bei diesem Algorithmus. Besonders auffällig ist auch, dass dieser Algorithmus im April Datensatz (DS1) um ein vielfaches weniger anomale Datenpunkte identifiziert als alle anderen zwei angewandten Modelle (siehe Tabelle 33) und dies aber bei klar ersichtlichen Ausschlägen des gekappten Signals. Einen großen Vorteil dieses Ansatzes stellt das interne Berechnen eines Grenzwertes (*Threshold*) dar. Dieser interne Grenzwert ändert sich zwar für

jeden Datensatz, es ist aber keine statistische Berechnung (bzw. kein manuelles Bestimmen durch den Knowledge Engineer) notwendig.

Bei diesem PoC und der gewählten Kontamination kann der LOF-Algorithmus keine akzeptable Detektionsleistung aufweisen. Im DS1 erkennt er bei den offensichtlichen Ausschlägen nur eine sehr geringe Anzahl an Anomalien in den Daten. Dazu kommen noch Falschklassifikationen im Normalbereich (direkt nach der ersten auffälligen Erhebung). Im DS2 kommt es wie bei allen anderen Algorithmen auch zu vielen Falschklassifikationen. Im DS3 wird nicht einmal der Stromabfall als anomal erkannt.

Der **kNN-Algorithmus** wird mit $k=5$ initialisiert und danach wird das Modell zu den untersuchten Daten gefittet. Die Entscheidung, ob ein vorliegender Punkt eine Anomalie ist oder nicht, wird über ein Abstandsmaß gefällt: der Algorithmus berechnet für jeden Messpunkt (einzelne Reihe in Dataframe in Abbildung 27), der eben durch 6 Merkmale in einem 6-dimensionalen Raum repräsentiert ist, die Abstände zu seinen nächsten 5 ($k=5$) Nachbarpunkten, die auch im 6-dimensionalen Raum abgebildet sind. Folglich erhält man pro Messpunkt 5 Abstandswerte, von denen ein Durchschnittswert berechnet wird. Ist dieser Durchschnittswert im Vergleich zu den anderen anomal hoch, kann der betrachtete Punkt sodann als Anomalie identifiziert werden. Der Grenzwert (siehe Tabelle 33) für die Entscheidung, ob eine Anomalie vorliegt oder nicht, wird nicht wie z.B. beim LOF-Algorithmus automatisiert *algorithmusintern* errechnet, sondern muss über einen statistischen Grenzwert (3-Sigma-Regel bzw. manuell durch den Knowledge Engineer) festgelegt werden. Es muss also ein brauchbarer Grenzwert (*Cut off value*) bestimmt werden, sodass auf der einen Seite nicht jeder kleine Ausschlag als Anomalie gewertet wird und auf deren Seite keine echte Anomalie unentdeckt bleibt. Die Methodik für die 3-Sigma-Regel ist in Kapitel 4.4.2.1 auf S.74 dargelegt.

Der kNN-Algorithmus erkennt die meisten Unregelmäßigkeiten im DS1. Hier scheint ein geeigneter Grenzwert verwendet zu werden. Beim DS2 allerdings kommt es auch hier zu Falschklassifikationen – um nur ca. 300 weniger als beim LOF. Im DS3 liegt eine akzeptable Anomalieerkennung vor. Die noch bestehenden Falschklassifikationen filtert der Falschalarmfilter, da der Anomalie Score zu diesen Zeitpunkten den Grenzwert nicht gravierend überschreitet.

Der **Clustering-Algorithmus kMeans** wird mit $k=1$ initialisiert, da von einem Cluster mit nur einem Mittelpunkt (*Mean*) ausgegangen wird. Jener Mittelpunkt repräsentiert den Clusterschwerpunkt der Messdaten der normalen Stromaufnahme der Einlaufftüre. Nun werden in den 6 Dimensionen (Merkmalen) die Abstände hin zu diesem Schwerpunkt berechnet und danach wieder ein Mittelwert über alle 6 Abstandswerte gebildet. Das weitere Vorgehen ist jenen aus den Ausführungen zum kNN-Algorithmus gleich, denn auch hier muss der Grenzwert für den Anomalie Score statistisch über die 3-Sigma-Regel (bzw. über den Knowledge Engineer) festgelegt werden. Der kMeans-Algorithmus ist der schnellste unter den drei betrachteten unüberwachten Ansätzen.

Im DS1 werden mit diesem Algorithmus um 108 mehr Anomalien erkannt als beim kNN, somit arbeitet der Algorithmus hier auch besser als der LOF. Im DS2 kommt es zu deutlich weniger Falschklassifikationen als wie bei kNN und LOF. Auffällig ist hingegen die hohe Anzahl an

identifizierten Anomalien im DS3. Im Allgemeinen aber liegt eine akzeptable Detektionsleistung vor.

Tabelle 33: Detektierte Anomalien in den Datensätzen (DSx) mit LOF, kNN und kMeans mit den dazugehörigen Grenzwerten

Algorithmus	Datensatz	Grenzwert	Normale Punkte	Anomale Punkte
LOF (cont. = 0.005)	DS1	intern	10630	54
	DS2	intern	345255	1732
	DS3	intern	316928	1593
kNN (k=5)	DS1	0.059	10404	280
	DS2	0.008	345570	1417
	DS3	0.007	318004	517
kMeans (k=1)	DS1	0.288	10296	388
	DS2	0.256	346177	810
	DS3	0.14	316232	2289

Es ergibt sich für jene drei Algorithmen folgende Bewertung, siehe Tabelle 34, nach den eingangs erwähnten Entscheidungskriterien. Mit Blick auf die Effizienz, die für eine zukünftige Online-Implementierung von Relevanz sein wird, kann der LOF-Algorithmus ebenfalls nicht überzeugen.

Tabelle 34: Zusammenfassende Bewertung der Leistung der unüberwachten Algorithmen (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0)

Algorithmus	Anomalie Score	Effizienz	Grenzwertbestimmung	Anomalie-detektion	Gesamtwertung
LOF	10	0	10	0	20
kNN	5	10	5	5	25
kMeans	5	10	5	5	25

5.3.1.3 Novelty Detection

Der grundlegende Unterschied bei diesem Ansatz ist, dass der Anomalieerkennung in den Daten ein Training des Modells vorausgeht. Die jeweiligen Modelle (LOF, Autoencoder, OC-SVM und iForest) werden nur mit Daten trainiert, bei denen durch ExpertInnenwissen bekannt ist, dass in diesem Zeitraum der Betrieb der Einlauffüre der Ofenanlage (nahezu) fehlerfrei gelaufen ist. Für das PoC wird dazu der Datensatz DS2 verwendet, der aus 346987 Dateninstanzen besteht. Im Allgemeinen ist der Vorteil dieses Ansatzes, dass mit dem Training durch den Knowlegde Engineer sehr genau gesteuertes richtiges Verhalten eintrainiert werden kann. Jeder Testdatensatz (oder neue ungesehene Datensatz) wird somit immer im Vergleich zum gesunden Trainingsdatensatz bewertet - nicht wie bei den unüberwachten Ansätzen, wo jeder Datensatz geschlossen für sich analysiert wird. Der halbüberwachte Ansatz bietet auch die Möglichkeit, dass die Modelle ständig mit neuen Trainingsdaten verbessert und adaptiert werden können, sodass sich infolgedessen die Detektionsgenauigkeit erhöht. Darstellungen über den zeitlichen Verlauf der Detektion sind aus Gründen der Lesbarkeit im Anhang (Kapitel 7.2.3 auf S.119) ersichtlich.

Dem **LOF-Algorithmus**, diesmal in Verwendung für die Novelty Detection, wird ebenfalls wie beim unüberwachten Ansatz eine Kontamination von 0.005 als einzigen Parameter vorgegeben. Es sei erwähnt, dass die Anomalieentscheidung auch hier algorithmusintern getroffen wird. Beim semiüberwachten Ansatz fällt die im Vergleich zu den anderen semiüberwachten Algorithmen lange Rechenzeit auf. Obwohl der Algorithmus mit DS2

eintrainiert ist, detektiert der Algorithmus auffällig mehr Anomalien besonders in den Datensätzen DS2 und DS3, ähnlich wie der OC-SVM wie später zu sehen ist. Im DS1 detektiert der LOF-Algorithmus ebenfalls sehr ungenau – siehe Abbildung 33. Grundsätzlich ist hier keine adäquate Detektionsleistung festzustellen. Hier schneidet sogar der unüberwachte Ansatz des LOF-Algorithmus besser ab.

Beim **Autoencoder** sei zu Beginn eine Besonderheit erwähnt: der Datensatz für das Einlernen (DS2) wird einem weiteren Splitting unterzogen, da für das Training des mehrschichtigen neuronalen Netzes auch ein Validierungsdatensatz gebraucht wird. So werden 277596 Samples für das Training und 69400 Samples für die Validierung beim Netzwerktraining verwendet. Durch das Trainieren und Validieren kann das Netz optimale Gewichte für die Neuronen und deren Übertragungsfunktionen finden (wie in Kapitel 4.4.1.5 auf S.69 beschrieben). Es wird folgende Netzwerkarchitektur gewählt: Eingangs- und Ausgangsschicht haben jeweils 6 Neuronen ($n=6$), weil dem Modell 6 Features zur Verfügung stehen. Für die Dimension der verborgenen Schichten m muss $m < n$ gelten, denn so ist der Autoencoder gezwungen nur die wichtigsten Informationen aus dem Datensatz zu extrahieren und zu erlernen. An der engsten Stelle (*Bottleneck*) des mehrschichtigen verborgenen Layers wird $m=2$ gewählt, weil nur zwei Gruppen (normal und anomal) identifiziert werden sollen.¹⁷¹ Abbildung 32 zeigt die vollständige Netzwerkstruktur, bei dem die für Autoencoder typische Sanduhrform mit dem Bottleneck in der Mitte in orange erkennbar ist. Am Ende des Trainings wird ein Validierungsfehler (*Validation loss*) von 0.11 % erreicht, was ein brauchbares Ergebnis darstellt.

Mit dem eingelernten Modell wird nun der Rekonstruktionsfehler zwischen Trainingsdaten und Autoencoder Output (Modelloutput) in Form des MSE gemessen. Mit diesem Fehlermaß wird im Anschluss der Grenzwert (Cut-off Value) für die Anomaliendetektion berechnet, wie es im vorigen Unterkapitel auch für kNN und kMeans gemacht wird. Es ergibt sich ein Grenzwert von 0.012 für die die Anomalieentscheidung. Danach wird das eingelernte Modell abgespeichert und für die weitere Anwendung in der Novelty Detection bereitgestellt.

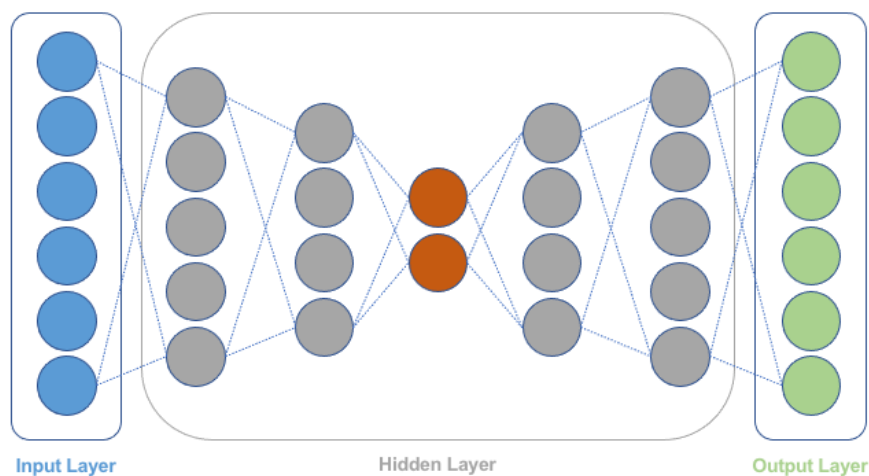


Abbildung 32: Netzwerkstruktur Autoencoder für PoC (Verbindungslinien nur angedeutet)¹⁷²

¹⁷¹ vgl. H. Wang, 2020a, S.3

¹⁷² Eigene Darstellung

Der Autoencoder schneidet von den semiüberwachten Algorithmen am zweitbesten ab. Im DS1 liegt eine adäquate Detektionsleistung vor, obwohl es zu einigen Falschklassifikationen kommt. So auch in den Datensätzen DS2 und DS3. Hier kann aber ein Falschalarmfilter Abhilfe schaffen. Das Lernen dieses mehrschichtigen neuronalen Netzes (*Deep Learning*) ist zwar sehr rechen- und dadurch zeitintensiv, in der Anwendung aber übertrifft der Autoencoder LOF und OC-SVM.

Dem **OC-SVM Algorithmus** wird ein $\text{Nu}=0.01$ als einziger Parameter vorgegeben. Alle anderen Parameter werden, wie auch bei den anderen Algorithmen, in den Default-Einstellungen belassen. Auffällig sind bei diesem Algorithmus die langen Rechenzeiten, sowohl im Training als auch im Testzenario in der Modellanwendung. Bei der Auswertung der erkannten Anomalien in den drei Datensätzen ist nur das Ergebnis beim DS1 brauchbar. In DS2 und DS3 kommt es zu übermäßig vielen Falschklassifikationen, ähnlich wie beim LOF-Algorithmus.

Die vierte angewandte Methode ist der **Isolation Forest Algorithmus**, welcher mit einer Kontamination von 0.005 eintrainiert wird. Dieser Algorithmus erreicht bei der Bewertung in Tabelle 36 als einziger Kandidat volle Punktezahl. Neben einem Anomalie Score und einer algorithmusinternen Grenzwertbestimmung arbeitet der Isolation Forest sowohl im Training und in der Testphase äußerst effizient. Ferner ist er im Vergleich zum Autoencoder sehr leicht initialisiert und angewandt, da nur wenige Parameter (in diesem Anwendungsfall nur einer) vorgegeben werden müssen. In allen drei Datensätzen liegt eine annehmbare Detektionsleistung vor.

Tabelle 35: Detektierte Anomalien in den Datensätzen (DSx) mittels Novelty Detection mit LOF, Autoencoder, OC-SVM und Isolation Forest

Algorithmus	Datensatz	Grenzwert	Normale Punkte	Anomale Punkte
LOF (cont. = 0.005)	DS1	intern	8376	2308
	DS2	intern	297885	49102
	DS3	intern	290607	27914
Autoencoder	DS1	0.012	9713	971
	DS2	0.012	340357	6630
	DS3	0.012	311088	7433
OC-SVM (nu = 0.01)	DS1	intern	9661	1023
	DS2	intern	309281	37706
	DS3	intern	269610	48911
Isolation Forest (cont. = 0.005)	DS1	intern	10107	577
	DS2	intern	345347	1640
	DS3	intern	316339	2182

Tabelle 36: Zusammenfassende Bewertung der Leistung der halbüberwachten Algorithmen (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0)

Algorithmus	Anomalie Score	Effizienz	Grenzwertbestimmung	Anomalie-detektion	Gesamtwertung
LOF	10	0	10	0	20
Autoencoder	5	10	5	5	25
OC-SVM	10	0	10	0	20
iForest	10	10	10	10	40

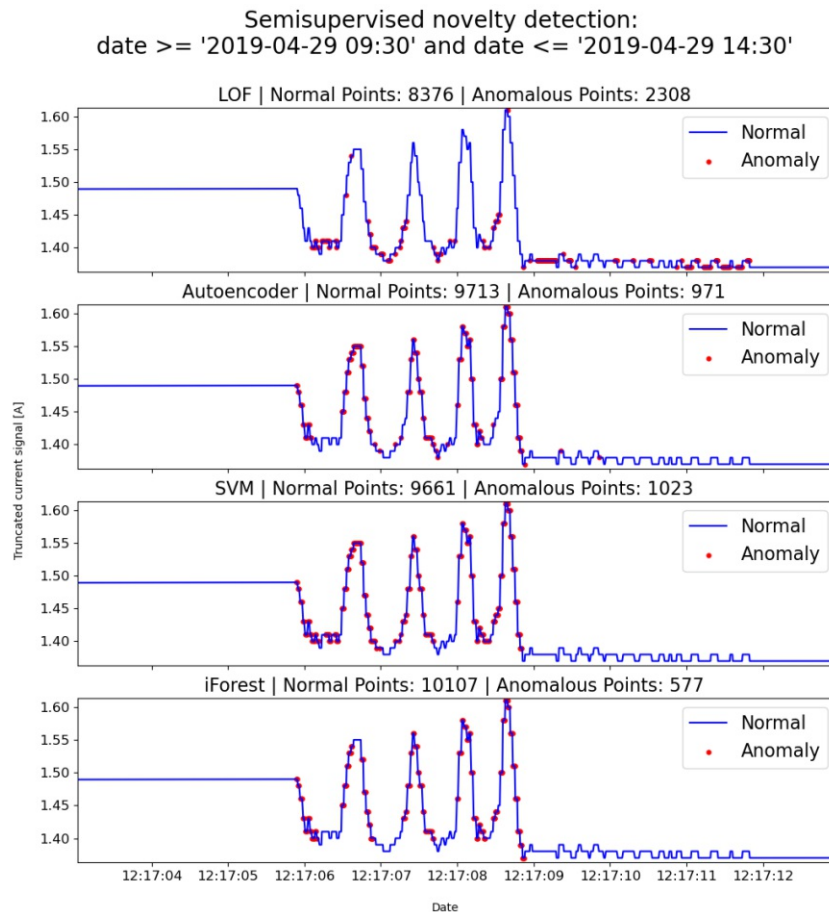


Abbildung 33: Zoom in ein einzelnes Öffnungssignal (DS1)

Wie im Theorieteil des Phasenmodells bereits angekündigt, wird speziell für diesen Anwendungsfall ein eigener Ansatz entwickelt. Zuerst wird der Ansatz erklärt und danach wird dieser auch als Analysealgorithmus angewandt. Im Anschluss an die Analyse wird der signalgruppenbasierte Ansatz nach den gleichen Kriterien wie die vorigen Algorithmen bewertet. Es sei erwähnt, dass sich bei der Anwendung das Datenpreprocessing sowie Postprocessing geringfügig zu den anderen Ansätzen unterscheidet. Der Übersichtlichkeit halber werden jene Ausführungen in einem Unterkapitel zusammengefasst.

5.3.1.4 Signalgruppenbasierter Ansatz mit iForest

Über statistische Merkmale wie Skewness, Mean, Kurtosis etc. werden die Zeitreihen der einzelnen Signalgruppen des Öffnungs- und Schließvorganges beschrieben und im Anschluss wird mittels Isolation Forest versucht, anomale Signalgruppen zu detektieren. Eine Signalgruppe ist entweder ein Öffnungs- oder Schließvorgang (wie in Abbildung 24 und Abbildung 25 dargestellt). Es wird also hier nicht festgestellt, ob einzelne Datensamples anomal sind oder nicht, sondern, ob sich ein gesamter Öffnungs- oder Schließvorgang anomal verhalten hat. Das ergibt eine grobgranulare Anomaliedetektion. Eine gesamte Zeitreihe/Signalgruppe bestehend aus z.B. 1500 Datensamples ($\vec{T}_1 = [T_{1,1}, T_{1,2}, \dots, T_{1,1500}]$) wird durch mehrere statistische Merkmale (siehe Tabelle 23) komprimiert dargestellt und definiert, sodass sich daraus ein Merkmalsvektor für diese Zeitreihe ergibt ($\vec{M}_1 = [M_{1,1}, M_{2,1}, \dots, M_{X,1}]$). Somit wird die gesamte Zeitreihe einer Transformation in der Darstellung unterzogen – siehe Tabelle 37 und Tabelle 38.

Tabelle 37: Ausgangsdarstellung aller Öffnungssignale des Datensatzes mit der Einteilung in Signal Label, Signal ID, Zeitstempel und gemessener Stromstärke

Signal Label	Signal ID	Zeitstempel	Stromstärke
Öffnen	1.0	T1.1	0.0
		T1.2	2.5
	
Öffnen	133.0	T133.1	0.0
		T133.2	2.6
		T133.3	2.7
	

Tabelle 38: Transformierte Darstellung, in der jeder Signal ID nun X statistische Merkmale zugeordnet sind

Signal ID	Merkmal 1	Merkmal 2	...	Merkmal X
1.0	M1.1	M2.1	...	MX.1
3.0	M1.3	M2.3	...	MX.3
5.0	M1.5	M2.5	...	MX.5
...
133.0	M1.133	M2.133	...	MX.133
...

Dieser Ansatz hat das Potenzial auch als eine Art Filter (in der Online Anwendung) für eine Vorauswahl von interessanten bzw. verdächtigen Signalgruppen verwendet zu werden, sodass die Datenmenge für die feingranulare Anomalieerkennung reduziert werden kann – so wie das Hofmockerl (2019) bei Selektion wertvoller Daten für die Datenübertrag aus PKW zum Backend zur Anwendung gebracht hat. Der Ansatz kann auch für eine effiziente Fehleranalyse von großen Zeiträumen angewendet werden.

Ein Öffnungs- oder Schließsignal aus den betrachteten Datensätzen besteht aus ca. 1400-1600 Messpunkten (*Samples*). Außerdem sei erwähnt, dass in diesem Fall die Messsignale nicht gekappt und die statistischen Merkmale nicht mit dem Sliding Window Ansatz berechnet werden. Es werden für diesen Ansatz auch mehr Merkmale berechnet, da hier eine erweiterte Dimensionalität hinsichtlich Effizienz verkräftbar ist. Durch das Datenpreprocessing wird jedem Öffnungs- und Schließsignal eine *Signal ID* innerhalb des untersuchten Datensatzes zugeordnet. Abbildung 34 zeigt einen Ausschnitt eines Dataframes mit den Signal IDs als Index und den verschiedenen Merkmalen, die gemäß Tabelle 23 berechnet werden. Abbildung 35 und Abbildung 36 stellen die Merkmale aufgetragen über die einzelnen Signal IDs dar.

signal_id	Skewness	Kurtosis	Max	Mean	Median	Std	Var	RMS	p10	p25	p50	p75	p90	IQR	Entropy	Approx_Int
2.0	5.564135	91.116627	3.01	1.380231	1.37	0.144724	0.020945	1.387792	1.36	1.37	1.37	1.38	1.39	0.01	7.290322	8.137840
4.0	-0.970341	108.125607	2.89	1.377960	1.38	0.118274	0.013989	1.383023	1.37	1.38	1.38	1.38	1.39	0.00	7.282212	8.052801
6.0	7.572668	104.235851	3.24	1.388935	1.38	0.152592	0.023284	1.397285	1.37	1.37	1.38	1.38	1.39	0.01	7.168399	7.250240
8.0	7.357296	111.777380	3.33	1.381867	1.38	0.161658	0.026133	1.391284	1.37	1.37	1.38	1.38	1.39	0.01	7.244325	7.788200
10.0	7.691149	127.167666	3.29	1.389105	1.39	0.148416	0.022027	1.397006	1.38	1.38	1.39	1.39	1.40	0.01	7.370563	8.873600
...

Abbildung 34: Dataframe für den signalgruppenbasierten Ansatz (hier nur Öffnungssignale)

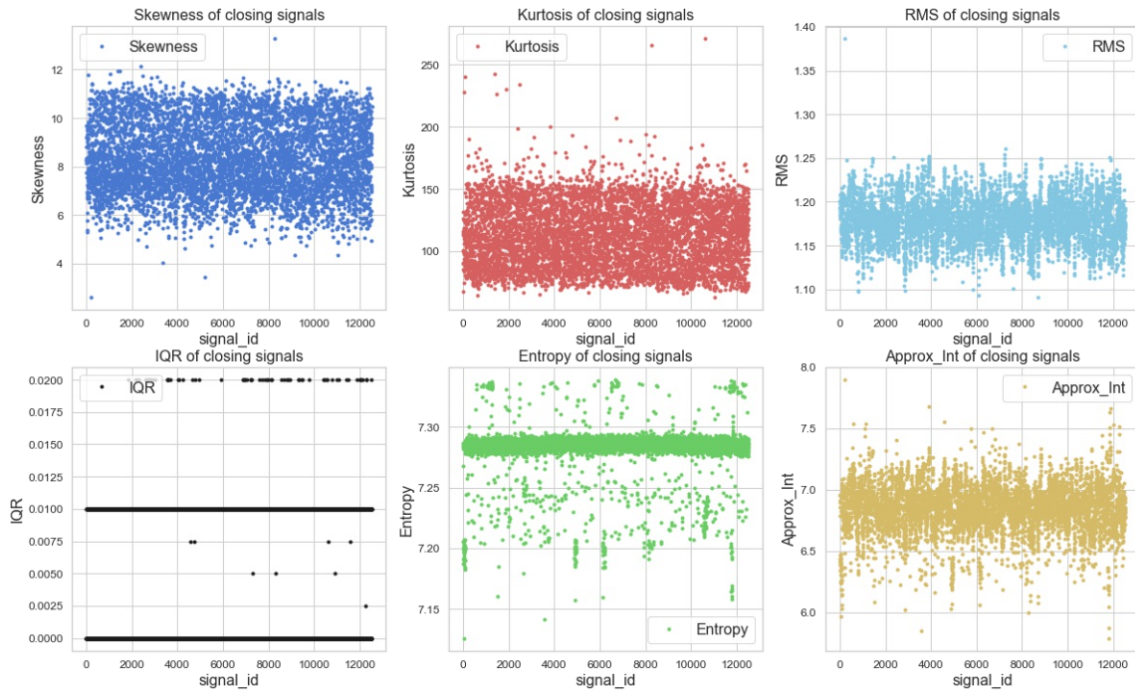


Abbildung 35: Darstellung der statistischen Merkmale über die Signal ID (Schließsignale DS5)

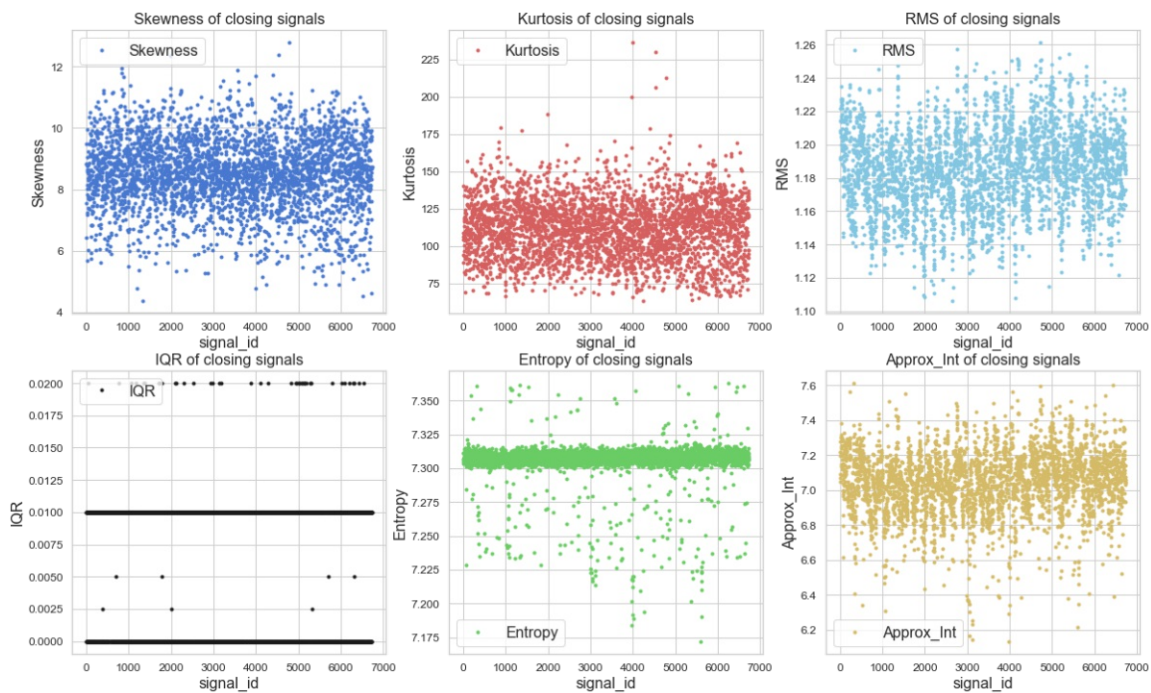


Abbildung 36: Darstellung der statistischen Merkmale über die Signal ID (Schließsignale DS6)

Der erstellte Dataframe mit offensichtlichen skalenmäßigen Unterschieden in den Merkmalen (siehe z.B.: zwischen Kurtosis und Skewness) muss vor der Anomaliedetektion noch mit dem MinMaxScaler normalisiert werden. Danach kann der normalisierte Dataframe dem iForest, hier als unüberwachter Algorithmus verwendet, übergeben werden. Dem iForest wird wieder eine Kontamination von 0.005 vorgegeben. Durch die unüberwachte Anomaliedetektion mit dem iForest Algorithmus werden anomale Signal IDs identifiziert. Die Anzahl der Detektionen hängt auch hier stark vom Kontaminationsparameter ab.

Die folgende Tabelle 39 gibt eine Übersicht über die Anzahl der detektierten anomalen Signale in den untersuchten Datensätzen. Es ist auch aufgeschlüsselt, ob es sich um Öffnungs- oder Schließsignale handelt.

Tabelle 39: Detektierte anomale Signal IDs in den Datensätzen (DSx) mittel iForest

Datensatz mit iForest (cont. = 0.005) analysiert	Öffnungssignale		Schließsignale	
	Normal	Anomal	Normal	Anomal
DS4	783	2	760	3
DS5	6254	13	6244	14
DS6	3360	8	3359	7

Tabelle 40: Zusammenfassende Bewertung der Leistung des signalgruppenbasierten Ansatzes mit iForest (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0)

Algorithmus	Anomalie Score	Effizienz	Grenzwertbestimmung	Anomalie-detektion	Gesamtwertung
Signalgruppenbasiert + iForest	10	10	10	0	30

In Tabelle 40 wird die Bewertung des Ansatzes zusammengefasst. Die Detektionsleistung dieses Ansatzes kann erst nach einer eingehenden Diagnose durch den Domain Expert (und Knowledge Engineer) beurteilt werden und zwar in jenen Schritten, die im Phasenmodell der Evaluierung bzw. der Ergebnisvisualisierung zugeordnet sind. Diese beiden Schritte ermöglichen es zum einen, eine genauere Untersuchung mittels einer Abfrage-Funktion (*query*) durchzuführen, bei der der Anomalie ein zeitlicher Kontext zugeordnet wird. Zum anderen kann mittels eines visuellen Vergleiches des als anomal identifizierten Signals mit einem normalen Referenzsignal die Form der Abweichung bestimmt werden – siehe Abbildung 39.

Die gesammelten Daten wurden nun bereits bereinigt, für die Modellierung aufbereitet und mit einem ausgewählten Algorithmus modelliert. Im nächsten Unterkapitel wird darauf eingegangen, wie die erlangten Informationen (Anomalie ja/ nein und Anomalie Score) bereitgestellt durch die angewandten Algorithmen und Ansätze weiterverarbeitet und für das CM genutzt werden können. Dieses Postprocessing ist die Grundlage für die darauffolgende Ergebnisvisualisierung.

5.3.2 Anomalie Scores und Alarmlogik mit Falschalarmfilter

Für die Bewertung der Algorithmen im vorigen Kapitel wurden bereits die Anomalieentscheidungen getroffen. Dies geschah algorithmusspezifisch entweder algorithmusintern oder über die Berechnung eines Grenzwertes mittels der 3-Sigma-Regel. Das heißt wiederum, dass unter anderem auch der Anomalie Score (für jeden Algorithmus eigene Werte) zur Weiterverwendung zur Verfügung steht. Jeder Algorithmus gibt den Anomalie Score in seiner eigenen Skala aus. So liefert der Isolation Forest z.B. Scores zwischen 1 und -1, der kNN hingegen nur positive Werte zwischen 0 und (theoretisch) unendlich.

Mit jenen Anomaliefaktoren werden nun die als anomal detektierten Dateninstanzen gemäß Tabelle 25 in Kritikalitätskategorien eingeteilt. Aus diesen Berechnungen können zwei

verschiedene Arten an Werte gezogen werden: zum einen eben die Übergangsgrenzwerte für die Kategorisierung und zum anderen auch die Anzahl, wieviele Dateninstanzen sich welchen Kategorien befinden. Ferner sei erwähnt, dass die Bestimmung dieser Werte (sv_{01} , sv_{12} , sv_{23}) beim statistischen und unüberwachten Ansatz für jeden untersuchten Datensatz aufs Neue berechnet wird. Beim halbüberwachten Ansatz hingegen werden die Grenzwerte (sv_{01} , sv_{12} , sv_{23}) durch das vorhergehende Training bestimmt.

Mit der getätigten Kategorisierung der Dateninstanzen kann die Alarmlogik mit dem Falschalarmfilter den Zustand der Maschine analysieren (siehe Kapitel 4.4.3 auf S.76). Alle Anomalie Scores unter sv_{12} , also normale Punkte und sonstige Anomalien, werden von der Alarmlogik nicht weiter beachtet. Jene Werte aber darüber, mäßige und kritische Anomalien, werden sehr wohl durch die Alarmlogik erfasst. Es wird vorgeschlagen, über einen Sliding Window Ansatz die Anzahl der Überschreitungen des errechneten Grenzwertes (sv_{12}) in einem vordefinierten Zeitfenster von 30min aufzusummieren. Übersteigt jene Summe der Überschreitungen in diesem bestimmten Zeitfenster den festgelegten Grenzwert (berechnet oder vorbestimmt), wird der Domain Expert benachrichtigt.

5.3.3 Ergebnisvisualisierung

Die Daten des vorigen Unterkapitels können nun für die Visualisierung aufbereitet werden. Für diesen Anwendungsfall werden für das Dashboard vier Schaubilder zur bereitgestellt. Jeweils ein Schaubild für 1) den Zeitreihenverlauf, 2) die Anomalie Scores, 3) die Alarmlogik und 4) für die Anomaliekategorien. Diese werden nun nachfolgend erklärt. Für den signalgruppenbasierten Ansatz wird eine eigene Darstellungsart gewählt, da dieser Ansatz eher diagnostisch zu verwenden ist.

5.3.3.1 Schaubild Zeitreihenverlauf

Es wird der bearbeitete (gekappte) Verlauf der Zeitreihe mit einer Anomaliekonnotation in Form von Markern auf anomalen Punkten angezeigt. Auf der Abszisse wird der Zeitindex (Datum und Uhrzeit) und auf der Ordinate die Stromstärke (in Ampere) aufgetragen. Grundsätzlich wird immer der gesamte Zeitraum des betrachteten Datensatzes angezeigt. Über ein Softwarewerkzeug (*Zoom in*) auf der Benutzeroberfläche können gewisse interessante Signalverläufe vergrößert dargestellt werden, sodass eine eingehende Diagnose durch das Personal möglich wird. Am oberen Rand der Darstellung befindet sich die Information, wieviele normale und anomale Messpunkte identifiziert werden. Diese Darstellung ist von Bedeutung, da damit der Verlauf des Anomalie Scores abgeglichen bzw. erklärt werden kann.

5.3.3.2 Schaubild Anomalie Scores

Zusätzlich wird auch der aussagekräftige Verlauf des Anomalie Scores ausgegeben. Im Schaubild des Scores werden zusätzlich mittels horizontaler Linien der Grenzwert für die Anomalieentscheidung (τ bzw. sv_{01}) und die anderen zwei Übergangswerte (sv_{12} , sv_{23}) angezeigt, sodass auch für das Personal eine schnelle Beurteilung des Zustandes möglich ist und eventuell eine Trendentwicklung abgeschätzt werden kann. Auf der Ordinate wird eben der Anomalie Score und auf der Abszisse wieder der Zeitindex aufgetragen.

5.3.3.3 Schaubild Alarmlogik

In dieser Darstellung ist der Verlauf der Summe an Grenzwertwertüberschreitungen (wie in Kapitel 4.4.3 auf S.76 dargelegt) ersichtlich. Das Monitoring dieses Verlaufes kann als Erweiterung zum Anomalie Scores Schaubild gesehen werden, denn erst durch den Falschalarmfilter, nämlich nur die Anomalien über sv_{12} zu beobachten, wird ein verständlicheres Bild über den Zustand der Anlage ersichtlich. Auf der Ordinate wird die Summe der Grenzwertverletzungen mit der zusätzlichen Information über die Fensterlänge (Beobachtungszeitraum) und auf der Abszisse der Zeitindex aufgetragen. Zusätzlich wird in Form einer horizontalen Linie der Grenzwert für diesen Verlauf mit einem numerischen Wert angezeigt.

5.3.3.4 Schaubild Anomaliekategorien

Die vierte und letzte Komponente des Dashboards ist eine Übersicht der einzelnen Anomaliekategorien aus der Anomaliebewertungsskala, die mit Tabelle 25 eingeführt wird. Das horizontale Balkendiagramm zeigt die Anzahl der Messpunkte in den vier verschiedenen Kritikalitätskategorien (sv_0 - sv_3) entsprechend dem definierten Farbcode. Mit dieser Darstellung lassen sich für den Domain Expert über den gesamten Analysezeitraum bereits sehr schnell Trends abschätzen, wenn sich z.B. der Anteil der sonstigen sowie mäßigen und im schlimmsten Fall kritischen Anomalien merklich erhöht.

Für den signalgruppenbasierten Ansatz wird ein anderer Weg eingeschlagen, denn dieser Ansatz eignet sich nicht für ein kontinuierliches CM. Der Ansatz zielt eher auf eine Anwendung als Offline-Fehlerdiagnose durch hochqualifiziertes Fachpersonal (z.B. Data Scientists) ab.

5.3.3.5 Visuelle Nachbereitung im signalgruppenbasierten Ansatz

In Abbildung 37 sind beispielhaft die Anomalie Scores der einzelnen Signal IDs der Öffnungssignale aus DS5 zusehen. Mit einer Abfrage-Funktion (Query) kann der Zeitbereich eines bestimmten anomalen Signals abgerufen werden, um so dann eventuell mit der verfügbaren Expertise des Instandhaltungspersonals den Grund für den anomalen Signalverlauf zu diesem Zeitpunkt zu klären – siehe Abbildung 38 mit Quell-Code. Die Anomalie kann also durch menschliches Zutun in einen zeitlichen Kontext gebracht werden. Dann können jene Signale, die als fehlerhaft identifiziert werden, durch den Domain Expert untersucht und mit einem berechneten Referenzsignal verglichen werden.¹⁷³

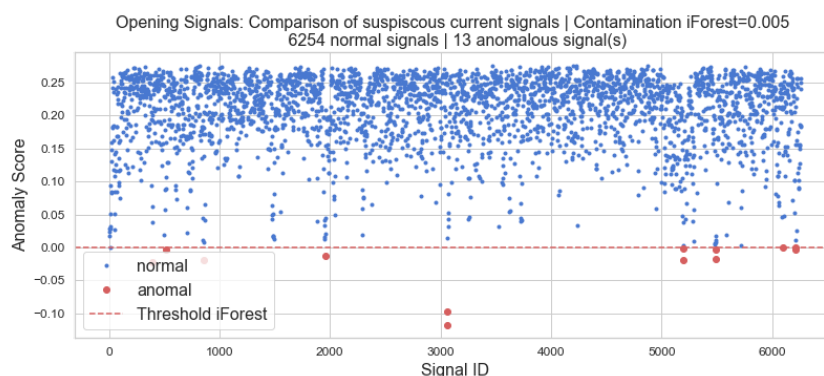


Abbildung 37: Anomalie Score über Signal IDs aufgetragen (DS5)

¹⁷³ Ansatz aus einer Vorarbeit zum Thema der vorliegenden Diplomarbeit: vgl. Fürst, 2020, S.4

```
# show time line of signal of interest
signal_of_interest = outlier_pos[0]
faulty_signal = processed_df.query("signal_id == " +str(signal_of_interest))
faulty_signal
```

signal_label	signal_id	date	current
opening	395.0	2020-05-04 20:23:53.090	0.00
		2020-05-04 20:23:53.095	1.37
		2020-05-04 20:23:53.100	1.37
		2020-05-04 20:23:53.105	1.37
		2020-05-04 20:23:53.109	1.37
	
		2020-05-04 20:24:00.561	0.43
		2020-05-04 20:24:00.566	0.43
		2020-05-04 20:24:00.570	0.43
		2020-05-04 20:24:00.575	0.43
		2020-05-04 20:24:00.580	0.00

1367 rows x 4 columns

Abbildung 38: Abfrage zu anomalen Öffnungssignal (Beispiel aus DS5)

Das Referenzsignal wiederum berechnet sich aus den verfügbaren Daten des untersuchten Datensatzes. In der Anwendung werden gemittelte Referenzsignale, jeweils für die Öffnungs- und Schließbewegung berechnet, herangezogen. Abbildung 39 schließt an das obige Beispiel an und visualisiert den Vergleich mit dem Referenzsignal – mehr dazu in Kapitel 5.4.2.3.

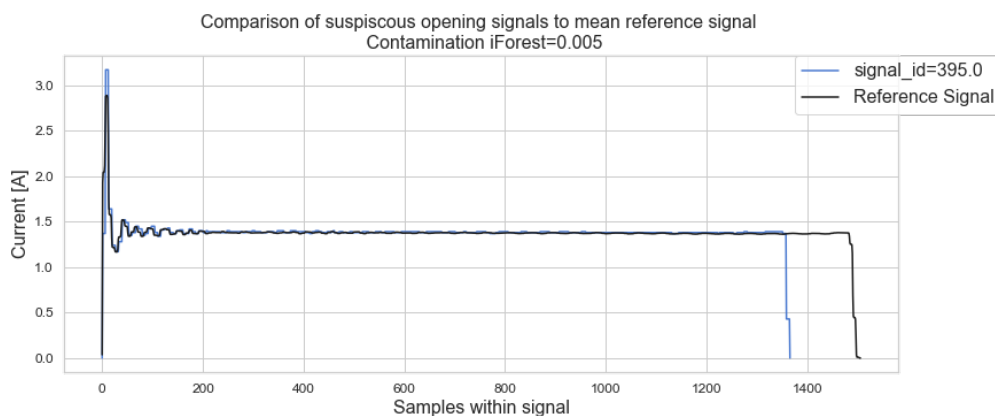


Abbildung 39: Vergleich mit Referenzsignal (Beispiel aus DS5)

5.4 Nutzerebene

Nun kann ein Prototyp eines Dashboards in der Nutzerebene für Anwendung an der Industrieofenanlage designt werden. Es werden alle vier oben genannten Schaubilder im Dashboard untergebracht. Es wird auch versucht, eine Evaluierung durch ExpertInnen darzustellen.

5.4.1 Prototyp Dashboard

Im Folgenden (Abbildung 40 und Abbildung 41) sind nun jeweils ein komplettes Dashboard für eine halbüberwachte Anomaliedetektion der Öffnungssignale aus DS3 einmal mit dem LOF-Algorithmus und einmal mit dem iForest dargestellt. Im Anhang sind zusätzlich Beispiele von Dashboards des HBOS- und kNN-Algorithmus zu sehen.

Bemerkung: Die Abszisse, in diesem Fall die Zeitachse, der drei Schaubilder für den Zeitreihenverlauf und Anomalie Score sowie der Alarmlogik ist im Dashboard gekoppelt. Sobald in einem der drei Graphen ein Zeitraum vergrößert dargestellt wird, wird derselbe Ausschnitt in anderen zwei Schaubildern ebenso in der Zoom-Darstellung abgebildet.

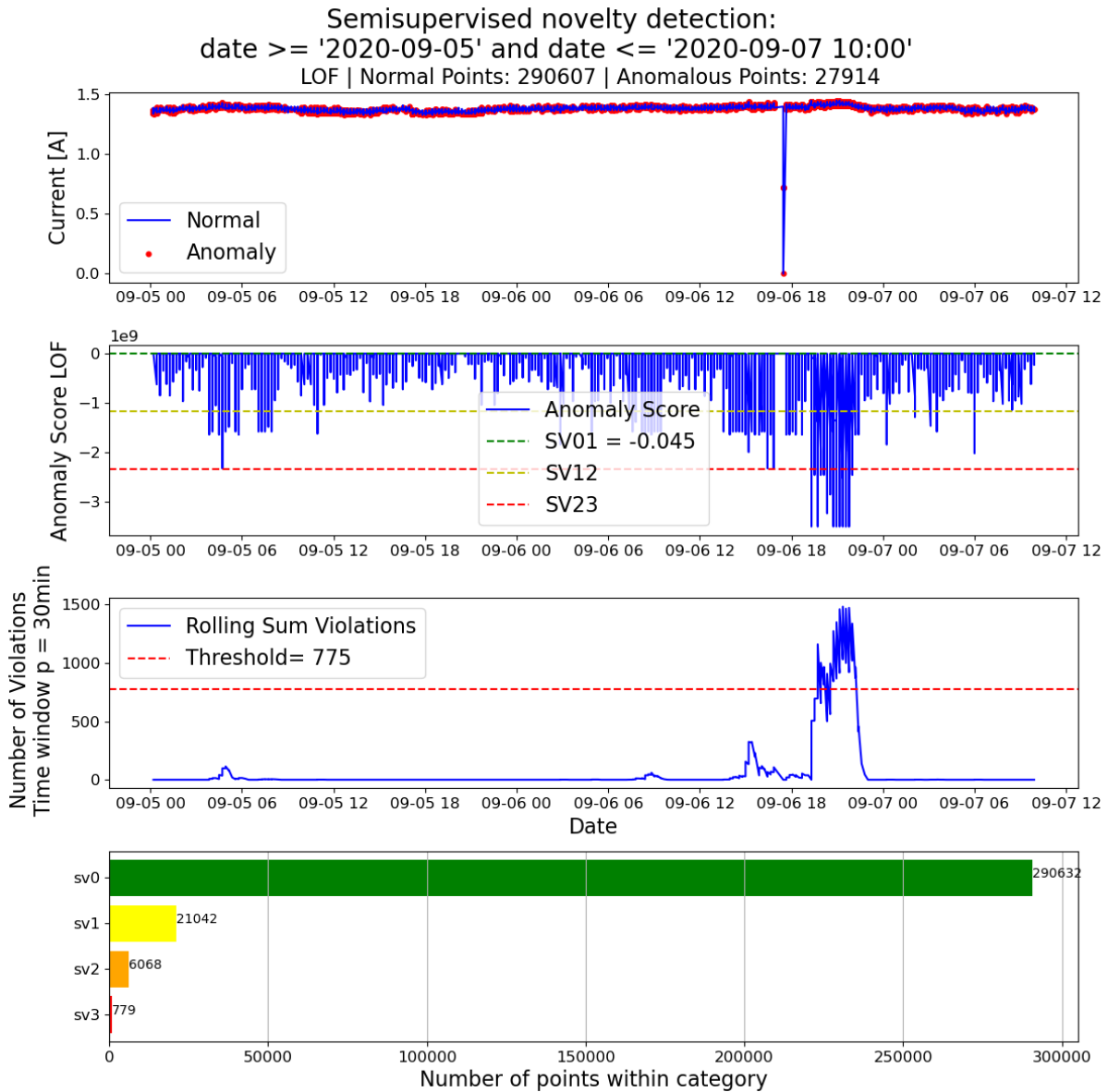


Abbildung 40: Beispiel eines Dashboards (Novelty Detection LOF von DS3 Öffnungssignal)

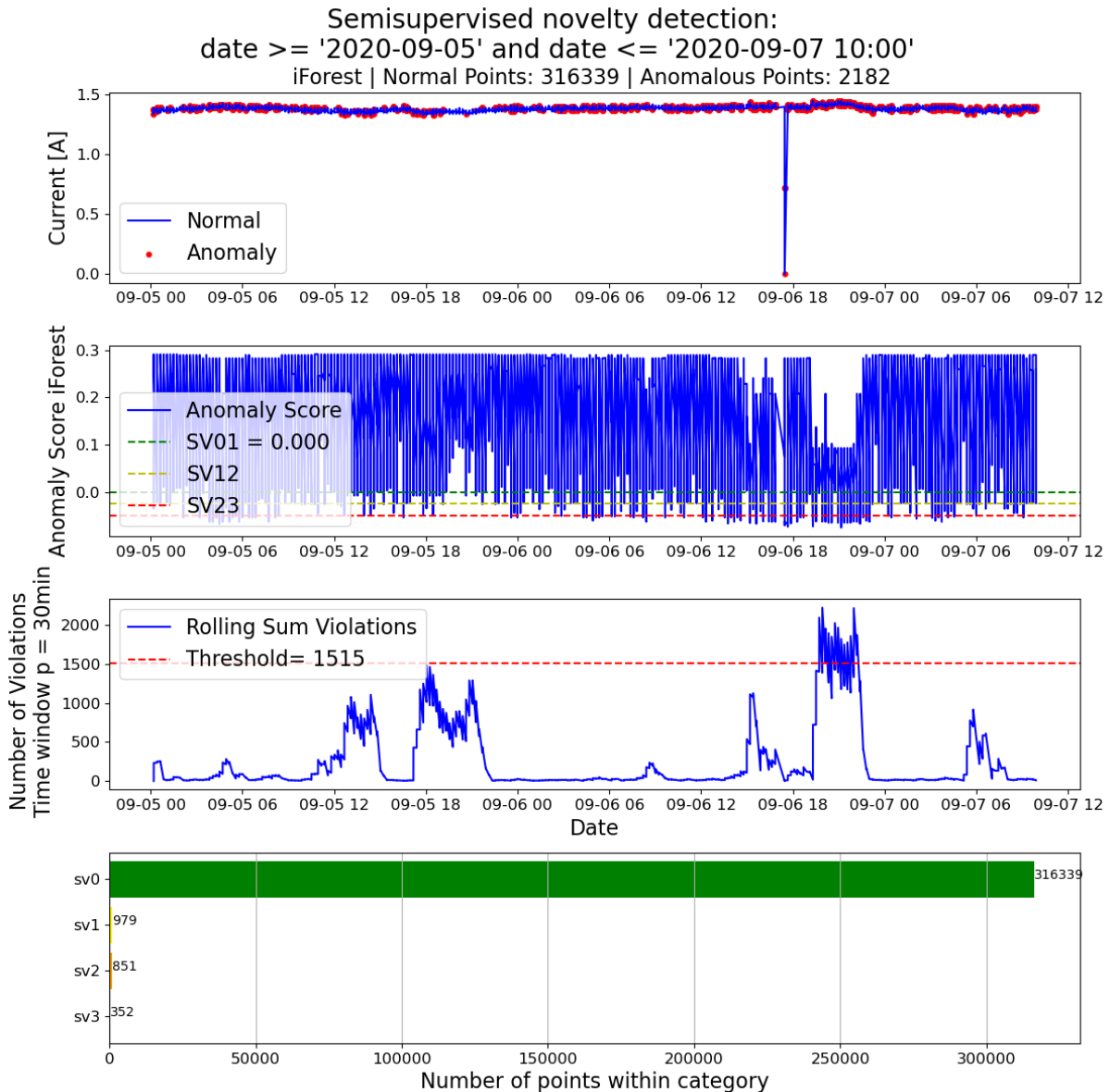


Abbildung 41: Beispiel eines Dashboards (Novelty Detection iForest von DS3 Öffnungssignal)

5.4.2 Evaluierung und Ableitung Instandhaltungsmaßnahmen

Aufgrund der vorliegenden Datenlage und dem sehr eingeschränkten Zugriff auf ExpertInnenwissen kann die Evaluierung bei diesem Anwendungsfall nur oberflächlich durchgeführt werden. Eine Ableitung von Instandhaltungsmaßnahmen ist nicht möglich. Für drei konkrete Fälle werden nachfolgend Beobachtungen angestellt bzw. Evaluierungen durchgeführt.

5.4.2.1 Dashboard LOF und iForest: DS3

In den Dashboards aus Abbildung 40 und Abbildung 41 kommt es in beiden Schaubildern für die Alarmlogik erst *nach* der offensichtlichen Anomalie (am 06.09.2020 kurz vor 1800 Uhr) zu einem bemerkbaren Anstieg in der Anzahl der mäßigen und kritischen Anomalien. Das gleiche Verhalten zeigt der Anomalie Score in beiden Algorithmen, obwohl beide Algorithmen die Unregelmäßigkeit detektieren und beide diese mindestens als sv_2 -Anomalie einordnen. Es

scheint hier erst nach dem Stromabfall zu einer Häufung von mäßigen und kritischen Anomalien zu kommen, obwohl der Verlauf des gekappten Stromsignals keine Unregelmäßigkeiten vermuten lässt. In beiden Analysen wird für die Alarmlogik der Grenzwert automatisiert mittels 3-Sigma-Regel berechnet.

5.4.2.2 Überblick Features vor und nach Jahreswartung

Bei der Analyse der dargestellten Merkmale von DS5 vor der Jahreswartung (Abbildung 35) und dem Überblick danach von DS6 in Abbildung 36 (beide repräsentativ nur Merkmale der Schließsignale) sind mit freiem Auge nur geringe bzw. keine relevanten Unterschiede festzustellen. Es kommt in manchen Merkmalen zu einzelnen Ausreißern. So ist im Merkmal *Kurtosis* im DS5 der Maximalwert über 250, im DS6 hingegen nur etwas über 225. In den Merkmalen *RMS*, *Entropy* und *Approx_Int* ist im DS6 etwas weniger Streuung in den Werten festzustellen. Ähnliches ist bei den Öffnungssignalmerkmalen von DS5 und DS6 zu beobachten. Jene Abbildungen sind im Anhang der Forschungsarbeit zu sehen, siehe Kapitel 7.2.4 auf S.122. Laut ExpertInnenwissen ist das Ergebnis plausibel. Es wird nämlich angenommen, dass die Wartungszyklen zu engmaschig sind und dadurch Bauteile viel zu früh gewartet bzw. getauscht werden (Nachteil der RCM-Instandhaltungsstrategie). Deshalb sind keine Ausprägungen in den Daten zu erkennen, die tatsächliche Anzeichen für Verbesserungen nach der Jahreswartung der Ofenanlage sind. Zudem sind folglich auch keine signifikanten Verschlechterungen feststellbar.

5.4.2.3 Vergleich eines Öffnungssignals mit dem Referenzsignal

In Abbildung 39 wird das Signal mit der ID 395 mit dem aus dem untersuchten Datensatz berechneten Referenzsignal verglichen. ID 395 scheint etwas kürzer zu sein als die Referenz, weist aber sonst keine Unregelmäßigkeiten auf. Laut der Expertise des Fachpersonals ist die Länge des Signals nicht aussagekräftig, wenn sonst kein anomaler Verlauf festzustellen ist. Daher liegt hier eine Falschklassifikation vor.

Die eben erklärten Schritte können aber trotzdem dazu beitragen, eine Ground Truth Datenbank aufzubauen. Aber auch hier ist zeitintensives personelles Zutun erforderlich, um nachhaltig das Detektionsverhalten zu verbessern.

Es folgen nun abschließende Betrachtungen zur Anwendung des Phasenmodells in der Industriefallstudie. Zum einen werden zwei Algorithmen ausgewählt, die sich bei jenem Anwendungsfall als besonders passend für die Anomaliedetektion erwiesen haben. Zum anderen werden identifizierte anomale Signalverläufe gesondert dargestellt.

5.4.3 Auswahl der Algorithmen

Bei Betrachtung der erstellten Bewertungstabellen setzen sich unter den gegebenen Umständen und gewählten Einstellungen zwei Algorithmen durch – siehe Tabelle 41. Zum einen der HBOS-Algorithmus und zum anderen der iForest-Algorithmus. Der HBOS ist dazu gedacht, für die Algorithmen des maschinellen Lernens, die ja im Fokus dieser Arbeit stehen, einen statistischen Gegenpart bzw. Vergleich (*Baseline*) darzustellen. Durch seinen einfachen Rechenalgorithmus arbeitet der HBOS auch bei größeren Datensätzen effizient. Gerade im Hinblick auf die zukünftige industrielle Anwendung, wo nicht von immer von einer leistungsstarken Rechnerinfrastruktur ausgegangen werden kann, stellt der HBOS aber einen

validen Kompromiss zwischen Effizienz und Detektionsgenauigkeit dar. Außerdem wird auch ein Anomalie Score und ein algorithmusinterner Grenzwert ausgegeben. Die Schnelligkeit bei den Berechnungen führen auf der anderen Seite zu Ungenauigkeiten (sofern bei dieser Informationslage feststellbar) bei der Anomaliedetektion. In Summe erreicht dieser Algorithmus 35 Punkte im verwendeten Bewertungsschema und damit die zweithöchste Punktezahll aller untersuchten Algorithmen. Mit in Summe 40 Punkten und somit der vollen Punktezahll hat der iForest-Algorithmus abgeschnitten. In der Verwendung als halbüberwachter Algorithmus weist dieser sowohl im Training als auch in der Anwendung auf Testdaten hohe Recheneffizienz auf und das auch bei größeren Datensätzen. Zusätzlich wird ein Anomalie Score (zwischen 1 und -1) und ein algorithmusinterner Grenzwert ($\tau = 0$) ausgegeben. Bzgl. der Anomaliedetektionsleistung kann sich der iForest gegenüber allen anderen ML-Algorithmen durchsetzen. Jener Algorithmus kann zusätzlich auch seine Effizienz im signalgruppenbasierten Ansatz unter Beweis stellen, wo höherdimensionale Datensätze zu verarbeiten sind.

Ferner sei für Algorithmen noch erwähnt, dass ein algorithmusspezifisches Feintuning der Parameter die Detektionsleistung verbessert. Die Kontamination wird bei der Bearbeitung des Anwendungsfalles für beide Algorithmen gleich gewählt, eine Änderung aber z.B. beim HBOS der Kontamination von 0.005 auf 0.05 bewirkt bereits ein besseres Detektionsergebnis – siehe Abbildung 61.

Tabelle 41: Zusammenfassung der Bewertung der Kandidatenalgorithmen

Erreichte Gesamtpunktezahll	
Algorithmus	Punkteanzahl
iForest	40
HBOS	35
kNN	25
kMeans	25
Autoencoder	25
LOF	20
LOF (Novelty Detection)	20
OC-SVM	20

In Abbildung 42 sind die untersuchten Algorithmen nochmals dargestellt und die ausgewählten Algorithmen, also HBOS und iForest, rot markiert.

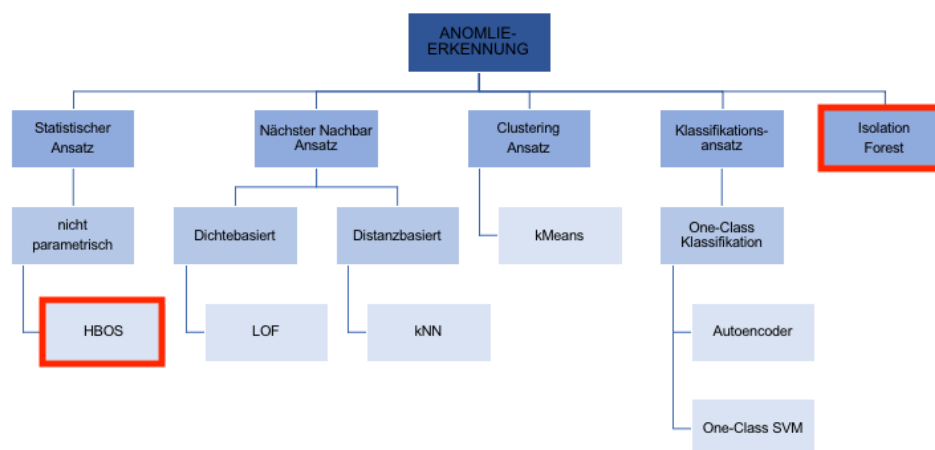


Abbildung 42: Übersicht der Kandidatenalgorithmen mit der Auswahl von HBOS und iForest

5.4.4 Identifizierte anomale Signalverläufe

Im Folgenden werden jene drei tatsächlichen Anomalien in der Vergrößerung dargestellt, die durch den iForest in den Daten erkannt werden. Die Anomalien entstammen dem DS1 und es werden das 1. und 2. Schaubild des Dashboards gezeigt. Zusätzlich wird aber auch das gesamte Dashboard für diesen Beobachtungszeitraum visualisiert. Die Darstellungen zur Detektion durch den HBOS (mit Kontamination=0.05) befinden sich aus Gründen der Übersichtlichkeit im Anhang (Abbildung 61 bis Abbildung 64). Die Ursache für jenes anomale Verhalten der Einlaufftüre beim Öffnen ist, wie bereits erwähnt, auf absichtlich angebrachte Gewichte (künstlich erzeugte Anomalien) zurückzuführen. Durch die zusätzliche Masse muss mehr Strom aufgenommen werden, um die Türe zu öffnen.

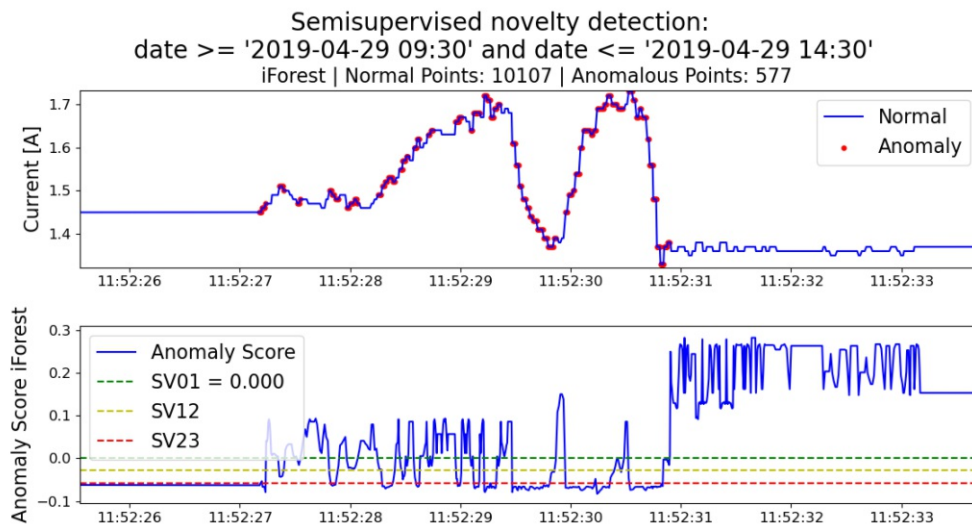


Abbildung 43: Vergrößerung auf 1. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal)

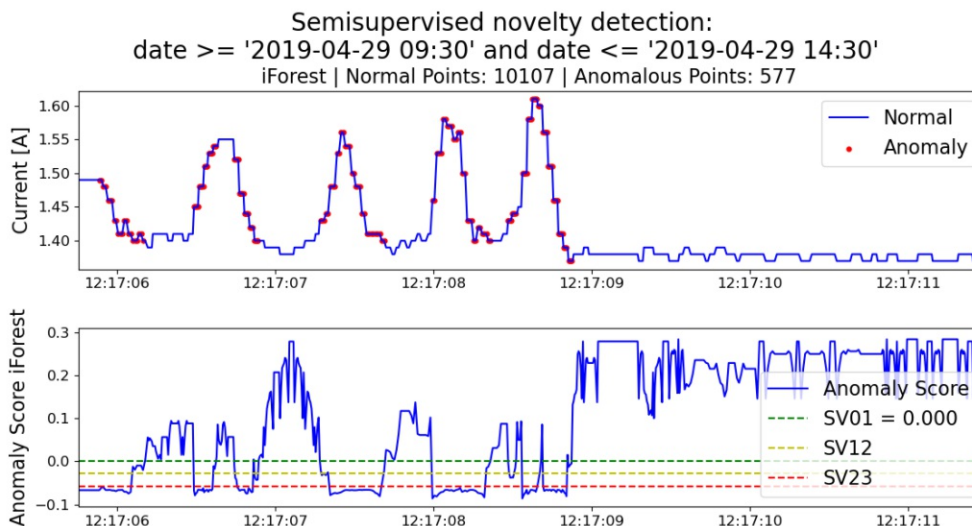


Abbildung 44: Vergrößerung auf 2. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal)

In den vergrößerten Darstellungen ist der Zusammenhang zwischen dem Anomalie Score und den Abweichungen im Stromverlauf sehr deutlich zu erkennen. Sobald z.B. in Abbildung 45 der Strom auf über 1.5 A ansteigt (um 12:41:49 Uhr) verändert sich sofort der Score und es werden feingranular Anomalien aller drei Kritikalitätsbereiche festgestellt. Wird das

Dashboard, genauer der Verlauf der Grenzwertüberschreitungen, in Abbildung 46 betrachtet, ist festzustellen, dass hier entweder die Fensterlänge oder der Grenzwert manuell verändert/ adaptiert werden müsste, um entsprechende Warnungen an das Personal auszugeben.

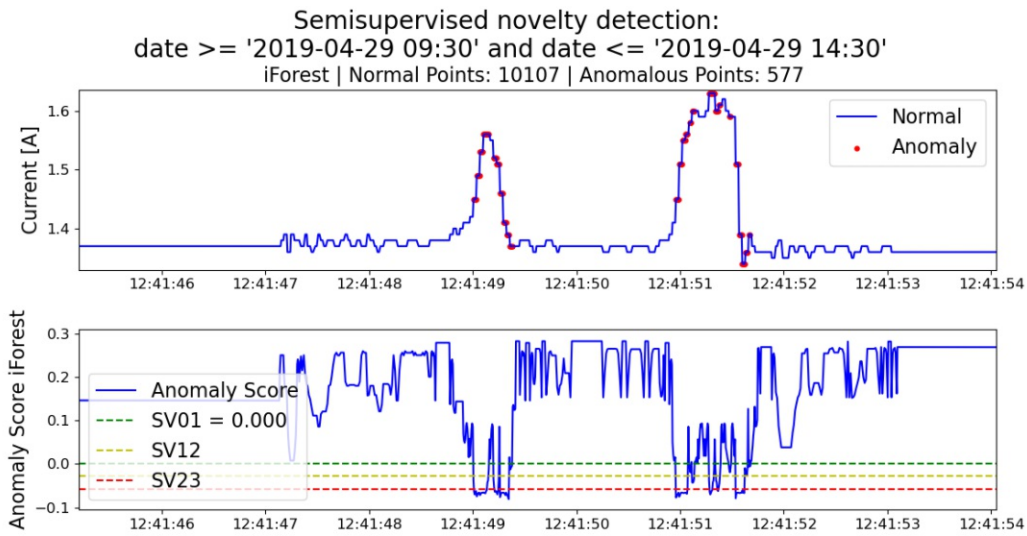


Abbildung 45: Vergrößerung auf 3. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal)

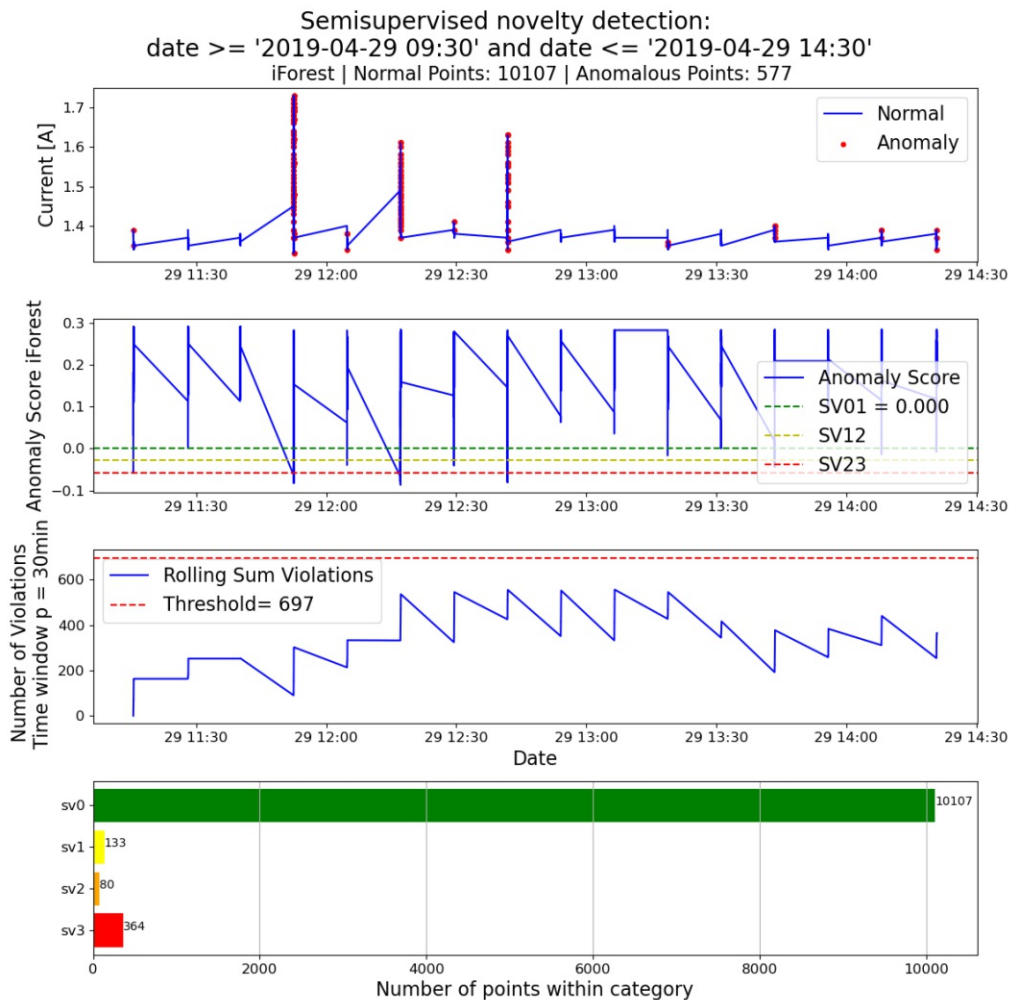


Abbildung 46: Dashboard für DS1 (Öffnungssignale) mit iForest

6 Zusammenfassung und Ausblick

Im Zuge dieser Arbeit ist untersucht worden, ob eine Zustandsüberwachung kritischer und hochkomplexer Industrieanlagen mittels Anomalieerkennung realisierbar ist. Dazu wurde ein Phasenmodell entwickelt, das eine Ablauflogik für diesen Zweck vorgibt, und darauf aufbauend wurde ein Softwareprototyp programmiert. Jenes *Phasenmodell für das CM mittels Anomalieerkennung* wurde im Anschluss an einer Industriefallstudie evaluiert. Bei der Fallstudie wurde ein kritisches Bauteil einer komplexen Wärmebehandlungsanlage betrachtet, die im Nachhinein mit Sensoren ausgestattet worden ist, sodass Daten (Stromaufnahme) für eine zustandsbasierte Instandhaltung generiert wurden. Das übergeordnete und langfristige Ziel dieser Maßnahme ist, weg von einer RCM-Instandhaltungsstrategie zukommen und eine zustandsbasierte Strategie (CBM) zu realisieren. Bei der Bearbeitung des Anwendungsfalles konnte gezeigt werden, dass sowohl mit statistischen Methoden als auch mit Ansätzen des maschinellen Lernens, welche im Fokus dieser Diplomarbeit stehen, ein CM mittels Anomalieerkennung möglich ist. Grundlage für die erläuterten Ausführungen ist eine ausführliche Internet- und Literaturanalyse zu drei Bereichen: CM von kritischen und hochkomplexen Anlagen, Informationsgewinnung unter schwieriger Datenausgangslage und eben Anomalieerkennung im Zuge von CM.

In diesem Kapitel werden die Forschungsfragen beantwortet und ein Abgleich der Ziele aus der Bearbeitung der Fallstudie vorgenommen. Zum Schluss wird nach der Erläuterung der Limitationen der Arbeit ein Ausblick für zukünftigen Forschungsbedarf gegeben.

6.1 Kritische Reflexion auf die Forschungsfragen

Die Beantwortung der Hauptforschungsfrage FF1 (siehe Tabelle 3) ist äußerst komplex sowie umfangreich und daher wurden vier Unterpunkte eingeführt, sodass die Beantwortung strukturierter und verständlicher wird. Die Beantwortung der Unterfragen (FF1.1-FF1.4) geschieht immer unter der Prämisse der Hauptforschungsfrage.

FF1 Wie kann man für hochkritische Anlagen unter fehlender bzw. begrenzter Ground Truth- und Ausfallsdatenlage ein CM System aufbauen?

Es kann unter Zuhilfenahme passender ML-Algorithmen der Zustand einer komplexen Anlage ohne Daten über die Ground Truth oder zum jeweiligen Ausfallverhalten beurteilt werden. Mittels Anomalieerkennung in den Mess- und Maschinendaten kann ohne Modellierungsaufwand abnormales Verhalten einer Anlage detektiert werden und so auf eventuellen Instandhaltungsbedarf geschlossen werden. Dies ist unter der Annahme möglich, dass sich Anomalien ausgelöst durch menschliche Fehler, Fehlfunktionen in Messinstrumenten und Veränderungen im Verhalten oder Fehlern in Systemen in den Daten äußern.

FF1.1 Mit welcher Methode der AE können außergewöhnliche Zustände festgestellt werden? Wie kann tatsächlich ein Mehrwert für die zustandsbasierte Instandhaltung generiert werden?

Aus der Sicht des maschinellen Lernens stehen verschiedene Ansätze für die Anomalieerkennung zur Verfügung (siehe Kapitel 2.4.4 auf S.32). Das Feld der möglichen Ansätze wird aber im Falle der begrenzten Datenausgangslage bzgl. fehlender Ground Truth und Ausfalldaten massiv verkleinert. So hat die Literaturrecherche (Kapitel 3.2 auf S.44) ergeben, dass das Problem des Einlernens der ML-Algorithmen bei der gegebenen Ausgangslage nicht auf der Datenebene gelöst werden kann. Das Problem kann nur auf Algorithmusebene, sprich durch die Wahl von passenden Algorithmen, gelöst werden. Die ausgewählten Algorithmen entspringen zum einen der statistischen Anomalieerkennung, dem unüberwachten Lernen, wo durch Clustering und dem Nächsten-Nachbar-Ansatz anomale Dateninstanzen identifiziert werden, und zum anderen dem halbüberwachten Lernen, wo durch das Einlernen z.B. nur des Gutzustandes abweichende Dateninstanzen gefunden werden können. Damit die Algorithmen verarbeitungsgerechte Daten erhalten, ist ein Datenpreprocessing und im Besonderen eine Merkmalsextraktion unabdingbar – speziell für Zeitreihendaten siehe Kapitel 4.3 auf S.63.

Für eine zustandsbasierte Instandhaltung entsteht dadurch ein Mehrwert, dass schon mit relativ einfach gesammelten Messdaten eine Zustandsfeststellung möglich wird. Bei der Verwendung von ML-Algorithmen müssen weder eine Prozessmodellierung durchgeführt noch eine Modellannahme getroffen werden, was die Anwendung bei komplexen Anlagen erleichtert. Dies zeigen auch die Arbeiten, die im Zuge der Literaturanalyse zu kritischen und hochkomplexen Anlagen untersucht wurden (siehe Kapitel 3.1 auf S.35). Die Zustandsüberwachung passiert somit rein datengetrieben. Für die Bearbeitung der Industriefallstudie steht nur eine univariate Zeitreihe (Messung der Stromaufnahme) zur Verfügung. Um die Anomaliedetektion zu verbessern, können mit den ausgewählten Algorithmen in Zukunft auch multivariate Zeitreihen bzw. Datensätze, sprich mehr Information über die Anlage, verarbeitet werden. Ferner bieten auch einige der untersuchten Algorithmen durch ihre effiziente Arbeitsweise die Möglichkeit für ein Online-CM, welches ja die Grundlage für die zustandsbasierte Instandhaltung ist.

FF1.2 Wie können die Ergebnisse aus der Datenverarbeitung kommuniziert und sinnvoll interpretiert werden?

Es ist für das Anlagenpersonal *am Shopfloor* sinnvoll, eine quantitative Rückmeldung vom Anomaliedetektionsprozess zu erhalten. Daher wird an das Personal zurückgegeben, wieviele der untersuchten Dateninstanzen anomal oder normal sind. Zusätzlich werden zu dieser binären Information (Anomalie ja/ nein) auch die Anomalie Scores der Messpunkte, also zu welchem Grad diese anomal sind, berechnet. Jene zwei Schlüsselinformationen werden ferner natürlich auch visualisiert und dies am besten in Form eines übersichtlichen Dashboards, worauf dann der Zustand der beobachteten Komponente sichtbar wird. Eine kompakte Visualisierung mit den wichtigsten Informationen für das Shopfloor-Personal stellt eine Kernkomponente der zustandsbasierten Instandhaltung dar und so werden z.B. in den Verlauf der Messdaten die anomalen Messpunkte markiert. Für die Visualisierung des Anomalie Scores ist es auch entscheidend, den errechneten Grenzwert für die Anomalieentscheidung auszugeben, da so durch das Personal der Verlauf des Anomalie Scores visuell interpretiert werden kann. Hier kann unkompliziert abgelesen werden, *wie normal/ anomal* gerade der Zustand des Systems ist. Eine zusätzliche Möglichkeit stellt auch die Visualisierung einzelner

zentraler Merkmale (Features) über die Zeit dar. Im Hinblick auf das Phasenmodell und die Interpretation ist festzustellen, dass hier die Zusammenarbeit verschiedener Domain Experts und Knowledge Engineers notwendig ist. Dies geht auch aus der Literaturanalyse hervor, dass generelles Anlagen- bzw. Domänenwissen essentiell für die Implementierung von CM und auch der Interpretation ist.

Aufgrund der fehlenden Ground Truth ist es nicht möglich, die Leistung der Anomaliedetektion mathematisch mit Performance-Metriken, wie in Kapitel 3.2.3.2 auf S.53 erläutert, zu validieren. Diese gravierende aber im Industriebetrieb häufig anzutreffende Limitation muss auch hier über das Fach- und Anlagenwissen des Personals ausgeglichen werden.

FF1.3 Wie können detektierte Anomalien einheitlich quantitativ bewertet werden?

Wie in der Beantwortung von FF1.2 bereits dargelegt, kann über den Anomalie Score der Grad der Abweichung bestimmt werden. Je höher der Score ist, desto eher wird die betrachtete Dateninstanz als Anomalie gesehen. Das einheitliche unter den verschiedenen untersuchten Algorithmen an der quantitativen Bewertung ist, dass eben der Anomalie Score herangezogen wird. Die Ermittlung desgleichen läuft hingegen unterschiedlich ab. Algorithmen wie LOF, iForest oder OC-SVM errechnen diesen algorithmusintern. Andere Ansätze wie der Autoencoder oder der kNN-Algorithmus geben Fehlermaße zurück, die als Anomalie Score benutzt werden. So können aber die einzelnen Dateninstanzen, egal auf welchem Weg der Anomalie Score ermittelt wird, untereinander verglichen werden. Dazu wird in Kapitel 4.4.2.2 auf S.75 eine Bewertungsmethodik vorgestellt.

FF1.4 Wie können die berechneten Ergebnisse in ein intelligentes Alarmsystem verpackt werden, sodass es für die Zustandsüberwachung der Anlage verwendet werden kann?

Um eine Flutung des Anlagenpersonals mit Alarmmeldungen zu vermeiden, werden aufbauend auf die Bewertung der Anomalien (Kategorisierung nach Kritikalität) nur bestimmte Anomaliearten (z.B. nur mäßige und kritische Anomalien) beobachtet. Die Beobachtung nur von bestimmten Anomaliekategorien wirkt wie ein Falschalarmfilter, da ja z.B. sonstige Anomalien vom Alarmsystem ignoriert werden. Am Dashboard kann somit die Anzahl der relevanten Grenzwertüberschreitungen in einem gewissen vorgegebenen Zeitfenster beobachtet werden. Überschreitet die jene Anzahl der aufsummierten Grenzwertverletzungen einen vorgegebenen Grenzwert, wird das Anlagenpersonal verständigt. Schwierigkeiten bereitet hier die Grenzwertfindung. Für einen Erstentwurf wird hier eine Grenzwertberechnung über die 3-Sigma-Regel vorgeschlagen. Es besteht aber auch die Möglichkeit, dass ein individueller Grenzwert durch den Domain Expert vorgegeben wird.

6.2 Abgleich der Ziele für die Bearbeitung der Fallstudie

Mit einem PoC wird im vorigen Kapitel überprüft, ob eine Anwendbarkeit des Phasenmodells für reale Systeme, wie jenes aus der Fallstudie, gegeben ist. Hier wird zusätzlich erörtert, ob die in Kapitel 1.1 auf S.3 erwähnten Zielvorgaben vom Phasenmodell in Bezug auf den Anwendungsfall erreicht werden.

Ziel 1: Passende Merkmale (Features) zur Beschreibung des Zustandes finden

Nach einer ausgiebigen Internet- und Literaturrecherche werden, wie in Kapitel 4.3.3 bzw. 5.2.1 beschrieben, für die Anomalieerkennung 6 statistische Merkmale mittels Sliding Window Ansatz mit einer Fensterlänge von $p=10$ errechnet. Mit dieser kleinen Fensterlänge wird garantiert, dass kurzfristige Veränderungen und Abweichungen in den Daten detektiert werden können. Wird die Fensterlänge größer gewählt, kommt es zu einer Glättung und wichtige Informationen können dadurch verloren gehen. Für den signalgruppenbasierten Ansatz, der allerdings nicht im Fokus der Arbeit steht, werden sogar 16 Merkmale ermittelt (nicht mit dem Sliding Window Ansatz). Jene Schritte passieren in der Verarbeitungs- und Analyseebene im Verarbeitungsteil des Phasenmodells und werden vom Knowledge Engineer durchgeführt.

Ziel 2: Passende Anomalieerkennungsalgorithmen finden (auch mit der Integration mehrerer Entscheidungsvariablen)

In Kapitel 4.4.1 werden verschiedene Algorithmen, die für die Anomalieerkennung in Frage kommen, erörtert. Diese basieren sowohl auf Clustering, Klassifikation als auch auf dem Nächster-Nachbar-Ansatz. Zusätzlich werden ein parameterfreier statistischer Ansatz und der Isolation Forest Algorithmus angewandt (Einteilung siehe Kapitel 2.4.4 und 2.4.5). In ihren Wirk- und Arbeitsweisen sind jene Algorithmen unterschiedlich, aber jeder dieser kann einen mehrdimensionalen Datensatz verarbeiten und eine Anomaliedetektion darin durchführen. Nach dem PoC haben sich der statistische Anomalieerkennungsalgorithmus HBOS und der Isolation Forest, ein Algorithmus aus dem Bereich des maschinellen Lernens, durchgesetzt. Beide kommen mit großen Datenmengen auf eine effiziente Weise zu recht und liefern auch, soweit beurteilbar, akzeptable Detektionsergebnisse. Dies ist besonders bemerkenswert, da für die Bearbeitung der Fallstudie nur eine stark begrenzte Rechnerleistung zur Verfügung steht. Jene Schritte passieren in der Verarbeitungs- und Analyseebene im Analyseteil des Phasenmodells und werden vom Knowledge Engineer durchgeführt.

Ziel 3: Anomalien erkennen und in Kategorien einteilen

Es werden durch die Algorithmen punktuelle Anomalien in den Datensätzen erkannt, wie der PoC darlegt (siehe Kapitel 5.3). Aufgrund der sperrigen Daten- und Informationslage kann keine kontextuelle Anomalie erkannt werden, da das Kontextwissen einfach fehlt. Somit ist keine Kategorisierung im Sinne einer Klassifikation nach Fehlerherkunft möglich. Es steht z.B. keine Repräsentation in den Daten zur Verfügung, die klar auf eine schlechte Schmierung der Einlaufftüre rückschließen lässt und die dann durch einen Klassifikationsalgorithmus als solche kategorisiert wird.

Ziel 4: Anomaliebewertungsskala definieren

Der Anomalie Score stellt einen weiteren Ausgabewert dar - neben der binären Information über das Vorliegen einer Anomalie oder nicht. Dieser beschreibt, wie anomal jene Dateninstanz ist. Genau dieser Score wird dazu verwendet, um eine Kategorisierung bzw. Bewertung nach Kritikalität der detektierten Anomalie vorzunehmen. Es wird in sonstige, mäßige und kritische Anomalien bzw. Werte des Anomalie Scores eingeteilt. Die Methodik dazu ist in Kapitel 4.4.2.2 niedergeschrieben. Auch jene Kategorisierung geschieht in der

Verarbeitungs- und Analyseebene im Analyseteil des Phasenmodells und kann als Nachbereitung der Anomalieerkennung verstanden werden. Denn bei der Nachbereitung geht es grundsätzlich darum, die Ergebnisse aus der Detektion zu verwenden und zu interpretieren.

Ziel 5: Einheitlichen Anomaliebericht entwickeln und Ergebnisse interpretieren

In der Nutzer-Ebene werden die Ergebnisse für das Instandhaltungspersonal aufbereitet und visualisiert. Das Personal bzw. der Domain Expert erhält seine Informationen über ein Dashboard, das relevante Informationen aufbereitet. In Kapitel 5.3.3 ist ein Prototyp eines solchen dargestellt. Darin enthalten ist der Zeitverlauf der Stromaufnahme im Beobachtungszeitraum und die Anzahl der detektierten Anomalien. Zusätzlich geben der Verlauf des Anomalie Scores, die Kurve der angefallenen Grenzwertüberschreitungen (siehe Ziel 6) und eine Aufschlüsselung der Anomalie nach der Bewertungsskala aus Ziel 4 weitere Einblicke in den Zustand des Systems. Die Aufbereitung des Reports ist für die statistische, unüberwachten, halbüberwachte Anomalieerkennung die gleiche. Die Interpretation der Ergebnisse gestaltet sich als äußerst schwierig, da kein bzw. nur sehr wenig Fachwissen vorhanden ist. Hier kann nur zwischen den einzelnen Algorithmen verglichen werden. Aber der Prototyp des Dashboards ist eine nützliche Grundlage für die zukünftige Interpretation der Ergebnisse durch ExpertInnen.

Ziel 6: Intelligentes Alarmsystem entwickeln: Regeln definieren, wann Alarm ausgelöst werden sollte

Wie in Ziel 5 bereits angedeutet, ist eine Komponente des Dashboards der Verlauf der für das Alarmsystem relevanten Grenzwertüberschreitungen. Das Alarmsystem baut auf die Anomaliebewertungsskala auf und berücksichtigt nur mäßige und kritische Anomalien dafür. In einem bewegten Fenster von 30min wird die Anzahl der Anomalien dieser beiden Kategorien aufsummiert und jene Summe wird beobachtet. Mit Hilfe einer sichtbaren Grenzwertlinie kann der Domain Expert beurteilen, ob ein vordefinierter zulässiger Wert überschritten wird. Es wird dafür ein statistischer Richtwert mit der 3-Sigma-Regel vorgeschlagen, aber es besteht auch die Möglichkeit, dass der Grenzwert durch den Domain Expert bestimmt wird. Dieses Unterfangen ist geprägt von *Trial and Error*. Die Methodik ist in Kapitel 4.4.3 dargelegt.

Somit ist die einzige Regel, die definiert wird, dass ein Alarm ausgelöst wird, wenn eben jener Grenzwert überschritten wird. Weitere Regeln, die eventuell Prozessphasen oder andere Einflüsse mitmodellieren, können aufgrund der gegebenen Daten- und Informationslage nicht formuliert werden.

Ziel 7: Qualitatives Phasenmodell für das CM mittels Anomalieerkennung entwickeln, das als Grundlage für einen Software-Prototyp verwendet werden kann

Auf Basis einer extensiven Literaturanalyse, wo sämtliche CM-Ansätze aus den unterschiedlichsten Industrien studiert wurden, wird im vierten Kapitel ein Phasenmodell für das CM mittels Anomalieerkennung eingeführt und beschrieben. Das Modell wird in Kapitel 5 einem PoC unterzogen. Das Phasenmodell ist das Artefakt aus der gestaltungswissenschaftlichen Methodik, nach der in dieser Diplomarbeit gearbeitet wird

(siehe 1.2.1). Für eine zukünftige Weiterentwicklung des Modells wird bereits in der Datenebene eine Ground Truth Datenbank vorgesehen, die in Zukunft z.B. für das Einlernen von überwachten Algorithmen oder die Berechnung von Performance-Metriken herangezogen werden kann.

Es ist aber hervorzuheben, dass jenes Phasenmodell auf realen Daten getestet wird. Dabei liefert es bereits für das CM brauchbare Ergebnisse. In der wissenschaftlichen Literatur hingegen werden mehrheitlich entweder nur simulierte oder aufwendig aufbereitete Datensätze untersucht.

6.3 Eingrenzung der Arbeit

Wie bereits erwähnt, ist keine Performanceevaluierung der Anomaliedetektion möglich. Die Dateninstanzen sind nicht gelabelt und daher können keine Performancemetriken wie z.B. F-Score, Konfusionsmatrix oder Accuracy berechnet werden. Ferner stellt das entwickelte Phasenmodell nur die Grundlage für einen Software-Prototyp dar und ermöglicht noch keine Anwendung in einem Online-Monitoring System. Hierzu müsste zusätzlich auf eine echtzeitfähige Datenkommunikation und Softwareimplementierung eingegangen werden, was aber nicht im Fokus der vorliegenden Arbeit steht. Außerdem steht bei dieser Arbeit für die Anomalieerkennung nur eine eingeschränkte Rechnerleistung (*Consumer-PC* kein Industrierechner) zur Verfügung.

Ferner können für die Modellierung nur univariate Zeitreihen herangezogen werden. Es besteht also nur *eine* Daten- bzw. Informationsquelle, nämlich rohe Stromaufnahmemessungen. Das führt auch zu Einschränkungen bzgl. des Alarmsystems, das nur sehr rudimentär Grenzwertverletzungen beobachtet. Es können aufgrund der fehlenden Ground Truth und des fehlenden Einblicks in das Verhalten der Anlage keine Fehlerklassen festgestellt noch eine Fehlereinflussanalyse (*Root Cause Analysis*) durchgeführt werden. Jene Informationen stellen aber die Grundlage für ein intelligenteres Alarmsysteme dar, wie es z.B. Fullen et al. (2017) zur Vermeidung von Alarmfluten präsentieren.

6.4 Ausblick

Nachdem ein erster Prototyp für das CM von kritischen und komplexen Anlagen präsentiert worden ist, gilt es hier nun mögliches Weiterentwicklung- und Forschungspotential zu dieser Thematik aufzuzeigen.

Im Phasenmodell wird in der Datenebene ein zusätzlicher Speicher zum Füllen vorgesehen. Dieser dient zum Erstellen einer Ground Truth Datenbank (Ground Truth Building), worin Informationen über Instandhaltungsmaßnahmen, richtig detektierten Anomalien etc. im zukünftigen laufenden Betrieb hinterlegt werden. Das Füllen dieser Datenbank ist äußerst personal- und zeitintensiv, da das Evaluieren und Annotieren von Anomalien und anderen Vorkommnissen nur manuell bewerkstelligt werden kann. Nur so können aber in Zukunft die Detektionsmodelle verfeinert und im Allgemeinen auch deren Detektionsleistung beurteilt werden. Eine vollautomatisierte Erkennung von Anomalien, Störungen und Veränderungen des Systems stellt eines der Ziele von intelligenten CPS dar.

Eine Erweiterung der Datengrundlage bzw. -quellen führt ebenfalls zu Verbesserungen in der Detektion. Durch die zukünftige Einbeziehung von z.B. Daten aus SCADA, MES, ERP und anderen Informationsquellen im Sinne von KBM können die gewählten Modelle gezielter trainiert und eingestellt werden. Um aus Sicht von CPS den Reifegrad des Systems erhöhen und einen Mehrwert generieren zu können, müssen diese zusätzlichen Informationen miteinander verbunden werden (*Information Linking*¹⁷⁴). Dadurch wird nicht nur die Detektionsleistung der Modelle, sondern auch die Entscheidungsunterstützung für das zuständige Personal verbessert. Mit der Erweiterung der Datengrundlage und zusammen mit einer Ground Truth Datenbank wird es auch möglich, Algorithmen aus dem Bereich des überwachten Lernens zu trainieren. Damit können unter der Voraussetzung, dass durch das Ground Truth Building gewisse Fehlermodi gespeichert worden sind, auch einzelne Fehlerkategorien klassifiziert werden. Sind nach einiger Zeit Repräsentationen von schlechten Daten bekannt und gelabelt, kann dann auch die Anwendung der Techniken aus Kapitel 3.2.3 auf S.49 untersucht werden.

Eine mögliche Weiterentwicklung betrifft auch das Dashboard, das im Zuge dieser Arbeit rudimentär als alleinstehende Übersicht skizziert wird. Jene Schaubilder des Dashboards sollten zukünftig in das bestehende GUI (Graphical User Interface) der Wärmebehandlungsanlage integriert werden. Hier gilt es auch zu prüfen, ob eine mobile Anwendung (Hand Held Devices) für das Instandhaltungspersonal einen Mehrwert im Betrieb schafft.

¹⁷⁴ vgl. Monostori et al., 2016, S.623

7 Anhang

7.1 Informationen zu Software Prototyp

Hier sind Informationen zur softwaretechnischen Umsetzung aus dem PoC dokumentiert. In der folgenden Tabelle 42 sind für die Anwendung des Phasenmodells in der Fallstudie die dazugehörigen Skripte angeführt. Die Skripte beinhalten alle Schritte des Phasenmodells: vom Preprocessing über die Anomalieerkennung bis hin zur Nachbereitung.

Tabelle 42: Dokumentation der Skripte für den Software Prototyp

Kapitel	Skriptname	Beschreibung
5.3.1.1	A1_HBOS_StatisticalAD	Jupyter Notebook für die statistische Anomalieerkennung mit dem HBOS Algorithmus.
5.3.1.2	A10_AllUnsupervisedAlgos_AD	Jupyter Notebook für die unüberwachte Anomalieerkennung mit LOF, kNN und kMeans.
5.3.1.3	A11_AllNoveltyDetectionAlgos_open	Jupyter Notebook, das die halbüberwachten Modelle auf Testdaten (PoC für Öffnungssignale) anwendet. Greift auf abgespeicherte/ trainierte Modell zu.
5.3.1.3	A3_LOF_NoveltyDetection_Training A7_Autoencoder_Training A8_OC-SVM_NoveltyDetection_Training A9_iForest_NoveltyDetection_Training	Trainingskripte für alle 4 halbüberwachten Algorithmen
5.3.1.4	A2_SignalGroupBased-iForest	Jupyter Notebook für den signalgruppenbasierten Ansatz, bei dem der iForest für die Anomalieerkennung angewandt wird.

7.2 Zusätzliche Darstellung für PoC der unüberwachten Ansätze

7.2.1 Darstellung zum statistischen Ansatz

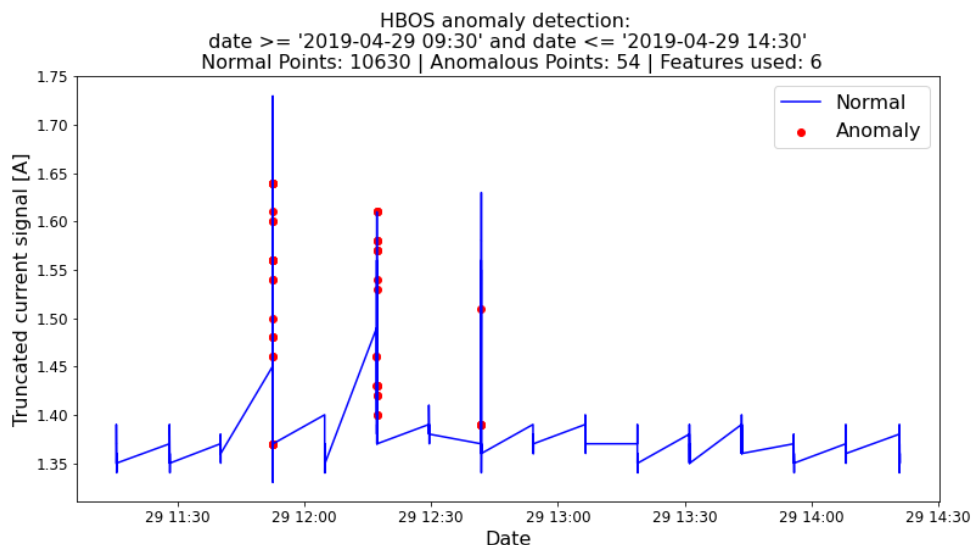


Abbildung 47: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS1

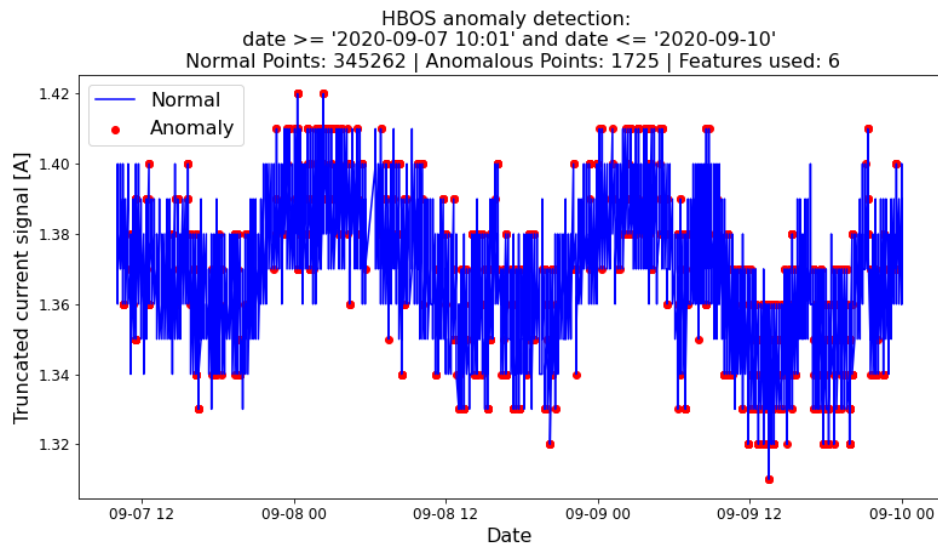


Abbildung 48: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS2

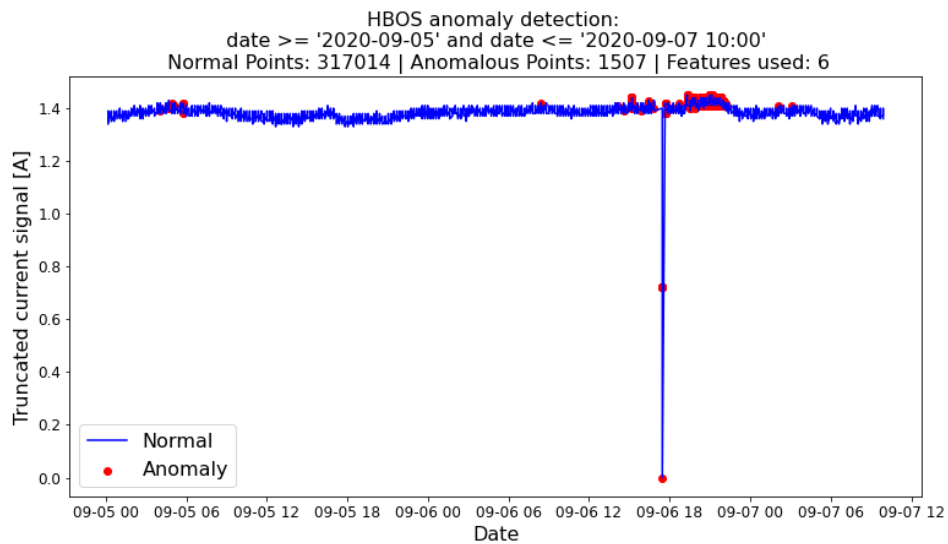


Abbildung 49: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS3

7.2.2 Darstellungen zum unüberwachten Ansatz

Unsupervised anomaly detection:
date >= '2019-04-29 09:30' and date <= '2019-04-29 14:30'

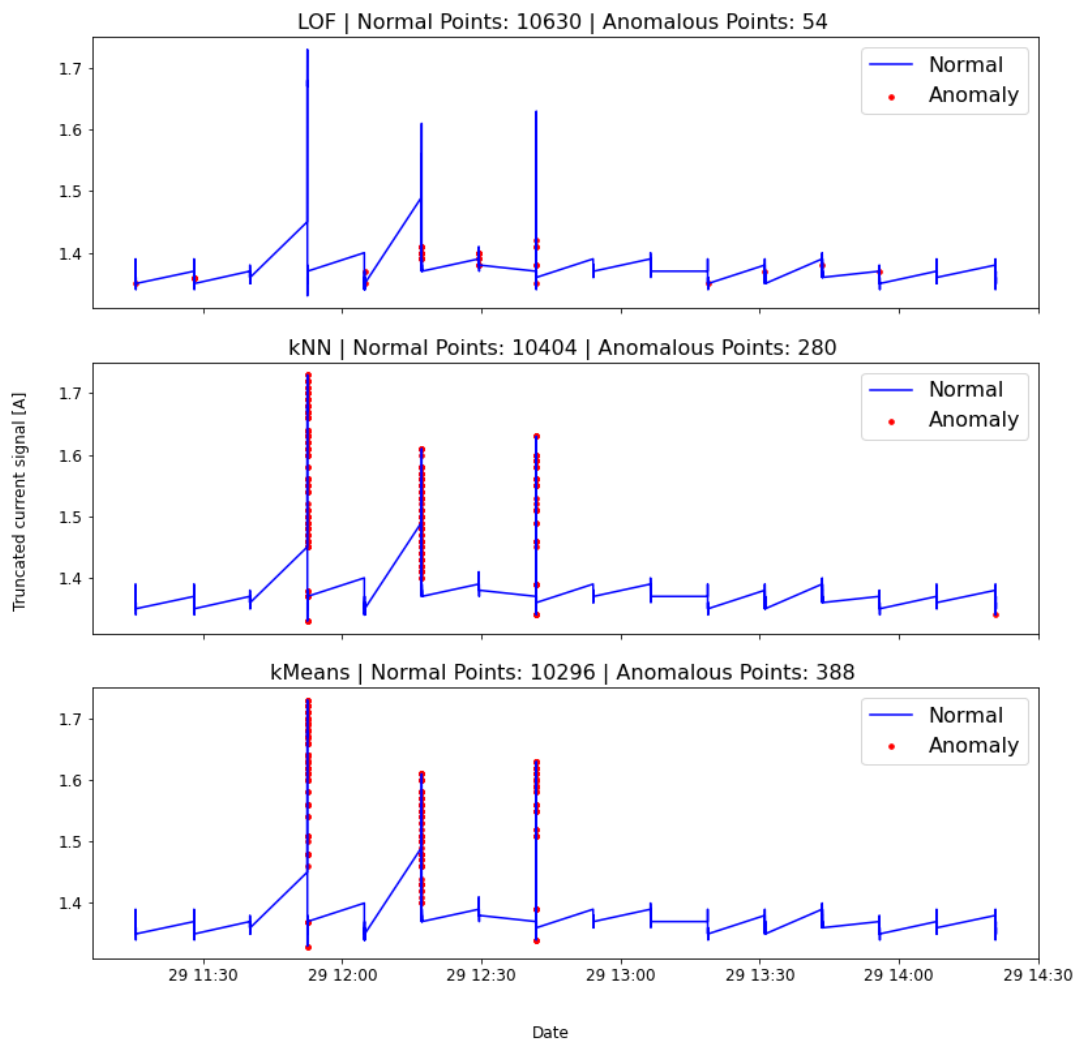


Abbildung 50: Darstellung Datensatz DS1 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen

Unsupervised anomaly detection:
date >= '2020-09-07 10:01' and date <= '2020-09-10'

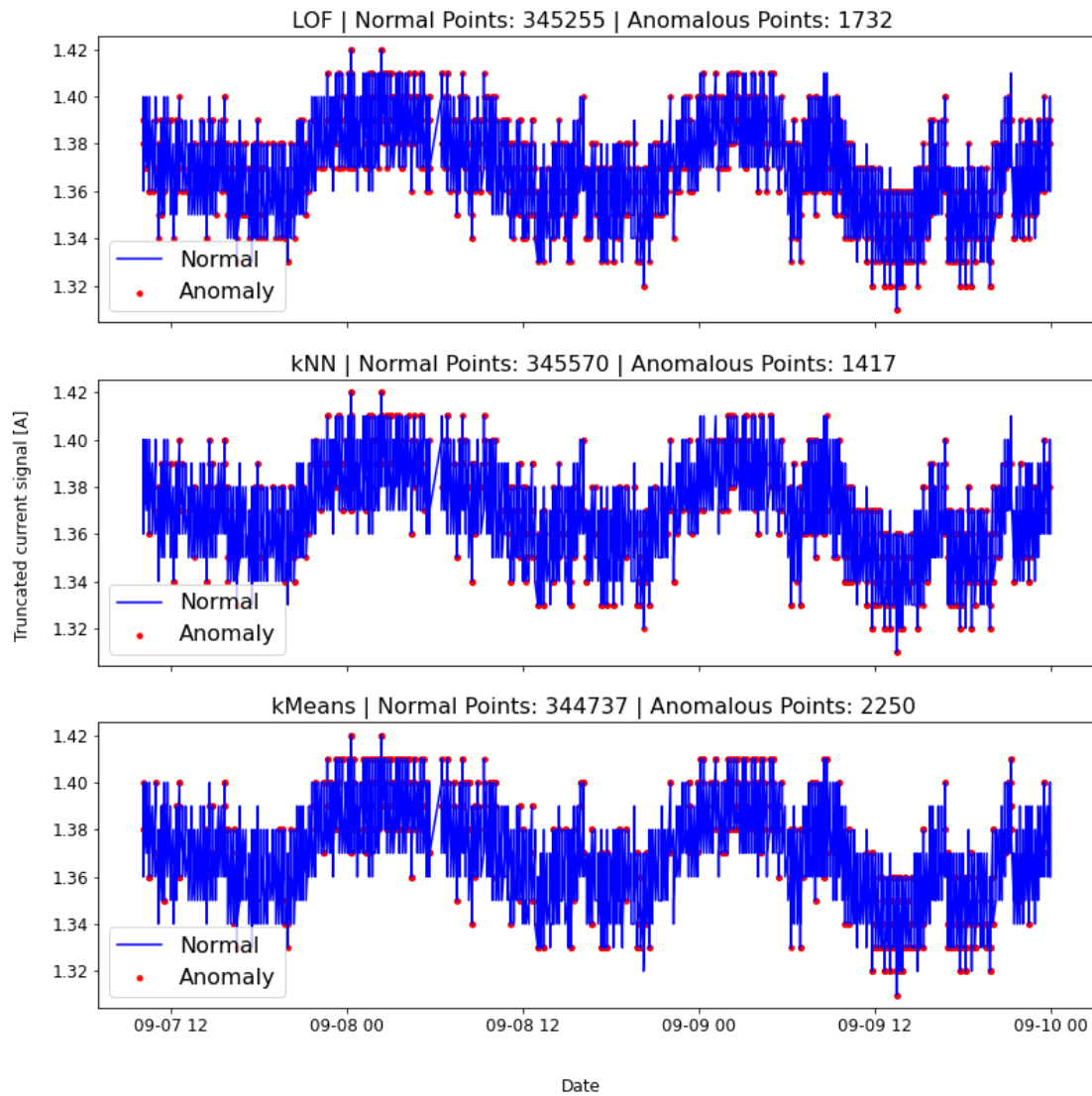


Abbildung 51: Darstellung Datensatz DS2 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen

Unsupervised anomaly detection:
date >= '2020-09-05' and date <= '2020-09-07 10:00'

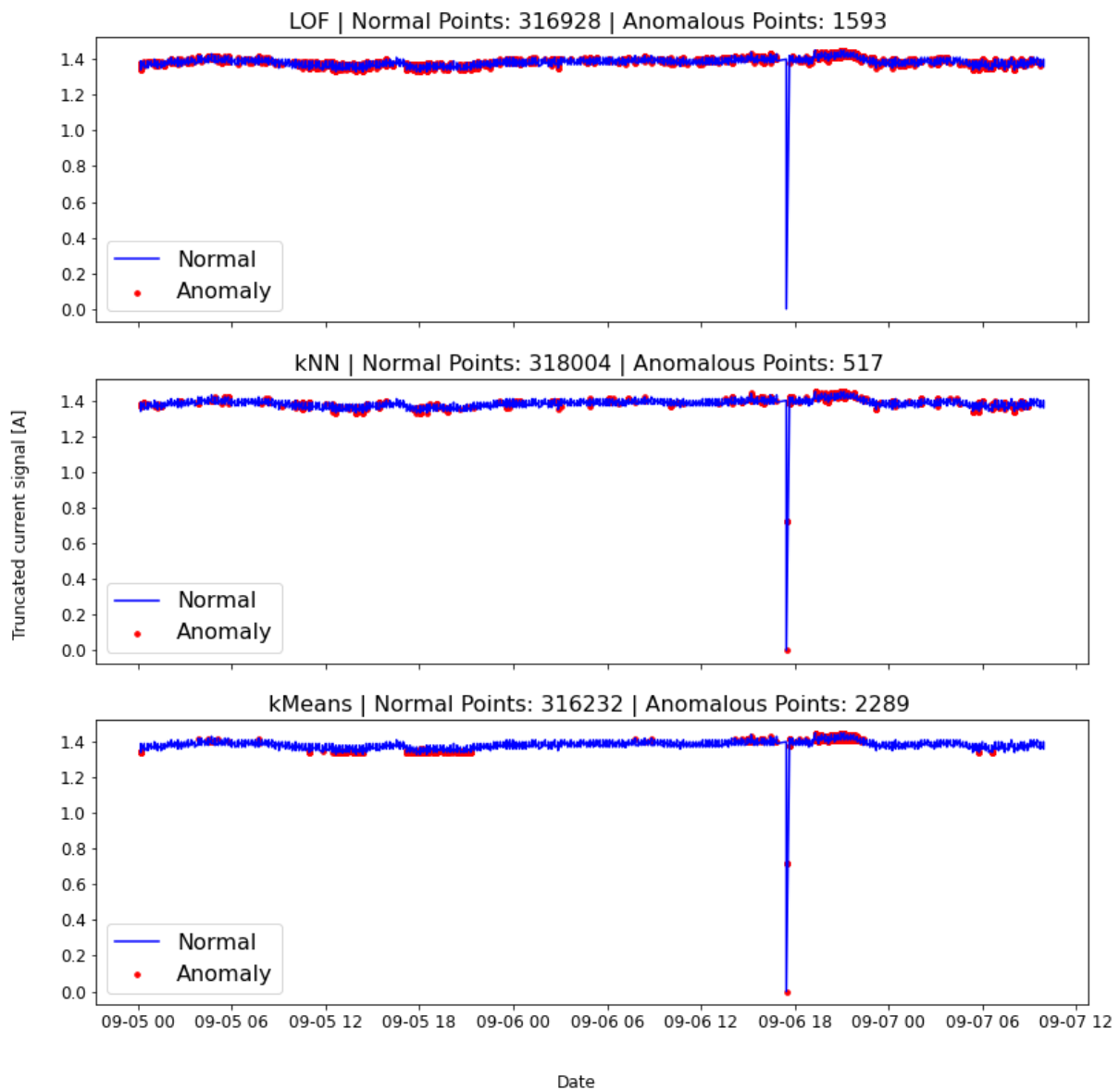


Abbildung 52: Darstellung Datensatz DS3 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen

7.2.3 Darstellungen zu den halbüberwachten Ansätzen

Semisupervised novelty detection:
 date >= '2019-04-29 09:30' and date <= '2019-04-29 14:30'

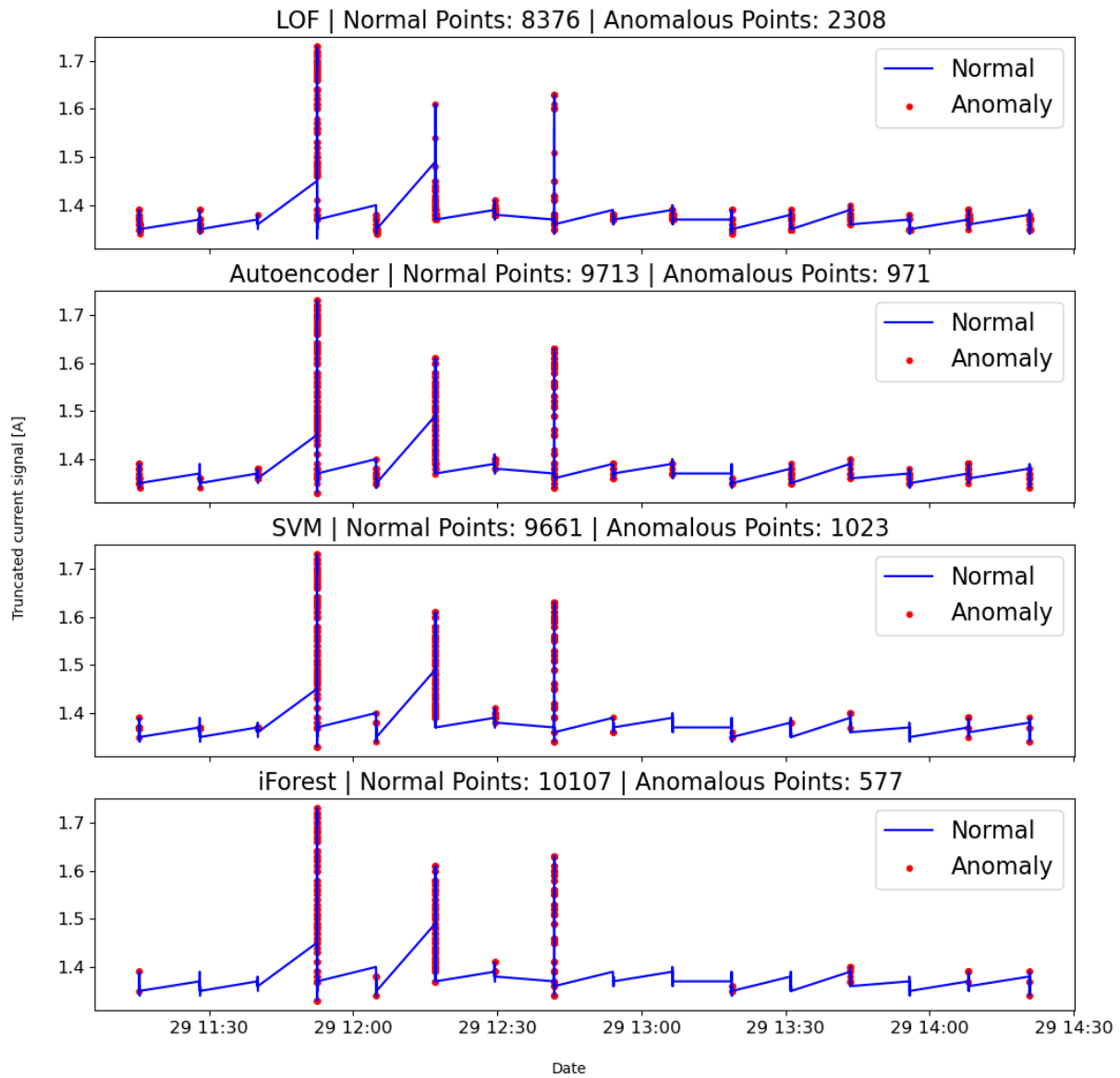


Abbildung 53: Darstellung Datensatz DS1 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen

Semisupervised novelty detection:
date >= '2020-09-07 10:01' and date <= '2020-09-10'

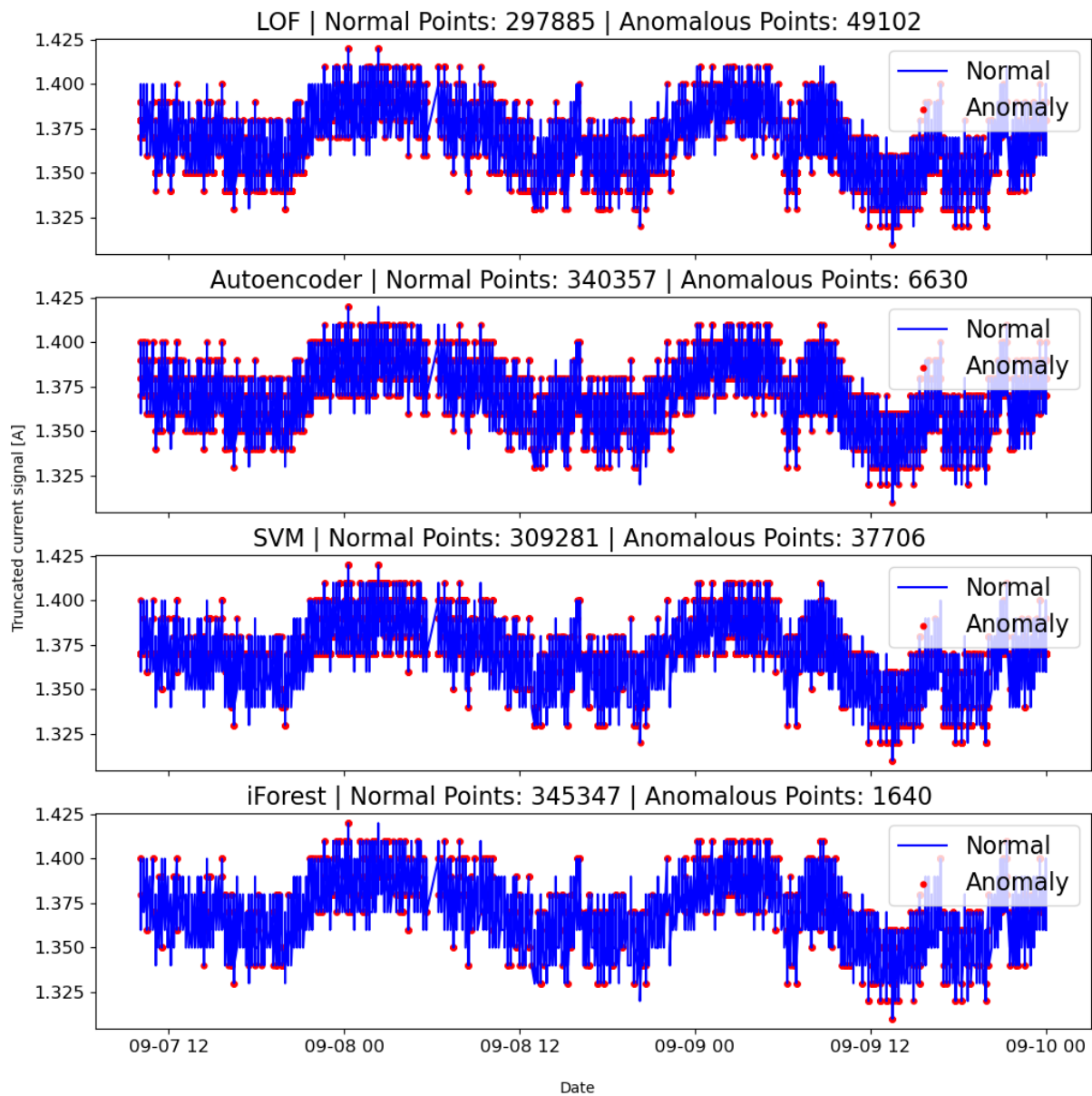


Abbildung 54: Darstellung Datensatz DS2 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen

Semisupervised novelty detection:
 date >= '2020-09-05' and date <= '2020-09-07 10:00'

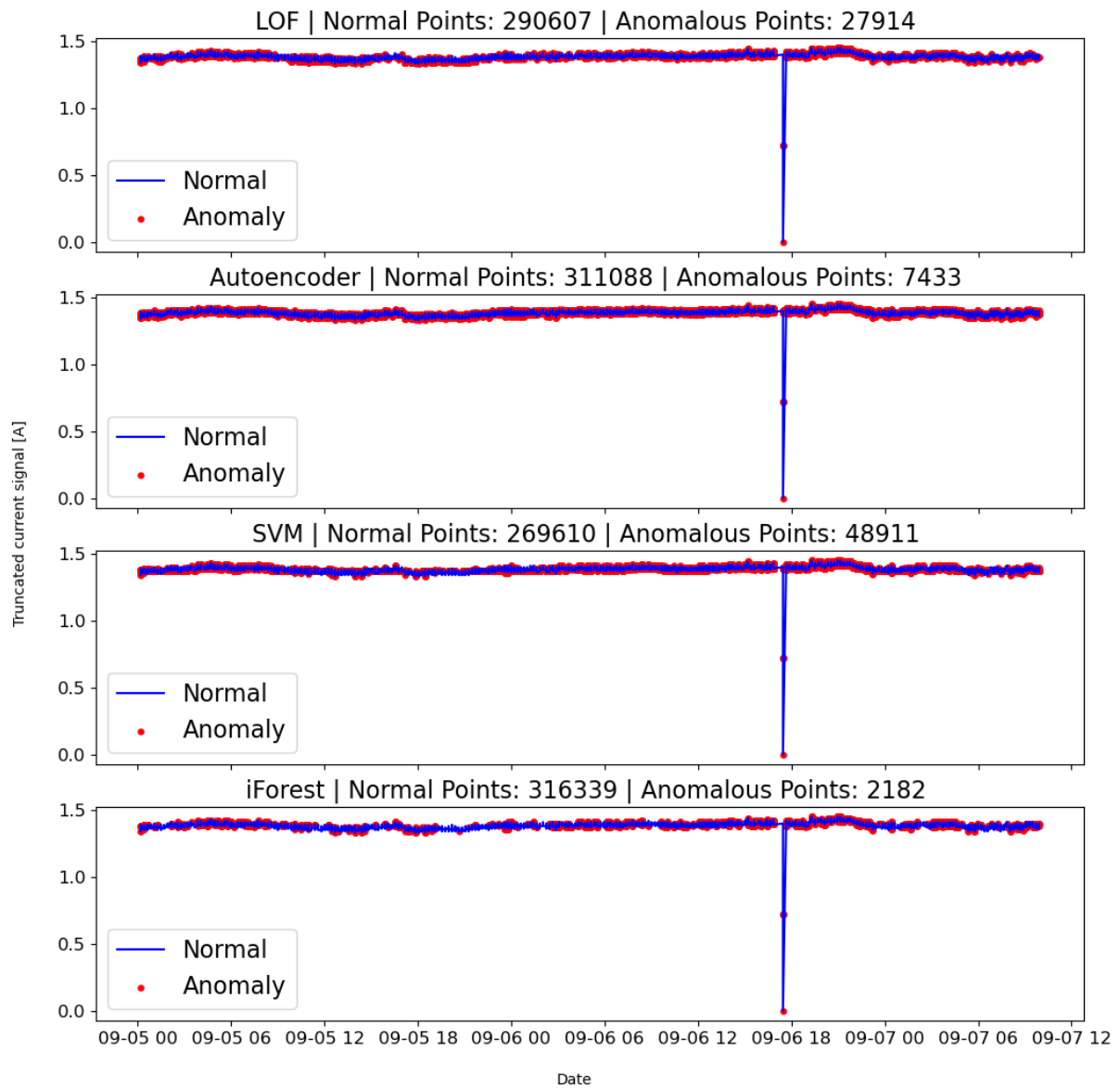


Abbildung 55: Darstellung Datensatz DS3 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen

7.2.4 Darstellungen zum signalgruppenbasierten Ansatz

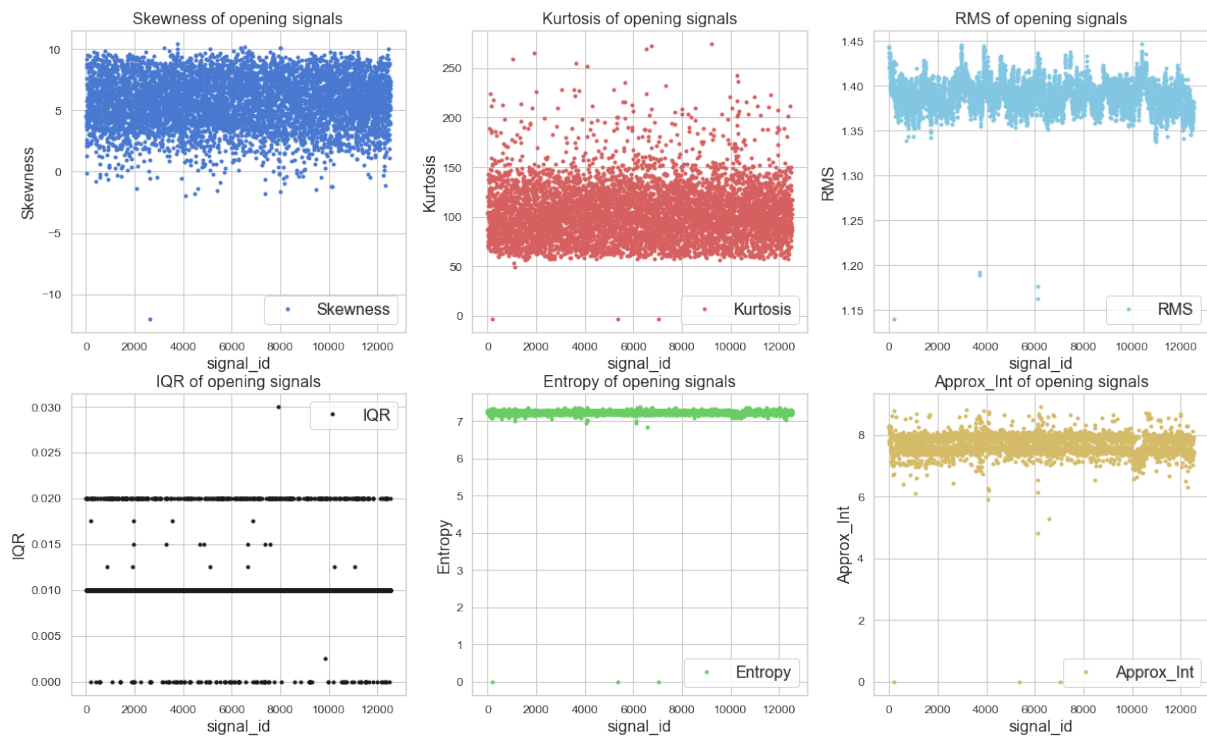


Abbildung 56: Ausgewählte Merkmale der Öffnungssignale aus DS5

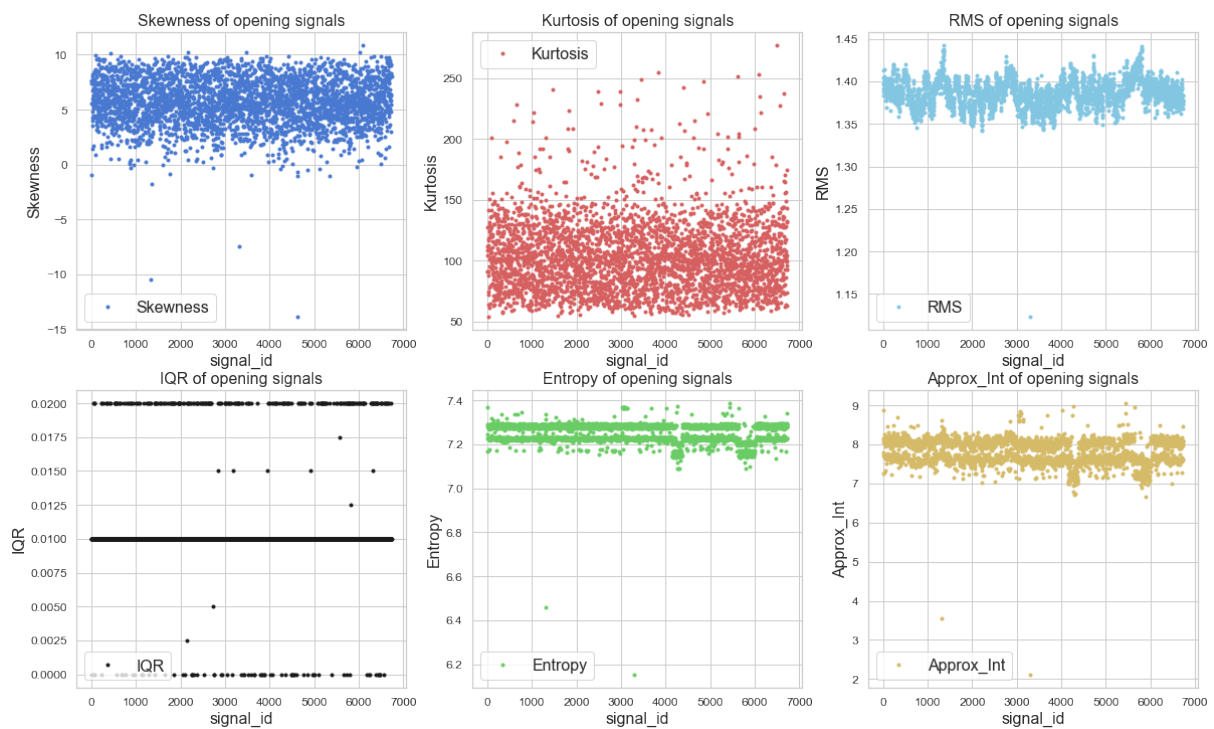


Abbildung 57: Ausgewählte Merkmale der Öffnungssignale aus DS6

7.2.5 Weitere Beispiele von Dashboards

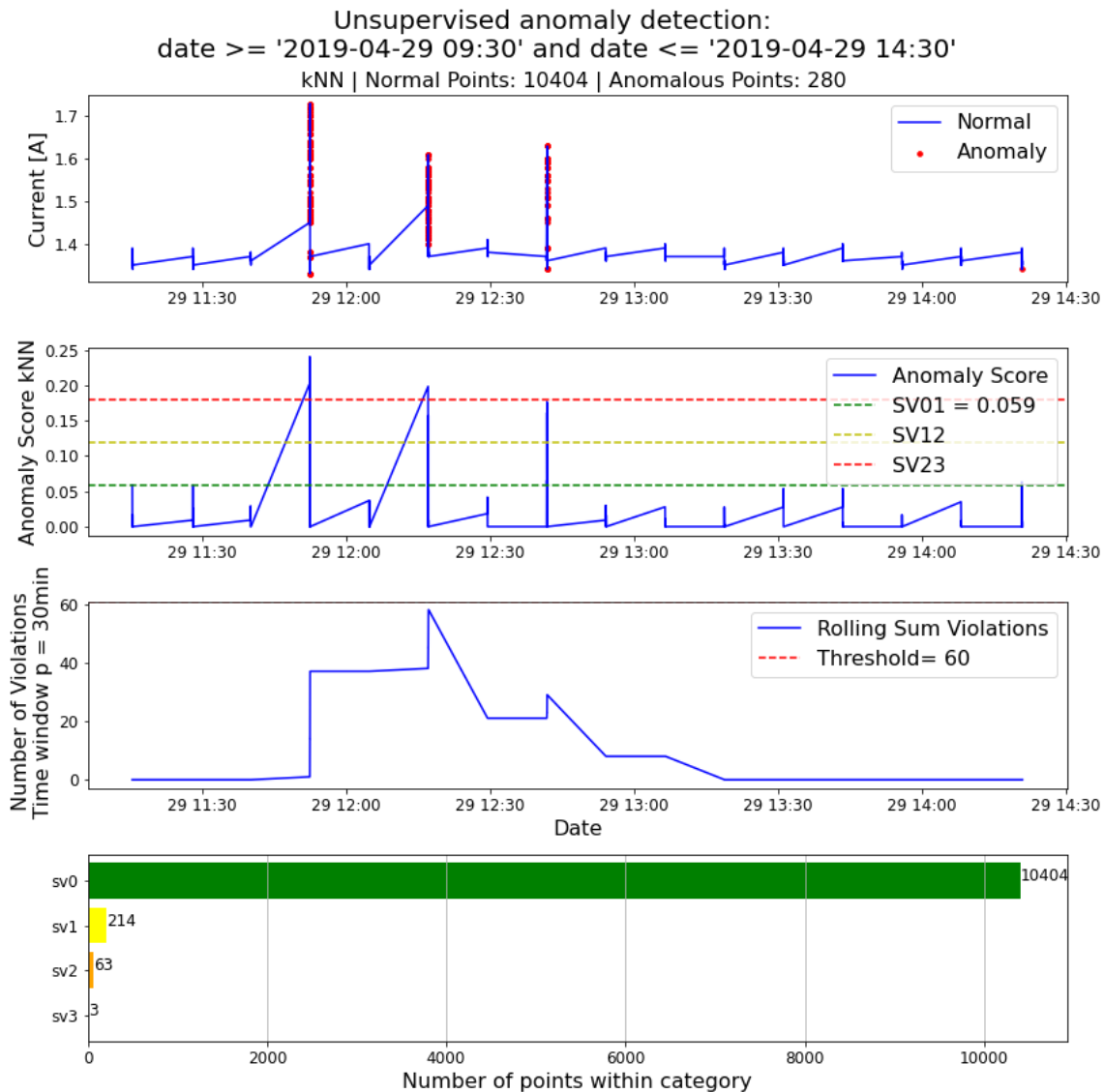


Abbildung 58: Beispiel eines Dashboards (kNN auf DS1 Öffnungssignal)

Für die Überwachung der Grenzwertüberschreitungen (drittes Schaubild in Abbildung 58) wurde eine Fensterlänge von 30 min gewählt, wie das in Kapitel 5.3.2 vorgeschlagen wird. Es kommt zu keiner Überschreitung des Alarmgrenzwertes (Threshold = 60). Würde z.B. 10 min gewählt werden, käme es tatsächlich zu einer Warnung, unter anderem weil sich auch der Alarmgrenzwert ändert – siehe folgendes Bild.

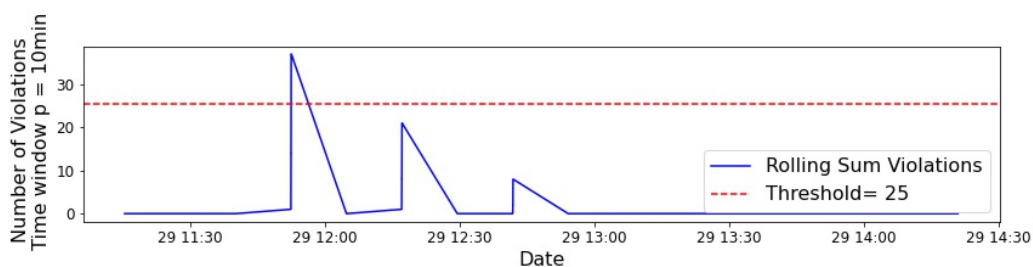


Abbildung 59: Alarmlogik mit p=10min (kNN auf DS1 Öffnungssignal)

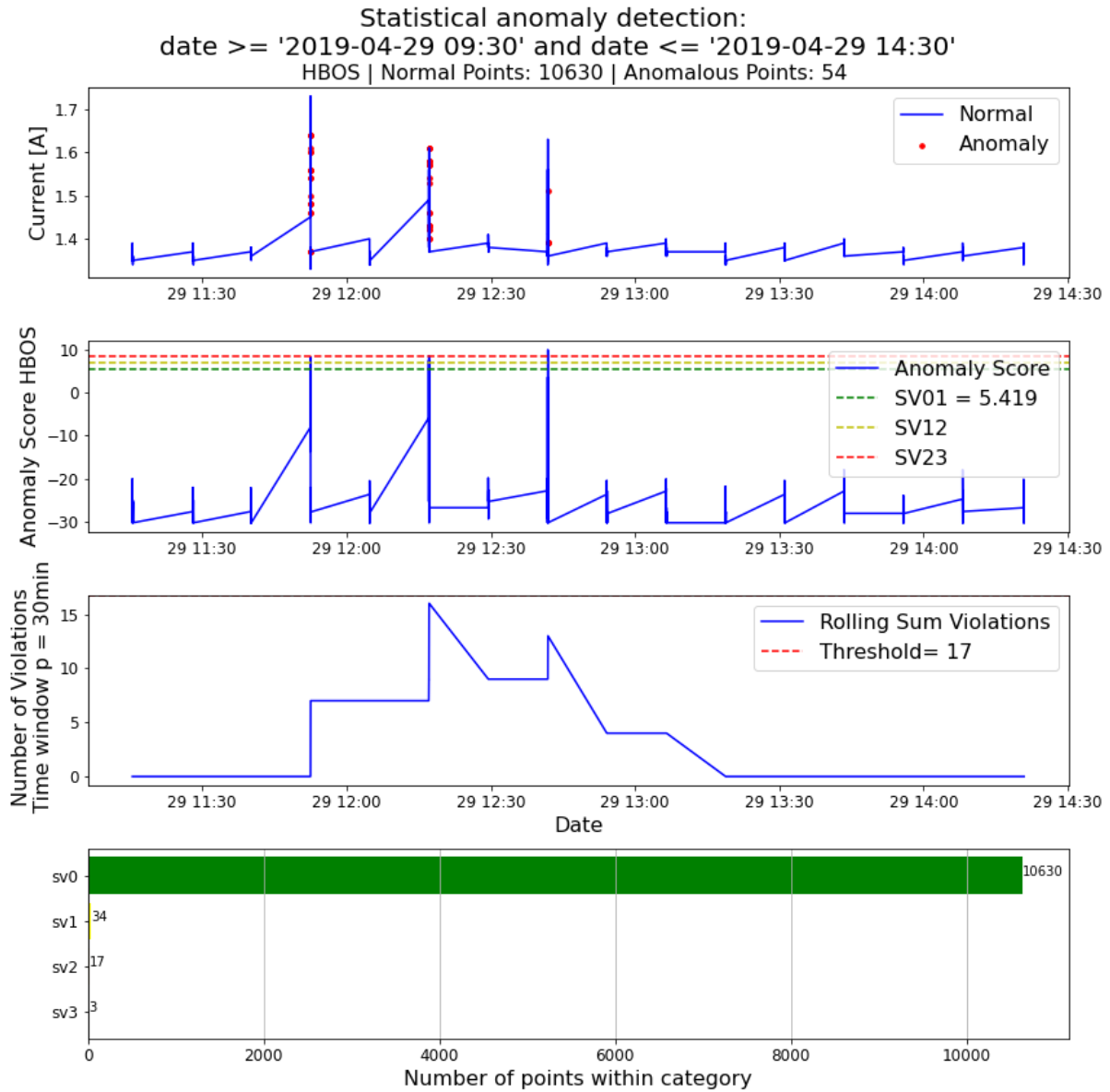


Abbildung 60: Beispiel eines Dashboards (HBOS auf DS1 Öffnungssignal)

7.2.6 Zusätzliche Darstellungen zu Kapitel 5.4.4

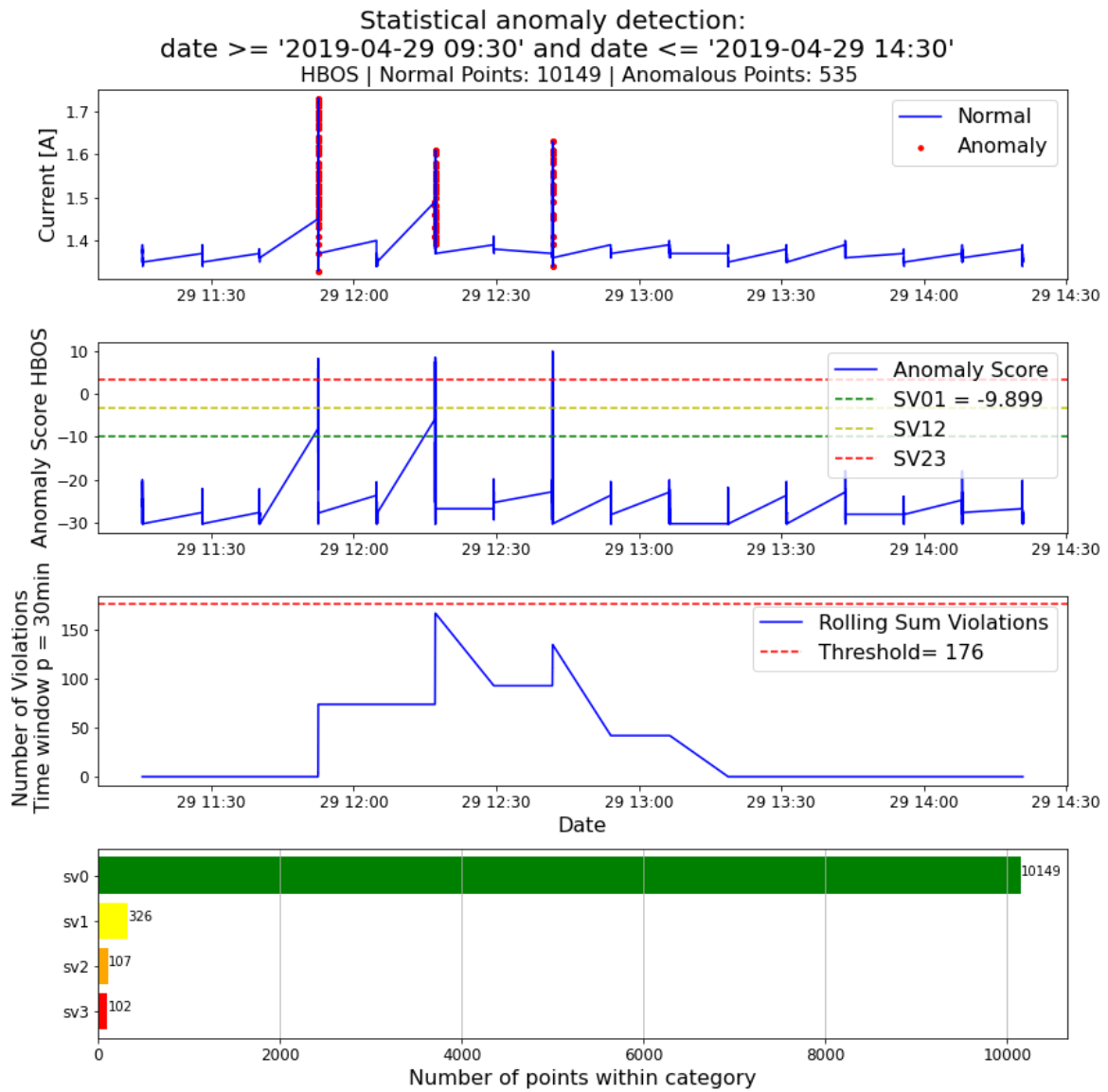


Abbildung 61: Beispiel eines Dashboards (HBOS mit Kontamination 0.05 auf DS1 Öffnungssignal, verbesserte Detektionsleistung)

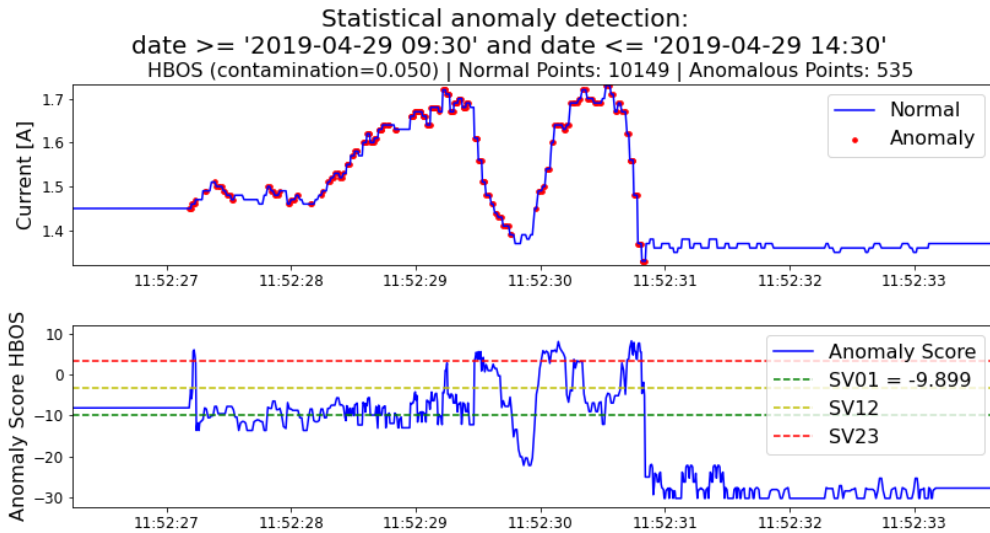


Abbildung 62: Vergrößerung auf 1. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal)

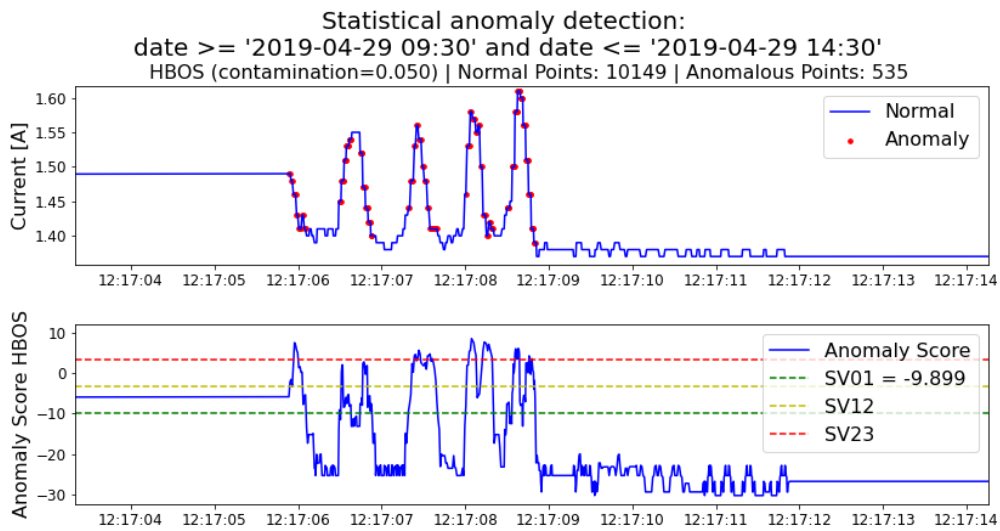


Abbildung 63: Vergrößerung auf 2. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal)

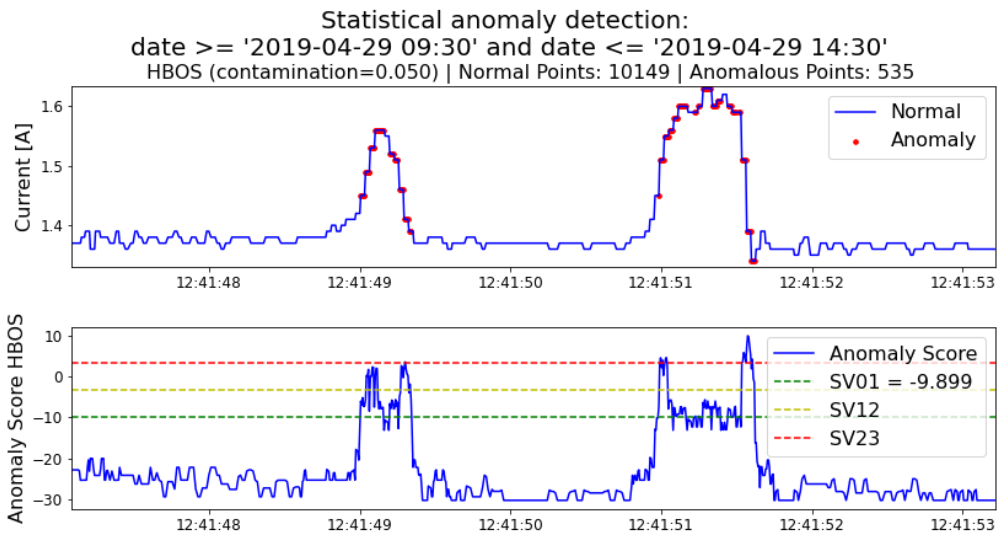


Abbildung 64: Vergrößerung auf 3. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal)

8 Literaturverzeichnis

- Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques. *Procedia Computer Science*, 60(1), 708–713. <https://doi.org/10.1016/j.procs.2015.08.220>
- Amer, M., Goldstein, M., & Abdennadher, S. (2013). Enhancing one-class Support Vector Machines for unsupervised anomaly detection. *Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description, ODD 2013*, 8–15. <https://doi.org/10.1145/2500853.2500857>
- Ansari, F., Glawar, R., & Nemeth, T. (2019). PriMa: a prescriptive maintenance model for cyber-physical production systems. *International Journal of Computer Integrated Manufacturing*, 32(4–5), 482–503. <https://doi.org/10.1080/0951192X.2019.1571236>
- Antonovskaya, G. N., Kapustian, N. K., Moshkunov, A. I., Danilov, A. V., & Moshkunov, K. A. (2017). New seismic array solution for earthquake observations and hydropower plant health monitoring. *Journal of Seismology*, 21(5), 1039–1053. <https://doi.org/10.1007/s10950-017-9650-8>
- Baasch, B., Gross, J. C., & Roth, M. (2018). Sensorgestützte Anomalie-Detektion zur Zustandsbewertung der Schiene mit Regelzügen. *ETR*, 12, 32–35.
- Bänsch, A., & Alewell, D. (2013). *Wissenschaftliches Arbeiten* (Vol. 11). Oldenbourg Wissenschaftsverlag GmbH.
- Baraldi, P., Canesi, R., Zio, E., Seraoui, R., & Chevalier, R. (2011). Signal grouping for condition monitoring of nuclear power plant components. *Advances in Safety, Reliability and Risk Management: ESREL 2011*, 1–13.
- Bichler, M. (2006). Design science in information systems research. *Wirtschaftsinformatik*, 48, 133–135. <https://doi.org/https://doi.org/10.1007/s11576-006-0028-8>
- Birla, S., Kohli, K., & Dutta, A. (2016). Machine Learning on imbalanced data in Credit Risk. *7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, IEEE IEMCON 2016*. <https://doi.org/10.1109/IEMCON.2016.7746326>
- Bonaldi, E. L., de Oliveira, L. E. de L., Moreira, F. dos S., Borges da Silva, L. E., Borges da Silva, J. G., & Lambert-Torres, G. (2014). Monitoring System for Auxiliary Motors in Thermal-Power Plants. *International Journal of Automation and Power Engineering*, 3(1), 53–57. <https://doi.org/10.14355/ijape.2014.0301.11>
- Braei, M., & Wagner, S. (2020). *Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art*. <http://arxiv.org/abs/2004.00433>
- Breitschopf, J. (2020). *A Procedural Model for Extracting Knowledge from Industrial Maintenance Reports*. Technische Universität Wien.
- Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Identifying Density-Based Local Outliers. *Proc. ACM SIGMOD 2000 Int. Conf. On Management of Data*.
- Carino, J. A., Delgado-Prieto, M., Zurita, D., Millan, M., Ortega Redondo, J. A., & Romero-Troncoso, R. (2016). Enhanced Industrial Machinery Condition Monitoring Methodology Based on Novelty Detection and Multi-Modal Analysis. *IEEE Access*, 4, 7594–7604. <https://doi.org/10.1109/ACCESS.2016.2619382>
- Cernuda, C. (2019). On the Relevance of Preprocessing in Predictive Maintenance for Dynamic Systems. In E. Lughofer (Ed.), *Predictive Maintenance in Dynamic Systems* (pp. 53–93). Springer Nature Switzerland AG. <https://doi.org/10.1007/978-3-030-05645-2>

- Chandola, V., Banerjee, A., & Kumarm, V. (2009). Anomaly detection: A Survey. *ACM Computing Surveys*, 1–22. <https://doi.org/10.1145/1541880.1541882>
- Chawla, N. V. (2010). Data Mining for Imbalanced Datasets: An Overview. In O. Maimon & L. Rokach (Eds.), *Data Mining and Knowledge Discovery Handbook* (2nd ed., pp. 875–886). Springer.
- Chebel-Morello, B., Nicod, J.-M., & Varnier, C. (2017). *From Prognostics and Health Systems Management to Predictive Maintenance 2* (7th ed.). Wiley. <https://doi.org/10.1002/9781119436805>
- Coble, J. B., Ramuhalli, P., Bond, L., Hines, J. W., & Upadhyaya, B. (2015). A review of prognostics and health management applications in nuclear power plants. *International Journal of Prognostics and Health Management*, 6(SP3), 1–22.
- Coble, J. B., Ramuhalli, P., Bond, L. J., Hines, W., & Upadhyaya, B. (2012). Prognostics and Health Management in Nuclear Power Plants: A Review of Technologies and Applications. *US Department of Energy*, 6(July), 1–22. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-21515.pdf
- CPS-Week. (2008). Cyber-Physical Systems Summit. *Cyper-Physical Systems Summit*, 19. http://iccps2012.cse.wustl.edu/_doc/CPS_Summit_Report.pdf
- Deistler, M., & Scherrer, W. (2018). Modelle der Zeitreihenanalyse. In *Mathematik Kompakt*. Birkhäuser. <http://link.springer.com/10.1007/978-3-319-68664-6>
- Demin, A. M., Naumenko, A. P., Gorchakova, A. A., & Odinets, A. I. (2020). Evaluation of Probability Errors in Condition Monitoring of Heat-Exchange Equipment. *Journal of Physics: Conference Series*, 1441(1). <https://doi.org/10.1088/1742-6596/1441/1/012055>
- DIN Deutsches Institut für Normung e.V. (2019). *DIN 31051 Grundlagen der Instandhaltung*. Beuth Verlag GmbH.
- Dorchain, M., & Schöning, H. (2017). Big Smart Data – Intelligent Operations, Analysis und Process Alignment. In B. Vogel-Heuser, T. Bauernhansel, & M. ten Hompel (Eds.), *Handbuch Industrie 4.0 Bd.2* (pp. 457–469). Springer Vieweg. <https://doi.org/10.1007/978-3-662-53248-5>
- Douzas, G., & Bacao, F. (2017). Self-Organizing Map Oversampling (SOMO) for imbalanced data set learning. *Expert Systems with Applications*, 82, 40–52. <https://doi.org/10.1016/j.eswa.2017.03.073>
- Egusquiza, M., Egusquiza, E., Valero, C., Presas, A., Valentín, D., & Bossio, M. (2018). Advanced condition monitoring of Pelton turbines. *Measurement*, 119, 46–55. <https://doi.org/10.1016/j.measurement.2018.01.030>
- Esmael, B., Arnaout, A., Fruhwirth, R. K., & Thonhauser, G. (2013). A Statistical Features Based Approach for Operations Recognition in Drilling Time Series. *International Journal of Computer Information Systems and Industrial Management Applications*, 5, 454–461.
- Ester, M., Kriegel, H.-P., Sander, J., & Xu, X. (1996). A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. *Proceeding of 2nd International Conference on Knowledge Discovery and Data Mining*, 226–231. <https://doi.org/10.11901/1005.3093.2016.318>
- Fast, M., & Palmé, T. (2010). Application of artificial neural networks to the condition monitoring and diagnosis of a combined heat and power plant. *Energy*, 35(2), 1114–1120. <https://doi.org/10.1016/j.energy.2009.06.005>

- Feng, Y., Wang, T., Hu, B., Yang, C., & Tan, J. (2020). An integrated method for high-dimensional imbalanced assembly quality prediction supported by edge computing. *IEEE Access*, 8, 71279–71290. <https://doi.org/10.1109/ACCESS.2020.2988118>
- Fernández, A., García, S., Galar, M., Krawczyk, B., Prati, R. C., & Herrera, F. (2018). *Learning from Imbalanced Datasets* (Vol. 21, Issue 9). Springer. <https://doi.org/10.1109/TKDE.2008.239>
- Fullen, M., Schuller, P., & Niggemann, O. (2017). Defining and validating similarity measures for industrial alarm flood analysis. *Proceedings - 2017 IEEE 15th International Conference on Industrial Informatics, INDIN 2017*, 781–786. <https://doi.org/10.1109/INDIN.2017.8104872>
- Fürst, P. (2020). *Univariate statistical monitoring of manufacturing components*.
- Ge, S., Jun, L., Datong, L., & Yu, P. (2015). Anomaly detection of condition monitoring with predicted uncertainty for aerospace applications. *2015 IEEE 12th International Conference on Electronic Measurement and Instruments, ICEMI 2015*, 1(3), 248–253. <https://doi.org/10.1109/ICEMI.2015.7494262>
- Genge, B., Haller, P., & Enachescu, C. (2019). Anomaly Detection in Aging Industrial Internet of Things. *IEEE Access*, 7, 74217–74230. <https://doi.org/10.1109/ACCESS.2019.2920699>
- Goeken, M. (Ed.). (2006). *Methode und Vorgehensmodell BT - Entwicklung von Data-Warehouse-Systemen: Anforderungsmanagement, Modellierung, Implementierung* (pp. 51–67). DUV. https://doi.org/10.1007/978-3-8350-9178-8_3
- Gofuku, A. (2014). Integrated diagnostic technique for nuclear power plants. *Nuclear Engineering and Technology*, 46(6), 725–736. <https://doi.org/10.5516/NET.04.2014.719>
- Goldstein, M., & Dengel, A. (2012). Histogram-based outlier score (HBOS): A fast unsupervised anomaly detection algorithm. *KI-2012: Poster and Demo Track*, 1, 59–63. [http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Histogram-based+Outlier+Score+\(+HBOS+\):+A+fast+Unsupervised+Anomaly+Detection+Algorithm#0](http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Histogram-based+Outlier+Score+(+HBOS+):+A+fast+Unsupervised+Anomaly+Detection+Algorithm#0)
- Granjon, P. (2011). Condition monitoring of motor-operated valves in nuclear power plants. *8th International Conference on Condition Monitoring and Machinery Failure Prevention Technologies 2011, CM 2011/MFPT 2011*, 1, 109–119.
- Güntner, G., Benisch, M., Dankl, A., & Isopp, J. (2015). *Roadmap der Instandhaltung 4.0*.
- Haixiang, G., Yijing, L., Shang, J., Mingyun, G., Yuanyue, H., & Bing, G. (2017). Learning from class-imbalanced data: Review of methods and applications. *Expert Systems with Applications*, 73, 220–239. <https://doi.org/10.1016/j.eswa.2016.12.035>
- Hendrickx, K., Meert, W., Mollet, Y., Gyselinck, J., Cornelis, B., Gryllias, K., & Davis, J. (2020). A general anomaly detection framework for fleet-based condition monitoring of machines. *Mechanical Systems and Signal Processing*, 139. <https://doi.org/10.1016/j.ymssp.2019.106585>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Hevner, B. A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information System. *MIS Quarterly*, 28(1), 75–105.

- Hodge, V., & Austin, J. (2004). A Survey of Outlier Detection Methodologies. *Artificial Intelligence Review*. <https://doi.org/10.1023/B>
- Hofmockel, J. (2019). *Anomalieerkennung in Kommunikationsdaten zur Datenselektion im Fahrzeug*. Karlsruhe Institut für Technologie.
- Isermann, R. (2011). *Fault-Diagnosis Applications*. Springer-Verlag Berlin Heidelberg.
- Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, 20(7), 1483–1510. <https://doi.org/10.1016/j.ymssp.2005.09.012>
- Jin, X., Guo, Y., Sarkar, S., Ray, A., & Edwards, R. M. (2011). Anomaly detection in nuclear power plants via symbolic dynamic filtering. *IEEE Transactions on Nuclear Science*, 58(1 PART 2), 277–288.
- Kamat, P., & Sugandhi, R. (2020). Anomaly detection for predictive maintenance in industry 4.0-A survey. *E3S Web of Conferences*, 170(May), 0–8. <https://doi.org/10.1051/e3sconf/202017002007>
- Kammerer, K., Hoppenstedt, B., Pryss, R., Stöckler, S., Allgaier, J., & Reichert, M. (2019). Anomaly detections for manufacturing systems based on sensor data—insights into two challenging real-world production settings. *Sensors (Switzerland)*, 19(24). <https://doi.org/10.3390/s19245370>
- Karner, M. (2019). *Phasenmodell zur Entwicklung einer werkzeug- und maschinenzustandsbedingten Produktionsreihenfolgeoptimierung* (Vol. 1). Technische Universität Wien.
- Kaur, H., Pannu, H. S., & Malhi, A. K. (2019). A systematic review on imbalanced data challenges in machine learning: Applications and solutions. *ACM Computing Surveys*, 52(4).
- Kendig, C. E. (2016). What is Proof of Concept Research and how does it Generate Epistemic and Ethical Categories for Future Scientific Practice? *Science and Engineering Ethics*, 22(3), 735–753. <https://doi.org/10.1007/s11948-015-9654-0>
- Klun, M., Zupan, D., Lopatič, J., & Kryžanowski, A. (2019). On the application of laser vibrometry to perform structural health monitoring in non-stationary conditions of a hydropower dam. *Sensors*, 19(17), 1–13. <https://doi.org/10.3390/s19173811>
- Krawczyk, B. (2016). Learning from imbalanced data: open challenges and future directions. *Progress in Artificial Intelligence*, 5(4), 221–232. <https://doi.org/10.1007/s13748-016-0094-0>
- Krig, S. (2014). *Computer Vision Metrics: Survey, Taxonomy, and Analysis*. Apress.
- Lahdelma, S., & Juuso, E. (2011). Trend analysis in condition monitoring of process equipments. *8th International Conference on Condition Monitoring and Machinery Failure Prevention Technologies 2011, CM 2011/MFPT 2011*, 2(2), 904–913.
- Lapira, E., Brisset, D., Davari Ardakani, H., Siegel, D., & Lee, J. (2012). Wind turbine performance assessment using multi-regime modeling approach. *Renewable Energy*, 45, 86–95.
- Lin, W. C., Tsai, C. F., Hu, Y. H., & Jhang, J. S. (2017). Clustering-based undersampling in class-imbalanced data. *Information Sciences*, 409–410, 17–26. <https://doi.org/10.1016/j.ins.2017.05.008>

- Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. *Proceedings - IEEE International Conference on Data Mining, ICDM*, 413–422. <https://doi.org/10.1109/ICDM.2008.17>
- Liu, J., Seraoui, R., Vitelli, V., & Zio, E. (2013). Nuclear power plant components condition monitoring by probabilistic support vector machine. *Annals of Nuclear Energy*, 56, 23–33. <https://doi.org/10.1016/j.anucene.2013.01.005>
- Liu, L., Peng, Y., Wang, L., Dong, Y., Liu, D., & Guo, Q. (2020). Improving EGT sensing data anomaly detection of aircraft auxiliary power unit. *Chinese Journal of Aeronautics*, 33(2), 448–455. <https://doi.org/10.1016/j.cja.2019.10.001>
- Lu, Q., Xie, X., Parlikad, A. K., & Schooling, J. M. (2020). Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance. *Automation in Construction*, 118(March), 103277.
- Lu, W., Li, Z., & Chu, J. (2017). A novel computer-aided diagnosis system for breast MRI based on feature selection and ensemble learning. *Computers in Biology and Medicine*, 83(September 2016), 157–165. <https://doi.org/10.1016/j.combiomed.2017.03.002>
- Ma, J., & Jiang, J. (2011). Applications of fault detection and diagnosis methods in nuclear power plants: A review. *Progress in Nuclear Energy*, 53(3), 255–266. <https://doi.org/10.1016/j.pnucene.2010.12.001>
- Madreiter, T. (2020). *Design and Development of a Prototype of a Text Understanding Tool for Maintenance 4.0 by Measuring Associations, Readability and Sentiment (TU-MARS)*. Technische Universität Wien.
- Mahdiyah, U., Irawan, M. I., & Imah, E. M. (2015). Integrating Data Selection and Extreme Learning Machine for Imbalanced Data. *Procedia Computer Science*, 59, 221–229. <https://doi.org/10.1016/j.procs.2015.07.561>
- Mao, W., Zhang, D., Tian, S., & Tang, J. (2020). Robust detection of bearing early fault based on deep transfer learning. *Electronics (Switzerland)*, 9(2), 1–27. <https://doi.org/10.3390/electronics9020323>
- Marais, H.-J., van Schoor, G., & Uren, K. R. (2016). Energy-base Fault Detection for an Autothermal Reformer. *IFAC-PapersOnLine*, 49(7), 353–358.
- Matyas, K. (2018). *Instandhaltungslogistik - Qualität und Produktivität steigern* (7th ed.). Carl Hanser Fachbuchverlag.
- Mehairjan, R. P. Y. (2017). Risk-Based Maintenance for Electricity Network Organizations. In *Risk-Based Maintenance for Electricity Network Organizations*. Springer. <https://doi.org/10.1007/978-3-319-49235-3>
- Mobley, R. K. (2002). *An Introduction to Predictive Maintenance* (2nd ed.). Elsevier Science.
- Monkova, K., Monka, P. P., Hric, S., Kozak, D., Katinič, M., Pavlenko, I., & Liaposchenko, O. (2020). Condition monitoring of Kaplan turbine bearings using vibro-diagnostics. *International Journal of Mechanical Engineering and Robotics Research*, 9(8), 1182–1188. <https://doi.org/10.18178/ijmerr.9.8.1182-1188>
- Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*, 65(2), 621–641. <https://doi.org/10.1016/j.cirp.2016.06.005>
- Moubray, J. (1996). *RCM - die hohe Schule der Zuverlässigkeit von Produkten und Systemen*. Verlag Moderne Industrie.

- Nemeth, T. (2020). *Vorgehensmodell zur Einführung einer präskriptiven Instandhaltungsstrategie und Reifegradbewertung unter Zuhilfenahme von Qualitätsmetriken*. Technische Universität Wien.
- o. V. (2013). *Empfehlung zu einer optimierten Proof-of-Concept-Unterstützung im Wissenstransfer*. Rat für Forschung und Technologieentwicklung. https://www.rat-fte.at/files/rat-fte-pdf/einzelempfehlungen/2013/131203_Empfehlung_Proof_of_Concept.pdf
- Pahl/ Beitz Konstruktionslehre. (2013). In J. Feldhusen & K.-H. Grote (Eds.), *Handbuch Produktentwicklung* (8th ed.). Springer Vieweg. <https://doi.org/10.3139/9783446445819.005>
- Papaelias, M., Cheng, L., Kogia, M., Mohimi, A., Kappatos, V., Selcuk, C., Constantinou, L., Muñoz, C. Q. G., Marquez, F. P. G., & Gan, T. H. (2016). Inspection and Structural Health Monitoring techniques for Concentrated Solar Power plants. *Renewable Energy*, 85(2016), 1178–1191. <https://doi.org/10.1016/j.renene.2015.07.090>
- Parsa, A. B., Taghipour, H., Derrible, S., & Mohammadian, A. (Kouros). (2019). Real-time accident detection: Coping with imbalanced data. *Accident Analysis and Prevention*, 129(May), 202–210. <https://doi.org/10.1016/j.aap.2019.05.014>
- Pawallek, G. (2016). *Integrierte Instandhaltung und Ersatzteillogistik* (2nd ed.). Springer-Verlag Berlin Heidelberg.
- Pecht, M. G., & Kang, M. (2018). Prognostics and Health Management of Electronics. In *Prognostics and Health Management of Electronics* (1st ed.). Wiley. <https://doi.org/10.1002/9780470385845>
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Picek, S., Heuser, A., Jovic, A., Bhasin, S., & Regazzoni, F. (2019). The Curse of Class Imbalance and Conflicting Metrics with Machine Learning for Side-channel Evaluations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(1), 209–237. <https://doi.org/10.46586/tches.v2019.i1.209-237>
- Polycarpou, M., Ellinas, G., Kyriakides, E., & Panayiotou, C. (2010). Intelligent health monitoring of critical infrastructure systems. *COMPENG 2010 - Complexity in Engineering*, 18–20.
- Pourpanah, F., Zhang, B., Ma, R., & Hao, Q. (2018). Anomaly Detection and Condition Monitoring of UAV Motors and Propellers. *Proceedings of IEEE Sensors*, 1–4. <https://doi.org/10.1109/ICSENS.2018.8589572>
- Quatrini, E., Costantino, F., Di Gravio, G., & Patriarca, R. (2020). Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities. *Journal of Manufacturing Systems*, 56(May), 117–132. <https://doi.org/10.1016/j.jmsy.2020.05.013>
- Ramdhani, A., Ramdhani, M. A., & Amin, A. S. (2014). Writing a Literature Review Research Paper: A step-by-step approach. *International Journal of Basic and Applied Science*, 03(01), 47–56.
- Ratanamahatana, C. A., Lin, J., Gunopulos, D., Keogh, E., Vlachos, M., & Das, G. (2010). Mining Time Series Data. In O. Maimon & L. Rokach (Eds.), *Data Mining and Knowledge Discovery Handbook* (2nd ed., pp. 1049–1077). Springer. https://doi.org/10.1007/978-3-540-72680-7_5

- Renström, N., Bangalore, P., & Highcock, E. (2020). System-wide anomaly detection in wind turbines using deep autoencoders. *Renewable Energy*, 157, 647–659. <https://doi.org/10.1016/j.renene.2020.04.148>
- Russel, S. J., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3rd ed.). Prentice Hall.
- Santos, P., Maudes, J., & Bustillo, A. (2015). Identifying maximum imbalance in datasets for fault diagnosis of gearboxes. *Journal of Intelligent Manufacturing*, 29(2), 333–351. <https://doi.org/10.1007/s10845-015-1110-0>
- Sanz, J. A., Bernardo, D., Herrera, F., Bustince, H., & Hagrais, H. (2015). A Compact Evolutionary Interval-Valued Fuzzy Rule-Based Classification System for the Modeling and Prediction of Real-World Financial Applications with Imbalanced Data. *IEEE Transactions on Fuzzy Systems*, 23(4), 973–990. <https://doi.org/10.1109/TFUZZ.2014.2336263>
- Schacht, S., & Lanquillon, C. (2019). *Blockchain und maschinelles Lernen*. Springer Vieweg. <https://doi.org/10.1007/978-3-662-60408-3>
- Schenk, M. (2010). *Instandhaltung technischer Systeme*. Springer-Verlag. <https://doi.org/10.1007/978-3-642-03949-2>
- Schölkopf, B., Williamson, R., Smola, A., Shawe-Taylor, J., & Platt, J. (1999). Support vector method for novelty detection. *Advances in Neural Information Processing Systems*, 582–588.
- Shameer, V. H., & Shameer, K. M. (2013). Proactive condition Monitoring Systems for Power Plants. *International Journal of Scientific and Research Publications*, 3(11), 1–5.
- Shumaker, B. D., Campbell, C. J., Sexton, C. D., Morton, G. W., McConkey, J. B., & Hashemian, H. M. (2012). Cable condition monitoring for nuclear power plants. *FIIW 2012 - 2012 Future of Instrumentation International Workshop Proceedings*, 97–100. <https://doi.org/10.1109/FIIW.2012.6378325>
- Steck-Winter, H. (2008). Integratives Instandhaltungsmanagement von Thermoprosessanlagen. *GASWÄRME International*, 57(7–8), 1–8.
- Steck-Winter, H., Stölting, C., & Unger, G. (2017). Vorausschauende Instandhaltung mit datengetriebener Zustandsüberwachung - Teil 1. *GASWÄRME International*, 66(5), 87–95.
- Steck-Winter, H., & Unger, G. (2020). Vorausschauende Instandhaltung für Thermoprosessanlagen - Teil 1: Anomaliekennung. *PROZESSWÄRME*, 01, 39–47.
- Strauß, P., Schmitz, M., Wöstmann, R., & Deuse, J. (2018). Enabling of Predictive Maintenance in the Brownfield through Low-Cost Sensors, an IIoT-Architecture and Machine Learning. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 1474–1483. <https://doi.org/10.1109/BigData.2018.8622076>
- Suzuki, T., Noda, T., Shibuya, H., & Suzuki, H. (2014). An anomaly detection system for advanced maintenance services. *Hitachi Review*, 63(4), 178–182.
- Tang, M., Ding, S. X., Yang, C., Cheng, F., Shardt, Y. A. W., Long, W., & Liu, D. (2019). Cost-sensitive large margin distribution machine for fault detection of wind turbines. *Cluster Computing*, 22(s3), 7525–7537. <https://doi.org/10.1007/s10586-018-1854-3>
- Theisen, M. R. (2017). *Wissenschaftliches Arbeiten: Erfolgreich bei Bachelor- und Masterarbeit* (17.). Verlag Franz Vahlen München.

- Traphöner, R. (2018). *Industrial Analytics : Von Daten zur Aktion*. In *Das industrielle Internet der Dinge und Industrie 4.0*. KS-Energy-Verlag.
- Valero, C., Egusquiza, E., Presas, A., Valentín, D., Egusquiza, M., & Bossio, M. (2017). Condition monitoring of a prototype turbine. Description of the system and main results. *Journal of Physics: Conference Series*, 813(1). <https://doi.org/10.1088/1742-6596/755/1/011001>
- Vluymans, S. (2019). *Dealing with Imbalanced and Weakly Labelled Data in Machine Learning using Fuzzy and Rough Set Methods*. Springer Nature Switzerland AG. <http://www.springer.com/series/7092>
- Wang, B., & Mao, Z. (2018). Detecting Outliers in Electric Arc Furnace under the Condition of Unlabeled, Imbalanced, Non-stationary and Noisy Data. *Measurement and Control (United Kingdom)*, 51(3–4), 83–93. <https://doi.org/10.1177/0020294018771097>
- Wang, H. (2020a). Unsupervised anomaly detection in railway catenary condition monitoring using autoencoders. *IECON Proceedings (Industrial Electronics Conference), 2020-October(October)*, 2636–2641. <https://doi.org/10.1109/IECON43393.2020.9254633>
- Wang, H. (2020b). Unsupervised anomaly detection in railway catenary condition monitoring using autoencoders Delft University of Technology Unsupervised anomaly detection in railway catenary condition monitoring using autoencoders. *The 46th Annual Conference of the IEEE Industrial Electronics Society, October*.
- Weber, F. (2020). *Künstliche Intelligenz Für Business Analytics* [Book]. Springer Fachmedien Wiesbaden GmbH.
- Xiao, J., Zhang, M., Tian, H., Huang, B., & Fu, W. (2018). Prognostics and health management system for hydropower plant based on fog computing and docker container. *IOP Conference Series: Earth and Environmental Science*, 121(4). <https://doi.org/10.1088/1755-1315/121/4/042029>
- Yan, Y., Chen, M., Shyu, M. L., & Chen, S. C. (2016). Deep Learning for Imbalanced Multimedia Data Classification. *Proceedings - 2015 IEEE International Symposium on Multimedia, ISM 2015*, 483–488. <https://doi.org/10.1109/ISM.2015.126>
- Zeng, X. J., Yang, M., & Bo, Y. F. (2020). Gearbox oil temperature anomaly detection for wind turbine based on sparse Bayesian probability estimation. *International Journal of Electrical Power and Energy Systems*, 123(April). <https://doi.org/10.1016/j.ijepes.2020.106233>
- Zhang, Y., Dong, Z. Y., Kong, W., & Meng, K. (2020). A Composite Anomaly Detection System for Data-Driven Power Plant Condition Monitoring. *IEEE Transactions on Industrial Informatics*, 16(7), 4390–4402. <https://doi.org/10.1109/TII.2019.2945366>
- Zhao, H., Liu, H., Hu, W., & Yan, X. (2018). Anomaly detection and fault analysis of wind turbine components based on deep learning network. *Renewable Energy*, 127, 825–834. <https://doi.org/10.1016/j.renene.2018.05.024>
- Zhao, J., Wang, W., & Sheng, C. (2018). Data-driven prediction for industrial processes and their applications. In L. Henry (Ed.), *Information fusion and data science*. Springer. <http://www.worldcat.org/oclc/1049171711%0Afile:///C:/Users/Annika/AppData/Local/Swiss Academic Software/Citavi 6/ProjectCache/kckvlrkzr7sprlrg4e6kdf1wzi35szsww3p2dj3b8rr/Citavi Attachments/7c1cb613-9db5-41a7-8abb-91284fea89e6.pdf>
- Zhong, S., Luo, H., Lin, L., & Fu, X. (2016). An improved correlation-based anomaly detection approach for condition monitoring data of industrial equipment. *2016 IEEE International*

Conference on Prognostics and Health Management, ICPHM 2016, May.
<https://doi.org/10.1109/ICPHM.2016.7542850>

- Zope, K., Singh, K., Nistala, S. H., Basak, A., Rathore, P., & Runkana, V. (2019). Anomaly detection and diagnosis in manufacturing systems: A comparative study of statistical, machine learning and deep learning techniques. *Proceedings of the Annual Conference of the Prognostics and Health Management Society, PHM, 11(1)*, 1–10.
<https://doi.org/10.36001/phmconf.2019.v11i1.815>

9 Abbildungsverzeichnis

Abbildung 1: Zusammenhang Problemfelder, Ziele und den vier Unterpunkten der Hauptforschungsfrage.....	6
Abbildung 2: Maßnahmen der Instandhaltung.....	13
Abbildung 3: P-F-Kurve zeigt den Verlauf des Zustandes.....	16
Abbildung 4: Konzept der wissensbasierten Instandhaltung.....	18
Abbildung 5: Die Reifegrad- und Komplexitätsstufen der wissensbasierten Instandhaltungsstrategien (KBM).....	19
Abbildung 6: Ausbaustufen des CM.....	22
Abbildung 7: Einteilung und Bezug der verschiedenen Begrifflichkeiten der Künstlichen Intelligenz.....	25
Abbildung 8: Prozessmodell CRISP-DM.....	26
Abbildung 9: Modellierung auf klassische Weise (links) und durch ML (rechts).....	26
Abbildung 10: Die drei Hauptgruppen des Maschinellen Lernens.....	28
Abbildung 11: Kollektive Anomalie (rot markiert) im Verlauf eines menschlichen Elektrokardiogramms.....	30
Abbildung 12: Klassifikationsschema für komplexe Anlagen.....	35
Abbildung 13: Qualität des Trainingsdatensatzes.....	45
Abbildung 14: Roher Zeitreihendatensatz über Strommessung im Monat April 2019.....	46
Abbildung 15: Beispiel für Verdichtung einer Zeitreihe.....	47
Abbildung 16: Ansätze für die Manipulation der Daten im Pre-Processing für den binären Fall: Mehrheitsklasse (hellblau) und Minderheitsklasse (violett).....	50
Abbildung 17: Phasenmodell für CM mittels Anomalieerkennung.....	62
Abbildung 18: Grundlegende feedforward Struktur eines Autoencoders.....	70
Abbildung 19: Isolation Forest – Darstellung des Unterschiedes zwischen schneller Absonderung (Y) und langsamer Absonderung (X).....	71
Abbildung 20: Isolation Forest – Darstellung der Baumstruktur und unterschiedliche Pfadlängen (Strukturtiefe).....	72
Abbildung 21: Verwendete Methoden der Anomalieerkennung.....	73
Abbildung 22: Beispiel eines Dataframes mit Messwerten, Features und Anomaliefaktor (Ergebnisse einer Analyse mit LOF).....	74
Abbildung 23: Darstellung eines gesamten Monats (September 2020).....	82
Abbildung 24: Stromstärkenverlauf (y-Achse) unter normalen Umständen.....	82
Abbildung 25: Stromstärkenverlauf (y-Achse) mit deutlich sichtbarem anomalem Verhalten beim Öffnen.....	82
Abbildung 26: kMeans (inkl. Center) geclustertes Öffnungs- und Schließsignal März 2020.....	85
Abbildung 27: Anfang des zu analysierenden Dataframes mit 6 Merkmalen inklusive der ursprünglichen Messung der Stromstärke (<i>current</i>).....	86
Abbildung 28: Gekapptes Signal mit 2 Features (DS1) mit drei auffälligen Ausschlägen.....	86
Abbildung 29: Gekapptes Signal mit 2 Features (DS2) ohne sichtbare Auffälligkeiten.....	87
Abbildung 30: Gekapptes Signal mit 2 Features (DS3) mit einem auffälligen Stromabfall....	87
Abbildung 31: Zoom in ein einzelnes Öffnungssignal (DS1).....	89
Abbildung 32: Netzwerkstruktur Autoencoder für PoC (Verbindungslinien nur angedeutet). 92	

Abbildung 33: Zoom in ein einzelnes Öffnungssignal (DS1)	94
Abbildung 34: Dataframe für den signalgruppenbasierten Ansatz (hier nur Öffnungssignale)	95
Abbildung 35: Darstellung der statistischen Merkmale über die Signal ID (Schließsignale DS5)	96
Abbildung 36: Darstellung der statistischen Merkmale über die Signal ID (Schließsignale DS6)	96
Abbildung 37: Anomalie Score über Signal IDs aufgetragen (DS5)	99
Abbildung 38: Abfrage zu anomalen Öffnungssignal (Beispiel aus DS5).....	100
Abbildung 39: Vergleich mit Referenzsignal (Beispiel aus DS5)	100
Abbildung 40: Beispiel eines Dashboards (Novelty Detection LOF von DS3 Öffnungssignal)	101
Abbildung 41: Beispiel eines Dashboards (Novelty Detection iForest von DS3 Öffnungssignal)	102
Abbildung 42: Übersicht der Kandidatenalgorithmen mit der Auswahl von HBOS und iForest	104
Abbildung 43: Vergrößerung auf 1. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal).....	105
Abbildung 44: Vergrößerung auf 2. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal).....	105
Abbildung 45: Vergrößerung auf 3. Anomalie (iForest mit Kontamination = 0.005 auf DS1 Öffnungssignal).....	106
Abbildung 46: Dashboard für DS1 (Öffnungssignale) mit iForest.....	106
Abbildung 47: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS1	114
Abbildung 48: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS2.....	115
Abbildung 49: Mit HBOS detektierte Anomalien dargestellt im Zeitverlauf des gekappten Signals für DS3.....	115
Abbildung 50: Darstellung Datensatz DS1 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen	116
Abbildung 51: Darstellung Datensatz DS2 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen	117
Abbildung 52: Darstellung Datensatz DS3 im Zeitverlauf mit markierten Anomalien aller unüberwachten Algorithmen	118
Abbildung 53: Darstellung Datensatz DS1 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen	119
Abbildung 54: Darstellung Datensatz DS2 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen	120
Abbildung 55: Darstellung Datensatz DS3 im Zeitverlauf mit markierten Anomalien aller halbüberwachten Algorithmen	121
Abbildung 56: Ausgewählte Merkmale der Öffnungssignale aus DS5	122
Abbildung 57: Ausgewählte Merkmale der Öffnungssignale aus DS6	122
Abbildung 58: Beispiel eines Dashboards (kNN auf DS1 Öffnungssignal).....	123
Abbildung 59: Alarmlogik mit $p=10\text{min}$ (kNN auf DS1 Öffnungssignal).....	123

Abbildung 60: Beispiel eines Dashboards (HBOS auf DS1 Öffnungssignal).....	124
Abbildung 61: Beispiel eines Dashboards (HBOS mit Kontamination 0.05 auf DS1 Öffnungssignal, verbesserte Detektionsleistung)	125
Abbildung 62: Vergrößerung auf 1. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal).....	126
Abbildung 63: Vergrößerung auf 2. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal).....	126
Abbildung 64: Vergrößerung auf 3. Anomalie (HBOS mit Kontamination = 0.05 auf DS1 Öffnungssignal).....	126

10 Formelverzeichnis

Formel 1: Mathematische Darstellung einer Zeitreihe	46
Formel 2: Beispielhafte Berechnung des Mittelwertes.....	64
Formel 3: Normalisierung von Variablen.....	66
Formel 4: Berechnung des Histogramm-basierten Anomaliefaktors HBOS	67
Formel 5: Berechnung des euklidischen Abstandsmaßes.....	68
Formel 6: Zusammenhang zwischen Input Layer und Hidden Layer mit nicht-linearer Aktivierungsfunktion.....	70
Formel 7: Zusammenhang zwischen Hidden Layer und Output Layer mit nicht-linearer Aktivierungsfunktion.....	70
Formel 8: Rekonstruktion des Eingangs über die gelernte Funktion	70
Formel 9: Berechnung des unteren (lower) und oberen (upper) Grenzwertes (τ).....	75
Formel 10: Formulierung des normalen Bereiches für d	75
Formel 11: Bestimmung von sv_{01}	76
Formel 12: Bestimmung der Spanne des anomalen Bereiches	76
Formel 13: Bestimmung von sv_{12}	76
Formel 14: Bestimmung von sv_{23}	76
Formel 15: Zusammenhang der Übergangswerte	76

11 Tabellenverzeichnis

Tabelle 1: Ausgangslage und Problemfelder	4
Tabelle 2: Ziele der Diplomarbeit	5
Tabelle 3: Hauptforschungsfrage mit vier Unterpunkten	5
Tabelle 4: Gang der Untersuchung	8
Tabelle 5: Paradigmenwechsel in der Instandhaltung	13
Tabelle 6: Gründe für die Einführung von CM	20
Tabelle 7: Gründe gegen die Einführung von CM	21
Tabelle 8: Synonyme und Nicht-Synonym von Anomalie	28
Tabelle 9: Aufbau des morphologischen Kastens für die Analyse von CM bei kritischen und hochkomplexen Anlagen.....	36
Tabelle 10: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (1/3).....	37
Tabelle 11: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (2/3).....	37
Tabelle 12: CM für hochkomplexe und kritische Anlagen: Ergebnisse der morphologischen Analyse (3/3).....	38
Tabelle 13: Fazit zum Forschungsbedarf bei komplexen Anlagen	44
Tabelle 14: Aufbau des morphologischen Kastens für die Informationsgewinnung bei unbalancierten Daten.....	47
Tabelle 15: Informationsgewinnung unter schlechter Ausgangsdatenlagen: Ergebnisse der morphologischen Analyse (1/2)	48
Tabelle 16: Informationsgewinnung unter schlechter Ausgangsdatenlagen: Ergebnisse der morphologischen Analyse (2/2)	48
Tabelle 17: Fazit zum Forschungsbedarf über Informationsgewinnung unter schlechter Ausgangsdatenlage	53
Tabelle 18: Aufbau des morphologischen Kastens für die Analyse von Publikationen zum Thema AE für CM	54
Tabelle 19: Anomalieerkennung für CM: Ergebnisse der morphologischen Analyse (1/2) ...	54
Tabelle 20: Anomalieerkennung für CM: Ergebnisse der morphologischen Analyse (2/2) ...	55
Tabelle 21: Fazit zum Forschungsbedarf über Anomalieerkennung für CM	58
Tabelle 22: Fortschreitendes Fenster für Berechnung der Merkmale	64
Tabelle 23: Beschreibung der verwendeten statistischen Merkmale.....	65
Tabelle 24: Vergleich der Kandidatenalgorithmen auf Basis der Literatur.....	73
Tabelle 25: Beschreibung der Kritikalitätskategorien (Severity Levels) mit Übergangsgrenzwerten.....	75
Tabelle 26: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2019	81
Tabelle 27: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2020	81
Tabelle 28: Beschreibung des verfügbaren Datensatzes der Einlaufftüre aus dem Jahr 2021	81
Tabelle 29: Merkmale der Normkurven für Februar und März 2020 (beispielhaft)	83

Tabelle 30: Verwendete Daten (Öffnungssignale) für das PoC.....	85
Tabelle 31: Detektierte Anomalien in den Datensätzen (DSx) mit HBOS	88
Tabelle 32: Zusammenfassende Bewertung der Leistung des statistischen Ansatzes (Anforderungen sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0).....	89
Tabelle 33: Detektierte Anomalien in den Datensätzen (DSx) mit LOF, kNN und kMeans mit den dazugehörigen Grenzwerten	91
Tabelle 34: Zusammenfassende Bewertung der Leistung der unüberwachten Algorithmen (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0).....	91
Tabelle 35: Detektierte Anomalien in den Datensätzen (DSx) mittels Novelty Detection mit LOF, Autoencoder, OC-SVM und Isolation Forest.....	93
Tabelle 36: Zusammenfassende Bewertung der Leistung der halbüberwachten Algorithmen (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0).....	93
Tabelle 37: Ausgangsdarstellung aller Öffnungssignale des Datensatzes mit der Einteilung in Signal Label, Signal ID, Zeitstempel und gemessener Stromstärke.....	95
Tabelle 38: Transformierte Darstellung, in der jeder Signal ID nun X statistische Merkmale zugeordnet sind	95
Tabelle 39: Detektierte anomale Signal IDs in den Datensätzen (DSx) mittel iForest.....	97
Tabelle 40: Zusammenfassende Bewertung der Leistung des signalgruppenbasierten Ansatzes mit iForest (sehr gut erfüllt = 10, erfüllt = 5, schlecht erfüllt = 0).....	97
Tabelle 41: Zusammenfassung der Bewertung der Kandidatenalgorithmen.....	104
Tabelle 42: Dokumentation der Skripte für den Software Prototyp.....	114

12 Abkürzungsverzeichnis

Abkürzung	Bedeutung
(OC-) SVM	(One Class) Support Vector Machine
AE	Anomalieerkennung
AS	Anomalie Score
AS	Anomalie Score
bzw.	beziehungsweise
CBM	Condition-based Maintenance
CM	Condition Monitoring
CMS	Condition Monitoring System
CPPS	Cyber-physische Produktionssysteme
CPS	Cyber-physische Systeme
CRISP-DM	Cross Industry Standard Process for Data Mining
d.h.	das heißt
DS	Datensatz
dt.	Deutsch
etc.	et cetera
FF	Forschungsfrage
FFT	Fast Fourier Transformation
h	Stunde
HBOS	Histogram-based Outlier Score
IH	Instandhaltung
Jh.	Jahrhundert
KBM	Knowledge-based Maintenance
KI (AI)	Künstliche Intelligenz (Artificial Intelligence)
kNN	K Nächster Nachbar
KNN (ANN)	Künstliches Neuronales Netz (Artificial Neural Network)
LOF	Local Outlier Factor
max.	maximal
MCSA	Motor Current Signature Analysis
MSE	Mean Squared Error
PCA	Principal Component Analysis
PdM	Predictive Maintenance
PoC	Proof of Concept
PresM	Prescriptive Maintenance
RCM	Reliability-Centered Maintenance
RCM	Reliability-centered Maintenance
RMS	Root Mean Square
RNN	Replikator Neuronales Netz
RUL	Remaining Useful Life
SCADA	Supervisory Control and Data Acquisition
SdT	Stand der Technik
SMOTE	Synthetic Minority Oversampling Technique
SOM	Self-organizing Maps
SV	Severtiy Level
SVDD	Support Vector Data Description

vgl.	vergleiche
WT	Wavelet Transformation
z.B.	zum Beispiel