Verhaltensverifizierung für Geschäftsprozesse basierend auf Testverfahren und Anomalieerkennung[1]

Kristof Böhmer[2]

Abstract: Obwohl Geschäftsprozesse (kurz Prozesse) in Organisationen maßgebliche Aufgaben übernehmen, wurden diese bisher nur unzureichend abgesichert. Dies führte dazu, dass Fehler in parallelen Prozessausführungen oder sicherheitskritische Vorfälle unerkannt blieben. Eine Limitierung, welche die Dissertation mittels neuer Verfahren begegnet. Hervorzuheben ist hierbei der Fokus auf ganzheitliche und vollautomatisierte Verfahren, um, unter anderem, das Zusammenspiel aller Prozesse in einer Organisation als Ganzes zu analysieren oder auch komplexe sicherheitskritische Vorfälle, wie kollektive Anomalien, zu erkennen. Durch den breiten Einsatz von Prozessen sind diese Verfahren nicht nur für Prozessexperten relevant, sondern auch für die Gesellschaft als Ganzes.

1 Einführung

Prozesse sind das *Herzblut* moderner Organisationen; sie bilden grundlegende Vorgänge ab, verarbeiten *personenbezogene* Daten, *verhindern* Gesetzesverstöße und *koordinieren* Maschinen, Menschen und Unternehmen. Kurz, heutzutage hängen selbst die Lebensmittel- und Energieversorgung direkt oder indirekt von korrekt arbeitenden Prozessen und deren Definitionen ab. Hierbei lassen sich diese als eine Art (grafische) Programmiersprache verstehen, vgl. Abb., 1, welche einen Prozess zur Kreditantragsbearbeitung zeigt.

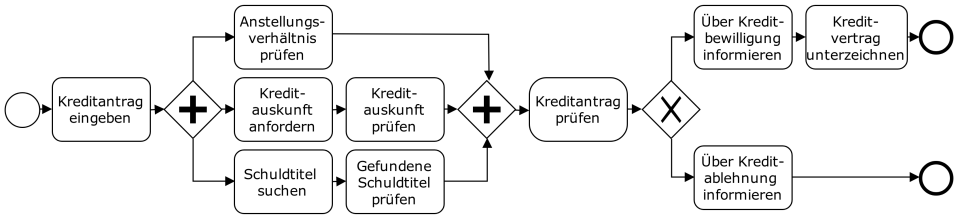

Abb. 1: Beispielhafter Prozess (Kreditantrag) in Business Process Model and Notation

Prozesse durchlaufen einen komplexen Lebenszyklus, welcher sich grob in deren *Definition* und *Ausführung* unterteilen lässt. Während der Definition wird festgelegt, wie die Ziele eines Prozesses erreicht werden können. Hierbei können selbst kleine Fehler eine große Auswirkung haben. Beispielsweise mussten 2015 60% der nordamerikanischen Starbucks-Franchisenehmer Kaffee *kostenlos* „verteilen“, da dieser aufgrund fehlerhafter Zahlungsprozesse von den Kunden nicht bezahlt werden konnte. Dieser und andere prozessbezogene Fehler führten bereits zu Milliardenkosten und haben das Vertrauen zwischen Kunden und betroffenen Organisationen, wie dem US National Grid, Bridgestone

[1] Englischer Titel der Dissertation: “Behavior Verification for Business Processes based on Testing and Anomaly Detection”

[2] Institut für Informatik, Universität Wien, Wien, Österreich, kristof.boehmer@univie.ac.at

oder Starbucks, belastet, vgl. [Zi14]. Daher stellt sich die Dissertation [B8] die Frage, wie solche Fehler frühzeitig erkannt werden können – vor allem deshalb, weil sich diese meist in komplexen, parallelisierten Definitionen „*verstecken*“, für welche sich die Fehlersuche, ohne Unterstützung durch automatische Verfahren, fast aussichtslos gestaltet [B8, S. 2].

Während der Ausführung wird das „grafische Programm“ Prozess instanziiert und durchlaufen. „IT-Sicherheit“ ist hierbei besonders relevant, da Prozesse oft *tief* in bestehende „IT-Landschaften“ integriert sind. Greifen diese doch während ihrer Ausführung auf unterschiedlichste Datenquellen zu und verarbeiten dabei *kritische* geschäftliche und personenbezogene Informationen. Hierdurch werden Prozesse auch zu einem interessantes Ziel für Angreifer und Betrüger, sodass prozessgetriebene Systeme oft auch bei sogenannten „Data Breaches“ beteiligt sind. Bei letzterem werden private und geschäftliche Daten (z.B. medizinische Analysen) aus einer Organisation unberechtigterweise ausgelesen. Untersuchungen aus dem Jahr 2016 zufolge sind hiervon jährlich 4,2 Milliarden Datensätze und Millionen von Personen betroffen, vgl. [Cy16]. Solche Vorfälle können, neben einem Vertrauensverlust auf Seiten der Kunden und Partner, auch in Geldstrafen resultieren. Die Dissertation stellt Verfahren bereit, um Angriffe auf Prozesse und deren missbräuchliche Verwendung *automatisch* zu erkennen – was durch die steigende Komplexität, Flexibilität und Dynamik der Prozessausführungen erschwert wird. Gilt es doch, beispielsweise echte Angriffe von ungewöhnlichen, aber *harmlosen Verhalten* und Fehlbedienung möglichst gut zu unterscheiden – obwohl beide einander auf den ersten Blick ähneln [B8, S. 120].

Bisher fehlte es jedoch an gründlichen Verfahren, um Prozesse *a*) automatisch auf *Fehler* zu prüfen und *b*) vor unerwünschter oder *missbräuchlicher Verwendung* zu *schützen*. Diese Forschungslücken werden von der Dissertation mittels *systematischer Literaturstudien* konkretisiert und passende Lösungsverfahren identifiziert, implementiert und evaluiert. Unter anderem wird hierzu *Machine Learning* eingesetzt, um für jeden Prozess zu bestimmen, wie in diesem am schnellsten Fehler gefunden werden können. Weiters werden neuartige *wahrscheinlichkeitsbasierte Algorithmen* entworfen, um unwahrscheinliches Ausführungsverhalten (Anomalien) – und damit potentielle Sicherheitsprobleme – zu identifizieren. Die hierbei entstandenen Forschungsbeiträge sind *nicht nur* für Sicherheits- oder Prozessexperten relevant, da die Gesellschaft und die in ihr operierenden Organisationen mehr und mehr von fehlerfreien sicheren Prozessen abhängig werden [B8, S. 12].

2 Hauptinhalt der Dissertation

In den letzten Jahren sind *Millionen von Prozessdefinitionen* für Bereiche wie Forschung, Entwicklung oder Bildung entstanden; allein ein großes Bergbauunternehmen wie BHP Billiton nutzt mehr als 100.000 davon. Durch die starke Verbreitung und häufig unkontrollierte (voll-)*automatische Ausführung* der Prozesse wird die Auswirkung von Fehlern in ihren Definitionen und Anomalien in deren Ausführungen stark erhöht und kann sich auch zu einer direkten Gefahr für Leib und Leben auswachsen, indem z.B. ein Fehler zur Zusammenstellung eines unverträglichen Medikamenten-Cocktails führt. Diese Dissertation schlägt daher Verfahren vor, um Prozesse auf Fehler (Abschn. 2.1) und Anomalien (Abschn. 2.2) möglichst schnell, gründlich und vollautomatisch zu überprüfen [B8, S. 4].

2.1 Erster Hauptteil: Fehlererkennung während der Definition eines Prozesses

Eine Standardlösung, um Fehler zu identifizieren, ist der Einsatz sogenannter Tests; einer Zusammenstellung von Daten, um *Prozesse auszuführen* und daraufhin zu überprüfen, ob diese das *erwartete Verhalten* zeigen. Diese Idee wird in unterschiedlichen Ausprägungen angewandt, z.B. um Prozessverhalten während Hochlastszenarien zu prüfen oder sicherzustellen, dass einzelne Prozessbestandteile korrekt zusammenarbeiten. Aufgrund dieser Diversität geht diese Dissertation zunächst der Frage nach, welche Testverfahren derzeit im Prozessbereich eingesetzt werden und welche Schwächen/Stärken diese aufweisen.

2.1.1 Systematische Literaturanalyse und Forschungslücken

Hierzu wurden, im Rahmen einer *systematischen Literaturanalyse*, Forschungsdatenbanken (wie SCOPUS, IEEE Xplore und DBLP) und 30 Journals/Konferenzbände nach prozessfokussierten Testverfahren durchsucht. 6638 Arbeiten wurden hierbei als potentiell relevant erkannt, von denen nach *mehreren Auswahlrunden* 159 detailliert analysiert wurden. Es zeigte sich, dass die derzeitige Forschung aus dem Bereich „Prozess-Tests“ stark von verwandten Gebieten wie den „Software-Tests“ beeinflusst wird. Dabei wird eine Vielzahl von Themen abgedeckt, wie Testgenerierung, Integrationstests, Regressionstests oder die Überprüfung vorgegebener Dienstgüteanforderungen [B8, S. 28 ff.].

Darüber hinaus stellen viele existierende Verfahren überraschend *umfangreiche Anforderungen* an deren Anwender (z.B. indem seltene formale Sprachen eingesetzt werden). Dies erschwert unserer Annahme nach deren Einsatz, weshalb in dieser Dissertation darauf geachtet wurde, einen hohen Automatisierungsgrad zu erreichen, sodass die vorgestellten Verfahren weitestgehend ohne Schulungen breit eingesetzt werden können. Abschließend zeigte sich auch ein *durchwachsenes Bild* hinsichtlich der *durchgeführten Evaluierungen* – wiesen doch viele Arbeiten keine oder nur eine unzureichende Evaluierung mit kleinen, selten frei verfügbaren, selbst generierten Datensätzen auf, siehe Abb. 2. Um diesem Trend zu begegnen, wurden die im Rahmen der Dissertation vorgestellten Verfahren *prototypisch implementiert* und mit öffentlichen *realen und realistischen Daten* evaluiert [B8, S. 49 ff.].

2.1.2 Testauswahl mittels Machine Learning

Bezüglich der von Software-Test-Verfahren inspirierten Arbeiten zeigte sich, dass diese kaum auf die *Unterschiede* zwischen Quellcode und Prozessdefinitionen, wie der unterschiedlichen Verhaltensgranularität, eingehen [B8, S. 27]. Dies führt dazu, dass die derzeit angewendeten Testverfahren Prozesse nur mit einer *unzureichender Gründlichkeit* analysieren und entsprechend Fehler übersehen. Um diese Lücke zu schließen, wurde im Rahmen der Dissertation ein neues, auf Machine Learning basierendes Verfahren vorgestellt. Dieses erlaubt es, Prozessdefinitionen und deren Bestandteile *a*) nach *Anwenderwunsch* (z.B. einer maximal möglichen Testausführungsdauer) und *b*) einer automatisch errechneten notwendigen *Testintensität* nach Fehlern zu durchsuchen [B8, S. 57 ff.].

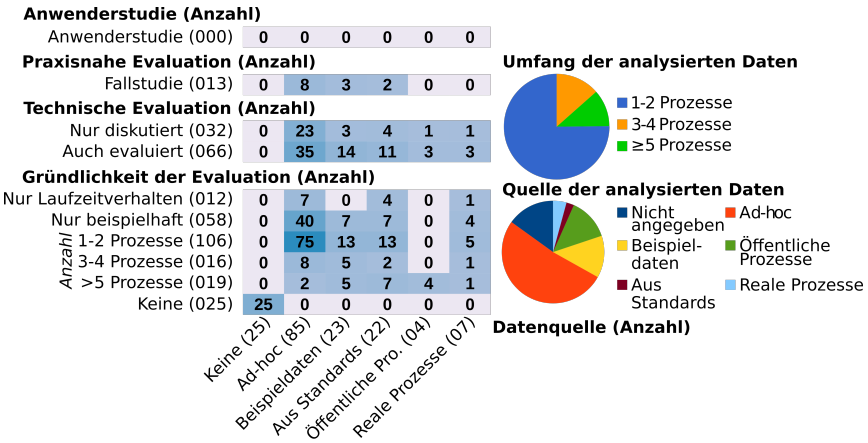

Abb. 2: Zusammenfassung der Evaluierungsqualität der analysierten Publikationen

In der Dissertation wird das vorgeschlagene Verfahren mit fünf bereits etablierten Verfahren – welche überwiegend aus dem Forschungsbereich der Softwareentwicklung in den Bereich Prozessfehlersuche übertragen wurden – verglichen. Hierbei konnte das vorgeschlagene Verfahren je nach Datensatz und Aufgabenstellung zwischen 3,5 und 10,3 Prozent mehr Fehler und Probleme identifizieren als die etablierten Vergleichsverfahren. Zusätzlich wurde noch erhoben, wie das vorgestellte Verfahren im Fall von Änderungen reagiert, beispielsweise weil nach einem erkannten Fehler die analysierte Prozessdefinition geändert wurde. Solche Änderungen passieren häufig und werden oft auch durch *externe Faktoren* wie Gesetzesänderungen erzwungen – eine hohe Performance in solchen Fällen ist daher maßgeblich für die praktische Anwendbarkeit eines Testverfahrens. Hier zeigte sich im Vergleich zur vollständigen Neuberechnung eine *Reduktion* der zu investierenden Rechenleistung zwischen 21,8 und 58513,5 Prozent. Gerade in Zeiten großer und umfangreicher Testsammlungen mit tausenden Einzeltests ist dies wichtig, um Tests auch bei immer knapper werdenden Entwicklungszyklen noch einbinden zu können [B8, S. 69].

2.1.3 Verifizierung von (versteckten) hoch parallelen Verhalten

Eine besondere Herausforderung bei der Fehlersuche stellt die den Prozessen inhärente Parallelität während deren Ausführungen dar. Insgesamt konnten zwei „Arten“ von Parallelität identifiziert werden. Einerseits die *explizite* Parallelität, welche während der Definition der Prozesse durch parallele Ausführungspfade (explizit) definiert wird. Selbst diese Art führt oft zu Fehlern aufgrund ungenügend berücksichtigter Überlappungen und damit einhergehender Nebeneffekte. Zusätzlich konnte die Dissertation die sogenannte *implizite* Parallelität identifizieren, die *bis jetzt* noch keine Berücksichtigung erfuhr [B8, S. 83 ff.].

Implizite Parallelitäten können ebenfalls die Ursache für zahlreiche Fehler sein, sind je doch, im Vergleich zu expliziten Parallelitäten, deutlich schwieriger zu *erkennen und einzuplanen*. Hervorgerufen wird dies durch den Umstand, dass diese, im Gegensatz zu ex-

pliziten Parallelitäten, nicht absichtlich eingebracht werden, sondern durch die häufige Parallelausführung mehrerer Prozessinstanzen „nebenbei“ (implizit) entstehen. Implizite Parallelitäten umfassen entsprechend unvorhersehbare, wechselnde und potentiell riskante Überlappungen und parallele Datenzugriffe, die aus dem normalen Geschäftsalltag und den dabei stattfindenden parallelen Ausführungen mehrerer Prozessinstanzen erwachsen.

Um implizite Parallelitäten zu identifizieren und effizient auf Fehler zu überprüfen, unterteilt die Dissertation Prozessdefinitionen in mehrere Teilbereiche, je nachdem, ob sich diese mit anderen Prozessdefinitionen während deren Ausführung nicht, teilweise, oder vollständig überlappen. Hierzu werden alle *historischen*, vollautomatisch aufgezeichneten Prozessausführungen einer Organisation analysiert, deren Ausführungsverhalten extrahiert und ermittelt, ob und wie es zwischen mehreren Prozessdefinitionen zu impliziten Parallelitäten kommt und wie *wahrscheinlich* diese in Fehlern resultieren. Dies erlaubt es, anschließend automatisch eine Sammlung von Tests zusammenzustellen, welche mit möglichst *geringem Zeitaufwand* besonders fehlerträchtige Teile von Prozessdefinitionen intensiv auf durch implizite Parallelitäten verursachte Fehler prüfen können [B8, S. 90 f.].

Insgesamt konnten während der Evaluierung in sechs realen Datensammlungen mehrere *hunderttausend implizite Parallelitäten* identifiziert werden [B8, S. 93]. Anschließend wurde das neu vorgeschlagene Verfahren mit zwei aus dem Software Engineering Bereich abstammenden Standardverfahren zur Zusammenstellung von prozessfokussierten Tests verglichen. Es zeigte sich, dass das vorgestellte Verfahren es erlaubt, mit impliziten Parallelitäten in Zusammenhang stehende Fehler *effizienter zu identifizieren* und so die für Testausführungen aufzuwendende Zeit von Tagen auf Stunden reduziert werden konnte, vgl. Abb. 3 und [B8, S. 94]. Die Datensätze stammen aus Callcentern (TeleClaim) und niederländischen Baubehörden (BPIC15).

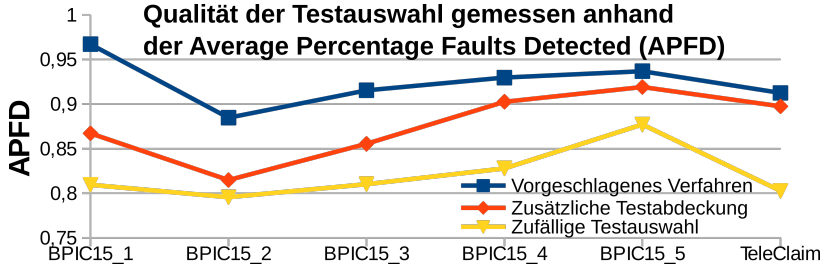

Abb. 3: Vergleich des vorgestellten Verfahrens mit zwei Alternativen

2.1.4 Demonstration der entwickelten Verfahren in den Energienetzen der Zukunft

Die zuvor vorgestellten Verfahren wurden im Rahmen des geförderten Forschungsprojektes PROMISE[2] in der *Praxis erprobt*. Hierbei konzentriert sich die Dissertation auf Prozesse zur Abrechnung und Steuerung von intelligenten Energienetzen und sogenannten Smart Metern. Letztere stellen eine *kritische Infrastrukturkomponente* dar, da Fehler in den zugehörigen Prozessen in landesweiten Blackouts resultieren können [B8, S. 97 ff.].

[2] Österreichische Forschungsförderungsgesellschaft (FFG), Projektnummer 849914

Eine besondere Herausforderung erwächst hierbei daraus, dass die verwendeten Prozesse äußerst komplex und verschachtelt sind und zahlreiche externe Datenquellen und Hardwarekomponenten zur Steuerung und Analyse des Netzzustands miteinbeziehen bzw. ansprechen. Gerade Letzteres zu berücksichtigen ist äußerst aufwändig, sodass dieser Aspekt von bestehenden Verfahren zumeist ignoriert oder sehr stark abstrahiert wird, was die Aussagekraft der Fehlersuchergebnisse beschränkt. Um dieser Einschränkung zu begegnen, wurden die zuvor beschriebenen Verfahren und Erkenntnisse mit Verfahren aus dem Bereich des Process-Mining kombiniert. Es konnte gezeigt werden, dass hierdurch reale Prozesse, Daten und Ausführungsumgebungen während der Fehlersuche flexibel miteinbezogen werden können. Dies ermöglicht es, alle Phasen einer Prozessdefinition (von den ersten Entwürfen bis hin zum Echtbetrieb) *nahtlos mit Fehlersuchmaßnahmen* zu begleiten. Hierdurch können Fehler frühzeitig und kostengünstiger behoben werden, als wenn erst nach Fertigstellung einer Prozessdefinition mit der Fehlersuche begonnen würde.

2.2 Zweiter Hauptteil: Anomalieerkennung während der Prozessausführung

Nach der Definition eines Prozesses wird das durch diesen beschriebene Verhalten zumeist voll- oder teilautomatisch von prozessgesteuerten IT-Systemen ausgeführt. Unter anderem werden hierdurch Energienetze gesteuert, die Produktionsabläufe in Fabriken koordiniert und medizinische Analysen standardkonform realisiert. Die hierzu eingesetzten Prozesse sind aus IT-Sicherheitssicht als *äußerst schützenswert* anzusehen. Prozesse benötigen und erhalten doch oft einen direkten Zugriff auf zahlreiche Systeme, Datenspeicher und IT-Landschaften innerhalb von (Partner-) Organisationen und bieten so einen vielversprechenden Einstiegspunkt für Angriffe und Betrügereien. In diesem Abschnitt wird daher die Frage geklärt, inwiefern die Ausführung von Prozessen überwacht werden kann, um Ausführungsverhalten zu identifizieren, welches auf Betrug, sicherheitskritische Ereignisse oder (un-)absichtliche fehlerhafte Verwendung hindeutet (sogenannte Anomalien).

2.2.1 Systematische Literaturanalyse und Forschungslücken

Um auch mit diesem Teil der Dissertation gezielt Forschungslücken zu identifizieren und zu schließen, wird auch dieser mit einer systematischen Literaturanalyse eingeleitet. Diese ist unseres Wissens nach die Erste in diesem Forschungsbereich, welche es erlaubt, einen vollständigen Überblick über den stark zersplitterten Bereich der Prozessverhaltensanalyse zu erlangen. Die erstellte Literaturanalyse identifizierte, basierend auf mehreren Forschungsdatenbanken (unter anderem Google Scholar, DBPL und IEEE Xplore), mehrere hundert potenziell relevante Publikationen, von denen 35 schlussendlich als relevant erkannt und näher analysiert wurden. Hierbei zeigte sich, dass das Interesse an der Thematik gestiegen ist bzw. die relevanten Publikationszahlen in den letzten Jahren zugenommen haben (3 im Jahr 2014 im Vergleich zu 10 im Jahr 2018). Derzeit scheint noch kein dominierendes Verfahren gefunden worden zu sein, da ein bunter *Mix an Technologien* und Konzepten mit unterschiedlichen Stärken, Schwächen und Zielen eingesetzt wird (z.B. statistische Analysen, neuronale Netze oder auch regelbasierte Verfahren), siehe Abb. 4.

Es zeigt sich, dass die existierenden Verfahren überwiegend die Analyse eindimensionaler Daten und die Erkennung einfacher „Point Anomalies“ (Punkt Anomalien) unterstützen. Unter Letzteren werden Anomalien verstanden, welche anhand eines punktuell stark herausstechenden Verhaltens identifiziert werden können (z.B. eine einzelne extrem hohe Überweisungssumme). Da Angreifer aber zumeist versuchen, ihre Aktivitäten zu verstecken, erachtet die Dissertation beispielsweise „Collective Anomalies“ (Kollektive Anomalien) als *deutlich realitätsnäher*. Bei diesen werden Angriffe in mehrere einzelne, für sich gesehen unauffällige, Einzelaktionen aufgespalten [B8, S. 111 ff.]. Nur Verfahren, die in der Lage sind, diese zu korrelieren und als Einheit zu analysieren, können diese sicher erkennen und eine umfassende Schutzwirkung gewährleisten. Ergo hat die Dissertation eine Reihe von neuartigen Verfahren vorgestellt, um solche und andere Beschränkungen aufzuheben – auf diese wird im Folgenden eingegangen [B8, S. 118-121].

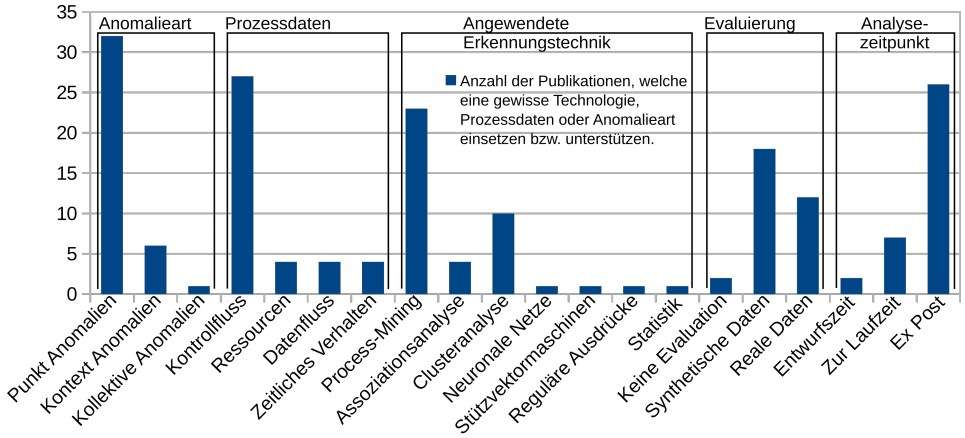

Abb. 4: Überblick über bestehende Anomalieerkennungsarbeiten für Prozesse

2.2.2 Anomalieerkennung in den ausgetauschten und verarbeiteten Daten

Prozesse verarbeiten und tauschen während ihrer Ausführung typischerweise eine Vielzahl von Datensätzen mit zahlreichen Systemen, Diensten und Partnerorganisationen aus. Jeder dieser Datensätze stellt eine potenzielle Bedrohung dar, da er dazu genutzt werden könnte, sicherheitskritisches Verhalten oder die Ausführung von Schadcode zu forcieren. Gegen solche Bedrohungen sind Prozessausführungen zumeist *nicht abgesichert*, nimmt doch die flexible, schnelle und unkomplizierte Einbindung unterschiedlicher Datenquellen einen höheren Stellenwert als IT-Sicherheit ein. Auch fehlen oft eine entsprechende Dokumentation und Standardisierung, um beispielsweise händisch Regeln aufstellen zu können, welche es erlauben, zwischen validen und bedrohlichen Datensätzen zu unterscheiden.

Die Dissertation löst diese Herausforderung mittels eines neuartigen Verfahrens, welches ausnützt, dass Prozessausführungen zumeist lückenlos aufgezeichnet werden. Anhand solcher Aufzeichnungen werden anschließend *automatisch Regeln* (in der Form von regulären Ausdrücken) abgeleitet, welche es erlauben, automatisch festzustellen, ob Datensätze hin-

sichtlich Struktur und Inhalt dem zuvor aufgezeichneten bzw. gewohnten/erwarteten Verhalten folgen. Durch den Einsatz von *regulären Ausdrücken* können die hierbei in zwei frei wählbaren Komplexitätsleveln anfallenden Regeln mit geringem Aufwand von Menschen gelesen und adaptiert werden um individuelle Anpassungen durchzuführen [B8, S. 126].

Das zuvor beschriebene Verfahren wurde in Abstimmung mit den Sicherheitsexperten von SBA Research evaluiert, um sicherzustellen, dass die angenommenen Bedrohungsszenarien als *relevant und realistisch* einzuschätzen sind. Insgesamt wurden hierbei 240.000 verschiedene Datensätze in drei unterschiedlichen Formaten (EDIFACT, XML, JSON) und verschiedenen Bedrohungsszenarien evaluiert. Als sicherheitskritisch einzustufende Datensätze konnten hierbei mit 59%-100% Genauigkeit (je nach Format und Bedrohungsszenario) korrekt erkannt werden, siehe Abb. 5. Das Verfahren ermöglicht es, hierbei auch automatisch zu ermitteln, wie stark ein als bedrohlich eingestufter Datensatz vom Erwarteten abweicht, um entsprechend auf *wechselnde Bedrohungen* zu reagieren [B8, S. 139].

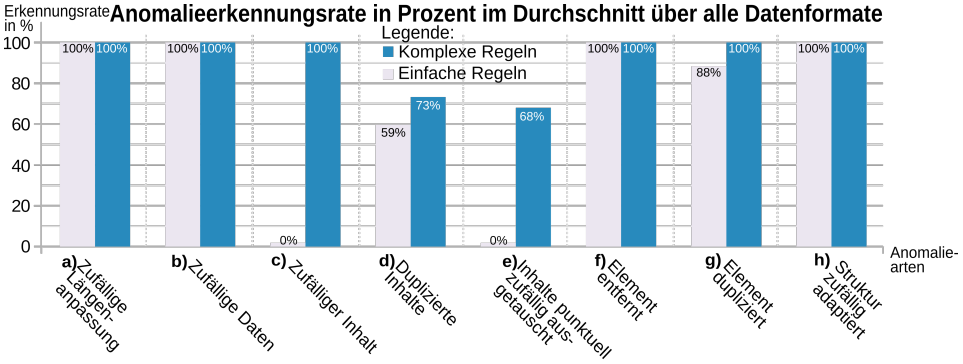

Abb. 5: Evaluierungsergebnisse zur Anomalieerkennung in Prozessdaten

2.2.3 Berücksichtigung aller Aspekte eines Prozesses

Das im vorangegangenen Abschnitt beschriebene Verfahren konzentriert sich vor allem auf die während einer Prozessausführung anfallenden und ausgetauschten Datensätze. Damit allein ist jedoch noch keine vollständige Absicherung möglich. Sind doch auch Aspekte wie z.B. die in einen Prozess eingebundenen (menschlichen) Ressourcen oder der während einer Ausführung durchlaufene Kontrollfluss sicherheitsrelevant – beispielsweise, um Verletzungen des Vier-Augen-Prinzips zu erkennen. Um eine vollständige Absicherung zu erreichen, müssen diese und weitere Aspekte *ganzheitlich Berücksichtigung* erfahren.

Die Dissertation bietet hierzu ein Verfahren, welches erlaubt, basierend auf aufgezeichneten Prozessausführungen die *Wahrscheinlichkeit* jedes möglichen Ausführungsverhaltens zu berechnen. Basierend auf der gängigen Annahme, dass Anomalien mit unwahrscheinlichem Verhalten gleichzusetzen sind, lassen sich diese hierüber identifizieren. Dieses neuartige Verfahren lässt sich nicht nur flexibel erweitern (je nachdem, welche Informationsquellen/Aspekte gerade zur Verfügung stehen), sondern erlaubt es auch, einzelne Ereignisse zu korrelieren. Hierdurch würde beispielsweise eine Kombination von leicht un-

wahrscheinlichen Ereignissen genauso als Sicherheitsproblem identifiziert werden wie ein einzelnes, sehr unwahrscheinliches Ereignis. Hierdurch können nicht nur versteckte Angriffe („Collective Anomalies“) identifiziert werden, sondern es ist auch möglich, Analysen während einer noch laufenden Prozessausführung durchzuführen (Ad-hoc) [B8, S. 163]. Vergleichbare Verfahren begannen bis zu diesem Zeitpunkt immer erst mit der Analyse, nachdem eine Prozessausführung vollständig abgeschlossen worden ist (Ex Post). Jedoch wurde zu diesem Zeitpunkt das sicherheitskritische Verhalten des Prozesses bereits vollständig durchlaufen und so z.B. ein System bereits erfolgreich attackiert. Im Gegensatz hierzu ermöglicht das im Rahmen der Dissertation vorgestellte Verfahren automatisch, während der Laufzeit des Prozesses jederzeit dessen Status einzuschätzen, sodass Angriffe frühzeitig, bereits in ihrer *Anfangsphase, gestoppt* werden können [B8, S. 112 ff.].

Um die Anwendbarkeit und Fähigkeiten des neuen Verfahrens zu evaluieren, wurden mehrere reale Datensätze herangezogen und auf Anomalien hin analysiert. Hierbei konnten diese mit einer Präzision von 82% gefunden werden. Allerdings werden auch teilweise Anomalien übersehen, was in einem Recall von 65% und Accuracy von 78% resultiert. Letzteres wurde hierbei von den befragten Sicherheitsexperten aber als wenig relevant beurteilt, da es ihnen für die angedachten Einsatzszenarien als wichtiger erschien, dass gemeldete Anomalien wirklich Anomalien sind, als dass alle Anomalien gefunden wurden, um den derzeit durch *Fehlalarme entstehenden Aufwand* zu minimieren [B8, S. 163].

2.2.4 Vollständige Absicherung einer Organisation

Bestehende Prozessanomalieerkennungsverfahren analysieren jeden Prozess und dessen Ausführungen individuell, unabhängig von allen anderen in einer Organisation anfallenden Prozessausführungen. Dies vereinfacht und beschleunigt den Analysevorgang, erlaubt es jedoch *Angriffe zu verstecken*, indem diese in mehrere „harmlose“ Bestandteile aufgeteilt und durch eine Kombination mehrerer Prozesse umgesetzt werden. Bis jetzt wurden solche Angriffe und die damit in Zusammenhang stehenden Anomalien nicht erkannt.

Die Dissertation überwindet diese Beschränkung durch eine Erweiterung des in Abschnitt 2.2.3 beschriebenen Verfahrens mit Algorithmen zur *Zeitreihenanalyse* [B8, S. 169]. Während hierdurch einerseits das Zusammenspiel mehrerer Prozesse (beispielsweise deren Reihenfolgen und Überlappungen) analysiert wird, kann andererseits die individuelle Wahrscheinlichkeit jeder Prozessausführung bestimmt werden. Beide Analysen zu kombinieren ermöglicht es nun, trotz großer heterogener Datenmengen alle Prozessausführungen in einer Organisation – samt deren Zusammenspiel – in ihrer Gesamtheit zu analysieren.

Das zuvor beschriebene Verfahren wurde anhand mehrerer realer, frei verfügbarer Datensätze evaluiert. Hierbei wurden Anomalien mit einer Genauigkeit von 78% erkannt. Hervorzuheben ist hierbei, dass dieses Ergebnis *trotz starker Fluktuationen* im Ausführungsverhalten erreicht werden konnte. Letzteres schlug sich unter anderem in wechselnden Ausführungszeiten und unterschiedlichen parallelen Ausführungen nieder welche die Unterscheidung zwischen (un-)wahrscheinlichem Verhalten erschwerte [B8, S. 176].

3 Zusammenfassung und Ausblick

Es zeigte sich, dass aufgrund der Komplexität und Vielschichtigkeit von Prozessdefinitionen und Ausführungen ein einzelnes isoliertes Verfahren alleine kaum ausreichend ist, um „alle“ Fehler oder „alle“ Anomalien zu identifizieren. Stattdessen ist es notwendig, *mehrere Verfahren* zu kombinieren. Dies wird mit den Verfahren in Abschnitt 2.2.4 und 2.1.4 für den Bereich Fehlererkennung bzw. der Erkennung von Sicherheitsproblemen demonstriert. Wir sehen es als wichtig an, weitere Verfahren zu entwickeln, welche sich, ähnlich der hier vorgestellten, à la *Plug und Play* einfach kombinieren lassen [B8, S. 187].

Die Ergebnisse dieser Dissertation fokussieren sich auf Prozesse und die im Rahmen von Prozessausführungen anfallenden Daten. Jedoch sind diese auch für *andere Datenquellen* und Forschungsbereiche relevant. Prozessähnliches Verhalten bzw. ähnliche Herausforderungen und Fragestellungen treten auch während der Entwicklung und Ausführung von Software, der Auswertung von Logfiles und innerhalb von Systemen zur Steuerung von Maschinen und von Telekommunikations- und Energienetzen auf. Letztere sind hierbei besonders interessant, da deren Verhalten mittels prozessähnlicher Methoden modelliert wird und auch bereits zentrale Datensammel- und Ausführungsplattformen existieren, die überwacht werden können. Erste Gespräche mit Sicherheitsunternehmen wie TendMicro über potentielle Interessenten aus dem *kanadischen Telekommunikationsbereich* verliefen vielversprechend und zielen darauf ab, Betrugsfälle und Fehler in den für die Anruf- und Netzverwaltung relevanten Systemen und Prozessen zu identifizieren [B8, S. 187 f.].

Literaturverzeichnis

[BRM18] Böhmer, Kristof; Rinderle-Ma, Stefanie: Association Rules for Anomaly Detection and Root Cause Analysis in Process Executions. In: International Conference on Advanced Information Systems Engineering. Springer, S. 3–18, 2018.

[B8] Böhmer, Kristof: Behavior Verification for Business Processes based on Testing and Anomaly Detection. Dissertation, Universität Wien, 2018.

[Cy16] CyberScout: ITRC Data Breach Reports. Technischer Report, 2016.

[Zi14] Zibelman, Audrey: PSC completes audit of national grid gas companies. Technischer Report, 2014.

Kristof Böhmer studierte Informatik und Wirtschaftsinformatik an der FH Technikum Wien und an der Universität Wien. Während des Studiums arbeitete er als Softwareentwickler und anschließend als wissenschaftlicher Mitarbeiter. Für [BRM18] wurde ihm der *Best Paper Award* von der “Conference on Advanced Information Systems Engineering 2018“ verliehen. Seine Beteiligung an der Lehre und Konzeptionierung neuer Lehrveranstaltungen führte dazu, dass er seine Forschungstätigkeit nun als Senior Lecturer an der Universität Wien fortsetzt, um eine Habilitation zu erlangen.