

Statistisches Model Checking und zeitlich begrenzte Erreichbarkeitsanalyse für hybride Petri-Netze mit mehreren stochastischen Variablen¹

Carina da Silva²

Abstract: Sicherheitskritische Systeme stellen einen wichtigen Teil des heutigen Lebens dar. Modellierung und formale Verifikation bieten Ansätze zur Analyse solcher Systeme im Hinblick auf Systemeigenschaften wie beispielsweise Zuverlässigkeit. In meiner Dissertation [Pi21] wird eine Unterklasse stochastischer hybrider Systeme betrachtet, die diskrete, kontinuierliche und stochastische Variablen kombiniert. Es werden neuartige Ansätze für die Evaluation von *hybriden Petri-Netzen mit allgemeinen Transitionen* (HPnGs) vorgestellt. Diese umfassen statistisches Model Checking für Modelle mit linearen und nichtlinearen kontinuierlichen Verläufen sowie die (zeitlich begrenzte) Erreichbarkeitsanalyse für nichtdeterministische Modelle. Darüber hinaus stellt die Dissertation einen Ansatz für eine Transformation von HPnGs in eine Unterklasse der stochastischen hybriden Automaten vor, die die Anwendung bestehender, für hybride Automaten entwickelter Methoden auf stochastische hybride Modelle ermöglicht. Der resultierende Fehler der vorgestellten Ansätze kann dabei genau charakterisiert werden.

1 Einleitung

Sicherheitskritische Systeme sind Systeme, deren Fehlverhalten oder Ausfall verheerende Konsequenzen haben können. Dazu zählen unter anderem kritische Infrastrukturen (wie zum Beispiel Strom- und Gastnetzwerke), nukleare Systeme, die medizinische Versorgung und das Transportwesen. Aufgrund ihrer Bedeutung und wachsenden Komplexität wächst der Bedarf an Methoden zur Evaluation sicherheitskritischer Systeme. Die Untersuchung solcher Systeme in der Praxis erweist sich jedoch oft als schwierig oder gar unmöglich. Hier bietet Modellierung einen beliebten alternativen Ansatz, bei dem nicht in das reale System eingegriffen wird. Mithilfe von Methoden des *Model Checkings* [BK08] können bestehende Modelle automatisiert auf Systemeigenschaften wie Zuverlässigkeit, Verfügbarkeit und Sicherheit überprüft werden. Da sich Modellklassen in ihrer Syntax und Semantik unterscheiden, gibt es eine Vielzahl von Model Checking Ansätzen.

Die Analyse *stochastischer hybrider Systeme* ist aufgrund der Ausdrucksstärke dieser mächtigen Modellklasse eine anspruchsvolle Aufgabe. Bestehende Ansätze skalieren häufig

¹ Englischer Titel der Dissertation: “Statistical Model Checking and Time-Bounded Reachability Analysis for Hybrid Petri Nets with Multiple Stochastic Variables”

² Westfälische Wilhelms-Universität Münster, Institut für Informatik, Einsteinstraße 62, 48149 Münster, Deutschland carina.dasilva@uni-muenster.de

nicht angemessen und basieren auf Abstraktionen, die zu einem Kompromiss zwischen Genauigkeit und Effizienz führen. Meine Dissertation [Pi21] stellt verschiedene Methoden zur Analyse sogenannter *hybrider Petri-Netze mit allgemeinen Transitionen* (HPnGs) [GR16] vor, die von statistischem Model Checking bis zur formalen Verifikation reichen. Der resultierende Fehler der Ansätze kann dabei charakterisiert werden.

HPnGs wurden bereits erfolgreich für die Analyse einer Wasseraufbereitungsanlage [GRH13] und in den Bereichen Smart Home [Gh15] und Elektromobilität [HR16] eingesetzt. Allerdings bergen bestehende Analyseansätze für HPnGs die Gefahr einer „Explosion“ des Zustandsraumes, da jede induzierte Zufallsvariable den Zustandsraum eines HPnGs um eine Dimension erweitert. Dies schränkt die Skalierbarkeit der Ansätze in der Praxis stark ein. Als Alternative zu Analyseverfahren stellt die meine Dissertation statistisches Model Checking für HPnGs vor und erweitert dieses Konzept für HPnGs mit nichtlinearem kontinuierlichen Verhalten, das durch Systeme gewöhnlicher Differentialgleichungen ausgedrückt wird. Des Weiteren stellt die Arbeit einen Ansatz für die zeitlich begrenzte Erreichbarkeitsanalyse von HPnGs vor, bei dem exakte Mengen erreichbarer Zustände bestimmt werden. Zur Berechnung der Wahrscheinlichkeit, definierte Zielzustände zu erreichen, wird dabei auf numerische Integration zurückgegriffen. Für den Umgang mit diskretem Nichtdeterminismus werden nichtprophetische und prophetische Strategien betrachtet.

Darüber hinaus wird eine Transformation von HPnGs in eine Unterklasse von stochastischen hybriden Automaten vorgestellt. Diese ermöglicht die Verwendung bestehender, für die Verifikation hybrider Automaten entwickelter Methoden für stochastische hybride Systeme. Diese Methoden werden in der Dissertation zu einer *Flowpipe*-basierten Erreichbarkeitsanalyse für die aus der Transformation resultierende Modellklasse erweitert. Dieses Analyseverfahren ist ebenfalls bis auf den Fehler der numerischen Integration exakt.

2 Stochastische hybride Systeme

Wir unterscheiden Systeme anhand der Art der Variablen, die zur Beschreibung der Eigenschaften eines Systems vonnöten sind. Ein diskretes System wird ausschließlich durch diskrete Variablen beschrieben, die Werte aus einer endlichen oder abzählbar unendlichen Menge annehmen. Dies kann zum Beispiel der binäre Zustand eines Geräts sein oder die Häufigkeit, wie oft ein bestimmtes Ereignis eintritt. In einem kontinuierlichen System nehmen die Variablen Werte aus einer unendlichen Menge an. Beispiele für kontinuierliche Variablen sind die Flüssigkeitsmenge in einem Gefäß oder physikalische Größen wie Temperatur oder Druck. Systeme, die sowohl diskrete als auch kontinuierliche Variablen kombinieren, bezeichnen wir als *hybrid*.

Ein System mit probabilistischem oder stochastischem Verhalten wird durch zufällige Ereignisse, wie zum Beispiel Systemausfälle, bestimmt. Das Auftreten dieser Ereignisse kann durch diskrete oder kontinuierliche Zufallsvariablen modelliert werden, denen (diskrete

oder kontinuierliche) Wahrscheinlichkeitsverteilungen zugeordnet sind. Wir verstehen dabei *stochastische* Variablen als von der Zeit abhängige Zufallsvariablen.

Es ist möglich, dass ein System in einem Modell nicht vollständig spezifiziert ist – sei es absichtlich oder aufgrund fehlender Informationen. Solche Modelle bezeichnen wir als nichtdeterministisch. Wir unterscheiden dabei zwischen diskretem und kontinuierlichem Nichtdeterminismus in Abhängigkeit davon, ob sich die Unterspezifikation auf diskrete oder kontinuierliche Variablen bezieht.

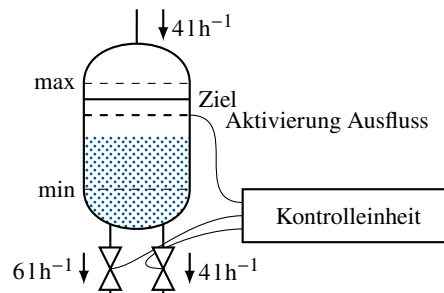


Abb. 1: Tank mit konstantem Einfluss und zwei kontrollierten Ausflussventilen [PSR21, Abb. 4].

Beispiel Abb. 1 zeigt die Skizze eines Tanks, der durch eine Pumpe dauerhaft gefüllt und durch zwei ein- und ausschaltbare Ventile entleert wird [PSR21, Abb. 4]. Die Flüssigkeit im Tank wird durch eine kontinuierliche Variable und die Zustände der Ventile durch zwei diskrete Variablen beschrieben. Die Kontrolleinheit des Tanks kann wählen, welches Ventil aktiviert werden soll, was zu einer diskreten nichtdeterministischen Entscheidung führt. Nach Deaktivierung sind beide Ventile für eine zufällige Zeitspanne blockiert, wobei die Dauer jeder Blockierungsphase durch eine eigene kontinuierliche Zufallsvariable beschrieben wird. Somit ist dieses System ein Beispiel für ein hybrides System mit stochastischem Verhalten und diskretem Nichtdeterminismus. Ein solcher Tank könnte Teil eines sicherheitskritischen Systems sein, in dem ein Über- oder Unterlauf der Flüssigkeit im Tank katastrophale Schäden verursacht.

Hybride Petri-Netz mit allgemeinen Transitionen Unsere Definition für HPnGs folgt Gribaudo und Remke [GR16]. Ein *hybrides Petri-Netz mit allgemeinen Transitionen* ist als ein Tupel $(\mathcal{P}, \mathcal{T}, \mathcal{A}, \mathbf{M}_0, \Phi)$ definiert. Die Menge $\mathcal{P} = \mathcal{P}^{disc} \cup \mathcal{P}^{cont}$ ist eine endliche Menge von diskreten und kontinuierlichen *Plätzen*. Die diskreten Plätze eines HPnGs enthalten eine natürliche Anzahl von *Marken*. Die kontinuierlichen Plätze enthalten dagegen eine *Flüssigkeit*, deren Flüssigkeitsstand durch einen reellen Wert ausgedrückt wird. Jede Markierung $\mathbf{M}_i$ des HPnGs setzt sich dabei aus einer Markenbelegung $\mathbf{m}_i$ und Flüssigkeitsständen $\mathbf{x}_i$ zusammen. $\mathbf{M}_0$ bezeichnet die initiale Markierung.

Die Menge $\mathcal{T} = \mathcal{T}^{imm} \cup \mathcal{T}^{det} \cup \mathcal{T}^{gen} \cup \mathcal{T}^{cont}$ ist eine endliche Menge von *Transitionen*. Wir unterscheiden zwischen unmittelbaren, deterministischen, allgemeinen und kontinuierlichen Transitionen. Plätze und Transitionen werden durch Kanten der Menge $\mathcal{A} = \mathcal{A}^{disc} \cup \mathcal{A}^{cont} \cup \mathcal{A}^{test} \cup \mathcal{A}^{inh}$ verbunden. Diskrete Kanten aus $\mathcal{A}^{disc}$ verbinden diskrete Plätze mit nichtkontinuierlichen Transitionen; kontinuierliche Kanten aus $\mathcal{A}^{cont}$ verbinden kontinuierliche Plätze und kontinuierliche Transitionen. Durch das *Feuern* einer Transition kann sich die aktuelle Markierung der mit ihr verbundenen Plätze ändern. Eine Test- oder Hemmkante aus $\mathcal{A}^{test}$ bzw. $\mathcal{A}^{inh}$ ermöglicht dabei das Kontrollieren einer Transition in Abhängigkeit der Markierung des mit ihr verbundenen Platzes. Alle nichtkontinuierlichen Transitionen ändern die Markenbelegung diskreter Plätze zu ihrem Feuerungszeitpunkt. Allgemeine Transitionen aus $\mathcal{T}^{gen}$ haben dabei zufällige Feuerungszeiten, die durch Zufallsvariablen beschrieben werden. Diese folgen absolut kontinuierlichen Wahrscheinlichkeitsverteilungen. Kontinuierliche Transitionen hingegen verändern die Flüssigkeitsstände kontinuierlich über die Zeit mit stückweise-konstanten Flußraten.

Die Details zur Semantik von HPnGs werden in der Dissertation erläutert. Die Parameterfunktionen aus dem Tupel Φ dienen dabei der Festlegung von Kapazitätsgrenzen, Feuerungszeiten, Flussraten für die kontinuierlichen Transitionen sowie Verteilungsregeln für Konflikte unter Transitionen und werden in dieser Kurzfassung nicht weiter ausgeführt.

3 Beiträge der Dissertation zum Stand der Wissenschaft

Die Beiträge der Dissertation zum Stand der Wissenschaft lassen sich in drei Teilgebiete aufteilen, die im Folgenden erläutert werden: statistisches Model Checking für HPnGs (Abschnitt 3.1), zeitlich begrenzte Erreichbarkeitsanalyse für HPnGs (Abschnitt 3.2) und der Übergang zu stochastischen hybriden Automaten (Abschnitt 3.3).

3.1 Statistisches Model Checking für HPnGs

Meine Dissertation präsentiert Algorithmen für die ereignisbasierte Simulation von HPnGs, basierend auf dem in meiner Masterarbeit [Pi16] entwickelten Ansatz. Dabei wird in jedem Simulationslauf ein Zufallswert für jede Feuerung einer allgemeinen Transition generiert. Zur statistischen Auswertung von Eigenschaften in HPnGs dient sogenanntes *statistisches Model Checking*. Dabei lässt sich der maximale resultierende statistische Fehler spezifizieren, der wiederum die Anzahl der erforderlichen Simulationsläufe bestimmt.

Wir möchten die Wahrscheinlichkeit, dass zu einem festen Zeitpunkt eine bestimmte definierte Eigenschaft in einem HPnG erfüllt ist, abschätzen. Da Simulation mit einer endlichen Anzahl an Simulationsläufen nie ein exaktes Ergebnis liefert, wird der Anteil der möglichen Verläufe, die die Eigenschaft erfüllen, über ein Konfidenzintervall abgeschätzt, sodass für ein Irrtumsniveau $\alpha \in [0, 1]$ die tatsächliche Wahrscheinlichkeit in $(100 \cdot (1 - \alpha))$

Prozent der Fälle von dem Konfidenzintervall überdeckt wird. Für diese Methode betrachtet die Dissertation vier Ansätze: das Standard-, das Wald-, das Clopper-Pearson- und das Score-Konfidenzintervall.

Eine Alternative zur Berechnung von Konfidenzintervallen bieten Hypothesentests. Diese entscheiden, ob die Wahrscheinlichkeit, dass die betrachtete Eigenschaft erfüllt ist, größer oder kleiner als ein definierter Schwellenwert ist. Die Dissertation betrachtet den sequentiellen Likelihood-Quotienten-Test, den Gauss Single Sampling Plan, den Gauss Confidence Interval Test, den Chow-Robbins Test und den Azuma-Test. Diese Tests bringen jeweils verschiedene Vorteile und Risiken mit sich, die in der Arbeit diskutiert werden.

Die in der Dissertation vorgestellten Algorithmen wurden in dem Simulator HYPEG³ implementiert, mit dessen Hilfe die verschiedenen Arten von Konfidenzintervallen und Hypothesentests in der Dissertation im Rahmen einer Fallstudie über einen Ladevorgang für Elektrofahrzeuge miteinander verglichen werden.

Simulation mit nichtlinearen kontinuierlichen Verläufen Die Dissertation erweitert den Modellformalismus der HPnGs um nichtlineare kontinuierliche Verläufe, die durch Systeme gewöhnlicher Differentialgleichungen beschrieben werden können. Dazu wird die Menge der Transitionen um sogenannte dynamische kontinuierliche Transitionen erweitert, deren aktuelle Flußrate von den aktuellen Werten der kontinuierlichen Variablen, also der Flüssigkeitsstände, abhängen kann.

Dementsprechend werden in der Dissertation die Methoden des statistischen Model Checkings für nichtlineare Modelle erweitert, wobei jedoch für die Bestimmung des Zeitpunktes des jeweils nächsten Ereignisses in der Simulation eine Approximation erforderlich ist. Um das nichtlineare Verhalten abzuschätzen, wird der kontinuierliche Teil des HPnGs in ein sogenanntes *quantisiertes Zustandssystem zweiter Ordnung* (QSS2) nach Kofman [Ko02] überführt. In diesem System wird jede kontinuierliche Variable durch einen Quantisierer erster Ordnung approximiert. Dabei ist sichergestellt, dass die lokale Differenz zwischen dem tatsächlichen Wert der kontinuierlichen Variablen und dem Wert des Quantisierers einen vordefinierten Schwellenwert nicht überschreitet. Sobald die lokale Differenz diesen Schwellenwert erreicht, wird der Wert des Quantisierers neu berechnet. Für stabile lineare zeitinvariante Systeme ist dabei der Fehler im zugehörigen quantisierten Zustandssystem zweiter Ordnung begrenzt und abhängig vom gewählten Schwellenwert. Abb. 2 skizziert einen möglichen Verlauf einer Variablen $x_i(t)$ und deren Quantisierer $q_i(t)$ über die Zeit t , unter Berücksichtigung des Schwellenwerts Δq_i .

Für das statistische Model Checking von HPnGs mit nichtlinearen Verläufen wird der Simulationsansatz in der Dissertation um die Neuberechnung der Quantisierer als zusätzliche Ereignisart erweitert. Für den Fall, dass beim Überprüfen einer Eigenschaft die Approximation zu ungenau ist, werden zusätzliche Ereignisse, also frühere Neuberechnungen

³ <https://zivgitlab.uni-muenster.de/ag-sks/tools/hypeg>

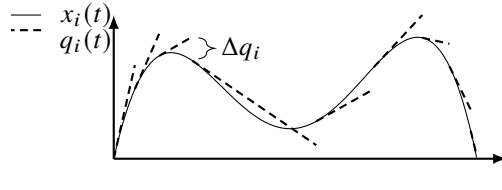


Abb. 2: Eingangs- und Ausgangstrajektorien in einem Quantisierer erster Ordnung, eigene Darstellung nach [Ko02, p.79, Figure 4].

des Quantisierers, ergänzt. Dieser Ansatz wird in der Dissertation in einer Fallstudie über das kinetische Batteriemodell [MM93] für nichtlineares Lade- und Entladeverhalten von Batterien validiert.

3.2 Zeitlich begrenzte Erreichbarkeitsanalyse

Meine Dissertation stellt einen Ansatz für die zeitlich begrenzte Erreichbarkeitsanalyse von HPnGs vor, der auf der symbolischen Zustandsraumdarstellung des sogenannten *Parametric Location Tree* (PLT) [Hü21] basiert. Diese Darstellung beschreibt das stochastische Verhalten eines HPnGs symbolisch in Abhängigkeit der Zufallsvariablen. Dabei werden in einer Baumstruktur Zustände mit identischen Werten der diskreten Variablen in Knoten zusammengefasst. Durch die Begrenzung der Zeit ist der resultierende Baum endlich und vollständig berechenbar.

Die zeitlich begrenzte Erreichbarkeitsanalyse bestimmt exakte Mengen von erreichbaren Zuständen basierend auf dem Parametric Location Tree und verwendet Monte-Carlo-Methoden für mehrdimensionale Integration zur Berechnung der Wahrscheinlichkeit, definierte Zielzustände innerhalb einer Zeitspanne $[0, t_{\max}]$, $t_{\max} \in \mathbb{R}_{\geq 0}$ zu erreichen. Jeder Knoten Λ_k des Parametric Location Tree enthält für jede Zufallsvariable s_i , $i \in \{1, \dots, n\}$ einen Wertebereich $[l_i, u_i]$, sodass der Knoten Λ_k genau dann erreicht wird, wenn alle n Zufallsvariablen einen Wert innerhalb des jeweiligen Bereichs annehmen. Die Wahrscheinlichkeit $p(\Lambda_k, t_{\max})$ einen Zielknoten Λ_k innerhalb der Zeitspanne $[0, t_{\max}]$ zu erreichen, wird dabei via mehrdimensionaler Integration wie folgt berechnet:

$$p(\Lambda_k, t_{\max}) = \int_{l_1}^{u_1} \int_{l_2}^{u_2} \dots \int_{l_n}^{u_n} \prod_{i=1}^n g_i(s_i) ds_n \dots ds_2 ds_1, \quad (1)$$

wobei für $i \in \{1, \dots, n\}$, g_i die zur Zufallsvariablen s_i gehörige Wahrscheinlichkeitsdichtefunktion ist. Für den letzten Schritt der numerischen Integration wird der statistische Fehler in der Dissertation abgeschätzt.

Strategien Wenn in einem HPnG zwei oder mehr deterministische oder unmittelbare Transitionen zum selben Zeitpunkt feuern sollen, entsteht diskreter Nichtdeterminismus.

Während bestehende Analyseverfahren für HPnGs einen solchen inhärenten diskreten Nichtdeterminismus durch Prioritäten und Gewichte probabilistisch auflösen, bleibt er in der zeitlich begrenzten Erreichbarkeitsanalyse erhalten. Die Dissertation untersucht stattdessen verschiedene Arten von Strategien (engl. *scheduler*), um nichtdeterministische Entscheidungen zu treffen. Meine Dissertation stellt Algorithmen zur Bestimmung maximaler und minimaler Wahrscheinlichkeiten für zeitlich begrenzte Erreichbarkeit vor, wobei über die Klassen der sogenannten nichtprophetischen und prophetischen Strategien optimiert wird.

Aufgrund der Verwendung des Parametric Location Tree können nichtprophetische Strategien dabei vom diskreten Teil aller vorherigen Zuständen, der sogenannten diskreten Vergangenheit, abhängen. Dabei betrachten wir für einen Zustand Γ_k eine Menge $C(\Gamma_k) \subseteq \mathcal{T}^{det} \cup \mathcal{T}^{imm}$ von deterministischen oder unmittelbaren Transitionen, die zum selben Zeitpunkt feuern sollen. Eine solche von der diskreten Vergangenheit abhängige, *nichtprophetische Strategie* ist definiert als eine messbare Funktion s , die jeder diskreten Vergangenheit, die zu einem Konflikt von Transitionen der Menge $C(\Gamma_k)$ im Zustand Γ_k führt, eine diskrete Wahrscheinlichkeitsverteilung über die Transitionen in $C(\Gamma_k)$ zuweist.

Da ein Pfad durch den Parametric Location Tree die diskrete Vergangenheit kodiert und für die nichtprophetische Strategie keine weiteren Informationen verfügbar sind, trifft eine solche Strategie immer dieselbe Entscheidung in einem Knoten des Baumes. Daher kann die maximale bzw. minimale Wahrscheinlichkeit, einen Zielzustand zu erreichen, bestimmt werden, indem der Baum rekursiv iteriert wird: Für jeden Konflikt können die Erreichbarkeitswahrscheinlichkeiten der entsprechenden Teilbäume verglichen und das jeweilige Maximum bzw. Minimum von unten nach oben gereicht werden, sodass die optimale Wahrscheinlichkeit letztendlich an die Wurzel gereicht wird.

Prophetische Strategien berücksichtigen hingegen zusätzlich zukünftige Feuerungszeiten der allgemeinen Transitionen. Sie „kennen“ also die Werte der Zufallsvariablen. Prophetische Strategien können (aufgrund ihres Wissens über die Zufallsvariablen und der symbolischen Darstellung des PLT) von der gesamten Vergangenheit abhängen. Sei für ein gegebenes HPnG, n die (maximale) Anzahl an Zufallsvariablen, die in diesem HPnG bis zu einer Zeitgrenze induziert werden. Eine von der Vergangenheit abhängige, *prophetische Strategie* für ein HPnG ist somit eine messbare Funktion s , die jedem Paar aus einer Vergangenheit, die zu einem Konflikt von Transitionen der Menge $C(\Gamma_k)$ im Zustand Γ_k führt, und einer Zuordnung von n positiven reellen Werten zu den Zufallsvariablen eine diskrete Wahrscheinlichkeitsverteilung über die Transitionen in $C(\Gamma_k)$ zuweist.

Da in einem HPnG per Definition keine Informationen über zukünftige Feuerungszeiten der allgemeinen Transitionen verfügbar sind, ist für die Berücksichtigung prophetischer Strategien eine Modellanpassung nötig. Diese ermöglicht die Vorberechnung der Feuerungszeiten und das Speichern dieser Zeiten mithilfe zusätzlicher kontinuierlicher Variablen. Für das angepasste Modell können dann optimale Wahrscheinlichkeiten, die prophetischen Strategien entsprechen, berechnet werden. Dafür wird ebenfalls der Parametric Location Tree iteriert

und ein resultierendes Optimierungsproblem gelöst. Die Details zur Modellanpassung und zum Optimierungsproblem sind in der Dissertation dargelegt.

Die Algorithmen für optimale nichtprophetische Strategien wurden in dem Tool `hpnmg`⁴ implementiert. Für den prophetischen Fall wurde ein Machbarkeitsnachweis erbracht, der jedoch die Verfügbarkeit eines effizienten Solvers für das zugrunde liegende Optimierungsproblem erfordert. In der Dissertation wird die Realisierbarkeit beider Ansätze in einer Fallstudie über eine Entscheidung zwischen einem Fahrzeug mit Elektroantrieb und einem Fahrzeug mit Verbrennungsmotor demonstriert.

3.3 Übergang zu stochastischen hybriden Automaten

Meine Dissertation stellt eine Transformation von HPnGs in eine Unterklasse stochastische hybrider Automaten vor, die die Anwendung bestehender analytischer Methoden ermöglicht. Diese Transformation basiert auf der Definition einer Semantik für ein gegebenes HPnG, die durch einen *singulären Automaten mit Zufallsuhren und zwingenden Sprüngen* ausgedrückt wird.

Wir folgen der Definition hybrider Automaten von Alur et al. [Al95]. Ein singulärer Automat ist ein hybrider Automat, in dem die erste Ableitung einer jeden kontinuierlichen Variablen konstant ist. Dabei wird in der Dissertation durch die Restriktion auf zwingende Sprünge kontinuierlicher Determinismus ausgeschlossen. Diskrete Zustandsänderungen erfolgen also nur zu festen Zeitpunkten. Die Erweiterung von singulären Automaten um Zufallsuhren ermöglicht die Modellierung von stochastischem Verhalten. Die Zeit bis zum Ablauf einer Zufallsuhr wird durch eine absolut kontinuierliche Wahrscheinlichkeitsverteilung beschrieben. Eine formale Definition dieser Modellklasse ist in der Dissertation gegeben.

Ein Algorithmus für die Überführung eines HPnGs in einen solchen Automaten wird in der Dissertation vorgestellt und wurde ebenfalls in das `hpnmg`-Tool implementiert. Die Machbarkeit wird in der Dissertation für einen Batterieladeprozess demonstriert.

Flowpipe-basierte Erreichbarkeitsanalyse Für die Unterklasse stochastischer hybrider Automaten, die wir durch die Transformation erhalten, stellt meine Dissertation eine neue Methode zur Berechnung von Wahrscheinlichkeiten für zeitlich begrenzten Erreichbarkeit vor. Der Ansatz basiert auf der Konstruktion einer sogenannten *Flowpipe* [Fr05], welche ein bewährtes Analyseverfahren für hybride Automaten ist. Dieser Ansatz liefert die Menge aller erreichbaren Zustände. Darauf aufbauend stellt meine Dissertation Algorithmen für die Berechnung optimaler Wahrscheinlichkeiten unter Berücksichtigung vergangenheitsabhängiger nichtprophetischer und prophetischer Strategien für singuläre Automaten mit Zufallsuhren vor. Durch eine geometrische Repräsentation der Zustandsmengen als konvexe Polytope kann dabei auf geometrische Operationen zurückgegriffen werden, die es

⁴ <https://zivgitlab.uni-muenster.de/ag-sks/tools/hpnmg>

ermöglichen, nichtprophetische und prophetische Wahrscheinlichkeiten mit vergleichbarem Aufwand zu berechnen. Die Menge der erreichbaren Zustände ist dabei exakt, wohingegen zur Berechnung von Wahrscheinlichkeiten erneut numerische Integration dient, sodass eine Abschätzung des statistischen Fehlers möglich ist. Die Komplexität der Algorithmen hängt dabei stark von den geometrischen Operationen ab.

Meine Dissertation validiert die nichtprophetischen Ergebnisse in einer Fallstudie über den Tank mit zwei Ventilen (siehe Abb. 1) mit Ergebnissen des Analyseansatzes für HPnGs. Für den prophetischen Fall wird die Machbarkeit anhand desselben Modells gezeigt, für das bisher kein anderes Tool in der Lage war Ergebnisse für höhere Dimensionen zu berechnen. Die Ergebnisse zeigen, dass die Algorithmen sowohl für die nichtprophetischen als auch für die prophetischen Strategien gleich effizient sind, wobei ihre Skalierbarkeit von der Effizienz der zugrunde liegenden Darstellung der Zustandsmengen abhängt.

4 Schlussbemerkung

Die in der Dissertation vorgestellten Methoden bieten neue Ansätze für die Evaluation der mächtigen Klasse der stochastischen hybriden Systeme, indem die Analyse von hybriden Petri-Netzen mit stochastischen Variablen mit Methoden der Erreichbarkeitsanalyse für hybride Automaten vereint wird. Die Verfahren erlauben dabei eine angemessene Abschätzung der induzierten Fehler. Die Ergebnisse der Fallstudien in der Arbeit demonstrieren, dass die Implementierungen auch für höhere Dimensionen präzise Ergebnisse liefern, wobei die Performanz von der Verfügbarkeit effizienter Solver für die Optimierung und numerische Integration sowie von skalierbaren Zustandsraumdarstellungen für hybride Automaten abhängt. Durch die Entwicklung der vorgestellten Methoden leistet die Dissertation einen Beitrag zur Analyse sicherheitskritischer Systeme.

Literatur

- [Al95] Alur, R.; Courcoubetis, C. A.; Halbwachs, N.; Henzinger, T. A.; Ho, P.-H.; Nicollin, X.; Olivero, A.; Sifakis, J.; Yovine, S.: The Algorithmic Analysis of Hybrid Systems. *Theoretical Computer Science* 138/, S. 3–34, 1995.
- [BK08] Baier, C.; Katoen, J.-P.: *Principles of Model Checking*. MIT Press, Cambridge, MA, USA, 2008.
- [Fr05] Frehse, G.: PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. In: *Proc. 8th Int. Workshop on Hybrid Systems: Computation and Control*. Bd. 3414. LNCS, Springer Berlin Heidelberg, S. 258–273, 2005.
- [Gh15] Ghasemieh, H.; Haverkort, B. R.; Jongerden, M. R.; Remke, A.: Energy Resilience Modelling for Smart Houses. In: *Proc. 45th IEEE/IFIP Int. Conf. on Dependable Systems and Networks*. IEEE, S. 275–286, 2015.

- [GR16] Gribaudo, M.; Remke, A.: Hybrid Petri Nets with General One-Shot Transitions. *Performance Evaluation* 105/, S. 22–50, 2016.
- [GRH13] Ghasemieh, H.; Remke, A.; Haverkort, B. R.: Survivability Evaluation of Fluid Critical Infrastructures Using Hybrid Petri Nets. In: *Proc. 19th IEEE Pacific Rim Int. Symposium on Dependable Computing*. IEEE, S. 152–161, 2013.
- [HR16] Hüls, J.; Remke, A.: Coordinated Charging Strategies for Plug-in Electric Vehicles to Ensure a Robust Charging Process. In: *Proc. 10th EAI Int. Conf. on Performance Evaluation Methodologies and Tools*. ICST, S. 19–22, 2016.
- [Hü21] Hüls, J.; Pilch, C.; Schinke, P.; Niehaus, H.; Delicaris, J.; Remke, A.: State-Space Construction of Hybrid Petri Nets with Multiple Stochastic Firings. *ACM Transactions on Modeling and Computer Simulation* 31/3, S. 1–37, 2021.
- [Ko02] Kofman, E.: A Second-Order Approximation for DEVS Simulation of Continuous Systems. *SIMULATION* 78/2, S. 76–89, 2002.
- [MM93] Manwell, J. F.; McGowan, J. G.: Lead Acid Battery Storage Model for Hybrid Energy Systems. *Solar Energy* 50/5, S. 399–405, 1993.
- [Pi16] Pilch, C.: Development of an Event-Based Simulator for Model Checking Hybrid Petri Nets with Random Variables, Masterarbeit, Westfälische Wilhelms-Universität Münster, 2016.
- [Pi21] Pilch, C.: Statistical Model Checking and Time-Bounded Reachability Analysis for Hybrid Petri Nets with Multiple Stochastic Variables, Dissertation, Westfälische Wilhelms-Universität Münster, 2021.
- [PSR21] Pilch, C.; Schupp, S.; Remke, A.: Optimizing Reachability Probabilities for a Restricted Class of Stochastic Hybrid Automata via Flowpipe-Construction. In: *Proc. 18th Int. Conf. on Quantitative Evaluation of Systems*. Bd. 12846. LNCS, Springer Cham, S. 435–456, 2021.



Carina da Silva geb. Pilch wurde am 28. Juni 1990 in Rheine, Deutschland, geboren. Sie schloss 2012 ihr duales Studium der Wirtschaftsinformatik (Bachelor) an der Hochschule Osnabrück als Beste ihres Studiengangs ab. Von 2014 bis 2016 studierte sie Informatik im Master an der Westfälischen Wilhelms-Universität Münster (WWU). Für ihre Masterarbeit über diskrete Ereignissimulation für hybride Petri-Netze mit Zufallsvariablen erhielt sie 2017 den *Preis des Fakultätentags Informatik für eine herausragende Masterarbeit*. Im Anschluss an ihr Studium erhielt sie das *Ada Lovelace Promotionsstudium 2016* des Fachbereichs Mathematik und Informatik der WWU. Ihre Promotion unter Be-

treuung von Prof. Dr. Anne Remke über statistisches Model Checking und zeitlich begrenzte Erreichbarkeitsanalyse für hybride Petri-Netze mit Zufallsvariablen schloss sie im Oktober 2021 mit Auszeichnung (*summe cum laude*) ab. Seit Februar 2022 ist sie als akademische Rätin am Institut für Informatik der WWU tätig.