

HOCHSCHULE FÜR TECHNIK, WIRTSCHAFT UND KULTUR LEIPZIG

MASTERARBEIT

ZUR ERLANGUNG DES AKADEMISCHEN GRADES EINES MASTER OF
SCIENCE (M.Sc.)

Realisierung konsistenter Microservice-Systeme unter Verwendung des Saga-Patterns

Autor

RICHARD WERNER

Erstprüfer

Dr. THOMAS RIECHERT

Zweitprüfer

M.Sc. JOHANNES ELSMANN

11. Januar 2024

HTWK

Hochschule für Technik,
Wirtschaft und Kultur Leipzig

Inhaltsverzeichnis

1	Einleitung	2
1.1	Motivation	2
1.2	Zielsetzung dieser Arbeit	2
1.3	Aufbau dieser Arbeit	2
2	Grundlagen	3
2.1	Grundlagen	3
2.1.1	System allgemein	3
2.1.2	System in der Softwareentwicklung	3
2.1.3	Zustand von Systemen	3
2.1.4	Transaktionen	3
2.1.5	ACID Eigenschaft von Transaktionen	4
2.1.6	Konsistenz auf Datenbankebene	4
2.2	Methoden für die Sicherstellung von Konsistenz	5
2.2.1	Transaktionen auf Datenbankebene	5
2.2.2	Transaktionen auf Anwendungsebene	5
2.2.3	Grenzen der Konsistenz in Verteilten Systemen	5
2.2.4	2 Phasencommit	5
2.3	Saga Pattern	6
2.3.1	Was sind die Probleme, die in verteilten ACID Transaktionen auftreten?	6
2.3.2	Woher kommt es?	6
2.3.3	Bestandteile des Musters	6
2.3.3.1	Funktionsweise	6
2.3.3.2	Anforderungen an Ts und Cs	7
2.3.3.3	Saga Execution Component	8
2.3.3.4	Formalisierung eines Saga-Zustandsautomaten als DEA	8
2.3.3.4.1	Formale Darstellung eines DEA	8
2.3.3.4.2	Saga als formale Sprache	8
2.3.3.5	Betrachtung des Zustands nach Erfolg/Misserfolg	10
2.3.3.6	Unterschiede des Saga-Modells zu Hector Garcia-Molinas Definition	11
2.3.3.7	Recovery-Mechanismen	11
2.3.3.8	Implementierungsformen des Patterns	14
2.3.4	Anwendungsgebiete des Patterns - Welche Usecases erlauben die Verwendung dieses Patterns? Welche nicht?	17
2.3.4.1	Langlebige Transaktionen - LLT	17
2.3.4.2	Bezug auf den Geschäftsprozess	17
2.3.4.3	Verteilte Systemlandschaft	17

2.3.4.4	Reaktion auf verschiedene Antwortmöglichkeiten in der Geschäftslogik	17
2.3.4.5	Fehlerfälle - Geschäftslogik und Ausfälle	17
3	Versuchsvorbereitung	18
3.1	Problemstellung	18
3.2	Zielstellung	18
3.3	Ausgangspunkt	19
3.4	Methodik	19
3.4.1	Schritt 1 - Entwurf und Implementierung eines GP	19
3.4.2	Schritt 2 - Messung der verschiedenen Implementierungen	20
3.4.3	Schritt 3 - Analyse der Messdaten	21
4	Versuchsdurchführung	22
4.1	Services	22
4.2	Lokale Transaktionen	23
4.3	Kompensierungen	24
4.4	Fachliche Kontextabgrenzung	24
4.4.1	Frontend	24
4.4.2	ArticleService	24
4.4.3	StockService	25
4.4.4	BankingServices	26
4.4.5	OrderService	26
4.5	Technische Kontextabgrenzung	27
4.5.1	ArticleService	27
4.5.2	StockService	28
4.5.3	BankingService	29
4.6	Ergebnisse	30
4.6.1	Ergebnisse aller Transaktionen	30
4.6.2	Ergebnisse aller Kompensierungen	31
4.7	Saga Execution Component	32
4.7.1	Rahmenbedingung für die Versuchsdurchführung	32
4.7.2	Ausführung eines DEAs	32
4.7.3	Modellierung eines DEAs	33
4.7.4	Konstruktion eines DEAs	34
4.8	Planung der Datenerfassung	39
4.8.1	Testszenarien	40
4.8.2	Fehlerquellen	40
4.8.3	Simulation der Testfälle	41
4.8.4	Datengenerierung	42
4.8.5	Messwerte	43
4.9	Implementierung des SmBasic	45
4.9.1	Strategie für die Konstruierung des DEAs SmBasic	45
4.9.2	StateAnalysisResult	45
4.9.3	TransactionAnalysisResult	48

4.10	Implementierung des SmBasicSafeRetries	48
4.10.1	Verhinderung eines Vorzeitigen Abbruchs	49
4.10.2	StateAnalysisResult	49
4.10.3	TransactionAnalysisResult	50
4.11	Implementierung des SmBasicNetworkFailureUnlimitedRetries	51
4.11.1	StateAnalysisResult	51
4.11.2	TransactionAnalysisResult	52
4.12	Das Problem der Wiederholbarkeit	53
4.13	Implementierung des SmIdempotencyBackwardRecovery	53
4.13.1	StateAnalysisResult	55
4.13.2	TransactionAnalysisResult	56
4.13.3	Alternative Sicherstellung der Konsistenz	57
4.13.3.0.1	Messung	57
4.14	Implementierung SmIdempotencyForwardRecovery	59
4.14.1	StateAnalysisResult	60
4.14.2	TransactionAnalysisResult	61
4.15	Laufzeitanalyse	61
4.15.1	Testszenario1	61
4.15.2	Testszenario2	62
4.15.3	Testszenario3	62
5	Ergebnisse der Versuchsdurchführung	64
5.1	Versuchsergebnisse	65
5.2	title	65
5.3	Technische Voraussetzungen	65
5.4	Technische Grenzen	65
5.5	Wissenschaftliche Berührungspunkte	66
5.5.1	CAP-Theorem	66
6	Ausblick, Ansatz für weitere Untersuchungen	I
	Abbildungsverzeichnis	II
	Literaturverzeichnis	III

1 Einleitung

1.1 Motivation

Wieso, Weshalb, Warum?

1.2 Zielsetzung dieser Arbeit

These: Mittels Saga-Pattern implementierte langlebige Transaktionen (LLT) ermöglichen Konsistenz in Microservicesystemen, die per Request-Response Pattern kommunizieren.

Leitfragen: Wie kann mithilfe von BASE-Eigenschaft und Softstate ausfallsichere Konsistenz hergestellt werden?

(Wie) kann der 2 Phasencommit in eine Saga-Architektur integriert werden?

1.3 Aufbau dieser Arbeit

- Kapitel 1: Theoretische Grundlagen: In diesem Kapitel sollen dem Leser die Grundlagen vermittelt werden, die er benötigt, um den Rest der Arbeit zu verstehen. Dazu gehören Begriffe und Konzepte aus der Welt der Microservices.
- Kapitel 2: Methodik: Ziel des Kapitels: Entwurf, Implementierung, Messen und Bewertung des Systems. Fokus auf Saga-Pattern, Konsistenz, Ausfallsicherheit -> Der Systementwurf und der Bewertungsprozess aus diesem Kapitel sollen in Kapitel 3 umgesetzt werden.
 - Bewertungskriterien
 - Entwurf und Implementierung eines reinen Saga-Systems
 - Abänderung der Implementierung durch
 - * Saga-Werkzeuge (Checkpoints, Recovery Mechanismen)
 - * 2 Phasencommit
- Kapitel 3: Ergebnisse aus Kapitel 2: Die Ergebnisse dieses Kapitels sollen in Kapitel 4 verwendet werden, um die anfängliche These und die Leitfragen zu beantworten.
- Kapitel 4: Diskussion - Bewerten der Ergebnisse in Bezug auf die These und der Leitfragen; Beantwortung der These und der Leitfragen

2 Grundlagen

2.1 Grundlagen

Um das in dieser Arbeit betrachtete Saga-Pattern zu verstehen, sollen zuerst einige Grundlagen erläutert werden. Besonders die im Titel der Arbeit enthaltenen Begriffe *System* und *Konsistenz* sollen in diesem Abschnitt erläutert werden.

2.1.1 System allgemein

Ein System beschreibt einen abgegrenzten Bereich der objektiven Realität. Außerhalb dieses Bereichs liegt die Umgebung, die somit nicht zum System gehört. Zwischen des Systems und seiner Umgebung befindet sich der Systemrand.

2.1.2 System in der Softwareentwicklung

In der Softwareentwicklung besteht ein System aus einer Menge miteinander interagierenden Softwarekomponenten. Diese Komponenten arbeiten an einem gemeinsamen Ziel. Neben der Software und deren Quellcode gehören auch Nutzerhandbücher, Tests, Bestandteile für die Instandhaltung sowie Spezifikationen und Konzepte zum System.

2.1.3 Zustand von Systemen

Ein Softwaresystem befindet sich zu jedem Zeitpunkt in einem Zustand. Der Wechsel eines Zustands ist die Folge von Nutzerinteraktionen und festgelegten Routinen. Damit das System reibungslos funktionieren kann, darf es nur zwischen gültigen Zuständen wechseln.

2.1.4 Transaktionen

Ein Übergang von einem Zustand in den nächsten Zustand im Modell des Zustandsautomats ist eine einzige Operation. Häufig äußert sich eine solche Operation jedoch in einer Folge von auszuführenden Operationen. Eine solche Folge von Operationen wird als Transaktion bezeichnet. Teil einer Transaktion kann beispielsweise eine oder mehrere Datenbankoperationen oder der Aufruf einer externen Schnittstelle sein. Transaktionen können auf verschiedenen Ebenen betrachtet werden. Auf Datenbankebene werden Transaktionen anders umgesetzt als auf Ebene der Geschäftslogik.

2.1.5 ACID Eigenschaft von Transaktionen

ACID ist ein Akronym, welches häufig verwendet wird, um Eigenschaften auszudrücken, die eine Transaktion auf Datenbankebene aufweisen sollte. Die Buchstaben stehen für *Atomicity* (Atomarität), *Consistency* (Konsistenz), *Isolation* (Isolation) und *Durability* (Dauerhaftigkeit).

Atomarität beschreibt hier das Alles-Oder-Nichts-Prinzip. Eine Transaktion, also eine Folge von Datenbankoperationen, muss entweder alle Operationen ausführen oder in einem Fehlerfall alle Änderungen auf den ursprünglichen Zustand zurückrollen. Als illustratives Beispiel soll das Szenario einer Überweisung dienen. Eine Überweisung besteht aus dem Erhöhen des Kontostands des Debitors und dem Verringern des Kontostands des Kreditors. Eine solche Transaktion kann fehlschlagen. Dabei ist sicherzustellen, dass die initialen Kontostände wiederhergestellt werden. Wird die Atomarität nicht gewährleistet, könnte sich die Gesamtsumme des im System enthaltenen Systems verändern, Geld geht also verloren oder Geld wird aus dem Nichts generiert. Das ist natürlich nicht akzeptabel.

Konsistenz lässt sich mit widerspruchsfrei übersetzen. War das System vor Ausführung der Transaktion widerspruchsfrei, also konsistent, dann ist es das nach Ausführung der Transaktion ebenso. Um dies zu gewährleisten, sind verschiedene Mechanismen im Datenbanksystem im Einsatz. Dies werden im folgenden Abschnitt beschrieben.

Isolation stellt sicher, dass sich parallel in Ausführung befindliche Transaktionen nicht gegenseitig beeinflussen können. Das bedeutet, dass eine Transaktion Teile der Datenbasis sperren können muss. Eine solche Sperre führt jedoch zu blockierendem Verhalten und schränkt somit die nebenläufige Benutzung der Datenbank ein.

Dauerhaftigkeit von Transaktionen muss gewährleistet sein, damit bei einem Ausfall Transaktionsdaten nicht verloren gehen. Um Dauerhaftigkeit zu erreichen, wird ein Transaktionslog geführt, welches im Ausfall verwendet werden kann, um die verlorenen Transaktionen nachzuspielen.

2.1.6 Konsistenz auf Datenbankebene

Auf Datenbankebene wird die Konsistenz durch drei Mechanismen sichergestellt: Bereichsintegrität, Entitätsintegrität, Referentielle Integrität und logische Konsistenz.

Die *Bereichsintegrität* stellt lediglich sicher, dass die Werte einer Spalte in einem definierten Wertebereich befinden.

Die *Entitätsintegrität* beschreibt die Eindeutigkeit eines Datensatzes und somit Fähigkeit, diesen Datensatz mittels Primärschlüssel eindeutig identifizieren zu können.

Die *Referentielle Integrität* gewährleistet, dass Relationen zwischen Datensätzen nicht auf nicht existierende Datensätze zeigen können. Ist ein Fremdschlüssel gesetzt, so muss der referenzierte Datensatz existieren.

Die in der Datenbank enthaltenen Daten drücken einen Sachverhalt aus. Die semantische Bedeutung dieser Daten kann nicht durch das Datenbanksystem sichergestellt werden. Es liegt in der Verantwortung des Entwicklers, allen Nutzerinteraktionen mit dem System die korrekten Transaktionen zuzuordnen. Ein System ist *logisch konsistent*, wenn kein logisch inkonsistenter Zustand erreichbar ist.

2.2 Methoden für die Sicherstellung von Konsistenz

Um einen konsistenten Zustand zu gewährleisten gibt es verschiedene Werkzeuge. Dazu gehören vor allem die Unterstützung von lokalen Transaktionen der Datenbank und der 2 Phasencommit. In diesem Abschnitt werden die (...) beschrieben.

2.2.1 Transaktionen auf Datenbankebene

Eine lokale Transaktion einer Anwendung wird oft durch eine Nacheinanderausführung von SQL-Statements realisiert. Zu Beginn wird dem DBMS signalisiert, dass die folgenden Operationen als atomare Transaktion zu interpretieren sind. Analog dazu gibt es ein Signal, welches das Ende einer solchen Folge markiert, den *Commit*. Tritt vor Erreichen des Commits ein Fehler auf, wird ein *Rollback* ausgeführt. Dieser Rollback überführt die Daten in den Zustand vor Beginn der Transaktion. Die Datenbank - Transaktion - Begin - Commit - Rollback - Aufruf aus der Anwendung

2.2.2 Transaktionen auf Anwendungsebene

- Operation ist ein Funktionsaufruf - Verkettung ist mittels try-catch Block behandelbar
 - Verantwortung des Entwicklers, dass alle Operationen erfolgreich sind - Verantwortung des Entwicklers, Fehler zu behandeln - Abwicklung der Transaktion per DBMS
- Transaktionen sinnvoll

2.2.3 Grenzen der Konsistenz in Verteilten Systemen

- Transaktion kann Aktion beinhalten, die eine Abhängigkeit aufruft (zB Aufruf einer externen Http-Schnittstelle) - Zentrales Problem: Wie stelle ich sicher, dass ein Aufruf angekommen ist? ..., dass der Aufruf erfolgreich war? Wie gehe ich vor, wenn eine Aktion einer Transaktion nicht geklappt hat? - Folge von abhängigen Operationen (= Substitution: Ergebnis eines Aufrufs ist Argument der nächsten Aufrufs)

2.2.4 2 Phasencommit

- 2 Phasen Commit als verteilte Umsetzung des Transaktionsvorgehens - zentraler Koordinator - Vorbereitungsphase: Alle teilhabende Akteure der Transaktion geben dem Koordinator die Bestätigung, dass die Operation ausgeführt werden kann. Damit sie dieses Versprechen halten können, beinhalten die Vorbereitungen oft Blockierungen auf Datenbankseite. - Commitphase: Koordinator gibt den Teilhabenden das Signal, ihre Operation auszuführen. Bei Erfolg werden auch alle Blockierungen aufgehoben. Die Transaktion wird als erfolgreich markiert. - Optionale Rollbackphase: Falls ein Teilhabender einen Fehler zurückgibt, werden alle ausgeführten Änderungen zurückgenommen (Rollback). Danach wird die Transaktion als abgebrochen markiert. Alle Blockierungen müssen zurückgenommen werden. - Nachteile: sehr hohe Chattines, sehr langsam, blockierend, geringer Throughput, komplexe Implementierung

2.3 Saga Pattern

2.3.1 Was sind die Probleme, die in verteilten ACID Transaktionen auftreten?

Im vorherigen Abschnitt wurden die mit dem ACID-Konsistenzprinzip einhergehenden Probleme dargestellt, wenn man sich in einem verteilten System befindet:

- Blockierung der Ressourcen
- Viele Netzwerkaufrufe - Chattiness
- Enge Kopplung der Dienste -

2.3.2 Woher kommt es?

Referenzierung des Papers 1987 Garcia

2.3.3 Bestandteile des Musters

2.3.3.1 Funktionsweise

Das Saga-Pattern ist ein Entwurfsmuster, um eine verteilte Transaktion abzubilden. Eine Transaktion wird hier auch durch eine Menge von auszuführenden Operationen gebildet. Auch für das Saga-Pattern gehört die Gewährleistung der ACID-Eigenschaft zu den Anforderungen. Die Art und Weise, wie diese Eigenschaften erreicht werden unterscheidet sich jedoch vom 2-Phasencommit. Anstatt alle teilnehmenden Operationen durch einen Befehl gleichzeitig auszulösen, werden alle Operationen sequentiell ausgeführt. Eine Operation ist im Saga-Pattern eine lokale Transaktion, die in sich geschlossen ist und ebenfalls die ACID-Eigenschaft erfüllen muss. Für eine solche Operation wird gleichzeitig eine Schnittstelle angeboten, die die Veränderungen rückgängig macht. Somit besteht die Möglichkeit eine Operation zu neutralisieren. Es wird also die Voraussetzung an den Entwickler gestellt, für jede angebotene Operation eine Umkehroperation bereitzustellen, die selbst eine lokale Transaktion darstellt. Im Paper werden lokale Transaktionen, die eine Operation der Transaktion darstellen, als Ts bezeichnet. Die dazugehörigen lokalen Transaktionen werden als Cs bezeichnet. Die Transaktion kann nun also ausgeführt werden. Jedes teilhabende T wird nacheinander ausgeführt. Tritt bei der Ausführung eines Ts ein Fehler auf, können alle bereits ausgeführten Operationen in ihren Ursprungszustand zurückgesetzt werden, indem in der umgekehrten Reihenfolge die notwendigen Cs aufgerufen werden. Im Fehlerfall wird der Ausgangszustand in allen Services wiederhergestellt und die Atomarität der Transaktion ist gewährleistet. Sind alle Operationen erfolgreich, wird nach Ausführung aller Ts der Endzustand erreicht und die Transaktion hat einen neuen Zustand hergestellt. Sowohl im erfolgreichen als auch im kompensierten Endzustand ist die Konsistenz gewahrt.

2.3.3.2 Anforderungen an Ts und Cs

Die einzelnen Operationen, die ausgeführt werden müssen, müssen also kompensiert werden können. Eine solches T wird als lokale Transaktion betrachtet, die in einem anderen Service stattfindet. Der aufrufende Service soll als S1 und der T durchführende Service als S2 bezeichnet werden. Der Effekt der Transaktion ist häufig eine Veränderung in der Datenbank von S2. Es wird nun betrachtet, welche verschiedenen Effekte T in der Datenbank haben kann und welchen Effekt das entsprechende C haben muss.

Äußert sich der Effekt von T in einem Insert, dann ist der kompensierende Effekt von C ein Delete. Somit ist dieses Element für andere Prozesse nicht mehr auffindbar. Der Zustand ist also identisch mit dem Zustand vor Durchführung von T. Anstatt das Element zu löschen kann eine Markierung des zuvor eingefügten Elements vorgenommen werden. Diese Markierung kann ein zusätzliches Feld sein oder eine zusätzliche Tabelle, die die gelöschten Elemente auflistet. Muss ein Prozess nun mit den gültigen Elementen der Tabelle arbeiten, wird zusätzlich diese Markierung geprüft. Es ist somit möglich, den Zustand vor Durchführung von T zu reproduzieren.

Wenn der Effekt von T ein Update ist, ist die Kompensierung unter Umständen schwieriger. Wenn der Effekt von T eine Erhöhung eines Feldes um n auslöst, dann muss der Effekt das selbe Feld um n verringern. Eine solche Paarung von T und C ist leicht zu implementieren.

Ist der Effekt von T ein idempotentes Update, dann muss S2 eine Historytabelle bereithalten, um den Ausgangszustand reproduzieren zu können. Angenommen das vom Update betroffene Feld hat anfangs den Wert n und der Effekt von T setzt den Inhalt des Feldes auf n -Strich, dann muss innerhalb einer lokalen Transaktion der Wert von n in einer Historytabelle abgespeichert werden und der neue Wert kann gesetzt werden. Wenn nun der Effekt von T kompensiert werden soll, wird der historische Wert n per Select ermittelt und im tatsächlichen Feld gesetzt werden.

Es ist außerdem möglich, dass ein T wiederum externe Schnittstellen aufruft. In diesem Fall kann die Kompensierungslogik nicht verallgemeinert werden. Es ist möglich, den Prozess so zu gestalten, dass ein solches T als Sub-Saga T_{Sub} modelliert wird. Dabei muss jedoch gewährleistet werden, dass bei Aufruf von C alle Kompensierungen von T_{Sub} aufgerufen werden.

Es ist außerdem hervorzuheben, dass der Effekt eines Ts neben Änderungen in der Datenbank oder Aufrufe von anderen Schnittstellen auch reale Geschäftsprozesse auslösen können. Ein solcher Prozess kann unter Umständen nicht kompensierbar sein. Hier kann auch weiter differenziert werden.

Ist der Effekt von T die Versendung eines Briefs, so kann diese Versendung nicht kompensiert werden. Ein Folgebrief kann jedoch als Kompensierung angesehen werden, die den ausgelösten Effekt neutralisiert. Im Folgebrief können beispielsweise Anweisungen stehen, die den Empfänger informieren, dass der vorherige Brief als ungültig angesehen werden kann. Der Effekt von T kann hier als kompensiert angesehen werden.

Es gibt jedoch auch Effekte, die nicht kompensierbar sind und im Scheitern einer Saga resultieren. In solchen Fällen kann das System in einen inkonsistenten Zustand überführt werden. Dieses Verhalten tritt immer dann auf, wenn der Effekt einer Transaktion in einer endgültigen Aktion resultiert.

2.3.3.3 Saga Execution Component

In Garcia-Molinas Paper wird eine Saga Execution Component beschrieben, welche alle ausgeführten Aktionen einer Saga protokolliert und die nächste auszuführende Aktion bestimmt. Grundlegend besteht diese Komponente aus einem Transaktionslog und einem Zustandsautomaten.

Der Transaktionslog ist eine Liste von Transaktionen und Kompensierungen, die als Kommandos dargestellt werden. Jedes Transaktionslog enthält ein Kommando, welches den Start (*BeginnSaga*) und den Abschluss (*EndSaga*) der Saga darstellt. Neben den Ts und Cs zwischen *BeginnSaga* und *EndSaga* können weitere Kommandos definiert werden, um den Kontrollfluss zu beeinflussen.

Der Zustandsautomat bestimmt aus den bisherigen Ts und Cs den nächsten Schritt.

2.3.3.4 Formalisierung eines Saga-Zustandsautomaten als DEA

2.3.3.4.1 Formale Darstellung eines DEA Der Prozessablauf einer Saga kann als deterministischer endlicher Automat angesehen werden. Ein DEA wird formal dargestellt als Tupel mit folgenden Elementen:

- Q : Zustandsmenge
- Σ : endliches Eingabealphabet
- $\delta : Q \times \Sigma \rightarrow Q$: Übergangsrelation
- $q_0 \in Q$: Startzustand
- $F \subseteq Q$: Menge an akzeptierenden Zuständen

2.3.3.4.2 Saga als formale Sprache Im vorherigen Abschnitt wurde die Saga Execution Component definiert als ein Tupel aus Transaktionslog und Zustandsautomat. Nun soll dieses Tupel in einen DEA überführt werden. Ein solcher DEA A_{Saga} akzeptiert die Sprache L_{Saga} , die alle gültigen Wörter enthält, die eine Saga darstellen.

Das Eingabealphabet Σ ist die Menge aller Elemente, die im Transaktionslog auftauchen können. Somit kann jedes Transaktionslog als Eingabewort aufgefasst werden.

Somit ist die von A_{Saga} akzeptierte Sprache $L_{Saga} = L(A_{Saga})$:

$$\forall w \in \Sigma^* : w \in L(A_{Saga}) \iff w \in L_{Saga}$$

Überführung einer Saga in einen DEA Um eine Saga in einen DEA überführen zu können, müssen zuerst einige Definitionen vorgenommen werden. Die Unterscheidung zwischen Ts und Cs wird im Modell eines Zustandsautomaten per Zustand ausgedrückt. Es muss also eine Abstrahierung vorgenommen werden, die Ts und Cs vereinigt. Diese Abstrahierung wird im Folgenden als *Aktion* A bezeichnet. Eine solche Aktion a_n wird immer im entsprechenden Zustand $q_n \in Q$ ausgeführt. In der folgenden Erläuterung kann die Zustandsmenge Q mit der Menge $T \cup C$ gleichgesetzt werden.

Das Eingabealphabet Σ drückt aus, welche möglichen Ergebnisse eine Aktion haben kann. Eine Aktion kann einerseits ein Aufruf einer externen Schnittstelle sein. Die Antwort dieser Schnittstelle kann das Ergebnis in unterschiedlichen Formen ausdrücken. Das können beispielsweise folgende Ausdrucksformen sein:

- Http-Statuscode
- Custom Http-Responsebody

Diese sind üblicherweise in einer Schnittstellendefinition aufgelistet. Im Folgenden wird davon ausgegangen, dass alle möglichen Antworten einer Http-Schnittstelle per Http-Statuscode ausgedrückt werden. Es wird ein Typ definiert, der für jede Aktion alle möglichen Http-Statuscodes enthält:

$$API - \text{Ergebnis } AE \in \{tn_{200}, tn_{201}, tn_{400}, tn + 1_{200}, tn + 1_{400}, tn + 1_{409}, \dots\}.$$

Eine Aktion kann neben dem Aufruf einer Schnittstelle eine interne Verarbeitung sein. Das könnte beispielsweise eine Prüfung auf Vorhandensein eines Feldes in einer vorangegangenen Schnittstellenantwort sein. Eine solche Aktion wird definiert:

$$\text{Internes Prozessergebnis } IPE \in \{tn_{Success}, tn_{Failure}, tn + 1_{Success}, tn + 1_{Failure}, \dots\}.$$

Ein Ergebnis einer Aktion wird also definiert als:

$$\text{Ergebnis } E = AE \cup IPE.$$

Das Eingabealphabet beinhaltet Elemente aus dem Ergebnistyp:

$$\Sigma = \text{Ergebnis}.$$

Ein Übergang von einem Zustand in den Folgezustand drückt somit aus, dass die Saga eine Aktion ausgeführt hat und dem Ergebnis entsprechend einen Zustandswechsel durchgeführt hat.

Der Startzustand q_0 ist die erste auszuführende Transaktion.

Ein Endzustand q_{f1} wird erreicht, nachdem die letzte auszuführende Transaktion erfolgreich beendet wurde. Ein weiterer Endzustand q_{f2} wird erreicht, nachdem die letzte Kompensierung erfolgreich beendet wurde. Der letzte Endzustand q_{f3} wird erreicht, nachdem die erste Kompensierung erfolglos beendet wurde.

Konfiguration Die Ausführung eines DEA kann mittels Konfigurationen dargestellt werden. Eine Konfiguration K ist definiert als:

$$K = (q, w) \in Q \times \Sigma^*$$

Der Automat wechselt in einen Folgezustand, indem er ein Element aus dem Eingabewort abarbeitet und eine passende Übergangsrelation in δ findet. Somit gilt:

$$q_1, q_2 \in Q \wedge u \in \Sigma \wedge v \in \Sigma^* : (q_1, u \circ v) \vdash (q_2, v) \implies \delta(q_1, u) = q_2$$

Außerdem können mehrere Konfigurationsübergänge mittels \vdash^* dargestellt werden:

$$K_1 \vdash^* K_2 \implies K_1 = K_2 \vee \exists K : K_1 \vdash K \wedge K \vdash^* K_2$$

2.3.3.5 Betrachtung des Zustands nach Erfolg/Misserfolg

Der Zustand des Systems soll nun in folgenden Fällen betrachtet werden:

1. Erfolgreicher Ablauf einer Saga
2. Scheitern der Saga nach n Schritten
3. Scheitern der Saga nach n Schritten und Scheitern der Kompensierung nach m Schritten

Die Ausführung der Saga als DEA soll an folgendem Beispiel illustriert werden:

$Saga = (Q, \Sigma, \delta, q_0, F)$ mit

$$Q = \{q_{t1}, q_{t2}, q_{t3}, q_{c1}, q_{c2}, q_{c3}, q_{f1}, q_{f2}, q_{f3}\}$$

$$\Sigma = \{t1_{200}, t1_{400}, t2_{Success}, t2_{Failure}, t3_{200}, t3_{400}, c1_{200}, c1_{400}, c2_{Success}, c2_{Failure}, c3_{200}, c3_{400}\}$$

$$\delta = \{((q_{t1}, t1_{200}), q_{t2}), ((q_{t2}, t2_{Success}), q_{t3}), ((q_{t3}, t3_{200}), q_{f1}), ((q_{t1}, t1_{400}), q_{f2}), ((q_{t2}, t2_{Failure}), q_{c1}), ((q_{t3}, t3_{400}), q_{c2}), ((q_{c1}, c1_{200}), q_{f2}), ((q_{c2}, c2_{Success}), q_{c1}), ((q_{c3}, c3_{200}), q_{c2}), ((q_{c1}, c1_{400}), q_{f3}), ((q_{c2}, c2_{Failure}), q_{f3}), ((q_{c3}, c3_{Failure}), q_{f3})\}$$

$$q_0 = q_{t1}$$

$$F = \{q_{f1}, q_{f2}, q_{f3}\}$$

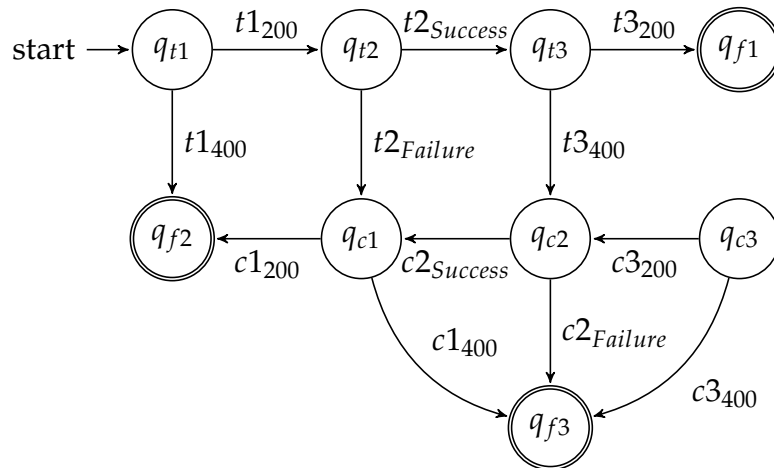


Abbildung 2.1: Darstellung einer Saga als Deterministischen endlichen Automaten

Endzustand q_{f1} Im Folgenden wird davon ausgegangen, dass die Aktionen der Zustände q_{t1} , q_{t2} und q_{t3} in einem erfolgreichen Ergebnis resultieren. Somit wird am Ende der Endzustand q_{f1} erreicht. Dieser Zustand drückt einen erfolgreichen Durchlauf einer Saga aus. Das Eingabewort $e_1 \in \Sigma^*$ ist $t1_{200} \circ t2_{Success} \circ t3_{200} \circ \#$.

Die Konfigurationsübergänge für e_1 sind:

$$\begin{aligned} & (q_{t1}, t1_{200} \circ t2_{Success} \circ t3_{200} \circ \#) \\ & \quad \vdash (q_{t2}, t2_{Success} \circ t3_{200} \circ \#) \\ & \quad \quad \vdash (q_{t3}, t3_{200} \circ \#) \\ & \quad \quad \quad \vdash (q_{f1}, \#) \end{aligned}$$

Endzustand q_{f2} Es wird nun davon ausgegangen, dass bei der Aktion im Zustand q_{t3} ein Ergebnis $t3_{400}$ erfolgt. Ein solches Ergebnis führt dazu, dass der Zustand q_{c2} erreicht wird. Hier wird davon ausgegangen, dass die Aktionen q_{c2} und q_{c1} erfolgreiche Ergebnisse haben. Das Eingabewort $e_2 \in \Sigma^*$ ist $t1_{200} \circ t2_{Success} \circ t3_{400} \circ c2_{Success} \circ c1_{200}$. Die Konfigurationsübergänge für e_2 sind:

$$\begin{aligned}
& (q_{t1}, t1_{200} \circ t2_{Success} \circ t3_{400} \circ c2_{Success} \circ c1_{200} \circ \#) \\
& \quad \vdash (q_{t2}, t2_{Success} \circ t3_{400} \circ c2_{Success} \circ c1_{200} \circ \#) \\
& \quad \quad \vdash (q_{t3}, t3_{400} \circ c2_{Success} \circ c1_{200} \circ \#) \\
& \quad \quad \quad \vdash (q_{c2}, c2_{Success} \circ c1_{200} \circ \#) \\
& \quad \quad \quad \quad \vdash (q_{c1}, c1_{200} \circ \#) \\
& \quad \quad \quad \quad \quad \vdash (q_{f2}, \#)
\end{aligned}$$

Endzustand q_{f3} Zuletzt soll der Zustand q_{f3} betrachtet werden. Dafür soll die Aktion in q_{t3} das Ergebnis $t3_{400}$ haben. Danach schlägt die Aktion q_{c2} fehl und liefert das Ergebnis $c2_{Failure}$. Das Eingabewort $e_3 \in \Sigma^*$ ist $t1_{200} \circ t2_{Success} \circ t3_{400} \circ c2_{Failure} \circ \#$. Die Konfigurationsübergänge für e_3 sind:

$$\begin{aligned}
& (q_{t1}, t1_{200} \circ t2_{Success} \circ t3_{400} \circ c2_{Failure} \circ \#) \\
& \quad \vdash (q_{t2}, t2_{Success} \circ t3_{400} \circ c2_{Failure} \circ \#) \\
& \quad \quad \vdash (q_{t3}, t3_{400} \circ c2_{Failure} \circ \#) \\
& \quad \quad \quad \vdash (q_{c2}, c2_{Failure} \circ \#) \\
& \quad \quad \quad \quad \vdash (q_{f3}, \#)
\end{aligned}$$

2.3.3.6 Unterschiede des Saga-Modells zu Hector Garcia-Molinas Definition

2.3.3.7 Recovery-Mechanismen

Eine Saga, die in der Ausführung einer Transaktion fehlschlägt, wechselt nach der Definition in die entsprechende Kompensierung und versucht, alle bis dahin ausgeführten Transaktionen zu kompensieren. Somit wird der Anfangszustand des Systems wiederhergestellt. Dieses Verhalten wird als Backward-Recovery bezeichnet.

Neben der Backward Recovery wird ein weiteres Verhalten vorgeschlagen, welches Forward-Recovery genannt wird. Das Ziel der Forward Recovery ist es, seltener in einem erfolglosen Endzustand zu gelangen. Im Modell der hier aufgestellten DEA-Saga sind die Zustände q_{f2} und q_{f3} . Um dies zu erreichen, werden Save-Points definiert. Ein Save-Point stellt einen Zustand dar, von dem bei einem Systemabsturz oder einem erfolglosen Ergebnis die Ausführung weitergeführt werden kann. Es wird im Fehlerfall Backward-Recovery bis zum nächsten Save-Point ausgeführt. Wird dieser erreicht, werden alle noch fehlenden Ts ausgeführt, um zum erfolgreichen Endzustand zu gelangen. Das bedeutet, dass von der Kompensierungskette zurück auf die Transaktionskette gesprungen wird.

Backward Recovery Der DEA einer Saga, die Backward-Recovery implementiert, ist im vorherigen Abschnitt beschrieben.

Forward Recovery Forward-Recovery ist auf verschiedenen Wegen erreichbar. Der erste Ansatz beinhaltet die Verwendung eines Save-Points. Der DEA aus Abschnitt soll um einen Checkpoint und Forward Recovery ergänzt werden. Es wird ein weiterer Zustand eingeführt, der nach erfolgreichem Ergebnis von q_{t1} erreicht wird. Der Checkpoint wird hier dargestellt als ein interner Prozessschritt q_{sp1} und hat somit die möglichen Ergebnisse $\in \{sp1_{Success}, sp1_{Failure}\}$. Es ist zu sehen, dass dieser DEA eine mögliche Endlosschleife zulässt. Wenn q_{sp1} erreicht wird und in q_{t2} oder q_{t3} immer ein erfolgloses Ergebnis auftritt, darf im Zustand q_{sp1} nur endlich oft der Übergang $sp1_{Success}$ gewählt werden.

Die Funktion f die in q_{sp1} ein internes Prozessergebnis IPE berechnet, sieht so aus:

$$f : \mathbb{N} \rightarrow IE$$

$maxSavepointExecutionCount \in \mathbb{N}$: Anzahl des Erreichens von q_{sp1} whrend der Ausführung der Saga

$$f(x) = \begin{cases} IE_{Success}, & x < maxSavepointExecutionCount \\ IE_{Failure}, & else \end{cases}$$

Die Anzahl an Ausführungen beginnend bei q_{t2} ist begrenzt. Es wird also solange Forward Recovery versucht, bis die Saga erfolgreich ist oder das Oberlimit $maxSavepointExecutionCount$ erreicht wird. Wenn dieses Oberlimit erreicht ist, wird die Forward Recovery aufgegeben und in den Zustand q_{c1} gewechselt.

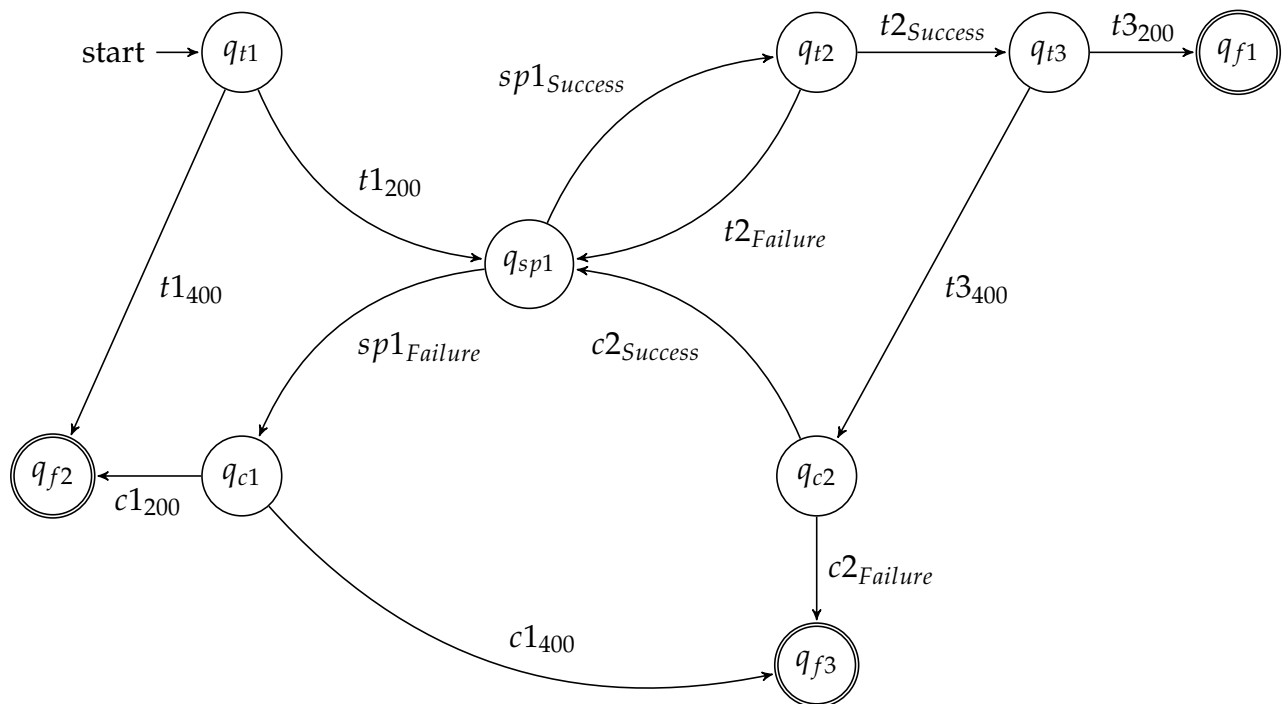


Abbildung 2.2: Forwardrecovery in einem DEA

Forward-Recovery kann alternativ auch als Retry interpretiert und somit ohne Save-Points realisiert werden. Einen solcher Retry kann sehr einfach in jedem Zustand ergänzt werden. Dazu wird eine Kante hinzugefügt, die im gleichen Zustand bleibt. Die Kante, die zuvor ein erfolgloses Ergebnis ausgedrückt hat, drückt nun ein Scheitern oberhalb des Retrylimits aus.

Der Typ Ergebnis wird dafür definiert als:

$$\text{Ergebnis } E = \{t1_{\text{Success}}, t1_{\text{Failure}}, t1_{\text{FinalFailure}}, \dots\}$$

Die Funktion fn_{AE} , die in dem jeweiligen Zustand q_{tn} das entsprechende API-Ergebnis AE berechnet, ist:

$$fn_{AE} : \mathbb{N} \times AE \rightarrow E$$

$maxSavepointExecutionCount_n \in \mathbb{N}$: Anzahl des Erreichens von q_{tn}
während der Ausführung der Saga

$$fn_{AE}(x, y) = \begin{cases} En_{\text{Success}}, y = tn_{200} \\ En_{\text{Failure}}, y \neq tn_{200} \wedge x < maxSavepointExecutionCount_n \\ En_{\text{FinalFailure}}, else \end{cases}$$

Die Funktion fn_{IE} , die in dem jeweiligen Zustand q_{tn} das entsprechende interne Prozessergebnis IPE berechnet, ist:

$$fn_{AE} : \mathbb{N} \times IPE \rightarrow \text{Ergebnis}$$

$maxSavepointExecutionCount_n \in \mathbb{N}$: Anzahl des Erreichens von q_{tn}
während der Ausführung der Saga

$$fn_{AR}(x, y) = \begin{cases} En_{\text{Success}}, y = tn_{\text{Success}} \\ En_{\text{Failure}}, y \neq tn_{\text{Failure}} \wedge x < maxSavepointExecutionCount_n \\ En_{\text{FinalFailure}}, else \end{cases}$$

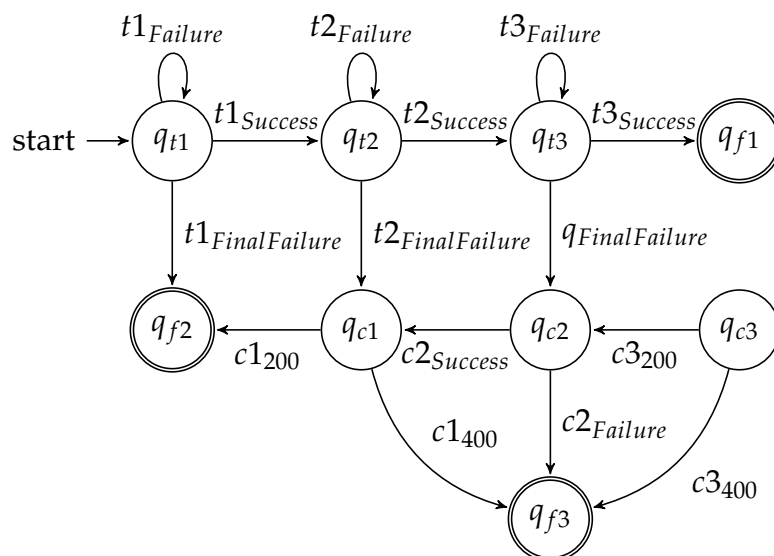


Abbildung 2.3: Backwardrecovery in einem DEA

Es kann außerdem verboten werden, dass in einer Implementierung von Forward-Recovery der Fall verboten wird, der zu einer Backward-Recovery führt. Dabei wird erreicht, dass es nur einen gültigen Endzustand gibt. Dieser Endzustand drückt einen erfolgreichen Abschluss der Saga aus. Dabei ist zu beachten, dass das wiederholte Ausführen einer Aktion schlussendlich zu einem erfolgreichen Ergebnis führen muss. Der DEA für dieses Verhalten sieht so aus:

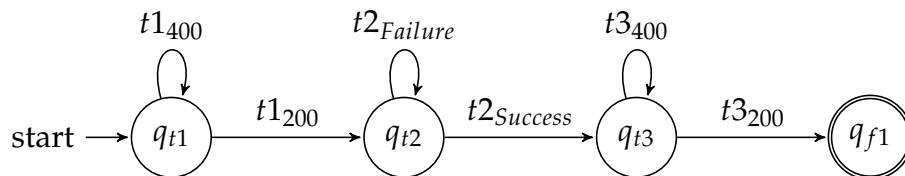


Abbildung 2.4: Erzwungene Forwardrecovery in einem DEA

Es ist zu sehen, dass in diesem DEA keine Zustände enthalten sind, die eine Kompensierungsaktion ausdrücken. Somit geht in dieser Implementierung der Gedanke der Kompensierung verloren, der eine zentrale Rolle im Saga-Pattern innehat. Bei wiederholtem Auftreten eines erfolglosen Ergebnisses endet die Saga nie.

Voraussetzung für Forward-Recovery Damit eine Forward-Recovery sinnvoll ist, muss die Möglichkeit bestehen, dass ein gescheitertes T bei erneutem Ausführen ein erfolgreiches Ergebnis liefert. Das ist abhängig von der Semantik des Ergebnisses. Ist ein T beispielsweise ein Aufruf einer Schnittstelle zum Buchen eines Hotels, so könnten erfolglose Ergebnisse beispielsweise folgende Bedeutungen haben:

1. Hotel ist im angefragten Zeitraum ausgebucht
2. Hotel ist im angefragten Zeitraum im Betriebsurlaub

Im ersten Fall ist eine Forward Recovery möglich. Wenn ein andere Kunde seine Reservierung storniert, ist es es möglich, dass bei erneutem Anfragen eine Reservierung zustande kommt, die vorher abgelehnt wurde.

Im zweiten Fall ist Forward-Recovery ohne Effekt. Wenn eine Hotelbuchung für einen Zeitraum angefragt wird, in dem das Hotel im Betriebsurlaub ist, wird auch bei wiederholter Anfrage keine Buchung zustande kommen.

2.3.3.8 Implementierungsformen des Patterns

Um eine Saga als Microservice-System zu implementieren, gibt es zwei verschiedene Herangehensweisen. Die zwei Formen der Implementierung werden als Orchestrierung und als Choreografie bezeichnet. Beide Ausprägungen des Saga-Patterns verfolgen denselben Zweck: den Gedanken, eine globale verteilte Transaktion in einem verteilten System in lokale Teiltransaktionen aufzuteilen, die mittels passender Kompensierung zurückgerollt werden können.

Die zwei Ausprägungen unterscheiden sich hauptsächlich in der Softwarearchitektur. Es ist zu beachten, dass beide Implementierungen denselben Geschäftsprozess abbilden können und somit als äquivalent angesehen werden können.

Im Folgenden sollen die beiden Implementierungsansätze vorgestellt werden. Um die Unterschiede zu verdeutlichen, soll in den nachfolgenden Erläuterungen von einem Geschäftsprozess ausgegangen werden, der Ts enthält, die Teil einer verteilten, globalen Transaktion sind. Jedes T soll eine andere Schnittstelle aufrufen. Jedes T hat ein entsprechendes C zugeordnet. Sowohl die Ts als auch die Cs entsprechen den Anforderungen, die in XXX beschrieben sind.

Orchestration Die Orchestrierung zentralisiert die Logik für eine Saga in einem einzigen Service. Dieser Service wird als Koordinator oder Orchestrator bezeichnet. Der Koordinator ist verantwortlich für die Einhaltung der Transaktionsanforderungen. Er ruft aktiv die restlichen teilhabenden Services auf und muss die Ergebnisse der Aufrufe auswerten. Die teilhabenden Services haben nur Verantwortung für die Korrektheit der Prozessierung ihre eigenen Servicegrenzen. Ein solcher vom Koordinator aufgerufener Service hat keine Kenntnis vom ablaufenden Geschäftsprozess.

Der Orchestrator stellt einen Prozessmanager dar. Als solcher muss dieser Service garantieren, dass eine gestartete Saga nicht abbricht. Damit ein Absturz des Orchestrators dies gewährleisten kann, muss der Zustand der gestarteten Saga persistiert werden. Häufig wird das Transaktionslog in einer Datenbank gespeichert und erlaubt damit die Weiterführung der Saga auch nach Absturz der Anwendung.

Choreografie Bei der Choreographie gibt es keinen koordinierenden Service. Alle teilhabenden Services kennen den Ablauf des Geschäftsprozesses. Die Logik ist über alle Services verteilt.

Ein Service ist auch hier für die Korrektheit der Prozessierung innerhalb der eigenen Servicegrenzen verantwortlich. Zusätzlich muss jeder Service nach der Prozessierung den Prozess weiterführen. Dazu gehören sowohl mögliche weitere Transaktionen als auch mögliche Kompensierungsaufrufe.

Kommunikationsstrategien Die Orchestration unterstützt sowohl synchrone als auch asynchrone Kommunikation mit den teilhabenden Services.

Bietet ein an der globalen Transaktion teilhabender Service eine synchrone Schnittstelle zur Verfügung, muss der Koordinator warten, bis der aufgerufene Service eine Antwort liefert und ist solange blockiert. Bei einem Ausfall des aufgerufenen Services hat der Koordinator keine Möglichkeit, die Transaktion fortzuführen. Die Verfügbarkeit aller Services zum Aufrufzeitpunkt ist Voraussetzung für den erfolgreichen Abschluss einer orchestrierten Saga. Dafür ist dem Koordinator in einem solchen Fall die Unerreichbarkeit des Services bekannt und kann entsprechend reagieren.

Des weiteren kann ein Service eine asynchrone Schnittstelle zur Verfügung stellen. Diese Schnittstelle kann eine Implementierung des asynchronen Request-Response Musters sein (Polling Pattern, Callback Pattern). Um eine asynchrone Request-Response Schnittstelle zu verwenden muss der Orchestrator das entsprechende Protokoll des Musters einhalten. Der Vorteil in der Verwendung asynchroner Kommunikation liegt darin, dass der Orchestrator nicht blockiert. In der Zeit zwischen der Platzierung der Anfrage und dem Erhalt der Antwort kann der Orchestrator die Prozessierung der aktuellen Saga pausieren und mit der Verarbeitung anderer Anfragen fortfahren. Der

Vorteil dieser Implementierungen ist die Entkopplung von Request und Response. Das zahlt sich in Fällen aus, in denen die Verarbeitung der Anfrage einen längeren Zeitraum in Anspruch nimmt.

Die Implementierung eines asynchronen Request-Response Musters ist wesentlich komplizierter als die Entwicklung einer synchronen Schnittstelle. Deshalb sollte dies als Implementierung einer lokalen Transaktion unter Verwendung einer Orchestrierung nur in Szenarien gewählt werden, die die Entkopplung von Anfrage und Antwort voraussetzen.

Schlussendlich bietet die Orchestrierung die Möglichkeit, asynchrone Messaging-Komponenten zu verwenden. Anstatt direkt miteinander zu kommunizieren platziert der Koordinator die Anfrage als Event in einer Messaging-Middleware und kann mit der Prozessierung der Saga pausieren. Der angefragte Service erhält dieses Event und kann eine beliebig lang andauernde Verarbeitung ausführen. Nachdem die Verarbeitung abgeschlossen ist, kann die Antwort wiederum als Event in der Middleware platziert werden. Der Koordinator erhält dieses Event und kann darin das Ergebnis ablesen.

Um eine Saga mittels Choreographie zu implementieren, sollte asynchrones Messaging verwendet werden. Da die Geschäftslogik über alle Komponenten verteilt ist, ist selten ein Service am Ergebnis des nächsten Transaktionsschrittes interessiert. Ein Service S_1 verarbeitet seinen Teil der Transaktion und informiert den nächsten Service S_2 über den Erfolg der Berechnung. S_2 ist so implementiert, dass er die Logik für seine eigenen Berechnungen kennt. Somit muss S_1 nicht über den Erfolg informiert werden. Ein Erfolg von der in S_2 ablaufenden Transaktion endet in einem Event für einen nachfolgenden Service S_3 . Die Kommunikation ist hier nicht auf ein Request-Response Muster ausgelegt, es werden Einweg-Nachrichten genutzt. Die Ausnahme ist ein erfolgloses Ergebnis in S_2 . In diesem Fall wird S_3 nicht per Event informiert. Es wird lediglich S_1 mit einem erfolglosen Ergebnis benachrichtigt. Als Reaktion auf dieses Event kann S_1 mit Forward- oder Backward-Recovery reagieren.

Die Implementierung einer Choreographie per Request-Response Muster ist nicht unmöglich. S_1 ruft S_2 per synchroner oder asynchroner Request-Response Schnittstelle auf. Daraufhin erhält S_1 eine Antwort mit dem Ergebnis von der Berechnung von S_2 . Bei einem Erfolg findet in S_1 jedoch keine Reaktion statt. Lediglich bei einem Misserfolg muss S_1 Kenntnis vom Ergebnis der Transaktion in S_2 haben. Somit hat die Verwendung einer Response nur einen Nutzen, falls ein Misserfolg vorliegt.

Des Weiteren hat die Verwendung einer synchronen Kommunikation in der Implementierung der Choreographie den Nachteil, dass es zu Blockierungen aller teilhabenden Services führt. Auch S_2 ruft S_3 synchron auf. Somit muss S_2 warten, bis die Response in S_3 erfolgt. Erst danach kann S_2 die Response für S_1 absenden. Dieses Verhalten wird als Aufrufkaskadierung bezeichnet und wirkt sich sowohl auf den Fall eines Erfolgs als auch den eines Misserfolgs aus.

Aus den genannten Gründen ist es zu empfehlen, bei der Implementierung einer Saga per Choreographie eine eventbasierte Architektur mit asynchronen Messaging-Komponenten zu verwenden.

2.3.4 Anwendungsgebiete des Patterns - Welche Usecases erlauben die Verwendung dieses Patterns? Welche nicht?

2.3.4.1 Langlebige Transaktionen - LLT

2.3.4.2 Bezug auf den Geschäftsprozess

2.3.4.3 Verteilte Systemlandschaft

2.3.4.4 Reaktion auf verschiedene Antwortmöglichkeiten in der Geschäftslogik

2.3.4.5 Fehlerfälle - Geschäftslogik und Ausfälle

Hier soll der Unterschied zwischen Fehlern in der Geschäftslogik und Fehler aufgrund Ausfällen erläutert werden.

3 Versuchsvorbereitung

3.1 Problemstellung

In 4 wurde das Saga-Pattern als ein Implementierungsmuster vorgestellt, welches ermöglichen soll, die ACID-Anforderungen in einem verteilten System nachzubilden. Ein verteiltes System steht immer vor der Herausforderung von Netzwerkfehlern. Verwenden Transaktionsteilnehmer eines Systems die Request-Response-Kommunikation, so besteht immer die Möglichkeit, dass einzelne Nachrichten ihr Ziel nicht erreichen. Wenn eine solche Kommunikation deterministischer Natur ist, kann der Sender seinen Request ohne Gefahr wiederholen. Die im Saga-Pattern verwendeten lokalen Transaktionen stellen jedoch keine deterministische Abfrage dar, sondern verfolgen das Ziel eines Zustandswechsels des Empfängers. Wiederholt der Sender seine Requests, führt dies zu ungewünschten Nebenwirkungen.

Es stellt sich die Frage, ob in Saga-Systemen, die Request-Response-Kommunikation verwenden, Konsistenz gewährleistet werden kann.

3.2 Zielstellung

Die folgenden Kapitel dienen dem Zweck, das Saga-Pattern hinsichtlich Systemkonsistenz zu untersuchen. Dabei wird davon ausgegangen, dass jegliche Kommunikation per Request-Response-Protokolle abläuft.

- 1 Es ist die Frage zu beantworten, unter welchen Bedingungen ein Microservice-System, welches mittels Saga-Pattern implementiert wurde, eine LLT abbilden kann.
- 2 Es sind Fehlerquellen und Fehlertypen zu identifizieren, die einen inkonsistenten Systemzustand verursachen können. Es sollen Lösungen im Rahmen des Saga-Patterns formuliert, implementiert und evaluiert werden.
- 3 Es soll eine Antwort darauf gefunden werden, welche Kriterien eine Schnittstelle erfüllen muss, um an einer LLT teilnehmen zu können.
- 4 Es soll beantwortet werden, ob aufgrund Netzwerkpartitionen auftretende Fehler in das Saga-Pattern integrierbar sind.

3.3 Ausgangspunkt

Es soll ein Geschäftsvorgang mittels Saga-Pattern in einem Microservicesystem entworfen, implementiert und bewertet werden. Die gewählte Geschäftsvorgang soll als LLT aufgefasst werden und eine verteilte Transaktion abbilden.

Es soll eine Implementierungsform des Saga-Patterns gewählt werden. In der Zielstellung wird ein System gefordert, welches Request-Response-Kommunikation verwendet. Somit kann die Verwendung von Messagingkomponenten ausgeschlossen werden. Die auf diese Komponenten ausgerichtete Implementierung per Choreografie wird deshalb nicht gewählt.

Als Implementierungsform des Saga-Patterns wird für diesen Versuch die Orchestrierung gewählt.

3.4 Methodik

In diesem Abschnitt soll das Vorgehen bei der Bearbeitung des Problems erläutert werden.

3.4.1 Schritt 1 - Entwurf und Implementierung eines GP

Entwurf eines Geschäftsprozesses Zur Untersuchung der Probleme soll ein Geschäftsprozess entworfen und als Saga-System implementiert werden. Der Durchlauf durch diesen Geschäftsprozess soll als LLT aufgefasst werden. Der Geschäftsprozess muss eine der in 4.13.3.0.1 beschriebenen Eigenschaften aufweisen, damit die Realisierung dieses Prozesses innerhalb einer Saga sinnvoll ist.

Es besteht die Anforderung an den zu entwerfenden Prozess, dass dieser durch eine Menge von lokalen Transaktionen abbildbar sein muss. Außerdem muss es möglich sein, Kompensierungen für jede dieser Transaktionen zu formulieren.

Imaginärer Bestell- und Lieferprozess Als abzubildender Geschäftsprozess soll ein Bestell- und Liefervorgang eines Online-Shops dienen. Der Bestellvorgang soll durch das Platzierung einer Bestellung ausgelöst werden. Die Benutzeroberfläche gehört nicht zum Scope des umzusetzenden Systems.

Als Ausgangspunkt soll folgender Geschäftsprozess dienen:

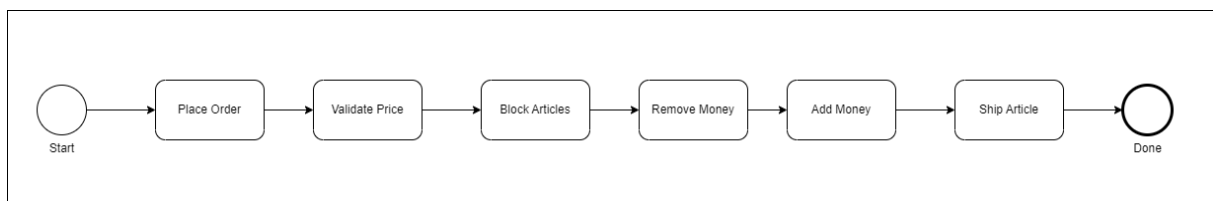


Abbildung 3.1: Vereinfachte Darstellung eines Bestell- und Lieferprozesses

Die zum Prozess gehörenden Schritte sind folgende:

Entgegennehmen der Bestellung Die Bestellung wird über ein imaginäres Frontend entgegengenommen. Dieses Frontend baut einen Request auf und sendet diesen per Http-Schnittstelle an das Backend. Dort wird der Request entgegengenommen und muss alle für die Abwicklung der Bestellung erforderlichen Daten enthalten. Dazu gehören der bestellende Nutzer, die geforderten Artikel und die Zahlungsinformationen. Beim Entgegennehmen wird die Bestellung initialisiert.

Validierung des Preises Der Bestellsrequest enthält eine Liste von den gewünschten Produkten und dem bekannten Preis pro Produkt. Um zu überprüfen, ob der dem Nutzer (dem Frontend) bekannte Preis mit dem aktuellen Preis übereinstimmt, muss dieser validiert werden.

Blockieren der Artikel Die geforderten Artikel sollten für diese Bestellung reserviert werden, bis der Bestellvorgang abgeschlossen ist. In einem Online-Shop wird angezeigt, wieviele Artikel auf Lager vorrätig sind. Beim Blockieren der Artikel wird dieser Betrag verändert. Somit sehen andere Nutzer nach Ausführung dieses Schrittes den aktuellen Wert der vorrätigen Artikel.

Zahlungsabwicklung Der berechnete Preis der Bestellung muss vom Konto des Kunden abgebucht werden. Das Konto des Händlers erhält denselben Betrag gutgeschrieben. Die Konten des Kunden und des Online-Shop-Besitzers müssen nicht bei derselben Bank liegen.

Auslösen der Lieferung Die blockierten Artikel werden versendet. Dieser Prozess dauert einen längeren Zeitraum an.

Abschluss der Lieferung Der Lieferant bestätigt die Übergabe der Waren an den Kunden.

Implementierung Nachdem der Geschäftsprozess definiert wurde, soll das Saga-System implementiert werden. In 2.3.3.4 wurde erläutert, wie die im Koordinator laufende SEC beschrieben werden kann. Die Implementierung soll durch diese Darstellungsform beschrieben werden können.

Für die Transaktionsteilnehmer gilt zu Beginn der Implementierung lediglich die Anforderung, dass die Schnittstellen per Request-Response-Muster aufgerufen werden. Dafür wird das Http-Protokoll verwendet.

3.4.2 Schritt 2 - Messung der verschiedenen Implementierungen

Die Bewertung der Implementierungen soll auf Grundlage von Messdaten erfolgen. Es soll nun beschrieben werden, wie die Erfassung dieser Daten erfolgen soll.

Systemtest Die Messdaten erfolgen in einer produktionsähnlichen Umgebung im Rahmen von Systemtests. Das erwartete Ergebnis ist ein konkreter Endzustand, der erreicht werden soll. Dieser Endzustand kann mit dem erreichten Endzustand verglichen werden.

Testkonfiguration Ein solcher Systemtest wird unter einer bestimmten Konfiguration durchgeführt. Die Konfiguration setzt sich zusammen aus einem Testcase und einem Netzwerkszenario.

Testcase Ein Testcase stellt eine konkrete Interaktion mit dem System dar. Die Testcases übernehmen die Aufgabe, die verschiedenen Fälle der Geschäftslogik auf Korrektheit zu überprüfen.

Netzwerkszenarien Ein Netzwerkszenario ist ebenfalls Teil der Testkonfiguration. Wird ein Systemtest durchgeführt, so beschreibt das Netzwerkszenario das konkrete Netzwerkverhalten.

Messgegenstand Das Ziel der Messung ist, Aussagen über die Konsistenz des Systems zu treffen. In Abschnitt 4.13.3.0.1 wurden verschiedene Vorgehensweisen dargestellt, wie die Konsistenz eines Systems gemessen werden kann.

Die verwendete Implementierung per Orchestrierung setzt das Vorhandensein eines Koordinators voraus. Die darin befindliche Steuerung der LLT durch die SEC gibt Auskunft über die ausgeführten lokalen Transaktionen einer Saga. Es kann für jede lokale Transaktion gemessen werden, wie oft die SEC davon ausgeht, dass eine Transaktion ausgeführt wurde. Analog dazu kann die tatsächlich ausgeführte Anzahl an Transaktionen bestimmt werden, indem die Sicht der Transaktionsteilnehmer verwendet wird. Stimmen die korrespondierenden Werte aller lokalen Transaktionen in beiden Sichten überein, kann davon ausgegangen werden, dass die LLT keine Inkonsistenzen in das System eingeführt hat.

Ein weiterer Anhaltspunkt für Konsistenzanomalien ist der erreichte Endzustand einer Transaktion. In 2.3.3.4 wurde ein Endzustand für einen DEA definiert, der erreicht wird, nachdem eine Saga in einer kompensierenden Aktion eine Fehlerantwort erhält. In solchen Fällen ist der Koordinator nicht in der Lage die LLT abzuschließen und endet in einem weder erfolgreichen noch kompensierten Zustand.

Da dieser Zustand einen Fall aufzeigt, in dem die Atomarität der LLT verletzt wird, ist das Auftreten solcher Endzustände ein unmittelbares Zeichen für Inkonsistenz.

Metriken TODO Beschreibung, wie die Messdaten in eine (oder mehrere) Kennzahlen umgewandelt wird

3.4.3 Schritt 3 - Analyse der Messdaten

4 Versuchsdurchführung

In diesem Kapitel soll die der in Kapitel 3 geforderte Versuch durchgeführt werden. Zunächst wird der initiale Systementwurf beschrieben. Dazu gehört die Modellierung der lokalen Transaktionen, die Implementierung der dafür vorgesehenen Services und die Implementierung des Koordinators.

Es wird im Anschluss ein initialer DEA verwendet und iterativ angepasst. Jede Anpassung resultiert aus Messergebnissen und daraus ableitbaren Schlüssen.

4.1 Services

Es sollen zuerst die Teilnehmerservices identifiziert werden.

Die Schnittstelle zwischen dem Backend-System und dem Benutzer stellt ein Frontend dar. In diesem Frontend werden dem Nutzer die Produkte dargestellt. Außerdem übernimmt das Frontend die Aufgabe der Verwaltung eines Warenkorbsystems. Der Nutzer kann Produkte zu seinem Warenkorb hinzufügen oder entfernen. Die Bestellung kann nun ausgelöst werden und an das Backend übermittelt werden.

Der Einstiegspunkt für die Abwicklung einer Bestellung soll der OrderService sein. Neben der Initialisierung dieser Bestellung und der Aktualisierung des Bestellungsstatus fallen aus Sicht der Prozessdefinition keine weiteren Aufgaben in den Bereich dieses Services. Die Aktualisierung des Bestellungsstatus ist sehr eng mit der Verwaltung des Prozesses aus Sicht des Koordinators verbunden. Deshalb kann der OrderService die Rolle des Koordinators übernehmen.

Die Artikeldaten sollen dem Nutzer und dem Geschäftsprozess in einer gemeinsamen Schnittstelle bekannt gemacht werden. Diese Aufgabe übernimmt ein eigener ArticleService.

Eine Aufgabengebiete ist die Verwaltung der Lagerbestände. Die Verwaltung des Lagers und den vorrätigen und reservierten Artikeln sowie die Verwaltung von Lieferungen übernimmt der StockService.

Zuletzt muss ein Service die Kontostände der Nutzerkonten und des Händlerkontos verwalten. Dies wird von einem BankService übernommen. Im Versuch sollen zwei Instanzen des BankServices verwendet werden, die zwei verschiedene BankServiceProvider darstellen sollen.

Name des Services	Aufgabe
Frontend	Nutzerschnittstelle (GUI), Anzeige der Produkte, Platzieren der Bestellung
OrderService	Entgegennehmen der Bestellung, Koordinierung des Bestellprozesses
ArticleService	API für die angebotenen Produkte und Preise
StockService	Verwaltung des Lagerbestands, Verwaltung des Lieferprozesses
BankingServices	Verwaltung von Kontonutzern und Kontoständen

Entwicklungsscope Für die Betrachtung des Bestell- und Lieferprozesses als LLT wird das Frontend außen vorgelassen. Die LLT beginnt mit der Entgegennahme eines Order-Requests im OrderService. Es werden lediglich die Backend-Services entwickelt, die Teil der LLT sind.

4.2 Lokale Transaktionen

Die einzelnen lokalen Transaktionen sollen nun identifiziert werden. Im Folgenden wird beschrieben, durch welchen Teilnehmer die lokale Transaktion jeweils ausgeführt wird.

Initialisierung Die Bestellung wird im OrderService entgegengenommen. Die Bestellung wird initialisiert. Der Saga-Prozess wird erstellt.

Validierung der Produktdaten Die in der Bestellung enthaltenen Produktdaten müssen validiert werden. Dies geschieht in zwei Schritten:

1. Abfrage aller in der Bestellung enthaltenen Produktdaten am ArticleService
2. Validierung

Blockierung der Artikel Die Ware wird im StockService für andere Bestellungen blockiert.

Geldabbuchung Das Käuferkonto muss belastet werden. Dabei wird der Geldbetrag des Käuferkontos in der entsprechenden Instanz des BankService verringert.

Geldzubuchung Das Händlerkonto bekommt den selben Geldbetrag gutgeschrieben. Dies geschieht ebenfalls in der entsprechenden Instanz des BankService.

Auslösung der Lieferung Die blockierten Artikel der Lieferung werden aus dem Lager entfernt und die Lieferung wird ausgelöst. Dies geschieht im StockService.

Lieferabschluss Die Ware trifft beim Kunden ein. Die Lieferung wird durch den Lieferanten bestätigt. Diese Information erreicht den StockService.

4.3 Kompensierungen

Jede an der LLT teilhabende lokale Transaktion muss kompensierbar sein, damit das Saga-Pattern funktionieren kann. Führt eine lokale Transaktion zu keinem Wechsel des Systemzustands, muss keine Kompensierung stattfinden.

Transaktion	Kompensierung
Initialisierung	
Validierung der Produktdaten	
Blockierung der Artikel	StockService - Freigeben der blockierten Artikel
Geldabbuchung	Erhöhen des Geldbetrages des Kundenkontos
Geldzubuchung	Verringern des Geldbetrages des Händlerkontos
Auslösung der Lieferung	Zurückrufen der Lieferung
Lieferabschluss	

4.4 Fachliche Kontextabgrenzung

Für die Realisierung des Microservicesystems im Rahmen dieser Arbeit wurde die Orchestrierung gewählt. Die Rolle des Koordinators übernimmt der OrderService. Der OrderService übernimmt die Annahme des Bestellprozesses und löst somit die Saga aus.

4.4.1 Frontend

In einem Online-Shop interagiert der Kunde per Frontend mit der Anwendung. Das Frontend soll übernimmt die grafische Schnittstelle zwischen Backend und dem Nutzer. Dazu gehört vor Allem die Darstellung der Artikel in einer Katalogansicht. Die darzustellenden Daten für eine solche Liste müssen zumindest Artikelbezeichnung und Artikelpreis enthalten. Diese Daten sollten aus einer API für Artikeldaten stammen. Darüber hinaus muss das Frontend einen Prozess unterstützen, in dem der Kunde ein Formular ausfüllt, welches die erforderlichen Daten für das Platzieren einer Bestellung enthält. Dazu gehört ein Warenkorbsystem sowie eine Authorisierung und Authentifizierung der Zahlungsidentität des Kunden. Die Bestellung kann also als Objekt mit folgenden Feldern zusammengefasst werden:

- Zahlungsinformationen des Kunden: BankId, UserId
- Liste der zu bestellenden Artikel, mit Artikel: ArticleId, ArticlePrice, Amount

Dieses Objekt kann an das Backend gesendet werden.

4.4.2 ArticleService

Dieser Service ist ein Service zum reinen Lesen der Produktdaten. Er soll eine Schnittstelle zur Verfügung stellen, die dem Frontend ermöglicht, den Produktkatalog abzufragen und darzustellen. Das Backend muss außerdem die Möglichkeit haben, die im Request

enthaltenen Artikelpreise zu validieren. Dazu benötigt der ArticleService eine Produktdatenbank. Da dieser Service ausschließlich die Produktdaten als Ressource behandelt, kann er RESTful implementiert werden.

4.4.3 StockService

Der Service soll den aktuellen Bestand an vorrätigen Artikeln abbilden. Es soll möglich sein, eine Menge an Artikeln für eine konkrete Bestellung zu reservieren. Eine Reservierung von einer Menge von Artikeln wartet auf die Auslösen der Lieferung.

Um dies zu erlauben, muss der aktuelle Lagerstand in einer Tabelle hinterlegt sein. Die Tabelle muss den aktuell verfügbaren Bestand pro Artikel ausdrücken.

Um eine Reservierung zu ermöglichen, muss es eine weitere Tabelle geben, die eine Menge von blockierten Artikeln für einen bestimmten Bestellprozess enthält. Beim Reservieren verringert sich der Bestand in der Bestandstabelle und erhöht sich in der Reservierungstabelle. Um die Konsistenz zu gewährleisten, müssen beide Operationen in einer lokalen Transaktion ausgeführt werden.

Um das Auslösen und Abschließen einer Lieferung zu ermöglichen, muss es eine Tabelle geben, die den Inhalt einer Lieferung und einen Status enthält. Wenn eine Lieferung ausgelöst wird, werden die für diesen Vorgang reservierten Artikel aus der Reservierungstabelle entfernt und in der Lieferungstabelle eingefügt. Diese Transaktion soll den physischen Prozess abbilden, die bestellten und für diese Bestellung blockierten Artikel aus dem Lager in das Transportfahrzeug und schließlich zum Kunden zu transferieren.

Die Übergabe der Ware an den Kunden stellt den finalen Schritt des Prozesses dar. Ist dies geschehen, gibt der Lieferant dem StockService die Bestätigung für die gelieferte Bestellung.

Die Blockierung eines Artikels muss kompensiert werden können, da sonst der reservierte Artikel nach Abbruch einer Bestellung nicht wieder freigegeben würde. Deshalb muss diese Kompensierung die Einträge aus der Blockierungstabelle entfernen und die Anzahl auf den Lagerbestand addiert werden. Dies soll ebenfalls in einer lokalen Transaktion ablaufen, um Konsistenz zu wahren.

Die Auslösung der Lieferung ist nur bedingt kompensierbar. Nachdem das Transportfahrzeug mit der Ware losgefahren ist und die Ware noch nicht übergeben hat, kann die Lieferung noch abgebrochen und somit kompensiert werden. Die Kompensierung muss also den Lieferant benachrichtigen und die Ankunft der Waren bestätigen. Nach der Saga-Definition soll die zu kompensierende Transaktion zurückgerollt werden. Deshalb werden die Waren aus der Lieferungstabelle zurück in die Reservierungstabelle geschrieben.

Der Abschluss einer Lieferung bildet die physische Warenübergabe an den Kunden ab. Eine Kompensierung ist hier nicht möglich. Da diese lokale Transaktion die letzte Transaktion ist und einen erfolgreichen Abschluss der Saga zur Folge hat, muss hier keine Kompensierung angeboten werden.

4.4.4 BankingServices

Im Geschäftsprozess wurde definiert, dass die Transaktion den Geldbetrag des Kundenkontos und des Händlerkontos in zwei separaten lokalen Transaktionen abwickeln können soll. Somit muss der BankingService jeweils eine Transaktion zum Erhöhen und zum Verringern des Geldbetrages anbieten. Der BankingService soll am Ende in zwei Instanzen laufen, die zwei verschiedene Banken darstellen sollen. Kunden- und Käuferkonto können, müssen aber nicht bei derselben Bank liegen.

Um dies zu ermöglichen benötigt der BankingService eine Tabelle, die seine Nutzer enthält. Zusätzlich benötigt der Service eine Tabelle, die den aktuellen Geldbetrag jedes Nutzers enthält. Außerdem sollten die einzelnen Transaktionen jedes Nutzers in einer separaten Tabelle gesichert werden. Für die reine Implementierung dieser Anwendung wäre dies nicht notwendig. Für den Nutzer eines BankingServices ist neben dem Kontostand auch die Liste an getätigten Transaktionen interessant, um die Ausgaben und Einnahmen zuordnen zu können. Im Rahmen dieser Implementierung wird die Tabelle zusätzlich für Analysezwecke verwendet werden.

Bei einer Anfrage, den Geldbetrag eines konkreten Nutzers zu erhöhen, wird in einer lokalen Transaktion der Betrag des Kontos in der UserCredit-Tabelle erhöht und die Differenz in der Transaktion-Tabelle eingetragen.

Der Service muss Anfragen zum Geldabbuchung ablehnen, wenn die Verringerung den Kontostand in den negativen Bereich fallen lassen würde. In diesem Fall wird die Transaktion abgebrochen.

Beide angebotenen Operationen benötigen eine zugehörige Kompensation, da sie den Datenbestand verändern. Die Verwendung des jeweils anderen Endpunktes ist semantisch bereits korrekt. Der Klarheit halber sollen zwei weitere Endpunkte eingeführt werden, die nur für die Kompensation verwendet werden sollen.

4.4.5 OrderService

Der OrderService übernimmt die Rolle des Koordinators im Orchestrator-Saga-Patterns. Die Bestellung wird entgegengenommen und vom OrderService initialisiert. Zur Initialisierung gehört die Generierung einer Vorgangsnummer sowie das Abspeichern der Bestellung in einer separaten Tabelle. Anhand dieser Tabelle wird persistiert, an welcher Stelle der Ausführung die Saga sich befindet, und in welchem Status die Bestellung ist. Die etwaigen ausgeführten Kompensationsschritte sind in ihrer eigenen Tabelle und werden der Vorgangsnummer zugeordnet. Die gewünschten Artikel einer Bestellung sind in eine separate Tabelle ausgelagert und verweisen auf die Saga-Tabelle.

Als Koordinator hat dieser Service die Verantwortung, die an der Saga beteiligten Services korrekt aufzurufen. Die Reihenfolge und die getroffenen Entscheidungen repräsentieren die Geschäftslogik.

Nach jedem Schritt persistiert der OrderService den Erfolg oder Misserfolg. Die Tabelle, in der die Schritte gespeichert werden, stellt das Saga Execution Log dar. Außerdem ruft der Service nach Feststellung eines Misserfolgs die Backward-Recovery auf.

Neben der Schnittstelle zum Platzieren der Bestellung soll dem Nutzer ermöglicht werden, die Bestellung zu stornieren. Dieser zusätzliche Endpunkt nimmt die Vorgangsnummer der zuvor ausgelösten Bestellung entgegen. Falls die Ware noch nicht beim

Kunden eingetroffen ist, kann hier die Bestellung abgebrochen werden. Eine solche Stornierung löst ebenfalls Backward-Recovery aus und soll den Initialzustand wiederherstellen. Diese Aktion stellt keine lokale Transaktion der globalen Transaktion dar; es ist eine Aktion, die von außen in den Bestellprozess eingreift. Damit ist die Stornierung kein T und hat somit kein zugehöriges C.

4.5 Technische Kontextabgrenzung

Bei der Modellierung der Datenbankschicht wurde das Database-per-Service Muster verwendet. Dieses Muster erlaubt eine sehr lose Bindung der Services und lässt die Datenbasis in der Verantwortung eines Services. Es ist möglich, ein Microservice-System zu implementieren, welches das Muster einer gemeinsamen Datenbank verwendet. Dies würde die Implementierung atomaren und konsistenten Transaktionen vereinfachen. Die Voraussetzungen für eine solche Implementierung sind jedoch nicht immer gegeben, da an der LLT teilhabende Services unter Umständen nicht in der Verantwortung des Entwicklerteams liegen könnten, welches die LLT zu implementieren hat. Aus diesem Grund wird im Rahmen der für diese Implementierung vorzunehmende Implementierung jeder Service als getrennte Komponente aufgefasst, die als alleinige Instanz auf ihre eigenen Daten zugreift und zugreifen kann.

4.5.1 ArticleService

Datenbankschicht Der ArticleService soll lediglich Daten aus der Datenbanksicht zurückliefern. Deshalb wird für diesen Service lediglich eine Tabelle benötigt. Die Tabelle *article* enthält für jeden anzubietenden Artikel den zugehörigen Namen und Preis.

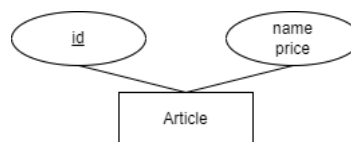


Abbildung 4.1: ER-Diagramm ArticleService

Schnittstellen Die Produktdaten sollen von dem Frontend abgefragt und dargestellt werden. Dabei werden alle vorhandenen Produktdaten selektiert und zurückgegeben. Zusätzlich soll der Koordinator eine gezielte Abfrage durchführen können, welche den Preis eines Artikels für eine gegebene ProduktId liefert. Beide Schnittstellen sind RESTful, da jeder Artikel als Ressource angesehen wird.

Da eine Bestellung mehrere unterschiedliche Artikel enthalten darf, wird zusätzlich eine Schnittstelle angeboten, die dem Aufrufer ermöglicht, mehrere Artikel per Id aufzulösen. Die angefragten ArtikelIds werden als Queryparameter übergeben.

Endpunkt	Http-Methode	Argumente
/api/articles	GET	optionale Einschränkung der Ids per Queryparameter
/api/articles/{id}	GET	ArticleId

4.5.2 StockService

Datenbankschicht Der StockService verwaltet vier Tabellen. Die zentrale Tabelle ist *articlestock* und stellt für jeden bekannten Artikel den auf Lager befindlichen Vorrat dar. Eine Reservierung für eine gegebene Vorgangsnummer wird in der Tabelle *blockedarticles* durch alle Tupel, bei denen diese Nummer auftritt. Die Lieferungen werden in der Tabelle *shipments* dargestellt. Auch hier gehört eine Vorgangsnummer zu den Spalten. Zusätzlich gibt es das Attribut *hasarrived*, was Auskunft über den Status der Lieferung gibt. Die zu einer Lieferung gehörenden Artikel und deren Menge sind in der Tabelle *shippedarticles* enthalten.

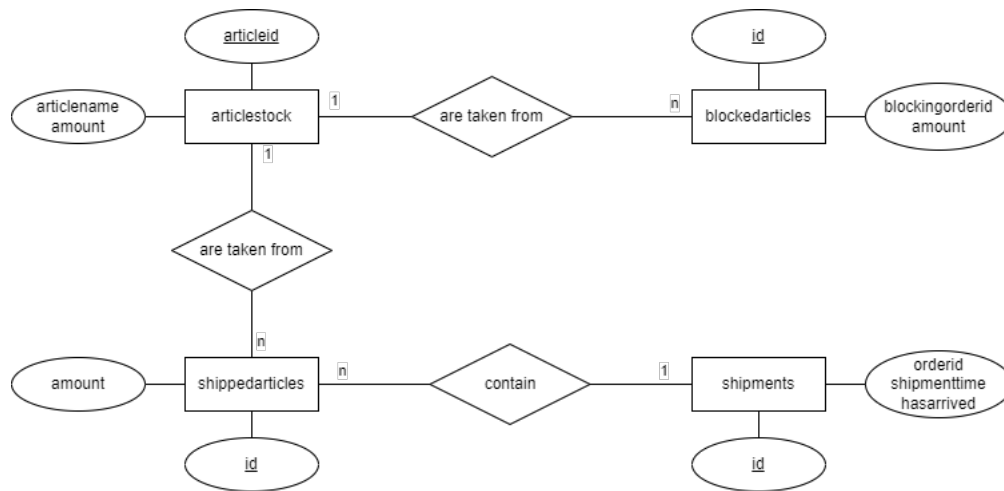


Abbildung 4.2: ER-Diagramm StockService

Schnittstellen Der Endpunkt */api/blocked-articles* überträgt frei verfügbare Artikel aus der Tabelle *articlestock* in die Tabelle *blockedarticles*. Als Argumente werden die zu blockierenden Artikel-Ids und Artikel-Mengen sowie die Vorgangsnummer benötigt. Teil der lokalen Transaktion sind folgende Schritte:

1. Reduzieren jedes Artikelvorrats in der Tabelle *articlestock*
2. Einfügen eines Elements in der Tabelle *blockedarticles* für jede zu blockierende Artikel-Id

Der Endpunkt */api/blocked-articles-compensation* stellt die Kompensierung für die Schnittstelle */api/blocked-articles* dar. Als Argument wird hier lediglich die Vorgangsnummer benötigt. Notwendige Schritte der auszuführenden lokalen Transaktion sind:

1. Selektieren aller Elemente aus *blocked-articles* mit der angefragten Vorgangsnummer
2. Löschen dieser Elemente
3. Erhöhen der Vorratsmengen in *articlestock* für jede Artikelblockierung

Der Endpunkt */api/start-shipment* erwartet die Vorgangsnummer als Argument. Die reservierten Artikel werden in eine Lieferung umgewandelt und versendet. Die Schritte der ablaufenden lokalen Transaktion sind:

1. Initialisieren eines Elements in *shipments* mit dem Status *hasarrived=0*
2. Selektieren und Löschen aller Elemente in *blockedarticles*, die die *OrderId* enthalten
3. Einfügen der Selektierungen in der Tabelle *shippedarticles*

Der Endpunkt */api/finish-shipment* wird ausschließlich vom Lieferanten verwendet und dient zur Bestätigung der Lieferung. Es wird lediglich der Status der entsprechenden *ShipmentId* in der Tabelle *shipments* auf 1 gesetzt.

Der Endpunkt */api/shipments* liefert lediglich den Status der angeforderten *ShipmentId*. Der Koordinator hat mit dem Aufruf von */api/start-shipments* die Lieferung ausgelöst. Der Koordinator hat mit der Schnittstelle */api/shipments* die Möglichkeit, den Status der Lieferung solange abzufragen, bis der Lieferant per Aufruf von */api/finish-shipment* den Lieferabschluss bestätigt. Die Kombination von */api/start-shipment*, */api/finish-shipment* und */api/shipments* können als Polling-Implementierung eines asynchronen Request-Response Musters aufgefasst werden.

Der letzte Endpunkt des StockServices ist */api/cancel-shipment* und bietet dem Koordinator die Möglichkeit, auf eine Stornierung zu reagieren. Bis die Lieferung abgegeben und bestätigt wurde, kann diese Schnittstelle verwendet werden, um die Lieferung abubrechen. Als Argument wird die *ShipmentId* benötigt.

Endpunkt	Http-Methode	Argumente
<i>/api/blocked-articles</i>	POST	<i>ArticleId</i> , <i>Amount</i> , <i>OrderId</i>
<i>/api/blocked-articles-compensation</i>	POST	<i>OrderId</i>
<i>/api/start-shipment</i>	POST	<i>OrderId</i>
<i>/api/finish-shipment</i>	POST	<i>ShipmentId</i>
<i>/api/shipments</i>	GET	<i>ShipmentId</i>
<i>/api/cancel-shipment</i>	POST	<i>ShipmentId</i>

4.5.3 BankingService

Datenbankschicht Zur Verwaltung des BankingServices gehören drei Tabellen. Die Tabelle *bankuser* enthält alle Nutzer, die Tabelle *bankusercredit* ordnet jedem Nutzer einen Kontostand zu und die Tabelle *bankusertransaction* stellt Veränderung des Kontostands der Tabelle *bankcredit* in der Tabelle *bankusertransaction* als Historie dar.

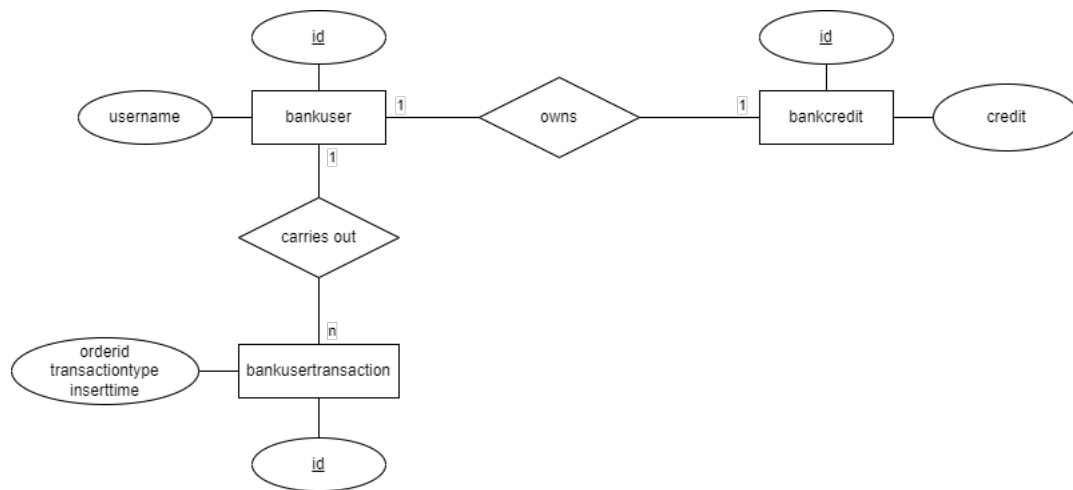


Abbildung 4.3: ER-Diagramm BankingService

Schnittstellen Der BankingService bietet jeweils eine Schnittstelle zum Erhöhen und zum Verringern des Kontostandes an. Dabei wird lediglich in der Tabelle *bankcredit* das Credit-Attribut erhöht oder verringert. Die Spalte ist im Datenbankmanagementsystem mit einer Einschränkung versehen, die verhindert, dass der Wert der Spalte unter 0 fällt. Die Veränderung des Kontostandes ist der erste Schritt der lokalen Transaktion. Der zweite Schritt ist das Einfügen eines neuen Elementes in der Tabelle *bankusertransaction*. In dieser Tabelle wird der Transaktionstyp festgehalten.

Endpunkt	Http-Methode	Argumente
/api/add-money	POST	UserId, Amount, OrderId
/api/add-money-compensation	POST	UserId, Amount, OrderId
/api/remove-money	POST	UserId, Amount, OrderId
/api/remove-money-compensation	POST	UserId, Amount, OrderId

4.6 Ergebnisse

Der entworfene Prozess soll nun als DEA dargestellt werden. Dafür sind alle möglichen Ergebnisse zu erfassen, die jede lokale Transaktion aus Sicht des Koordinators liefern kann.

4.6.1 Ergebnisse aller Transaktionen

Transaktion	Ergebnis	Bedeutung
Initialize Saga	Success	Bestellung ist initialisiert
Get Article Data	200	Artikeldaten wurden vom ArticleService empfangen
	404	Artikel wurde nicht gefunden
Validate Price	Success	Preis aus Bestellung und aus dem System stimmen überein
	Failure	Preise aus Bestellung und aus dem System stimmen nicht überein

Block Articles	200 409 429	Produkte wurden reserviert Conflict (Lagervorrat ist erschöpft) Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Remove Money	200 409 429	Geldbetrag auf dem Konto wurde verringert Lokale Transaktion ist fehlgeschlagen (Konto ist nicht gedeckt) Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Add Money	200 409 429	Geldbetrag auf dem Konto wurde erhöht Lokale Transaktion ist fehlgeschlagen Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Start Shipment	200 409 429	Lieferung wurde ausgelöst Lokale Transaktion ist fehlgeschlagen Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Check No Cancellation	Success Failure	Es wurde keine Stornierung festgestellt Es wurde eine Stornierung festgestellt
Get Shipment Status	200 404	Status wurde vom StockService empfangen Lieferung existiert nicht
Check Shipment Status	Success Failure	Lieferstatus signalisiert abgeschlossene Lieferung Lieferstatus signalisiert noch nicht abgeschlossene Lieferung

4.6.2 Ergebnisse aller Kompensierungen

Transaktion	Ergebnis	Bedeutung
Initialize Saga Compensation	Success	
Get Article Data Compensation	Success	
Validate Price Compensation	Success	
Block Articles Compensation	200 404 409 429	Reservierung wurde aufgehoben Reservierung wurde nicht gefunden Lokale Transaktion ist fehlgeschlagen Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Remove Money Compensation	200	Geldbetrag auf dem Konto wurde erhöht

	409	Lokale Transaktion ist fehlgeschlagen
	429	Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Add Money Compensation	200	Geldbetrag auf dem Konto wurde erhöht
	208	Transaktion wurde auf vorherige Anfrage bereits kompensiert
	404	keine zugehörige kompensierbare Transaktion gefunden
	409	Lokale Transaktion ist fehlgeschlagen
	429	Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl
Start Shipment Compensation	200	Lieferung wurde abgebrochen
	404	Lieferung existiert nicht
	409	Lokale Transaktion ist fehlgeschlagen
	410	Lieferung wurde nicht abgebrochen, da sie bereits abgeschlossen ist
	429	Mehrere Transaktionen behindern sich und lokale Transaktion schlägt fehl

4.7 Saga Execution Component

In 4.1 wurde festgelegt, dass der OrderService die Rolle des Koordinators übernimmt. Das bedeutet, dass der OrderService die Saga Execution Component enthält. Als solche hat der OrderService die Verantwortung, die an der LLT teilhabenden Services aufzurufen und auf die Ergebnisse zu reagieren. In diesem Abschnitt werden die dafür notwendigen Implementierungsdetails dargestellt.

4.7.1 Rahmenbedingung für die Versuchsdurchführung

Die SEC übernimmt die Aufgabe, einen DEA auszuführen. Im Rahmen des Versuchs sollen mehrere DEAs konstruiert und durch die selbe SEC ausgeführt werden. Die SEC muss also flexibel genug implementiert werden, damit eine Parametrisierung der Ausführung mit einem DEA als Argument möglich ist.

4.7.2 Ausführung eines DEAs

Zunächst soll der Ablauf eines Durchlaufs eines DEAs innerhalb der SEC dargestellt werden. Es soll nun davon ausgegangen werden, dass ein DEA definiert wurde.

1. Nach Eingang einer Bestellung wird der Initialzustand gewählt, um die Ausführung des DEAs zu starten.
2. Jeder Zustand korrespondiert mit einer auszuführenden Aktion. Diese Aktion wird ausgeführt.

3. Eine Aktion resultiert in einem Ergebnis. Dieses Ergebnis stellt ein Element aus der Menge des Eingabealphabets dar. Dieses Element wird zusammen mit dem Zustand in der Datenbank gespeichert.
4. Die Ausführung des Zustands wird beendet.
5. Die SEC bestimmt den nächsten Zustand. Und führt die korrespondierende Aktion aus.
6. Die Aktion resultiert in einem Ergebnis. Das Ergebnis wird in der Datenbank gespeichert.
7. Die Ausführung des Zustands wird beendet.
8. Die SEC wiederholt diesen Prozess solange bis ein Endzustand erreicht wird.

4.7.3 Modellierung eines DEAs

Die Modellierung eines DEAs ist in Codebeispiel 4.1 abgebildet.

```

1 public class SimpleStateMachine
2 {
3     public List<string> States;
4     public string InitialState;
5     public List<string> EndStates;
6     public List<string> Sigma;
7     public List<Tuple<Tuple<string, string>, string>> Relations;
8
9
10    public SimpleStateMachine(List<string> states,
11        string initialState,
12        List<string> endStates,
13        List<string> sigma,
14        List<Tuple<Tuple<string, string>, string>> relations)
15    {
16        States = states;
17        InitialState = initialState;
18        EndStates = endStates;
19        Sigma = sigma;
20        Relations = relations;
21    }
22 }
```

Codebeispiel 4.1: Modellierung eines DEA in C#

Relations Das Feld *Relations* stellt Liste von möglichen Zustandsübergängen dar. Die SEC kann aus einem Zustand und einem Element aus Sigma den entsprechenden Zustandsübergang berechnen. Damit diese Berechnung deterministisch ist, darf für einen gegebenen Zustand und einen gegebenen Element aus Sigma nur ein Element existieren.

4.7.4 Konstruktion eines DEAs

Nun soll ein solcher DEA initialisiert werden. Dazu wird der Konstruktor dieser Klasse aufgerufen. Es soll folgender Automat konstruiert werden:

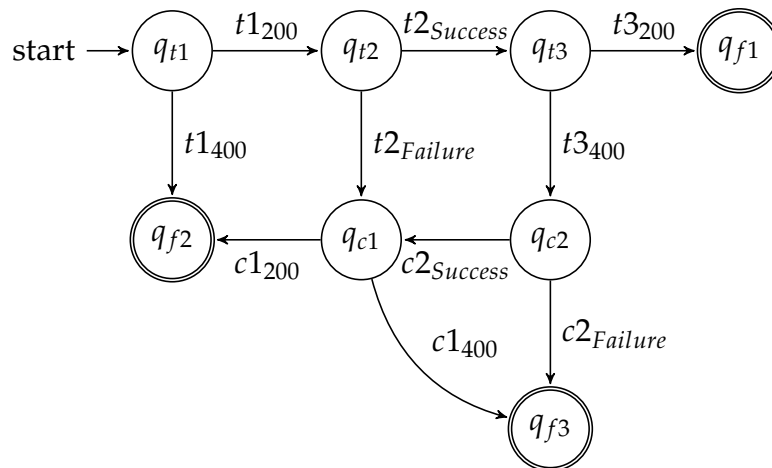


Abbildung 4.4: Zu konstruierender DEA

Die Initialisierung ist in Codebeispiel 4.2 abgebildet:

```
1 public class ExampleDea
2 {
3     // representation of states
4     public static string Q_T1 = "qt1";
5     public static string Q_T2 = "qt2";
6     public static string Q_T3 = "qt3";
7     public static string Q_C1 = "qc1";
8     public static string Q_C2 = "qc2";
9     public static string Q_F1 = "qf1";
10    public static string Q_F2 = "qf2";
11    public static string Q_F3 = "qf3";
12
13    // representation of sigma
14    public static string T1_200 = "t1_200";
15    public static string T1_400 = "t1_400";
16    public static string T2_Success = "t2_Success";
17    public static string T2_Failure = "t2_Failure";
18    public static string T3_200 = "t3_200";
19    public static string T3_400 = "t3_400";
20    public static string C1_200 = "c1_200";
21    public static string C1_400 = "c1_400";
22    public static string C2_200 = "c2_200";
23    public static string C2_400 = "c2_400";
24
25    public SimpleStateMachine ConstructExampleDea()
26    {
27        var states = new List<string>
28        {
```

```

29     Q_T1, Q_T2, Q_T3, Q_C1, Q_C2, Q_F1, Q_F2, Q_F3,
30 };
31
32 var initialState = qt1;
33
34 var sigmaElements = new List<string>
35 {
36     T1_200, T1_400,
37     T2_Success, T2_Failure,
38     T3_200, T3_400,
39     C1_200, C1_400,
40     C2_200, C2_400
41 };
42
43 var endStates = new List<string>
44 {
45     Q_F1, Q_F2, Q_F3
46 };
47
48 var relations = new List<
49     Tuple<Tuple<string, string>, string>>
50 {
51     BuildRelation(Q_T1, T1_200, Q_T2),
52     BuildRelation(Q_T1, T1_400, Q_F2),
53     BuildRelation(Q_T2, T2_Success, Q_T3),
54     BuildRelation(Q_T2, T2_Failure, Q_C1),
55     BuildRelation(Q_T3, T3_200, Q_F1),
56     BuildRelation(Q_T3, T3_400, Q_C2),
57     BuildRelation(Q_C1, C1_200, Q_F2),
58     BuildRelation(Q_C1, C1_400, Q_F3),
59     BuildRelation(Q_C2, C2_200, Q_C1),
60     BuildRelation(Q_C2, C2_400, Q_F3)
61 };
62
63 return new SimpleStateMachine(states, initialState, sigmaElements
64     , endStates, relations);
65 }
66
67 private Tuple<Tuple<string, string>, string> BuildRelation(
68     string inputState,
69     string inputSigmaElement,
70     string newState)
71 {
72     return new Tuple<Tuple<string, string>, string>(
73         new Tuple<string, string>(inputState, inputSigmaElement),
74         newState);
75 }

```

Codebeispiel 4.2: Modellierung eines Beispiel DEA in C#

Verwaltung der DEAs Nach Vorbild des Beispiels in Codebeispiel 4.2 werden alle ausführbaren DEAs definiert. Diese Initialisierung geschieht innerhalb der in Codebeispiel 4.3 definierten Klasse.

```
1 public interface IStateMachineMapper
2 {
3     StateMachine MapToStateMachine(int smValue);
4 }
5
6 public class StateMachineMapper : IStateMachineMapper
7 {
8     private readonly StateMachine Sm1;
9     private readonly StateMachine Sm2;
10    // more StateMachineDefinitions
11
12    public StateMachine MapToStateMachine(int smValue) {
13        switch (smValue)
14        {
15            case 1:
16                return Sm1;
17            case 2:
18                return Sm2;
19            // ...
20        }
21
22        throw new UnknownStateMachineException($"Unknown StateMachine
23            for value [{smValue}].");
24    }
25 }
```

Codebeispiel 4.3: Modellierung eines StateMachineMappers in C#

Per Dependency Injection kann die SEC diese Klasse verwenden. Per Strategie-Pattern wird in einer Funktion der gewünschte DEA ermittelt werden.

Kontrollfluss der SEC Die SEC verwendet den StateMachineMapper, um den gewünschten DEA auszuführen. Die tatsächliche Ausführung findet in einer separaten Komponente, dem StateMachineExecutor statt. Diese Klasse enthält eine Funktion *ExecuteStateMachine*, die für einen DEA und ein Eingabewort den aktuellen Zustand berechnet. Dazu wird jedes Element des Eingabeworts abgearbeitet. Für jedes Element und den aktuellen Zustand wird in der Funktion *FindRelation* die zugeordnete Relation berechnet. Der in der Relation enthaltene Folgezustand wird gesetzt und das abgearbeitete Element des Eingabeworts wird entfernt.

Das Ergebnis der Berechnung ist eine Liste von Konfigurationsübergängen. Eine Konfiguration wird durch die in Codebeispiel 4.4 dargestellten Klasse modelliert.

```

1 public class StateMachineConfiguration
2 {
3     public List<string> Word { get; set; } = new();
4     public string State { get; set; } = string.Empty;
5
6     // Clone Function
7 }

```

Codebeispiel 4.4: Modellierung einer StateMachineConfiguration in C#

Ein Konfigurationsübergang stellt den Wechsel von einer Konfiguration in eine Folgekonfiguration dar. Dabei wird die Länge des Eingabeworts stets verringert.

```

1 public class StateMachineConfigurationTransition
2 {
3     public StateMachineConfiguration C1 { get; set; }
4     public StateMachineConfiguration C2 { get; set; }
5     public Tuple<Tuple<string, Status>, string> Relation { get; set; }
6
7     public StateMachineConfigurationTransition(
8         StateMachineConfiguration c1,
9         StateMachineConfiguration c2,
10        Tuple<Tuple<string, string>, string> relation)
11    {
12        C1 = c1;
13        C2 = c2;
14        Relation = relation;
15    }
16 }

```

Codebeispiel 4.5: Modellierung einer StateMachineConfigurationTransition in C#

Solange das Eingabewort noch nicht vollständig abgearbeitet wurde, werden Konfigurationsübergänge berechnet. Die resultierende Liste von Konfigurationsübergängen beschreibt eindeutig den gewählten Graphen.

```

1 public interface IStateMachineExecutor
2 {
3     List<StateMachineConfigurationTransition> ExecuteStateMachine(
4         StateMachine sm, List<Status> word);
5 }
6
7 public class StateMachineExecutor : IStateMachineExecutor
8 {
9     public List<StateMachineConfigurationTransition>
10        ExecuteStateMachine(StateMachine sm, List<string> word)
11    {
12        List<StateMachineConfigurationTransition> result = new();
13
14        StateMachineConfiguration current = new StateMachineConfiguration
15    {

```

```

14     Word = word,
15     State = sm.InitialState
16 };
17
18 while (current.Word.Count > 0)
19 {
20     StateMachineConfiguration c1 = StateMachineConfiguration.Clone(
21         current);
22
23     var relation = FindRelation(sm.Relations, current);
24
25     string nextState = relation.Item2;
26
27     current.State = nextState!;
28     current.Word.RemoveAt(0);
29
30     StateMachineConfigurationTransition transition = new()
31     {
32         C1 = c1,
33         C2 = new StateMachineConfiguration
34         {
35             State = nextState,
36             Word = current.Word
37         },
38         Relation = relation
39     };
40
41     result.Add(transition);
42 }
43
44 return result;
45 }
46
47 private Tuple<Tuple<string, string>, string> FindRelation(
48     List<Tuple<Tuple<string, string>, string>> relations,
49     StateMachineConfiguration currentConfiguration)
50 {
51     foreach (var relation in relations)
52     {
53         var relStartState = relation.Item1.Item1;
54         var relWord = relation.Item1.Item2;
55
56         if (currentConfiguration.State.Equals(relStartState) &&
57             currentConfiguration.Word.First() == relWord)
58         {
59             return relation;
60         }
61     }

```

```

62     throw new NoRelationException($"No Relation found for State = [{
        currentConfiguration.State}] and Element = [{
        currentConfiguration.Word.First()}]");
63 }
64 }

```

Codebeispiel 4.6: Modellierung einer StateMachineExecutors in C#

Das Ergebnis der Berechnung ist die Liste von Konfigurationsübergängen. Der letzte Konfigurationsübergang enthält den Zielzustand, der noch auszuführen ist. Über den ActionExecutor wird die mit diesem Zustand korrespondierende Aktion ausgeführt. Die Kommunikation der von der SEC verwendeten Klassen ist in Abbildung 4.5 abgebildet. Die Funktion *GetTransactionsForOrderSaga* greift auf die Datenbanktabelle *ordersagatransactions* zu und liefert das Transaktionslog. Das Transaktionslog wird lediglich von den mit einem Zustand korrespondierenden Aktionen ergänzt. Die SEC selbst greift nur lesend auf dieses Log zu.

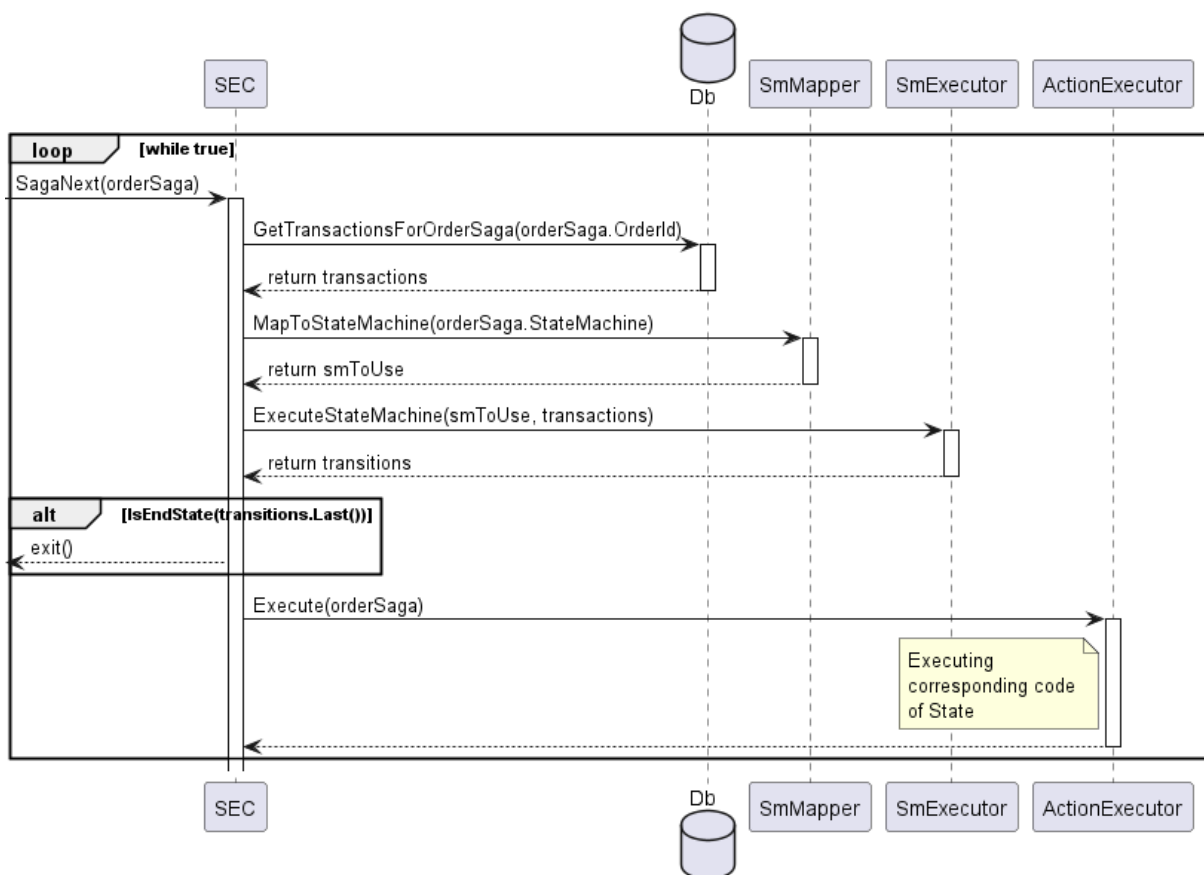


Abbildung 4.5: Kontrollfluss der SEC

4.8 Planung der Datenerfassung

Auf Grundlage des nun bekannten Systems sollen die Testfälle und Testszenarien definiert werden.

4.8.1 Testszenarien

Ein Testszenario soll das Verhalten des Netzwerks beschreiben. Ziel der in diesem Kapitel stattfindenden Untersuchung ist eine robuste Saga-Implementierung, die in allen möglichen Testszenarien ein konsistentes Verhalten des Systems gewährleistet.

4.8.2 Fehlerquellen

Zuerst ist zu identifizieren, an welchen Stellen eine Kommunikation in einem verteilten System mittels Request-Response-Muster fehlschlagen kann. Im folgenden Beispiel wird dies anhand einer simplen Kommunikation illustriert, die aus einem Request und einer Response besteht. Es wird davon ausgegangen, dass die Verarbeitung des Requests zu einer Änderung des Systemzustands des Empfängers führt.

Szenario 1 Im ersten Szenario entstehen keine Netzwerkfehler. Dieses Szenario ist der Ausgangspunkt. Die Korrektheit der Saga in diesem Fall ist eine Voraussetzung für die Formulierung und Analyse in folgenden Szenarien.

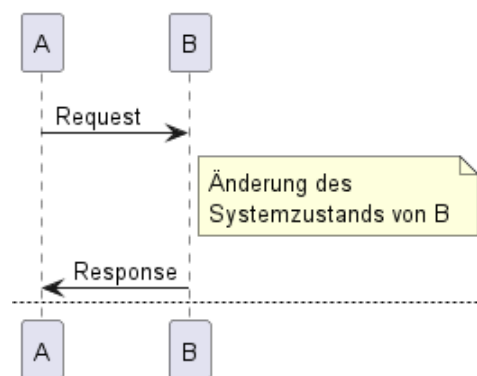


Abbildung 4.6: Sequenzdiagramm für Szenario 1

Szenario 2 Es können Netzwerkfehler auftreten, die verhindern, dass der Request den Empfänger erreicht. Dabei findet keine Verarbeitung der Nachricht im Empfängerservice statt. Es findet weder eine Veränderung des Systemzustands des Empfängers noch eine Versendung einer Response statt.

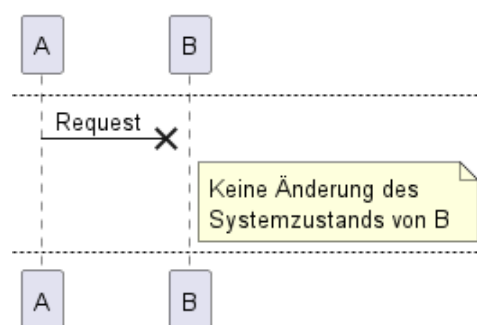


Abbildung 4.7: Sequenzdiagramm für Szenario 2

Im Rahmen dieses Versuchs wird das Auftreten solcher Fehler in Testszenario 2 simuliert.

Szenario 3 Findet ein Netzwerkfehler nach der Verarbeitung des Requests im Empfängerservice statt, erreicht die Response den Sender nicht. Die abgeschlossene Verarbeitung des Requests hat zu einer Veränderung des Systemzustands im Empfängerservice geführt. Dies führt dazu, dass der Sender keine Kenntnis über den Erfolg oder Misserfolg des ursprünglichen Requests hat.

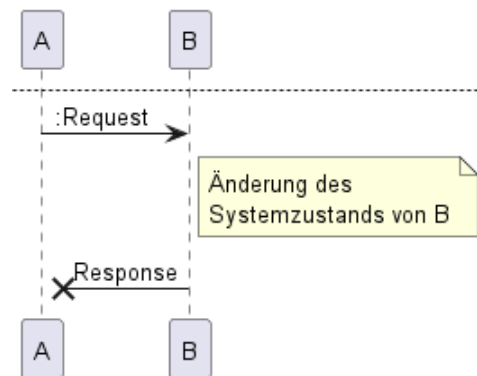


Abbildung 4.8: Sequenzdiagramm für Szenario 3

Im Rahmen dieses Versuchs wird das Auftreten solcher Fehler in Testszenario 3 simuliert. Zusätzlich treten in Testszenario 3 die Netzwerkfehler des Testszenario 2 auf. Das Testszenario 3 simuliert somit ein Netzwerkverhalten, welches verschiedene Arten von Netzwerkfehlern abdeckt. Wenn eine LLT unter den im Testszenario 3 geschaffenen Bedingungen Konsistenz gewährt, kann die These angenommen werden.

4.8.3 Simulation der Testfälle

Die zu simulierenden Testfälle werden durch einen separaten Service durchgeführt, die TestApi. Die Schnittstellen, die direkt mit der Durchführung der LLT interagieren sind:

Service	Schnittstelle	Beschreibung	Akteur
OrderService	<i>POST /api/orders</i>	Platzieren einer Bestellung	Frontend (Kunde)
StockService	<i>POST /api/finish-shipment</i>	Lieferbestätigung	Lieferant
OrderService	<i>POST /api/cancel-order</i>	Stornierung	Frontend (Kunde)

FinishOrders Der erste Testfall simuliert eine erfolgreiche Verarbeitung des Bestell- und Lieferprozesses. Die TestApi generiert Bestellungen und ruft den entsprechenden Endpunkt zum Platzieren im OrderService auf. Für jede der Bestellungen wird in der TestApi gewartet, bis die Lieferung ausgelöst wurde. Dann wird die Lieferbestätigung simuliert, indem der entsprechende Endpunkt im StockService aufgerufen wird. Der Koordinator erhält die Möglichkeit, den erfolgreichen Endzustand zu erreichen. Dies ist der erwartete Endzustand. Dieser Testfall wird als *FinishOrders* bezeichnet.

CancelOrders Der zweite Testfall simuliert eine Stornierung der Bestellung. Die TestApi generiert Bestellungen und platziert diese. Nachdem die Lieferung ausgelöst wurde, platziert die TestApi die Stornierung.

Der Koordinator erkennt die Stornierung und hat die Verantwortung, die Lieferung zu stoppen und im Anschluss alle lokalen Transaktionen zu kompensieren. In diesem Testfall werden alle Kompensierungen aufgerufen. Dieser Testfall wird mit *CancelOrders* bezeichnet.

Der erwartete Endzustand dieser Bestellung ist *FailedWithCompensation*.

4.8.4 Datengenerierung

Um den Ablauf der Services zu simulieren, müssen Daten in jedem Teilsystem generiert werden. Dabei wird in dieser Versuchsdurchführung zwischen zwei Arten der Datengenerierung unterschieden: statische und dynamische Datengenerierung.

Statisch generierte Daten Zu den statisch generierten Daten gehören die Daten, die manuell einmalig generiert und anschließend in die Datenbank eingefügt werden.

Im ArticleService werden die Daten der Produkttabelle generiert. Dazu gehören die verschiedenen Produktbezeichnungen und Preise.

In den zwei BankServices werden die Daten der Nutzertabellen generiert. Für jeden BankService werden 100 verschiedene Nutzer erstellt. Initial erhält jeder dieser Nutzer einen ausreichend großen Geldbetrag als Startguthaben.

Dynamisch generierte Daten Die in der TestApi generierten Bestellungen werden dynamisch erzeugt. Jede Bestellung wählt einen zufälligen BankService-Nutzer und eine Menge von zwischen 1 und 10 verschiedenen Artikeln mit einer zufälligen Menge zwischen 1 und 4.

Eine solche zufällig generierte Bestellung ist in Codebeispiel 4.7 abgebildet.

```
1 {
2   "consument": {
3     "userId": "Xena",
4     "bankId": "Bank1"
5   },
6   "requestedArticles": [
7     {
8       "articleId": 42,
9       "articlePrice": 99.0,
10      "amount": 2
11    },
12    {
13      "articleId": 16,
14      "articlePrice": 49.99,
15      "amount": 3
16    }
17  ]
}
```

Codebeispiel 4.7: Json für dynamisch generierte Bestellung

4.8.5 Messwerte

Um die verschiedenen Messungen vergleichen zu können, werden die Messungen eines DEAs in jedem Testfall und in jedem Testszenario durchgeführt. Nach der Messung sollen daraus Aussagen über die Konsistenz und über die Korrektheit der modellierten LLT getroffen werden. Dazu werden folgende Messwerte erhoben:

StateAnalysisResult Dieser Teil des Messergebnisses verwendet die im Koordinator enthaltenen Zustände. Als Scope wird ein konkreter Testfall, ein konkretes Testszenario und ein DEA festgelegt.

Messwert	Beschreibung
totalCount	Anzahl der Sagas
successfullCount	Anzahl der Sagas mit Endzustand $q_{Success}$
finishedCount	Anzahl der Sagas mit Endzustand $\neq q_{Pending}$
pendingCount	Anzahl der Sagas mit Endzustand $q_{Pending}$
failedWithCompensation-Count	Anzahl der Sagas mit Endzustand $q_{failedWithCompensation}$
failedWithoutCompensation-Count	Anzahl der Sagas mit Endzustand $q_{failedWithoutCompensationCount}$
hasCorrectEndstateCount	Anzahl der Sagas mit dem erwarteten Endzustand des Testfalls
containsAllExpectedLogs-Count	Anzahl der Sagas, deren Transaktionslog alle erwarteten Logs des Testfalls aufweist
isSuccessfullTestInstance-Count	Anzahl der Sagas mit dem erwarteten Endzustand und erwarteten Transaktionslogs des Testfalls

Für jeden dieser Werte gibt wir einen normalisierter Wert berechnet, der ins Verhältnis zum Messwert *totalCount* gesetzt wird. Da diese Werte ausschließlich aus der Sicht des Koordinators gemessen werden, geben diese Werte lediglich Auskunft über den erreichten Endzustand einer Saga. Eine Saga mit dem Endzustand $q_{Success}$ ist nicht gleichbedeutend mit einer konsistenten LLT.

TransactionAnalysisResult Um Aussagen über die Konsistenz einer LLT zu treffen, werden die durchgeführten Transaktionen, die im Transaktionslog des Koordinators festgehalten sind, mit den durchgeführten Transaktionen der Teilnehmerservices verglichen. Für jede Saga kann der Unterschied zwischen Transaktionsanzahl aus Koordinatorsicht und aus Teilnehmerservicesicht berechnet werden. Enthält eine Saga mindestens eine Transaktion, bei der dieser Unterschied auftritt, wird sie als inkonsistent bezeichnet. Die Summe der Unterschiede pro Transaktionstyp kann ebenfalls gebildet werden. Es ergibt sich folgende Tabelle:

Messwert	Beschreibung
diffRemoveMoney-Transaction	Summe der Unterschiede über alle Sagas für Transaktionstyp RemoveMoney
diffAddMoneyTransaction	Summe der Unterschiede über alle Sagas für Transaktionstyp AddMoney
diffRemoveMoney-CompensationTransaction	Summe der Unterschiede über alle Sagas für Transaktionstyp RemoveMoneyCompensation
diffAddMoney-CompensationTransaction	Summe der Unterschiede über alle Sagas für Transaktionstyp AddMoneyCompensation
diffBlockArticles-Transaction	Summe der Unterschiede über alle Sagas für Transaktionstyp BlockArticles
diffStartShipment-Transaction	Summe der Unterschiede über alle Sagas für Transaktionstyp StartShipment
diffBlockArticles-CompensationTransaction	Summe der Unterschiede über alle Sagas für Transaktionstyp BlockArticlesCompensation
diffStartShipment-CompensationTransaction	Summe der Unterschiede über alle Sagas für Transaktionstyp StartShipmentCompensation
consistentSagas	Anzahl der konsistenten Sagas

ExecutionTimeAnalysisResult Schlussendlich wird ein weiteres Messergebnis definiert. Dieses Ergebnis dient dazu, die verschiedenen DEAs hinsichtlich ihrer Laufzeit zu untersuchen. Dabei wird die Differenz der ersten und letzten Transaktion im Log des Koordinators gebildet.

Messwert	Beschreibung
minRuntime	minimale Laufzeit aller Sagas [s]
maxRuntime	maximale Laufzeit aller Sagas [s]
avgRuntime	durchschnittliche Laufzeit aller Sagas [s]
medianRuntime	50% Quantil der Laufzeit aller Sagas [s]
upperQuartileRuntime	75% Quantil aller Sagas [s]
lowerQuartileRuntime	25% Quantil aller Sagas [s]

Die Analyse der Laufzeiten trägt keine Bedeutung für Aussagen bezüglich der Konsistenz oder Korrektheit einer LLT. Ein wesentliches Werkzeug für die Definition der verschiedenen DEAs sind Retries. Die ExecutionTimeAnalysisResults geben Auskunft, inwiefern die Laufzeit einer Saga beeinflusst wird.

4.9 Implementierung des SmBasic

Der DEA der ersten Implementierung wird im Folgenden als SmBasic bezeichnet. Dieser DEA soll das grundlegende Prinzip des Saga-Patterns unter Verwendung der Backward-Recovery implementieren. Jeglicher Fehler führt dazu, dass die SEC eine Kompensierung der Saga verfolgt.

4.9.1 Strategie für die Konstruierung des DEAs SmBasic

Alle Erfolge eines Ts führen zum folgenden T. Alle anderen Ergebnisse führen für Ts zu einem Zustandswechsel zu dem nächstkleineren C. Erfolgreiche Cs führen zum nächstkleinerem C. Alle anderen Ergebnisse führen für Cs zu einem Zustandswechsel in den Zustand *FailedWithCompensation*. Das letzte T führt bei Erfolg zu einem Übergang in den Zustand *Done*. Ebenso führt C_1 bei Erfolg zu einem Übergang in den Zustand *FailedWithCompensation*.

Ergebnistyp	Zustand	Ergebnis e	Folgezustand
API-Ergebnis	T_n	$e \in \{Tn_{200}\}$	T_{n+1}
API-Ergebnis	T_n	$e \notin \{Tn_{200}\}$	C_{n-1}
IPE	T_n	$e \in \{Tn_{Success}\}$	T_{n+1}
IPE	T_n	$e \notin \{Tn_{Success}\}$	C_{n-1}
API-Ergebnis	C_n	$e \in \{Cn_{200}\}$	C_{n-1}
API-Ergebnis	C_n	$e \notin \{Cn_{200}\}$	<i>FailedWithoutCompensation</i>
IPE	C_n	$e \in \{Cn_{Success}\}$	C_{n-1}
IPE	C_n	$e \notin \{Cn_{Success}\}$	<i>FailedWithoutCompensation</i>

Aus diesem Regelwerk ergibt sich der in Abbildung 4.9 dargestellte DEA.

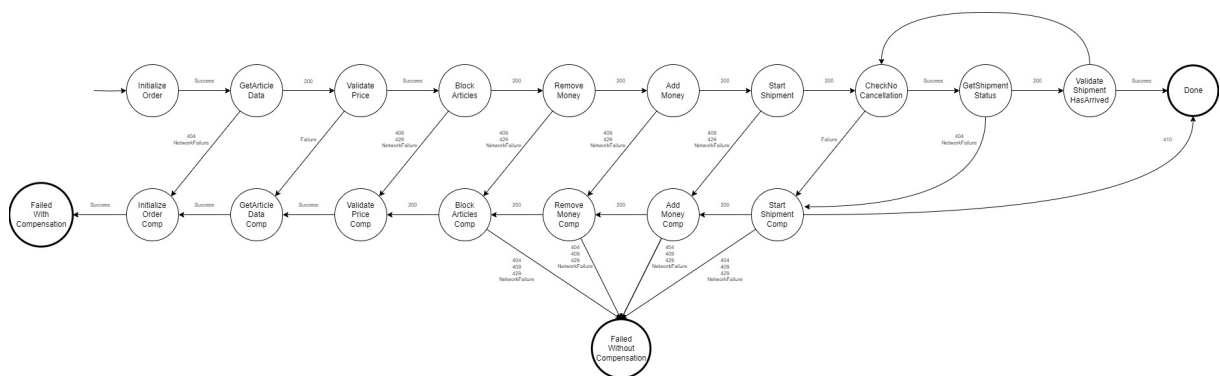


Abbildung 4.9: DEA für SmBasic

4.9.2 StateAnalysisResult

Testfall FinishOrders Folgende Tabelle bildet das StateAnalysisResult der Messung des SmBasic in Testfall FinishOrders.

Messwert	S1	S2	S3
successfullPercentage	0.80	0.42	0.19
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.20	0.53	0.72
failedWithoutCompensation-Percentage	0.0	0.06	0.10
hasCorrectEndstatePercentage	0.80	0.42	0.19
containsAllExpectedLogs-Percentage	0.80	0.38	0.15
isSuccessfullTestInstance-Percentage	0.80	0.38	0.15

Die Messung zeigt, dass bereits in Testszenario 1 nur 80% der Sagas zum erwarteten Endzustand führen. Der Anteil der Sagas, die den Zustand *Success* erreichen, wird mit jedem Testszenario geringer: 80% in Testszenario S1, 42% in S2 und 19% in S3.

Das ist damit zu begründen, dass jeglicher Fehler in der Ausführung des SmBasic zur Kompensierung führt. Zu den Fehlern, die zur Kompensierung (für Ts) oder zum Zustand *FailedWithoutCompensation* (für Cs) führen, gehören neben den Fehlern, die einen kritischen Konflikt ausdrücken auch vorübergehende Fehler (API-Ergebnisse mit *tn₄₂₉*) und in S2 und S3 Netzwerkfehler.

Dies drückt sich außerdem in dem Messwert *failedWithoutCompensation* aus, der ebenfalls in jedem Testszenario größer wird.

In Tabelle 4.9 ist das Transaktionslog einer Saga abgebildet, die aufgrund eines vorübergehenden Fehlers abgebrochen wurde.

Zustand	Ergebnis
InitializeOrder	InitializeSagaSuccess
GetArticleData	GetProductData200
ValidatePrice	ValidatePriceSuccess
BlockArticles	BlockArticles429
ValidatePriceCompensation	ValidatePriceCompensationSuccess
GetArticleDataCompensation	GetProductDataCompensationSuccess
InitializeOrderCompensation	InitializeSagaCompensationSuccess

Tabelle 4.9: Transaktionslog für Saga im Testfall 1 und Testszenario 1

Testfall CancelOrders In ?? ist das StateAnalysisResult für den Testfall CancelOrders dargestellt. Hier zeigt sich die Berechtigung des Messwertes *isSuccessfullTestInstance-Percentage*. Der erwartete Endzustand *FailedWithCompensation* wird in diesem Testfall erwartet und in Testszenario 1 in 95% aller Sagas erreicht. Der Messwert *containsAll-ExpectedLogsPercentage* zeigt, dass in Testszenario 1 lediglich 87% die erwarteten Logs

enthalten. Das bedeutet, dass ein Anteil der Sagas mit Endzustand *FailedWithCompensation* aufgrund eines Fehlers zur Kompensierung gewechselt haben und nicht wie erwartet den Zustand *CheckNoCancellation* erreicht haben. Somit stellen diese Sagas keine erfolgreichen Testinstanzen mehr dar.

Messwert	S1	S2	S3
successfullPercentage	0.0	0.0	0.0
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.95	0.77	0.75
failedWithoutCompensation-Percentage	0.05	0.23	0.25
hasCorrectEndstatePercentage	0.95	0.77	0.75
containsAllExpectedLogs-Percentage	0.87	0.27	0.06
isSuccessfullTestInstance-Percentage	0.87	0.27	0.06

Abgebrochene Sagas Der Messwert *failedWithoutCompensationPercentage* stellt den Anteil der Sagas dar, die aufgrund eines Fehlers während einer Kompensierung die Ausführung abbrechen. Im konstruierten SmBasic gibt es keine Retries. Das bedeutet, dass jede Saga, die zwei fehlerhafte Ergebnisse im Log enthält, in diesem Zustand landet. Ein Beispiel dafür ist im Transaktionslog in Tabelle 4.23 abgebildet.

Zustand	Ergebnis
InitializeOrder	InitializeSagaSuccess
GetArticleData	GetProductData200
ValidatePrice	ValidatePriceSuccess
BlockArticles	BlockArticles200
RemoveMoney	RemoveMoney200
AddMoney	AddMoney200
StartShipment	StartShipment200
CheckNoCancellation	CheckNoCancellationSuccess
GetShipmentStatus	GetShipmentStatus200
ValidateShipmentHasArrived	ShipmentHasArrivedFailure
CheckNoCancellation	CheckNoCancellationSuccess
GetShipmentStatus	GetShipmentStatusNetworkFailure
StartShipmentCompensation	StartShipmentCompensation200
AddMoneyCompensation	AddMoneyCompensationNetworkFailure

Tabelle 4.11: Transaktionslog für Saga im Testfall CancelOrders und Testszenario 2

4.9.3 TransactionAnalysisResult

In Tabelle 4.24 sind die TransactionAnalysisResults für beide Testfälle dargestellt.

	S1	S2	S3
FinishOrders	1	1	0.87
CancelOrders	1	1	0.81

In beiden Testfällen treten unter den Bedingungen von Testszenario 1 und 2 keine Inkonsistenzen auf. In Testszenario 3 führen 87% im Testfall *FinishOrders* und 81% im Testfall *CancelOrders* aller Sagas zu mindestens zu einem inkonsistenten Zustand innerhalb der Teilnehmerservices.

Neben den Sagas, die im Endzustand *FailedWithoutCompensation* landen, führen auch Sagas zu einem inkonsistenten Systemzustand, die nach einem Netzwerkfehler mit der Kompensierung fortfahren. Ein Beispiel dafür ist das Transaktionslog in Tabelle 4.13. Der BankService hat die lokale Transaktion *RemoveMoney* erfolgreich ausgeführt. Die Response ging verloren, weshalb der Koordinator mit der Kompensierung fortgefahren hat. Die lokale Transaktion *RemoveMoney* wurde nicht kompensiert. Fachlich stellt dieses Saga-Log einen Bestellprozess dar, der abgebrochen wurde. Das Geld des Kundenkontos wurde abgebucht und nicht rückerstattet. Der Saga-Prozess hat keine Kenntnis von diesem fachlichen Fehler.

Zustand	Ergebnis
InitializeOrder	InitializeSagaSuccess
GetArticleData	GetProductData200
ValidatePrice	ValidatePriceSuccess
BlockArticles	BlockArticles200
RemoveMoney	RemoveMoneyNetworkFailure
BlockArticlesCompensation	BlockArticlesCompensation200
ValidatePriceCompensation	ValidatePriceCompensationSuccess
GetArticleDataCompensation	GetProductDataCompensationSuccess
InitializeOrderCompensation	InitializeSagaCompensationSuccess

Tabelle 4.13: Transaktionslog einer Saga für *CancelOrders* im Testszenario 3

4.10 Implementierung des SmBasicSafeRetries

Der nächste DEA verwendet den SmBasic als Grundlage und soll das Problem des vorzeitigen Abbruchs verhindern. Dabei sollen keine neuen Inkonsistenzquellen eingeführt werden.

4.10.1 Verhinderung eines Vorzeitigen Abbruchs

Netzwerkfehler Für alle Transaktionen, die nicht zu einer Änderung des Systemzustands eines Teilnehmerservices führen, können Retries im Falle eines Netzwerkfehlers eingeführt werden. Dazu gehören *GetArticleData* und *GetShipmentStatus*.

Lastfehler Behindern sich mehrere parallele lokale Transaktionen innerhalb eines Teilnehmerservices, kommt es zu einer Race Condition (Wettlaufsituation). Dabei gewinnt die erste lokale Transaktion T1 und kann wie gewohnt abgeschlossen werden. Alle lokalen Transaktionen, die innerhalb der Bearbeitungszeit von T1 auf die gesperrten Ressourcen zugreifen, schlagen fehl. Die aus diesem Fehler resultierende Response enthält den Http-Statuscode 429 und wird vom Koordinator auf ein entsprechendes Ergebnis gemappt. Dieses Verhalten ist für den StockService und die BankServices implementiert.

Antwortet ein Service mit einer solchen Response, ist der Fehler durch einen Retry auflösbar. Das bedeutet, dass für die lokalen Transaktionen *BlockArticles*, *RemoveMoney*, *AddMoney* und *StartShipment* ein Retry eingeführt werden kann. Ebenso kann diese Strategie auf alle zugehörigen Kompensierungen angewendet werden.

DEA SmBasicSafeRetries Aus den beschriebenen Anpassungen ergibt sich der Sm-BasicSafeRetries in Abbildung 4.10.

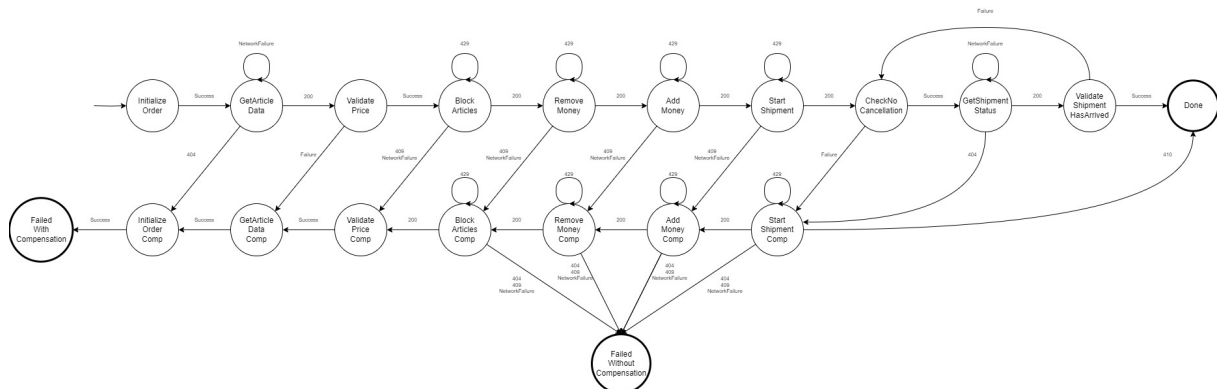


Abbildung 4.10: DEA für SmBasicSafeRetries

4.10.2 StateAnalysisResult

Das StateAnalysisResult von SmBasicSafeRetries und SmBasic sind wie erwartet sehr ähnlich. Im Testfall FinishOrders ist zu sehen, dass die Werte für *isSuccessfulTestInstancePercentage* deutlich höher sind. Die vorzeitigen Abbrüche aufgrund von Last- und Netzwerkfehlern an unkritischen nicht-transaktionellen Stellen wurden durch das Einführen von Retries eliminiert. In Testszenario 1 führt dies dazu, dass 100% der Sagas erfolgreich sind. Das gilt auch für den Testfall CancelOrders.

Testfall FinishOrders

Messwert	S1	S2	S3
successfullPercentage	1.0	0.65	0.39
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.0	0.31	0.47
failedWithoutCompensation-Percentage	0.0	0.05	0.15
hasCorrectEndstatePercentage	1.0	0.65	0.39
containsAllExpectedLogs-Percentage	1.0	0.65	0.39
isSuccessfullTestInstance-Percentage	1.0	0.65	0.39

Testfall CancelOrders

Messwert	S1	S2	S3
successfullPercentage	0.0	0.0	0.0
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	1.0	0.77	0.64
failedWithoutCompensation-Percentage	0.0	0.24	0.37
hasCorrectEndstatePercentage	1.0	0.77	0.64
containsAllExpectedLogs-Percentage	1.0	0.47	0.17
isSuccessfullTestInstance-Percentage	1.0	0.47	0.17

4.10.3 TransactionAnalysisResult

Das TransactionAnalysisResult zeigt, dass der Messwert *consistentSagasPercentage* im Vergleich zu SmBasic sinkt. Das ist damit zu erklären, dass die vorzeitigen Abbrüche im SmBasic das Ergebnis deutlich maskiert haben. Durch die vorzeitigen Abbrüche im SmBasic war die Gesamtzahl an Transaktionen niedriger. Das bedeutet, dass es weniger Möglichkeiten gab, einen Fehler zu verursachen, der zu Inkonsistenz führt.

Die Inkonsistenz ist bei dem Testfall für CancelOrders niedriger als bei FinishOrders. Das hat denselben Grund, der Testfall CancelOrders durchläuft zusätzlich zu den Ts immer die zugehörigen Cs und kann somit in häufigeren Zuständen Inkonsistenzen verursachen.

	S1	S2	S3
FinishOrders	1	1	0.74

	S1	S2	S3
CancelOrders	1	1	0.54

4.11 Implementierung des SmBasicNetworkFailureUnlimitedRetries

Der SmBasicNetworkFailureUnlimitedRetries baut auf das Konzept des vorherigen DEAs SmBasicSafeRetries auf. Es hat sich gezeigt, dass der Anteil der erfolgreichen Sagas erhöht werden kann, indem auf Netzwerkfehler per Forwardrecovery reagiert wird. Das Ziel dieses DEAs ist, den Anteil der vorzeitig abgebrochenen Sagas zu erhöhen. Dafür werden für die Ts *BlockArticles*, *RemoveMoney*, *AddMoney* und *StartShipment* sowie für die zugehörigen Cs ein Retry für Netzwerkfehler eingeführt. Es entsteht der DEA in Abbildung 4.11.

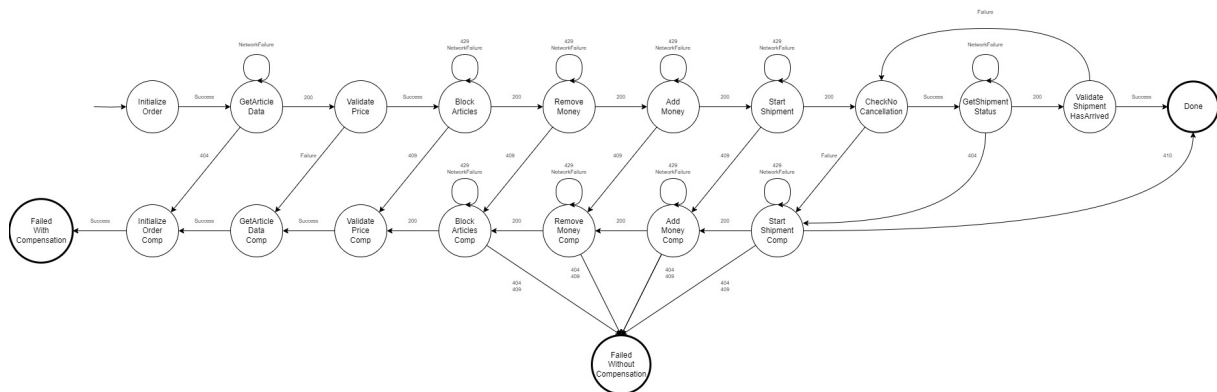


Abbildung 4.11: DEA für SmBasicNetworkfailureUnlimitedRetries

4.11.1 StateAnalysisResult

Das StateAnalysisResult zeigt, dass das Einführen von Retries für transaktionale Zustände dazu führt, dass der gewünschte Endzustand öfter erreicht wird. Testszenario 3 enthält in Testfall FinishOrders 90% und in Testfall CancelOrders 74% erfolgreiche Testinstanzen. Aus Sicht des Koordinators kann auf Netzwerkfehler mit einem Retry erfolgreich reagiert werden, um zum nächsten Zustand zu gelangen.

Testfall FinishOrders

Messwert	S1	S2	S3
successfullPercentage	1.0	1.0	0.91
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.0	0.0	0.0

Messwert	S1	S2	S3
failedWithoutCompensation-Percentage	0.0	0.0	0.1
hasCorrectEndstatePercentage	1.0	1.0	0.91
containsAllExpectedLogs-Percentage	1.0	1.0	0.91
isSuccessfulTestInstance-Percentage	1.0	1.0	0.91

Testfall CancelOrders

Messwert	S1	S2	S3
successfulPercentage	0.0	0.0	0.0
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	1.0	1.0	0.74
failedWithoutCompensation-Percentage	0.0	0.0	0.27
hasCorrectEndstatePercentage	1.0	1.0	0.74
containsAllExpectedLogs-Percentage	1.0	1.0	0.74
isSuccessfulTestInstance-Percentage	1.0	1.0	0.74

4.11.2 TransactionAnalysisResult

In Tabelle 4.24 sind die TransactionAnalysisResults für beide Testfälle dargestellt.

	S1	S2	S3
FinishOrders	1	1	0.67
CancelOrders	1	1	0.36

Hier zeigt sich, dass im Vergleich zum SmBasicSafeRetries die Kennzahl *consistentSagas-Percentage* deutlich kleiner wird. Konsistenz des Systems hat sich durch die Einführung der Änderungen verringert.

Aus Sicht des Koordinators ist der SmBasicNetworkFailureUnlimitedRetries erfolgreicher, der Vergleich von der Koordinator- und Teilnehmersicht zeigt jedoch, dass Transaktionen stattfinden, die der Koordinator nicht kennt.

Es zeigt sich außerdem, dass diese Fehler lediglich in Testszenario 3 auftreten. Die fehlerverursachenden Transaktionen sind genau die, bei denen die Response auf dem Rückweg verloren geht. Der Koordinator interpretiert dies im Kontext dieses Zustandsautomaten als wiederholbar und führt die Transaktion erneut aus. Dadurch wird im entsprechenden Teilnehmerservice die Transaktion mehr als einmal ausgeführt.

4.12 Das Problem der Wiederholbarkeit

In der Analyse des `SmBasicNetworkFailureUnlimitedRetries` hat sich gezeigt, dass die für die 4 Ts *BlockArticles*, *RemoveMoney*, *AddMoney* und *StartShipment* und ihre zugehörigen Cs eingeführten Retries zu inkonsistentem Verhalten in Testszenario 3 geführt haben. Das Problem besteht darin, dass lokale Transaktionen bei Wiederholung erneut ausgeführt werden. Dem Koordinator fehlt die Information, ob die lokale Transaktion im Fall eines Netzwerkfehlers bereits ausgeführt wurde oder nicht.

Implementierung von idempotentem Verhalten Es wird ein idempotentes Verhalten benötigt, bei dem der Koordinator gefahrlos Aufrufe an den Teilnehmerservice wiederholen kann. Dazu muss jeder Teilnehmerservice die ausgeführten Transaktionen mit einer zugehörigen `RequestId` speichern. Taucht ein Request mit einer bereits verwendeten `RequestId` auf, wird der Request nicht erneut bearbeitet, sondern eine Response mit dem Statuscode 208 zurückgegeben. Damit erhält der Aufrufer die Information, dass der Request bereits erfolgreich verarbeitet wurde.

Um idempotentes Verhalten zu implementieren, muss ein Service jeden erfolgreichen Request mit der zugehörigen `RequestId` abspeichern. Diese Information werden in einer Tabelle persistiert. Die Prüfung, ob ein Request prozessiert werden kann, ist eine Fallunterscheidung. Wenn ein Eintrag in der Idempotenztafel existiert, der in `RequestId` und Transaktion übereinstimmt, wird der Request mit 208 abgelehnt. Existiert kein solcher Datensatz, kann die Transaktion prozessiert werden.

Idempotente DEAs Die drei DEAs `SmBasic`, `SmBasicSafeRetries` und `SmBasicNetworkFailureUnlimitedRetries` verwenden die nicht-idempotenten Implementierungen der Teilnehmerservices. Damit nicht-idempotente und idempotente DEAs verglichen werden können, sind alle Teilnehmerservices hinsichtlich Idempotenz konfigurierbar. Die Fallunterscheidung, die bereits ausgeführte Transaktionen ablehnt, wird bei einer nicht-idempotenten Konfiguration des Services übersprungen. Die folgenden zwei DEAs verwenden eine idempotente Konfiguration.

4.13 Implementierung des `SmIdempotencyBackwardRecovery`

Der erste idempotente DEA wird als `SmIdempotencyBackwardRecovery` bezeichnet. Im Falle eines Netzwerkfehlers bei einem T wird ein Übergang zum entsprechenden C eingeführt; die Saga wird also versucht zurückzurollen, unabhängig ob das T ausgeführt wurde oder nicht. In Abbildung 4.12 ist der Fall abgebildet, dass ein T einen Netzwerkfehler verursacht ohne eine Zustandsänderung im Teilnehmerservice zu bewirken. Abbildung 4.13 zeigt den Ablauf im Fall eines Netzwerkfehlers mit Zustandsänderung.

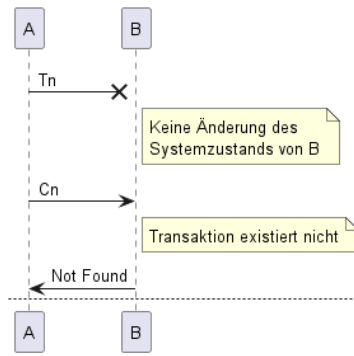


Abbildung 4.12: Sequenzdiagramm für Idempotentes Verhalten bei wiederholten Anfragen in Szenario 3

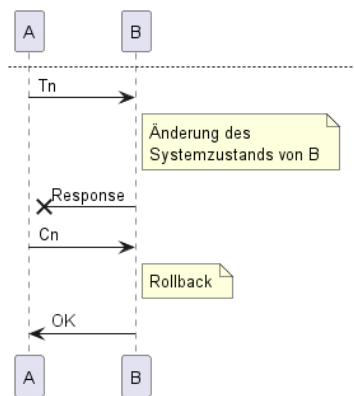


Abbildung 4.13: Sequenzdiagramm für Idempotentes Verhalten bei wiederholten Anfragen in Szenario 3

Solche Fehler treten jedoch auch bei den Cs auf. Deshalb müssen diese auch adressiert werden. Bei Fehlschlagen eines Cs könnte in den Zustand FailedWithoutCompensation gewechselt werden. Dies soll jedoch verhindert werden. Da die Teilnehmerservices idempotentes Verhalten unterstützen, können Cs wiederholt werden, bis ein eindeutiges Ergebnis vorliegt. In folgenden Fällen kann ein Übergang zum nächsten C eingeführt werden:

- 200: Die Transaktion wurde erfolgreich kompensiert
- 208: Die Transaktion wurde in einem vorherigen Schritt bereits erfolgreich kompensiert
- 404: Die Transaktion ist nicht bekannt und muss nicht kompensiert werden

Im Falle eines Konflikts (409) muss jedoch weiterhin auf den Zustand FailedWithoutCompensation gewechselt werden.

Der resultierende Zustandsautomat ist in Abbildung 4.14 abgebildet.

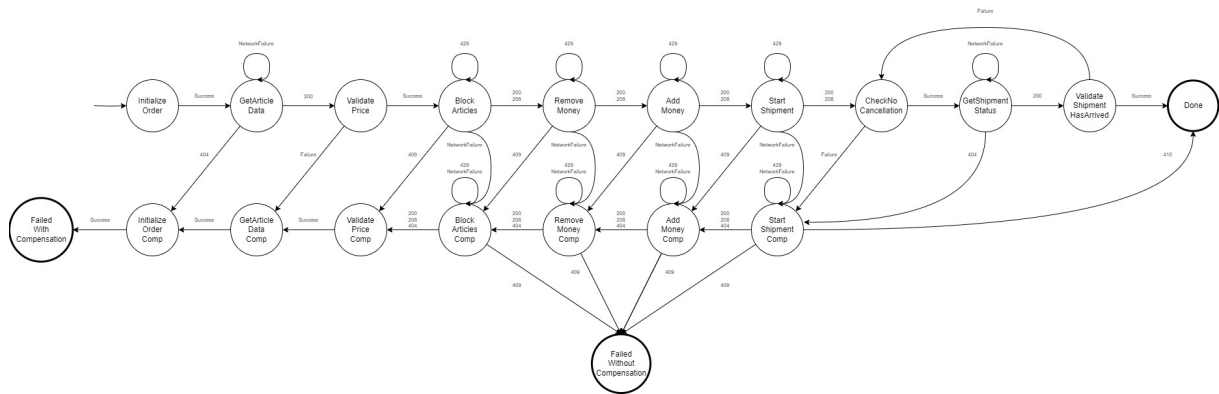


Abbildung 4.14: DEA für SmIdempotencyBackwardRecovery

4.13.1 StateAnalysisResult

Das StateAnalysisResult zeigt einen hohen Anteil an vorzeitig abgebrochenen Sagas. Das ist mit dem Konzept der Backwardrecovery begründet. Lediglich TestszENARIO 1 liefert in beiden Testfällen eine Erfolgsrate von 100%.

Testfall FinishOrders

Messwert	S1	S2	S3
successfullPercentage	1.0	0.63	0.44
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.0	0.38	0.57
failedWithoutCompensation-Percentage	0.0	0.0	0.0
hasCorrectEndstatePercentage	1.0	0.63	0.39
containsAllExpectedLogs-Percentage	1.0	0.63	0.44
isSuccessfulTestInstance-Percentage	1.0	0.63	0.44

Testfall CancelOrders

Messwert	S1	S2	S3
successfullPercentage	0.0	0.0	0.0
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	1.0	1.0	1.0
failedWithoutCompensation-Percentage	0.0	0.0	0.0
hasCorrectEndstatePercentage	1.0	1.0	1.0

Messwert	S1	S2	S3
containsAllExpectedLogs-Percentage	1.0	0.68	0.44
isSuccessfulTestInstance-Percentage	1.0	0.68	0.44

4.13.2 TransactionAnalysisResult

In Tabelle 4.24 sind die TransactionAnalysisResults für beide Testfälle dargestellt. Überraschend ist hier der niedrige Anteil an konsistenten Sagas in Testszenario 2 und 3.

	S1	S2	S3
FinishOrders	1	1	0.74
CancelOrders	1	1	0.74

Die Ursache dafür liegt in der Berechnung der Kennzahl sowie dem Aufbau des Zustandsautomaten. Für die Berechnung der Kennzahl werden die Differenzen der jeweiligen Transaktionen nach Koordinator- und Teilnehmersicht gebildet. Nur wenn diese für jedes T und jedes C übereinstimmen fließt das Ergebnis als erfolgreich in die Kennzahl ein.

Konkret soll nun diese Messungenauigkeit betrachtet werden. Wird die Anzahl einer Transaktion in Koordinatorsicht berechnet, wird das Transaktionslog verwendet. Dabei soll das in ?? dargestellte Transaktionslog verwendet werden.

Das Log zeigt eine Saga, die aufgrund eines Netzwerkfehlers im Zustand *StartShipment* zur Kompensierung wechselt. Zur Berechnung für die Kennzahl *consistentSagasPercentage* wird auch die Anzahl der Transaktionen mit dem Zustand *StartShipment* und dem Ergebnis *StartShipment200* oder *StartShipment208* berechnet. Für den *SmIdempotencyBackwardRecovery* bedeutet ein Netzwerkfehler in den kritischen Ts, dass das dazugehörige C die Änderungen kompensiert oder fortführt, falls der Netzwerkfehler keine Zustandsänderungen bewirkt hat. Das Zählen der Transaktionen mit dem Zustand *StartShipment* und dem Ergebnis *StartShipment200* oder *StartShipment208* ist für diesen DEA also keine korrekte Berechnung, um Konsistenz zu messen.

Zustand	Ergebnis
InitializeOrder	InitializeSagaSuccess
GetArticleData	GetProductData200
ValidatePrice	ValidatePriceSuccess
BlockArticles	BlockArticles200
RemoveMoney	RemoveMoney200
AddMoney	AddMoney200
StartShipment	StartShipmentNetworkFailure
StartShipmentCompensation	StartShipmentCompensationNetworkFailure

Tabelle 4.23: Transaktionslog für Saga im Testfall CancelOrders und Testszenario 2

Zustand	Ergebnis
StartShipmentCompensation	StartShipmentCompensation208
AddMoneyCompensation	AddMoneyCompensation200
RemoveMoneyCompensation	RemoveMoneyCompensation200
BlockArticlesCompensation	BlockArticlesCompensation200
ValidatePriceCompensation	ValidatePriceCompensationSuccess
GetArticleDataCompensation	GetProductDataCompensationSuccess
InitializeOrderCompensation	InitializeSagaCompensationSuccess

Tabelle 4.23: Transaktionslog für Saga im Testfall CancelOrders und Testszenario 2

4.13.3 Alternative Sicherstellung der Konsistenz

Damit der Zustandsautomat trotz dieser verfälschten Messung bewertet werden kann, wird eine Alternative benötigt. Um eine Aussage über die Konsistenz zu treffen, kann der Inhalt der eigentlichen Tabellen der Services verwendet werden.

Alternative Konsistenzdefinition Als Konsistenzkriterien dienen folgende Annahmen:

- Die Summe des Geldes im System bleibt gleich.
- Die Summer aller Artikel im System bleibt gleich.

Einordnung dieser Definition Diese Vorgehensweise kann entscheiden, ob das System nach den definierten Regeln im konsistenten Zustand bleibt oder ob eine Transaktion das System in einen inkonsistenten Zustand überführt hat. Dies ist eine binäre Messung, über die Qualität der Konsistenz kann im vorliegenden System, unter Verwendung dieses Zustandsautomaten und unter Verwendung des aktuellen Versuchsaufbaus keine Aussage getroffen werden.

Nach den genannten Annahmen ist das System auch konsistent, wenn zwei parallele Sagas fehlschlagen und eine Saga *AddMoney* und die andere Saga *RemoveMoney* jeweils doppelt mit dem (zufällig) identischen Betrag ausführen. Die Menge des Geldes im System bleibt trotz Auftreten eines solchen hypothetischen Bugs konsistent.

Diese Erläuterung soll verdeutlichen, dass die sehr vage Definition von Konsistenz mit Vorsicht verwendet werden sollte. Für diesen Automaten soll dies jedoch ausreichen.

4.13.3.0.1 Messung Die Messung erfolgt manuell. Die Summe des im System befindlichen Geldes wird vor Ausführung der Tests gemessen. Dabei ist jedes Konto mit einem Startcredit von 15000.00 initialisiert. Tritt ein Konsistenzfehler bei Verwendung der BankServices auf, so wird dies in diesem Statement deutlich, wenn sich die zwei Werte *expectedCreditSum* und *actualCreditSum* unterscheiden.

```

1 select case when
2   15000.00 * cast(
3     (select count(*) from bank1user) +
4     (select count(*) from bank2user) as float)

```

```

5  = cast(
6    (select sum(credit) from bank1credit) +
7    (select sum(credit) from bank2credit) as float)
8  then 1 else 0 end as mightBeConsistent;

```

Die Anzahl der Artikel wird mit einem vergleichbaren Statement auf Konsistenz überprüft. Die Summe der Artikel wird über die drei Tabellen des StockServices gezählt. Ändert sich diese Zahl nach Ausführung der Tests, ist ein Konsistenzfehler aufgetreten.

```

1  select case when
2    (select 15000 * count(*) from articlestock as expectedarticlesum)
3    =
4    (select sum(amount) as amount from (
5      select articleid as articleid , amount as amount from articlestock
6      union
7      select articleid , sum(amount) as amount from blockedarticles
8        group by articleid
9      union
10     select articleidfk as articleid , sum(amount) as amount from
11       shippedarticles group by articleidfk) as actualarticlesum
12  )
13  then 1 else 0 end as mightBeConsistent;

```

Ändert sich in beiden Tests die Summe nicht, ist laut Section 4.13.3 die notwendige Bedingung für Konsistenz erreicht. Das Gesamtergebnis berechnet sich durch folgendes Statement:

```

1  with moneyMightBeConsistent as (
2    select case when
3      (select 15000 * count(*) from articlestock as expectedarticlesum)
4      =
5      (select sum(amount) as amount from (
6        select articleid as articleid , amount as amount from articlestock
7        union
8        select articleid , sum(amount) as amount from blockedarticles
9          group by articleid
10       union
11       select articleidfk as articleid , sum(amount) as amount from
12         shippedarticles group by articleidfk) as actualarticlesum
13     )
14     then 1 else 0 end as mightBeConsistent),
15  articleMightBeConsistent as (
16    select case when
17      15000.00 * cast(
18        (select count(*) from bank1user) +
19        (select count(*) from bank2user) as float)
20      = cast(
21        (select sum(credit) from bank1credit) +
22        (select sum(credit) from bank2credit) as float)
23      then 1 else 0 end as mightBeConsistent)

```

```

22 select moneyMightBeConsistent.mightBeConsistent as
    moneyMightBeConsistent ,
23 articleMightBeConsistent.mightBeConsistent as
    articleMightBeConsistent ,
24 case when
25     moneyMightBeConsistent.mightBeConsistent
26     =
27     articleMightBeConsistent.mightBeConsistent
28 then 1 else 0 end as mightBeConsistent
29 from moneyMightBeConsistent , articleMightBeConsistent ;

```

Ergebnis Die Messung ist für beide

	S1	S2	S3
moneyMightBeConsistent	1	1	1
articleMightBeConsistent	1	1	1
mightBeConsistent	1	1	1

Tabelle 4.24: Messwert *altConsistentSagasPercentage* für
SmIdempotencyBackwardRecovery

4.14 Implementierung SmIdempotencyForwardRecovery

Die Auswertung der Ergebnisse des SmIdempotencyBackwardRecovery hat gezeigt, dass die Strategie der BackwardRecovery Konsistenz gewährleisten kann. Dabei trat jedoch erneut das Problem des vorzeitigen Abbruchs auf. Das erste Vorkommen eines Netzwerkfehlers innerhalb eines Ts führte zur Kompensierung. Der nächste zu implementierende Zustandsautomat verfolgt zwei Ziele: eine möglichst hohe Erfolgsrate sowie Konsistenz. Mittels ForwardRecovery kann eine Weiterführung der Saga erzwungen werden. Abgebrochen wird lediglich in Zuständen, bei denen ein Ergebnis auftritt, das nicht behebbar ist.

Für Ts ist lediglich ein Ergebnis wie 409 unbehebbar und es wird zum vorherigen C gewechselt. Für Netzwerkfehler werden Retries eingeführt. Aufgrund der Idempotenz der Teilnehmerservices ist dies problemlos möglich. Nur bei einem eindeutigen Ergebnis wird fortgefahren (200, 208) oder abgebrochen (409).

Der resultierende Zustandsautomat SmIdempotencyForwardRecovery ist in Abbildung 4.15 abgebildet.

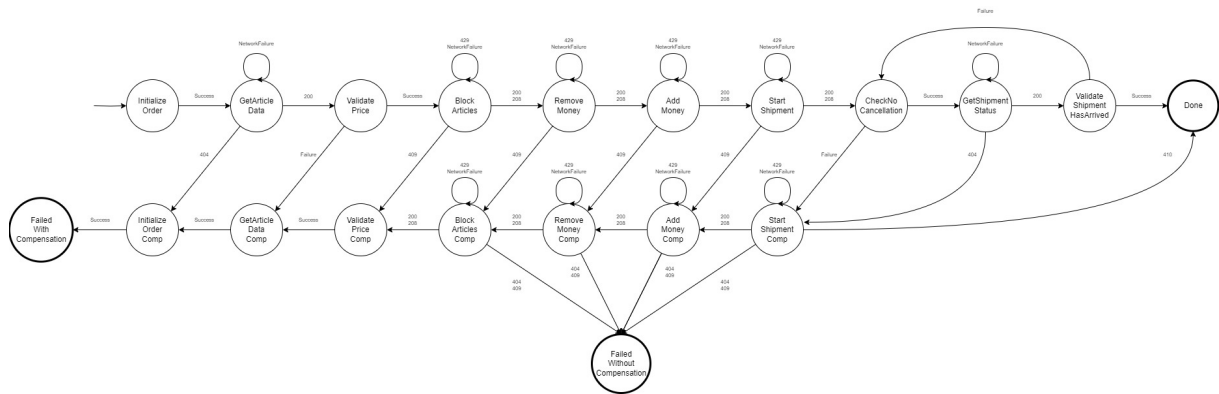


Abbildung 4.15: DEA für SmIdempotencyForwardRecovery

4.14.1 StateAnalysisResult

Das StateAnalysisResult zeigt, dass unabhängig vom Testfall und Testszenario alle Sagas im erwarteten Endzustand münden.

Testfall FinishOrders

Messwert	S1	S2	S3
successfullPercentage	1.0	1.0	0.91
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	0.0	0.0	0.0
failedWithoutCompensation-Percentage	0.0	0.0	0.1
hasCorrectEndstatePercentage	1.0	1.0	1.0
containsAllExpectedLogs-Percentage	1.0	1.0	1.0
isSuccessfullTestInstance-Percentage	1.0	1.0	1.0

Testfall CancelOrders

Messwert	S1	S2	S3
successfullPercentage	0.0	0.0	0.0
finishedPercentage	1.0	1.0	1.0
pendingPercentage	0.0	0.0	0.0
failedWithCompensation-Percentage	1.0	1.0	1.0
failedWithoutCompensation-Percentage	0.0	0.0	0.0
hasCorrectEndstatePercentage	1.0	1.0	1.0
containsAllExpectedLogs-Percentage	1.0	1.0	1.0

Messwert	S1	S2	S3
isSuccessfulTestInstance-Percentage	1.0	1.0	1.0

4.14.2 TransactionAnalysisResult

In Tabelle 4.24 sind die TransactionAnalysisResults für beide Testfälle dargestellt. Es ist erkennbar, dass die Konsistenz in beiden Testfällen für alle Testszenarios eingehalten wird.

	S1	S2	S3
FinishOrders	1	1	1
CancelOrders	1	1	1

4.15 Laufzeitanalyse

Das primäre Werkzeug der Optimierung der Zustandsautomaten war die Einführung von Retries. Es ist zu erwarten, dass die Einführung von Retries die Laufzeit verlängert. Im Folgenden sind die Ergebnisse der Laufzeitanalyse per Boxplot dargestellt. Als Visualisierung wird ein modifizierter Boxplot verwendet. In jedem Diagramm sind das obere und untere Quartil, der Median, das Maximum und Minimum sowie Ausreißer ablesbar. Jeder Boxplot stellt die Werte eines DEAs dar. Aus Gründen der Übersicht wurden die langen Bezeichnungen der Zustandsautomaten durch folgende Nummerierung ersetzt:

Zustandsautomat	Nummerierung
SmBasic	1
SmBasicSafeRetries	2
SmBasicNetworkFailureUnlimitedRetries	3
SmIdempotencyBackwardRecovery	4
SmIdempotencyForwardRecovers	5

Es ist erkennbar, dass die Laufzeit für alle Automaten sehr nah beieinander liegt. Da im ersten Szenario keine Netzwerkfehler auftauchen, sind die Werte sehr wenig gestreut. Die Ausreißer sind ebenfalls erkennbar.

4.15.1 Testszenario1

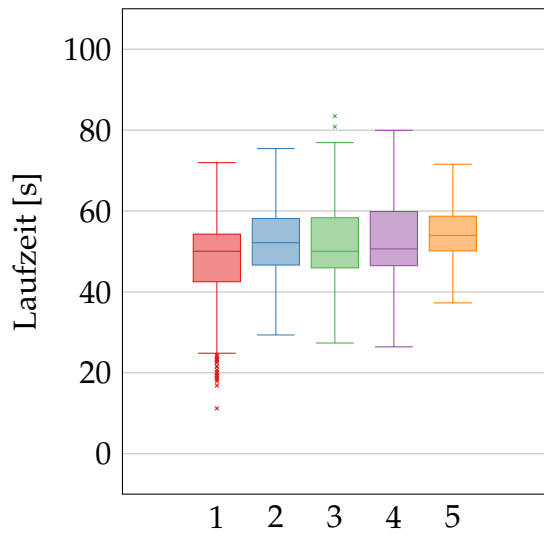


Abbildung 4.16: Boxplot FinishOrders in Szenario 1

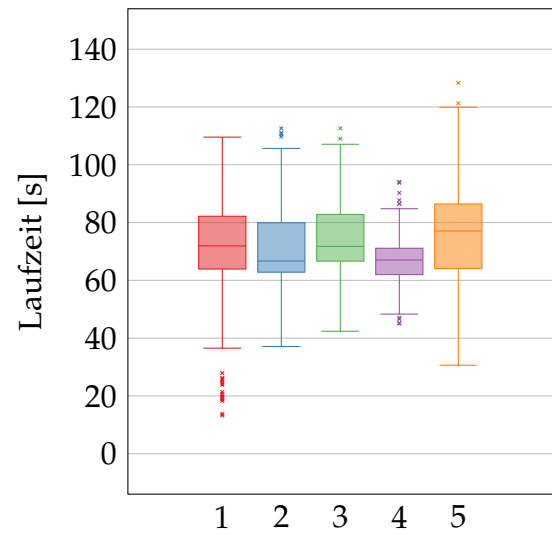


Abbildung 4.17: Boxplot CancelOrders in Szenario 1

4.15.2 TestszENARIO2

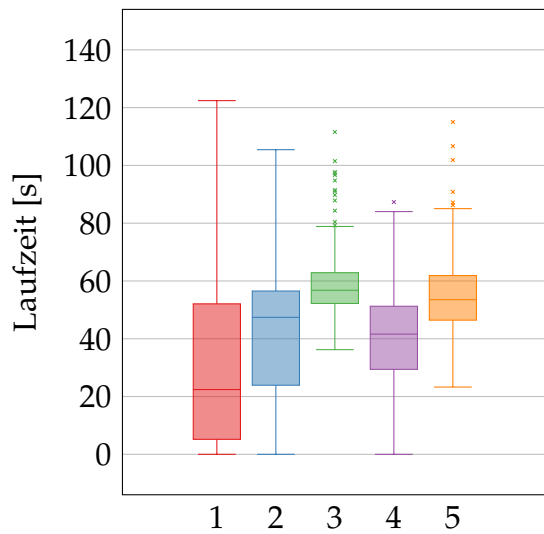


Abbildung 4.18: Boxplot FinishOrders in Szenario 2

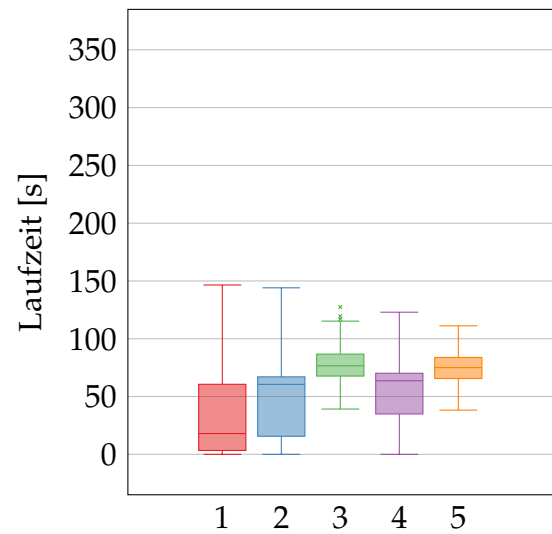


Abbildung 4.19: Boxplot CancelOrders in Szenario 2

4.15.3 TestszENARIO3

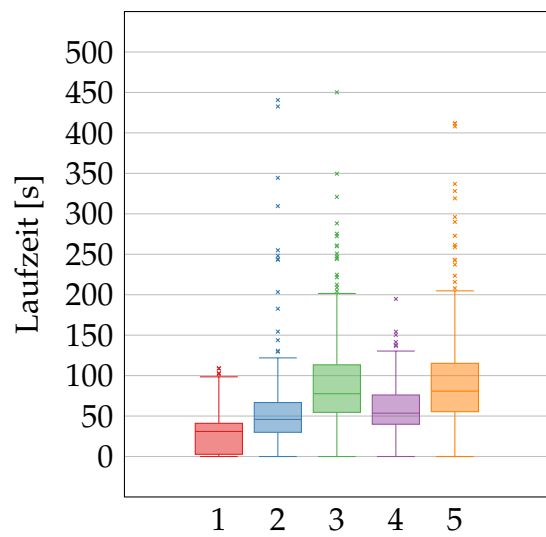


Abbildung 4.20: Boxplot FinishOrders in Szenario 3

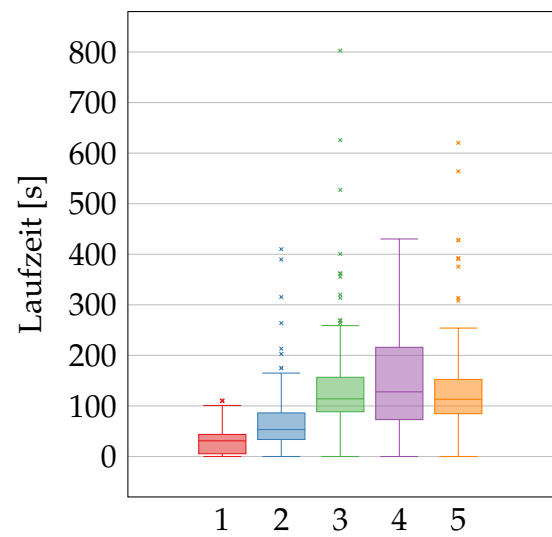


Abbildung 4.21: Boxplot CancelOrders in Szenario 3

5 Ergebnisse der Versuchsdurchführung

5.1 Versuchsergebnisse

5.2 title

Was konnte gezeigt werden

Welche Schlüsse konnten gezogen werden

Was konnte nicht gezeigt werden

5.3 Technische Voraussetzungen

Welche Voraussetzung müssen bestehen, damit ausfallsichere Konsistenz gewährleistet werden kann

5.4 Technische Grenzen

Welche technischen Grenzen wurden erreicht

5.5 Wissenschaftliche Berührungspunkte

5.5.1 CAP-Theorem

Zusammenhang CAP-Theorem (Wenn Partitionstoleranz, dann entweder Konsistenz oder Verfügbarkeit) Tradeoff zwischen Erfolgswahrscheinlichkeit und Konsistenz: Begriff LLT enthält langlebig-> Warten im Fall eines Netzwerkausfalls ist ok. Konsistenz wird weiter gewahrt

6 Ausblick, Ansatz für weitere Untersuchungen

Abbildungsverzeichnis

2.1	Darstellung einer Saga als Deterministischen endlichen Automaten . . .	10
2.2	Forwardrecovery in einem DEA	12
2.3	Backwardrecovery in einem DEA	13
2.4	Erzwungene Forwardrecovery in einem DEA	14
3.1	Vereinfachte Darstellung eines Bestell- und Lieferprozesses	19
4.1	ER-Diagramm ArticleService	27
4.2	ER-Diagramm StockService	28
4.3	ER-Diagramm BankingService	30
4.4	Zu konstruierender DEA	34
4.5	Kontrollfluss der SEC	39
4.6	Sequenzdiagramm für Szenario 1	40
4.7	Sequenzdiagramm für Szenario 2	40
4.8	Sequenzdiagramm für Szenario 3	41
4.9	DEA für SmBasic	45
4.10	DEA für SmBasicSafeRetries	49
4.11	DEA für SmBasicNetworkfailureUnlimitedRetries	51
4.12	Sequenzdiagramm für Idempotentes Verhalten bei wiederholten Anfra- gen in Szenario 3	54
4.13	Sequenzdiagramm für Idempotentes Verhalten bei wiederholten Anfra- gen in Szenario 3	54
4.14	DEA für SmIdempotencyBackwardRecovery	55
4.15	DEA für SmIdempotencyForwardRecovery	60
4.16	Boxplot FinishOrders in Szenario 1	62
4.17	Boxplot CancelOrders in Szenario 1	62
4.18	Boxplot FinishOrders in Szenario 2	62
4.19	Boxplot CancelOrders in Szenario 2	62
4.20	Boxplot FinishOrders in Szenario 3	63
4.21	Boxplot CancelOrders in Szenario 3	63

Literatur

- [1] H. Garcia-Molina und K. Salem, "Sagas," *ACM SIGMOD Record*, Jg. 16, Nr. 3, S. 249–259, 1987, ISSN: 0163-5808. DOI: 10.1145/38714.38742.