Verifying Compliance in Process Choreographies:
Foundations, Algorithms, and Implementation

Walid Fdhila\textsuperscript{a,}, David Knuplesch\textsuperscript{b}, Stefanie Rinderle-Ma\textsuperscript{c} and Manfred Reichert\textsuperscript{d}

\textsuperscript{a}Security Business Austria (SBA-research), Vienna, Austria, wfdhila@sba-research.org
\textsuperscript{b}alphaQuest GmbH, Ulm, Germany, d.knuplesch@alphaquest.de
\textsuperscript{c}Technical University of Munich, Department of Informatics, Boltzmannstrasse 3, Garching, Germany, stefanie.rinderle-ma@tum.de
\textsuperscript{d}Institute of Databases and Information Systems, Ulm University, Ulm, Germany, manfred.reichert@uni-ulm.de

ARTICLE INFO

Keywords:
- Distributed business processes
- Business rules
- Compliance management
- Process choreography
- Business process compliance
- Global compliance rules
- Rule decomposition

ABSTRACT

The current push towards interoperability drives companies to collaborate through process choreographies. At the same time, they face a jungle of continuously changing regulations, e.g., due to the pandemic and developments such as the BREXIT, which strongly affect cross-organizational collaborations. Think of, for example, supply chains spanning several countries with different and maybe even conflicting COVID19 travelling restrictions. Hence, providing automatic compliance verification in process choreographies is crucial for any cross-organizational business process. A particular challenge concerns the restricted visibility of the partner processes at the presence of global compliance rules (GCR), i.e., rules that span across the process of several partners. This work deals with the question how to verify global compliance if affected tasks are not fully visible. Our idea is to decompose GCRs into so called assertions that can be checked by each affected partner whereby the decomposition is both correct and lossless. The algorithm exploits transitivity properties of the underlying rule specification, and its correctness and complexity are proven, considering advanced aspects such as loops. The algorithm is implemented in a proof-of-concept prototype, including a model checker for verifying compliance. The applicability of the approach is further demonstrated on a real-world manufacturing use case.

1. Introduction

Gartner regards interoperability as “strategic imperative”\textsuperscript{1} for healthcare. Especially the global push by digitalization and the current pandemic require the collaboration and integration of (business) partners and organizations. Process technology serves as enabler for process-oriented collaborations between distributed business partners, realized and implemented through so-called process choreographies. Applications include healthcare (34), blockchain-based processes (47; 46), multi-modal logistics scenarios (7; 10), and supply chains (22). Digitalization and ongoing changes due to, for example, the pandemic situation or the BREXIT flood enterprises and organizations with updated or even new regulations at a fast pace. For example, “bank regulations change every 12 minutes”\textsuperscript{2}. Regulatory frameworks comprise application-independent frameworks such as the GDPR on “data processing boundaries of the personal data of European Unionâ€™s citizens” (65) and the ISO 27001 security standard\textsuperscript{3} as well as application-specific ones, e.g., the WHO regulations defined in the context of COVID19\textsuperscript{4}. As a consequence, in our globalized world, regulations and their changes affect process collaborations (54) and lead to an increased need for compliance verification in process choreographies.

1.1. Problem Statement

What are the particular challenges with respect to compliance verification in process choreographies? Let us illustrate them by an example. Figure 1 depicts the choreography model of a supply chain scenario adapted from (22). It involves five process partners, i.e., Bulk Buyer, Manufacturer, Middleman, Supplier, and Special Carrier that interact through

\textsuperscript{1}https://gtnr.it/3vGFB7f
\textsuperscript{2}https://thefinanser.com/2017/01/bank-regulations-change-every-12-minutes.html/
\textsuperscript{3}https://www.iso.org/isoiec-27001-information-security.html
\textsuperscript{4}https://www.who.int/teams/regulation-prequalification/covid-19
Verifying Compliance in Process Choreographies

message exchanges. First, the Bulk Buyer orders a set of products from the Manufacturer (e.g., an aircraft). The manufacturing of the product requires several sub-products (intermediates) to be provided by different suppliers. In this scenario, we assume that only one intermediate is required and provided by the Supplier. After processing the order, hence, the Manufacturer sends an order for the intermediate (e.g., the fuselage or engines) to the Middleman. The Middleman forwards the order of the intermediate to the Supplier and sends an order for a special transport to the Special Carrier. The Special Carrier requests the details on the transport from the Supplier and the Supplier provides them to the Special Carrier, followed by sending the waybill for the intermediate. The Special Carrier sends a notice on the arrival of the intermediate to the Manufacturer, which then delivers the product to the Bulk Buyer.

Figure 1: Choreography model for a supply chain – running example with five process partners

Imagine now that the partners and the choreography are subject to the Global Compliance Rules (GCR) depicted in Fig. 2, which stem from legal regulations and standards such as GDPR or ISO 27001:

C1 After Production a Final test must be performed.
C2 Pack Intermediate is required before Transport Intermediate.
C3 Each Transport intermediate requires Permission of authority. Further on, the transporter must pass a Safety Check.

Obviously, none of the GCR can be directly verified on basis of the choreography model in Fig. 1 as none of the public and message exchanging tasks corresponds to any of the tasks referred to in the GCR.

<table>
<thead>
<tr>
<th>Global Compliance Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1: After production a final test is required.</td>
</tr>
<tr>
<td>C2: The intermediate has to be packed before it is transported.</td>
</tr>
<tr>
<td>C3: Each transport of the intermediate requires permission of authority. Further, the transporter must pass a safety check before.</td>
</tr>
</tbody>
</table>

Let us have a look at the public processes of the partners involved in the choreography as shown in Fig. 3. These public process models contain all public tasks that are visible to the other partners, including the tasks that exchange messages, but also other visible tasks such as Production at the Manufacturer. Based on the public process models, C1 and C2,
Verifying Compliance in Process Choreographies as depicted in Fig. 2, can be verified: C1 refers to public tasks of the Manufacturer process, which obviously complies with C1, i.e., public task Production is followed by public task Final Test. C2 can be verified over the Supplier and Special Carrier processes. The order between tasks Pack Intermediate and Transport Intermediate is determined by the message exchange between sending and receiving Waybill Intermediate. As opposed to C1 and C2, C3 cannot be verified based on the public processes of the partners as there are no public tasks for Safety check and Get permission of authority.

Figure 3: Public processes (collaboration model) – running example with five process partners cooperating in a supply chain (adapted from (22))

The presumption is that C3 also refers to private tasks of the partners, i.e., tasks that are only present in the private process models of the partners. In general, private process models of the partners implement and possibly extend the behavior of the corresponding public models. As opposed to public tasks, private tasks are not visible to the partners. Figure 4 shows the private process models of partners Special Carrier and Middleman where private tasks are highlighted in gray color. Although private tasks are usually hidden to other partners, restrictions over them might exist. In the supply chain, for example, C3 refers to private tasks Safety Check for partner Special Carrier and Get permission of authority for partner Middleman. If private tasks are affected by a GCR, no information about how and when these tasks are executed, or how they are connected to other nodes of the corresponding private process model, becomes visible to the other partners. Usually, this happens when a collaborating partner p1 imposes the execution of a specific task that must exist in its private process and comply with a given rule involving another partner p2. Partner p1 should then ensure the existence of such task and that it follows the imposed rule.

As can be seen from the example depicted in Figs. 1–4, GCRs constrain actions of multiple partners and/or the interactions between them. Ensuring the compliance of process choreographies with a GCR is crucial and challenging (32) as a partner “only has the visibility of the portion of the process under its direct control” (48). Reconsider GCR C3 as an example. It asks for a safety check accomplished by a private task of the Special Carrier. To cope with this issue, assertions can be used. An assertion (A) corresponds to a commitment of a partner guaranteeing that its private/public process complies with the imposed rule (22). Figure 5 depicts the two assertions A1 and A2: the Middleman agrees to get the permission of the authority before ordering the special transport (A1). Moreover, the Special Carrier commits
Verifying Compliance in Process Choreographies

Figure 4: Private processes of partners Special Carrier and Middleman, omitting message exchanges (adapted from (22))

to perform a safety check before transporting the intermediate (A2). In combination, assertions A1 and A2 enable checking GCR C3.

Figure 5: Assertions by partners Middleman and Special Carrier

1.2. Contribution

Overall, this leads to the overarching research question \( RQ \) tackled in this work:

\( RQ: \) How to verify GCRs in a decentralized setting of a process choreography where no central coordinator with complete knowledge on the private and public tasks of all partners exists?

In literature, there is a “knowledge gap” when it comes to compliance verification in process choreographies (32). (48) tackles the problem of checking a GCR on private tasks based on IoT-enabled artifacts. However, not all process choreography settings with compliance requirements feature IoT-enabled artifacts. Hence, this work aims at providing a formal approach that is independent of any technology or application. The central idea is to decompose the GCR into assertions in a lossless way, i.e., the verification of all assertions guarantees the one of the GCR. Note that this solves the problem as assertions may be checked separately by each of the partners. Hence, infringing the privacy of any partner is avoided.

The decomposition algorithm presented in this article exploits transitivity properties of the underlying GCR specification and was originally presented in (23). The decomposition relies on transitivity properties of the underlying GCR specification. The transitivity properties are shown by the example of a translation to first order predicate logic. Similarly, for example, (57) presents declarative patterns based on Linear Temporal Logic (LTL).

In our approach, GCRs are specified in a pattern-based and visual way using the eCRG formalism (40). This means that a GCR may be composed of so called antecedence patterns and consequence patterns. The patterns can be
connected reflecting pre-/post-conditions of the respective GCR. C1 in Fig. 2, for example, connects antecedence pattern Production with consequence pattern Final test, demanding that after the production a final test is required. Note that antecedence and consequence patterns may require occurrence (i.e., something must happen) and absence (i.e., something must not happen). In (23), we relied on simple rules that consist of single antecedent and multiple occurrence patterns. Aside the decomposition algorithm itself, (23) provides basic proofs, simple GCR decomposition scenarios, and the embedding of the approach in the overall digitalized change and compliance management framework C³Pro. This article extends and elaborates the results presented in (23) in several directions:

- We allow for additional and more complex compliance rules with multiple antecedence patterns. This significantly increases the complexity of the theoretical considerations as well as the one of the provided GCR decomposition scenarios. As a result, we obtain new theorems and algorithms.
- The decomposition proofs are extended to cover the additional complexity of the GCR; in particular they now consider loops as well.
- The decomposition algorithm with extensions is prototypically implemented and integrated with the C³Pro framework, which deals with both change and compliance in process choreographies.
- A model checker for verifying decomposition correctness is provided.
- A manufacturing use case illustrates the applicability of the approach. Specifically, the use case demonstrates the applicability of the approach beyond regulatory compliance, i.e., it shows how decomposition can be used to lift implicit connections to explicit assertions.
- The related work section is significantly extended.

The remainder of the paper is structured as follows: Section 2 provides fundamentals required for understanding this work, and Section 3 introduces the foundations for GCR decomposition (including transitivity theorems). Section 4 then presents the decomposition algorithm for global compliance rules, whereas Section 5 deals with the automated verification of the resulting decompositions based on model checking. Sections 6 and 7 cover the evaluation of the approach, i.e., the implementation and application of the algorithms. Section 8 discusses related work. Section 9 concludes the paper with a summary and an outlook.

2. Fundamentals

This section presents definitions and formal backgrounds for global compliance rules (GCRs) to be obeyed by a process choreography $y$. A choreography includes three types of overlapping models: (i) a private model representing the executable process and including both private and public activities (see Fig. 4 for examples of private process models), (ii) a public model (also called the interface of the process) that solely includes the public activities and the interactions of a given partner (see Fig. 3 for the public process models of our running example), and (iii) a choreography model providing a global view on the interactions between all partners (see Fig. 1 for the choreography model of our running example) (21). Compared to (21; 2), this paper assumes that public activities are not necessarily interactions with other partners, but may additionally represent tasks made visible by the corresponding partners. Therefore, both interactions and non-interaction public activities of a single partner are described in a public model. The latter serves as public (restricted) view on the private model of the partner, which “describes the internal logic of a partner including its private and public activities” (6). For a formal definition of process choreography, we refer to Definition 1.

Definition 1 (Choreography (21)). We define a choreography $y$ as a tuple $(P, \mathcal{G}, \Pi, \mathcal{L}, \psi, \Gamma, \xi)$ where

- $P$ is the set of all participating partners,
- $\mathcal{G}$ is the choreography model representing the interactions $I$ between partners in $P$ (cf. Fig. 1),
- $\Pi = \{\pi_p\}_{p \in P}$ is the set of all private models (cf. Fig. 4),
- $\mathcal{L} = \{l_p\}_{p \in P}$ is the set of all public models (cf. Fig. 3),
- $\psi = \{\psi_p : l_p \leftrightarrow \pi_p\}_{p \in P}$ is a partial mapping function between nodes of the public and private models.

http://www.wst.univie.ac.at/communities/c3pro
Verifying Compliance in Process Choreographies

- $\Gamma: I \leftrightarrow I'$ is a partial mapping function between nodes of different public models.
- $\xi: G \leftrightarrow 1 \times 1$ is a partial mapping function between nodes of the choreography model and the public models.

As depicted in Figures 1, 3 and 4, choreography, public and private models are defined as graphs, where nodes are either activities (i.e., interaction, public or private activities) or gateways (e.g., sequence, exclusive or parallel), and arrows are the dependencies between them. As described above, each of these three models use specific type of activity nodes (e.g., interaction activities for choreography models). Because the focus of this paper is mainly on GCR decomposition, we abstract their respective formal definitions, but the reader may refer to (21) for more details.

While function $\psi$ maps the activities of the public models to those of the private models, function $\Gamma$ determines the dependencies between the interactions of different public models (e.g., $\Gamma(\text{Request details (Special carrier)}) = \text{Request details (Supplier)}$). Finally, function $\xi$ represents the dependencies between the activities in the choreography model and those of the public models (e.g., $\xi(\text{order}) = \{\text{order (Bulk buyer)}, \text{order (Manufacturer)}\}$). Note that in the examples above, connected interaction activities (i.e., the send and the corresponding receive) of different public models have the same labels, while in practice, it is possible to have them different.

Based on functions $\psi$ and $\Gamma$, certain soundness properties of choreography $y$ can be checked, including structural and behavioral compatibility between public models, and consistency between public and private models (15). Structural consistency requires that for each public activity of the public model of a partner $p$, there should be a matching element in the corresponding private model of $p$, but not vice versa (21). Structural compatibility states that for each interaction activity of the public model of a partner $p$, there should be a matching interaction activity in the public model of another partner. Note that this is a necessary, but not yet sufficient condition for ensuring compatibility and consistency—the models’ behaviors (control flow dependencies) should also be compatible and consistent. In this paper, we assume that the choreography $y$ is sound.

In previous work (20), multiple formal languages employed for business process compliance modelling and checking (e.g., linear temporal logic LTL, event calculus EC, extended compliance rule graph eCRG) were compared. It was shown that most of these languages can deal with most qualitative time patterns, and can therefore be used to model the compliance constructs addressed in this paper. Similar results were proven in (30). In order to specify these constructs as well as transitivity properties required for the GCR decomposition, this work utilizes the visual eCRG (extended Compliance Rule Graph) language (42; 38; 36). The eCRG language offers a visual rule notation for expressing compliance rules over process choreographies and is based on first order predicate logic (cf. Fig. 6). To distinguish between a precondition (i.e., antecedence) and corresponding postconditions (i.e., consequences), an eCRG can be partitioned into an antecedence pattern and a consequence pattern. The antecedence pattern specifies when the compliance rule is triggered (i.e., activated), whereas the consequence pattern specifies what the rule demands. As compliance rules may require the occurrence or absence of certain activities or interactions (i.e., message exchanges), the antecedence and consequence patterns are further sub-divided into occurrence and absence nodes. Sequence conditions between these events can be expressed using directed connectors between the respective nodes. We use the following notation: $\text{[A]}$: Antecedence occurrence; $\text{[X]}$: Antecedence absence; $\text{[A]}$: Consequence occurrence; $\text{[X]}$: Consequence absence. Fig. 6 introduces the elements of the eCRG language. For a formal definition of eCRG, we refer to Def. 2.

**Definition 2 (Global Compliance Rule (GCR) structure).** Given a process choreography $y = (P, G, \Pi, L, \psi, \Gamma, \xi)$ (cf. Def. 1), let $A$ be the set of private and public non-interaction activities and $I$ be the set of interaction activities. Then: A GCR $r$ is defined as tuple $r = (N, \rho, \varphi, \text{type}, \text{pattern})$ with

- $N$ being the set of nodes,
- $\rho: N \rightarrow P$ returning the partner responsible for a node.
- $\varphi: N \times N \rightarrow \{\rightarrow, \rightarrow, \emptyset\}$ returning the sequence flow connector between two nodes, i.e., consequence sequence and antecedence sequence connectors respectively.
- $\text{type}: N \rightarrow A \cup I$ mapping each node to an activity or an interaction (i.e., message exchange).
- $\text{pattern}: N \rightarrow \{\text{[A]}, \text{[X]}, \text{[C]}, \text{[X]}\}$
Verifying Compliance in Process Choreographies

Extended Compliance Rule Graph Language (eCRG)

<table>
<thead>
<tr>
<th>Process Perspective</th>
<th>Interaction Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Antecedence</strong></td>
<td><strong>Consequence</strong></td>
</tr>
<tr>
<td><strong>Occurrence</strong></td>
<td><strong>Sequence</strong></td>
</tr>
<tr>
<td>Task</td>
<td>Task</td>
</tr>
<tr>
<td>Antecedence Connectors</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Task</td>
</tr>
<tr>
<td>Consequence Sequence</td>
<td></td>
</tr>
<tr>
<td>Absence</td>
<td>Absence</td>
</tr>
<tr>
<td>Task</td>
<td>Task</td>
</tr>
<tr>
<td>Consequence Sequence</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>Receiver</td>
</tr>
<tr>
<td>_sender</td>
<td>Message</td>
</tr>
<tr>
<td>Message</td>
<td>Receiver</td>
</tr>
<tr>
<td>_sender</td>
<td>Message</td>
</tr>
<tr>
<td>_sender</td>
<td>Message</td>
</tr>
</tbody>
</table>

Figure 6: Elements of the eCRG language

Think of an eCRG as a graph of connected nodes, where each node is assigned to a particular partner (e.g., in C1, \(\rho(\text{production}) = \text{manufacturer}\)). A node may either be a private, non-interaction public activity, or an interaction (see Figure 6). Given two nodes of an eCRG, function \(\varphi\) returns the sequence flow connector as depicted in Figure 6, where a dashed arrow (i.e., consequence connector) connects an antecedence pattern to a set of consequence patterns (e.g., C1: After production a final test is required), and an antecedence connector expresses a relation between antecedence patterns solely (i.e., the pre-condition). For example, assume that we change C3 as follows: \(\text{Get\_permission\_of\_authority} \rightarrow \text{safety\_check} \rightarrow \text{transport\_intermediate}\). Then: if the pre-condition (i.e., execution of activity \(\text{Get\_permission\_of\_authority}\) followed by the one of activity \(\text{safety\_check}\)) is met, the post condition (i.e., activity \(\text{transport\_intermediate}\)) will be triggered. Finally, function pattern evaluates whether a node is an antecedence or consequence, and whether or not it should occur.

3. Global Compliance Rule Decomposition Theorems

This section introduces the theoretical foundations for the decomposition of global compliance rules (including theorems and proofs) illustrated by a number of examples, which we have extracted from the application scenario introduced in Section 1. Section 3.1 first describes the basic idea of our approach (i.e., why do we need to decompose a GCR), followed by the presentation, proofs and illustrations of the theorems in Section 3.2.

3.1. Basic Idea

Our method for the decentralized checking of global compliance rules relies on the decomposition of the original GCR into a set of assertions that can be checked locally by each partner and collectively reproduce the behavior of the GCR (cf. Fig. 7). A communication between partners is only required in the setup phase to deduct the assertions. During runtime, however, no further compliance-related communication becomes necessary for checking the GCR unless a local assertion becomes violated. The decomposition of a GCR into a set of assertions is based on well-grounded theorems, which ensure that if a conjunction of hypotheses is true, the conclusion (GCR) is true as well.

3.2. Theorems

In this section, we provide a decomposition method for selected global compliance patterns and show how they can be applied in a collaborative setting. In particular, we prove a set of theorems required for ensuring the correctness of our decomposition method. Each theorem represents a possible decomposition of a given compliance pattern.

We illustrate the translation of a GCR into a First Order Logic (FOL) expression using basic equivalences as in Def. 3.

**Definition 3 (Basic Equivalences).** Based on (41), the following equivalences hold by definition. Predicate \(x(t, ty)\) describes that at the point in time \(t\) an activity (message) of type \(ty\) was executed (i.e., sent or received).

- \(\Box A \land \Box B \equiv \forall a : (x(a, A) \rightarrow (\exists b : (x(b, B) \land a < b)))\)
- \(\Rightarrow \forall a \exists b : (x(a, A) \rightarrow (x(b, B) \land a < b))\)
First Author et al.: Preprint submitted to Elsevier

For example, GCR \( \text{Production} \rightarrow \text{Final test} \) is translated into: \( \forall a : (x(a, \text{Production}) \rightarrow \exists b : x(b, \text{Final test}) \land a < b) \). Thereby, relation \( < \) expresses a temporal precedence between points in time \( a \) and \( b \). The decomposition algorithm presented in Section 4 exploits the transitivities for GCR as in Theorem 1. Specifically, by combining transitive relations, where each relation can be checked locally by a single partner, it becomes possible to reconstruct the original GCR behavior. Theorem 1 ensures that the behavior of the derived assertions reproduces the behavior of the GCR, but not vice versa.

**Theorem 1 (Transitivities).**

Let \( A, B, \) and \( C \) be three activity or message types. Then:

\[ a. \text{The rightwards transitivity holds:} \quad [A] \rightarrow [B] \land [B] \rightarrow [C] \Rightarrow [A] \rightarrow [C] \]

\[ b. \text{The leftwards transitivity holds:} \quad [A] \rightarrow [B] \land [B] \rightarrow [C] \Rightarrow [A] \rightarrow [C] \]

In the following, the correctness of Theorem 1 is proven applying Def. 3.

**Proof 1 (Rightwards Transitivity).**

Let \( A, B, \) and \( C \) be three activities or interactions. Then \( [A] \rightarrow [B] \land [B] \rightarrow [C] \)
\[ \Rightarrow \forall a \exists b : (x(a, A) \rightarrow (x(b, B) \land a < b)) \land \forall b \exists c : (x(b, B) \rightarrow (x(c, C) \land b < c)) \]
\[ \Rightarrow \forall a \exists b, c : \left( (x(a, A) \rightarrow (x(b, B) \land a < b)) \land (x(b, B) \rightarrow (x(c, C) \land b < c)) \right) \]
\[ \Rightarrow \forall a \exists b, c : \left( (x(a, A) \rightarrow x(b, B) \rightarrow (x(c, C) \land a < b < c)) \right) \]
\[ \Rightarrow \forall a \exists c : (x(a, A) \rightarrow (x(c, C) \land a < c)) \Rightarrow [A] \rightarrow [C] \text{ q.e.d.} \]
Verifying Compliance in Process Choreographies

**Figure 8:** Examples 1–3

Leftwards transitivity can be proven similarly by replacing ‘<’ with ‘>’.

**Corollary 1.** Let A, B, C, and D be activities or interactions. Then

\[ A \prec B \land B \prec C \land C \prec D \Rightarrow A \prec C \land C \prec D \Rightarrow A \prec D \]

In the following, we use Examples (1) - (3) (cf. Fig. 8), which we extracted from our running example (cf. Figs. 3 and 4), in order to illustrate how we use Theorem 1 for decomposing a simple compliance rule of type \([A] \rightarrow [B]\) that involves two private tasks A and B of two different partners \(p_1\) and \(p_2\) respectively.

- **Example (1):** \(\text{get permission of authority} \rightarrow \text{safety check}\). In this example, both activities are private, which would normally require **Middleman** and **Special carrier** to share runtime information about the execution time of the respective activities. In turn, this would require an agreement on a time synchronization protocol that considers network failures and message transmission delays. This can be solved by identifying a transitive relation between the two private activities that include an interaction activity. According to Theorem 1, the interaction activity **order special transport** between **Middleman** and **Special carrier** fulfills the conditions \(A_1\) and \(A_2\): \([\text{get permission of authority}] \rightarrow [\text{order special transport}]\) and \([\text{order special transport}] \rightarrow [\text{safety check}]\).

- **Example (2):** \(\text{process order} \rightarrow \text{produce intermediate}\). In this example, **Manufacturer** and **Supplier** do not engage in any direct interaction. However, by looking at the public processes of the collaboration model from Fig. 3, it becomes possible to identify a double transitive relation through **Middleman**, which interacts with both partners. Therefore, using Corollary 1, the transitive relations (assertions): \([\text{process order}] \rightarrow [\text{order intermediate}]\), \([\text{order intermediate}] \rightarrow [\text{waybill for intermediate}]\), and \([\text{waybill for intermediate}] \rightarrow [\text{produce intermediate}]\) reproduce the behavior of \([\text{process order}] \rightarrow [\text{produce intermediate}]\). **Middleman**, which has initially not been involved in the GCR, becomes involved in the derived assertions. We call **Middleman** an intermediary partner.

- **Example (3):** \(\text{prepare transport} \rightarrow \text{safety check}\). In this example, it is not possible to identify any transitive relation between **Supplier** and **Special carrier** that involve private activities **prepare transport** and **safety check**. The interaction activity **waybill for intermediate** connects both partners immediately after the activities in question, which discards any possibility of a transitive relation. In this case, it is not possible to satisfy Theorem 1 and, hence, additional message exchanges become necessary to inform about the execution state of the activities involved in the GCR. Message exchanges can be either synchronous or asynchronous. Asynchronous message exchange only allows for reactive GCR checking and, therefore, detecting violations after their occurrence. Synchronous message exchange, in turn, is proactive as it enforces the GCR with new
restrictions to the process models, e.g., the execution of activity safety_check becomes enabled only after receiving a synchronization message (i.e., about whether or not prepare_transport is executed). Supplier shall also inform Special_carrier in case activity prepare_transport is not executed, as this does not prevent activity safety_check from being executed according to the GCR.

Rightwards transitivity (cf. Theorem 1.a) directly ensures the correctness of the assertions derived in the above examples. It should be clear that the correctness of the derived assertions in Example (2) can be directly concluded based on Corollary 1. The same examples can be also used to illustrate leftwards transitivity.

**Theorem 2 (Zig zag Transivities).**
Let A, B, and C be three activity or message types. Then:

a. The rightwards zig zag transitivity holds for the consequence absence:

$$\overline{B} \rightarrow A \land \overline{B} \rightarrow \overline{C} \Rightarrow \overline{A} \rightarrow \overline{C}$$

b. The leftwards zig zag transitivity holds for the consequence absence:

$$\overline{A} \rightarrow B \land \overline{C} \rightarrow \overline{B} \Rightarrow \overline{C} \rightarrow \overline{A}$$

**Proof 2 (Rightwards Zig Zag Transitivity of Absence).**
Let A, B, and C be activities or interactions. Then:

$$\overline{B} \rightarrow A \land \overline{B} \rightarrow \overline{C}$$

$$\Leftrightarrow \forall a \exists b : \left( x(a, A) \rightarrow (x(b, B) \land b \leq a) \right) \land \forall b, c : \left( x(b, B) \rightarrow (\neg x(c, C) \lor c \leq b) \right)$$

$$\Rightarrow \forall a \exists b : \left( x(a, A) \rightarrow (x(b, B) \land b \leq a) \right) \land \forall b, c : \left( x(b, B) \rightarrow (\neg x(c, C) \lor c \leq b) \right)$$

$$\Rightarrow \forall a \exists b : \left( x(a, A) \rightarrow (x(b, B) \land b \leq a) \right) \land \forall b, c : \left( x(b, B) \rightarrow (\neg x(c, C) \lor c \leq b) \right)$$

$$\Rightarrow \forall a \exists b : \left( x(a, A) \rightarrow (x(b, B) \land b \leq a) \right) \land \forall b, c : \left( x(b, B) \rightarrow (\neg x(c, C) \lor c \leq b) \right)$$

$$\Rightarrow \forall a, c : \left( x(a, A) \rightarrow (\neg x(c, C) \lor c \leq a) \right) \Rightarrow A \rightarrow \overline{C}$$

Leftwards zig zag transitivity of absence can be proven similarly by replacing ‘<’ with ‘>’ and ‘≤’ with ‘≥’.

In the following, we use Examples (4) and (5) from Fig. 9 to illustrate and discuss how Theorem 2 can be used to decompose a GCR of type rightwards zigzag $A \rightarrow \overline{C}$. Note that these two examples are adopted from the running example we introduced in Section 1 in order to fulfill the decomposition requirements.

- Example (4): quick_test_intermediate → transport_intermediate. In this example, transport_intermediate and order_special_transport in Special_carrier belong to different XOR branches, which means that the
execution of activity transport\_intermediate implies the non-execution of activity order\_special\_transport and vice versa (fulfilling assertion A₁: order\_special\_transport \rightarrow transport\_intermediate). Additionally, in Manufacturer, the interaction activity order\_special\_transport and the private activity quick\_test\_intermediate belong to the same XOR branch, and fulfill assertion A₂: (order\_special\_transport) \rightarrow (quick\_test\_intermediate).

According to Theorem 2.a, the conjunction of A₁ and A₂ reproduces the behavior of the original GCR. Note that process compatibility ensures that whenever sending order\_special\_transport occurs in Special\_carrier, receiving order\_special\_transport should occur in Manufacturer as well. At the presence of loops that encapsulate the depicted process part of Special\_carrier, the XOR fragment can be executed multiple times possibly leading to an alternate execution of the corresponding branches. For example, if in the first loop iteration, transport\_intermediate is executed and quick\_test\_intermediate is not executed, then, to this point both derived assertions are satisfied. Let us assume that a future iteration over the XOR fragment in the context of the same process instance triggers quick\_test\_intermediate execution, thus, violating the original GCR.

iteration 1: special\_carrier: {transport\_intermediate}
iteration 1: manufacturer ()
iteration 2: special\_carrier: {transport\_intermediate, order\_special\_transport}
iteration 2: manufacturer: {order\_special\_transport, quick\_test\_intermediate}

Combined trace: {transport\_intermediate, order\_special\_transport, order\_special\_transport, quick\_test\_intermediate}

By looking at the combined trace, it becomes clear that the GCR is violated. Unfortunately, this would require both partners to exchange the traces and use a common time stamping system to obtain the same chronological order of activities. Using the theorems, however, the Manufacturer can locally run its derived assertion against its own execution trace of the same process instance, and identify the violation. Note that the decomposition does not enforce the processes with new restrictions (except when no transitivity could be derived), but uses the existing control flow and interactions between partners to derive assertions that can be used for a decentralized checking of the original GCR.

- Example (5): quick\_test\_intermediate \rightarrow transport\_intermediate. In Fig. 9, quick\_test\_intermediate always happens after arrival\_of\_intermediate ensuring quick\_test\_intermediate \rightarrow arrival\_of\_intermediate. The second part of the decomposition can be directly derived from the process control flow of Special\_carrier: transport\_intermediate \rightarrow arrival\_of\_intermediate. The same reasoning applies to this example at the presence of loops. The correctness of Example (5) concludes from the leftwards zig zag transitivity (cf. Theorem 2.b), whereas Example (4) relies on the rightwards zig zag transitivity of the absence (cf. Theorem 2.a). The decomposition process is not limited to these scenarios and, as aforementioned, the decomposition cannot always be automated, but might require manual interaction and processing. Altogether, the decomposition eases global compliance rule checking, where each partner checks its corresponding derived assertions locally. A GCR is rechecked only if at least one of the derived assertions is not evaluated to true. Note that this does not necessarily imply that the GCR is violated.

**Theorem 3 (Rightwards Chaining Transitivity).**

Let A, B, C, and D be activities or interactions such as A \rightarrow B \rightarrow C \rightarrow D; if A and B occur, C and D shall occur afterwards. Let m₁, m₂, and m₃ be three interactions such as:

1. \((m₁) \rightarrow A\)
2. \((m₁) \rightarrow B \rightarrow (m₂)\)
3. \((m₂) \rightarrow C \rightarrow (m₃)\)
4. \((m₃) \rightarrow D\)

Then: Whenever (1) \land (2) \land (3) \land (4) evaluates to true, A \rightarrow B \rightarrow C \rightarrow D is true as well.

**Proof 3 (Rightwards Chaining Transitivity).**

1. \land (2):
   \[
   \forall a \exists m₁ : \left( x(a,A) \rightarrow x(m₁,M₁) \land (m₁ < a) \right) \land \forall m₁, \forall b, \exists m₂ : \left( (x(m₁,M₁) \land x(b,B) \land m₁ < b) \rightarrow \right.
   \]
Verifying Compliance in Process Choreographies

\[(x(m_2, M_2) \land b < m_2)\]

\[\forall a \exists m_1 \forall b \exists m_2 \colon (x(a, A) \land x(m_1, M_1) \land (m_1 < a) \land (x(m_1, M_1) \land x(b, B) \land m_1 < b) \land (x(m_2, M_2) \land b < m_2)\]

\[\forall a \exists m_1 \forall b \exists m_2 : (x(a, A) \land x(b, B) \land a < b \land (x(m_1, M_1) \land (m_1 < b)) \land (x(m_2, M_2) \land b < m_2)\]

\[\forall a \forall b \exists m_2 \colon (x(a, A) \land x(b, B) \land a < b \land (x(m_2, M_2) \land b < m_2) \land \forall m_2 \exists c \exists m_3 \colon (x(m_2, M_2) \rightarrow x(c, C) \land x(m_3, M_3) \land m_2 < c \land c < m_3)\]

\[\forall a \forall b \exists c \exists m_3 : (x(a, A) \land x(b, B) \land a < b \land (x(c, C) \land x(m_3, M_3) \land b < c \land c < m_3) \land \forall m_3 \exists d : (x(m_3, M_3) \rightarrow x(d, D) \land m_3 < d)\]

- Example (6): \text{get_permission_authority} \rightarrow \text{prepare_transport} \rightarrow \text{transport_intermediate} \rightarrow \text{production}. In this example, all activities involved in the GCR are private and belong to separate partners. According to the process models shown in Figs. 3 and 4, each partner can separately derive the corresponding assertion based on Theorem 3 and involving the corresponding activity in the GCR.

1. \text{Middleman} \text{fwd_order_intermediate} \rightarrow \text{get_permission_authority}
2. \text{Supplier} \text{fwd_order_intermediate} \rightarrow \text{prepare_transport} \rightarrow \text{waybill_for_intermediate}
3. \text{Special_carrier} \text{waybill_for_intermediate} \rightarrow \text{transport_intermediate} \rightarrow \text{arrival_of_intermediate}
4. \text{Manufacturer} \text{arrival_of_intermediate} \rightarrow \text{production}

In this example, partners will first engage in a setup phase, in which they agree on the interaction activities that satisfy all derived assertions following the assertions’ templates of Theorem 3. For example, \text{Middleman} will start by identifying relations in its process of type \text{interaction_activity} \rightarrow \text{get_permission_authority} where \text{interaction_activity} must be a message exchange with \text{Supplier} that is the partner being responsible for the following antecedence occurrence \text{prepare_transport}. In this example, \text{Middleman} and \text{Supplier} have only one interaction that satisfies the derived assertion (1); however, it is also possible to identify several alternatives. The combination of the four derived assertions reproduce the behavior of the original GCR when all assertions are true.

The following theorem represents a generalization of Theorem 3 with \(n\) antecedences’ occurrences and \(m\) consequences’ occurrences. Note that the previous example also illustrates Theorem 4 with \(n = 2\) and \(m = 2\).

**Theorem 4 (Generic Rightwards Chaining Transitivity).**
Let \(A_1 \cup \ldots \cup A_n\) and \(C_1 \cup \ldots \cup C_m\) be \(n+m\) activities, \(\text{\[A_1\] \rightarrow \ldots \rightarrow A_n \rightarrow \ldots \rightarrow C_m\}]\); if all \(A_i\) occur such that \(\forall i < n, A_i < A_{i+1}\) holds, and all \(C_j\) should occur afterwards such that \(\forall j < m, C_j < C_{j+1}\) holds. Let \(m_i\), where \(1 \leq k < n+m-1\) be interactions such that:

1. \(M_k \rightarrow A_1\)
2. \(M_{i-1} \rightarrow A_i \rightarrow M_i\) where \(1 < i < n\)
3. \(M_{i-1} \rightarrow A_i \rightarrow M_i\)
4. \(M_{i+j-1} \rightarrow C_j \rightarrow M_{i+j}\) where \(1 \leq j < m\)
5. \(M_{i+m-1} \rightarrow C_m\)
Then: Whenever (1) Λ (2) Λ (3) Λ (4) Λ (5) evaluates to true, \( A_1 \rightarrow A_2 \rightarrow \cdots \rightarrow A_n \rightarrow C \rightarrow C_1 \rightarrow \cdots \rightarrow C_m \) is true as well.

**Proof 4 (Generic Rightwards Chaining Transitivity).**

(1) :⇔ ∀a∃m_1 : (x(a, A) → x(m_1, M_1) Λ (m_1 < a))

(2) :⇔ \( \bigwedge_{1<i<n} (\forall a_{i-1} \exists a_i : (x(m_{i-1}, M_{i-1}) Λ x(a_i, A_i) Λ m_{i-1} < a_i) → (x(m_i, M_i) Λ m_i < a_i)) \)

(3) :⇔ (\forall m_{n-1} \forall a_n \exists m_n : (x(m_{n-1}, M_{n-1}) Λ x(a_n, A_n) Λ m_{n-1} < a_n) → (x(m_n, M_n) Λ a_n < m_n))

(1) Λ (2) Λ (3): when evaluated to true, this ensures that all \( A_i \) were executed, and all these executions combined lead to \( M_n \) as a consequent. This includes the case where all \( A_i \) execute in ascending order. So, if we consider this particular order, the formula leading to \( M_n \) becomes true.

(4) :⇔ \( \bigwedge_{1\leq j<m} (\forall m_{n+j-1} \forall c_j \exists m_{n+j} : (x(m_{n+j-1}, M_{n+j-1}) Λ x(c_j, C_j) Λ m_{n+j-1} < c_n) → (x(m_{n+j}, M_{n+j}) Λ m_{n+j} < c_j)) \)

(5) :⇔ (\forall m_{n+m-1} \exists c_m : (x(m_{n+m-1}, M_{n+m-1}) → (x(c_m, C_m) Λ m_{n+m-1} < c_m))

(4) Λ (5): This formula transitively ensures that whenever \( M_{n+j-1} \) is executed, there is at least one execution in ascending order of all \( C_j \). \( M_{n+j-1} \) becomes the link between all antecedence patterns and consequent patterns. Therefore, the conjunction of formulas (1) to (5) ensures that whenever an instance containing an ordered execution of \( A_i \) should lead to an ordered execution of execution of \( C_j \). Note that this conjunction represents a stronger constraint than the original GCR. However, as these formulas are deducted directly from the actual processes, they do not add new constraints.

**Theorem 5 (Between Pattern 1).**

Let \( A, B \) and \( C \) be three activities. \( A \rightarrow \overrightarrow{M_1} \rightarrow C \rightarrow \overrightarrow{M_2} \rightarrow B \) if \( A \) and \( B \) occur and \( B \) occurs after \( A \), then \( C \) must occur in between.

(1) \( A \rightarrow M_1 \oplus M_2 \rightarrow C \rightarrow B \)

(2) \( M_2 \rightarrow M_1 \rightarrow B \)

(3) \( M_1 \rightarrow C \rightarrow \overrightarrow{M_2} \rightarrow B \)

Then: Whenever (1) Λ (2) Λ (3) evaluates to true, \( A \rightarrow \overrightarrow{C} \rightarrow B \) is true as well.

**Proof 5 (Between Pattern 1).**

(1) :⇔ ∀a, x(a, A) → ∃m_1 ∃m_2, x(m_1, M_1) Λ x(m_2, M_2) Λ (a < m_1) Λ (m_2 < m_1)

(2) :⇔ ∀b, x(b, B) → ∃m_2 ∃m_3, x(m_2, M_2) Λ x(m_3, M_3) Λ (m_2 < m_3)

(3) :⇔ ∀m_1 ∀m_2, x(m_1, M_1) Λ x(m_2, M_2) → ∃c, x(c, C) Λ (m_1 < c < m_2)

(1) Λ (2) :⇔ ∀a∀b, x(a, A) Λ x(b, B) → ∃m_1 ∃m_2 ∃m_3, x(m_1, M_1) Λ x(m_2, M_2) Λ x(m_3, M_3) Λ (a < m_1) Λ (m_2 < m_3) Λ (m_3 < c)

(2) Λ (3) :⇔ ∀a∀b, x(a, A) Λ x(b, B) → ∃m_1 ∃m_2 ∃m_3, x(m_1, M_1) Λ x(m_2, M_2) Λ x(m_3, M_3) Λ (a < m_1) Λ (m_2 < m_3) Λ (m_3 < c)

(1) Λ (2) Λ (3) :⇔ ∀a∀b, x(a, A) Λ x(b, B) Λ a < b → ∃m_1 ∃m_2 ∃m_3, x(m_1, M_1) Λ x(m_2, M_2) Λ x(m_3, M_3) Λ (a < m_1) Λ (m_2 < m_3) Λ (m_3 < c)

(2) Λ (3) :⇔ ∀a∀b, x(a, A) Λ x(b, B) Λ a < b → ∃m_1 ∃m_2 ∃m_3, x(m_1, M_1) Λ x(m_2, M_2) Λ x(m_3, M_3) Λ (a < m_1) Λ (m_2 < m_3) Λ (m_3 < c)

(1) Λ (2) Λ (3) :⇔ ∀a∀b, x(a, A) Λ x(b, B) Λ a < b → ∃c, x(c, C) Λ (a < c < b)

- Example (7): \( \overrightarrow{order_intermediate} \rightarrow \overrightarrow{prepare_transport} \rightarrow \overrightarrow{transport_intermediate} \). Again, in this example, we consider the worst case scenario where each activity referred to by the GCR belongs to a different process partner. In this example, Middleware has one single alternative as it only has two interaction activities with Special_carrier and Supplier respectively, which follow the assertion template (1) of Theorem 5; i.e., each execution of \( order_intermediate \) must be followed (not necessarily immediately) by \( f_wd_order_intermediate \),
Verifying Compliance in Process Choreographies

which, in turn, should not be preceded by any order_special_transport execution. Similarly, Special_carrier and Supplier should identify assertions that follow rule templates (2) and (3) respectively.

Note that the Between Pattern $A \rightarrow C \rightarrow B$ can be also checked using chaining transitivity $A \rightarrow C \rightarrow B$. However, this adds a stronger assumption on $C$ and $B$ that should follow $A$ whenever it occurs. For example, this holds in the running example (cf. Fig. 3), as order_intermediate transitively implies prepare_transport, which, in turn, transitively implies transport_intermediate.

1. $Middleman \rightarrow (order\_intermediate \rightarrow (fwd\_order\_intermediate))$

2. $Special\_carrier \rightarrow (order\_special\_transport \rightarrow (fwd\_order\_intermediate))$

3. $Supplier \rightarrow (fwd\_order\_intermediate \rightarrow (prepare\_transport \rightarrow (waybill\_for\_intermediate))$

Theorem 6 (Between Pattern 2).

Let $A$, $B$ and $C$ be three activities $A \rightarrow C \rightarrow B$ if $A$ and $B$ occur and $B$ occurs after $A$, then $C$ shall occur in between.

1. $M_1 \rightarrow A \rightarrow M_2 \rightarrow M_3 \rightarrow M_4$

2. $M_1 \rightarrow B \rightarrow M_2 \rightarrow M_4$

3. $M_3 \rightarrow M_2 \rightarrow B$

4. $M_2 \rightarrow M_3 \rightarrow C$

Then: Whenever (1) ∧ (2) ∧ (3) ∧ (4) evaluates to true, $A \rightarrow C \rightarrow B$ is true as well.

Proof 6 (Between Pattern 2).

1. $∀a, x(a, A) \rightarrow ∃m_1 ∃m_2 ∃m_3 ∃m_4, x(m_1, M_1) ∧ x(m_2, M_2) ∧ x(m_3, M_3) ∧ x(m_4, M_4) ∧ (m_1 < a < m_2 < m_3 < m_4)$

2. $∀m_1 ∀m_2, x(m_1, M_1) ∧ x(b, B) ∧ x(m_2, M_2) → ∃m_3, x(m_2, M_2) ∧ (b < m_2 < m_4)$

3. $∀m_3 ∀m_4, x(m_3, M_3) ∧ x(b, B) → ∃m_4, x(m_4, M_4) ∧ (m_3 < m_4)$

4. $∀m_1 ∀m_2, x(m_2, M_2) ∧ x(m_3, M_3) → ∃c, x(c, C) ∧ (m_2 < c < m_3)$

Using (1):

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → ∃m_1 ∃m_2 ∃m_3 ∃m_4, x(m_1, M_1) ∧ x(m_2, M_2) ∧ x(m_3, M_3) ∧ x(m_4, M_4) ∧ (m_1 < a < m_2 < m_3 < m_4) ∧ (a < b < m_4) \lor m_4 < b)$

Using (2), if $b$ happens before $m_3$, then $m_3$ should not happen in between:

$∀a, b, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_1, M_1) ∧ x(m_2, M_2) ∧ x(m_3, M_3) ∧ x(m_4, M_4)) ∧ ((m_1 < a < m_2 < m_3 < m_4) \lor (m_1 < a < m_2 < m_3 < m_4 < b))$

Using (3), if $m_3 < b$, then there should be $m_3$ in between:

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < b))$

Using (4), if $m_3 < b$, then there should be $m_3$ in between:

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < b)) (∃m_5, x(m_5, M_5) ∧ (m_3 < m_5 < b))$

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < m_5 < b))$

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < m_5 < b)) (∃m_5, x(m_5, M_5)) ∧ (m_3 < m_5 < b)$

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < m_5 < b)) (∃m_5, x(m_5, M_5)) ∧ (m_3 < m_5 < b)$

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < m_5 < b)) (∃m_5, x(m_5, M_5)) ∧ (m_3 < m_5 < b)$

$∀a, x(a, A) ∧ x(b, B) ∧ a < b → (x(m_2, M_2) ∧ x(m_3, M_3) ∧ (a < m_2 < m_3 < m_5 < b)) (∃m_5, x(m_5, M_5)) ∧ (m_3 < m_5 < b)$
Verifying Compliance in Process Choreographies

\[ \forall a \forall b \exists m_1 \exists m_2 \exists c, \ x(a, A) \land x(b, B) \land a < b \rightarrow (x(m_2, M_2) \land x(m_5, M_5) \land x(c, C)) \land (a < m_2 < c < m_5 < b) \]

In order to illustrate Theorem 6, we apply the following adaptations to the running example (cf. Figs. 1 - 4):

(i) After receiving request_details, Supplier prepares the details (prepare_details), then informs Middleman about the start of intermediate production (production_status) before sending back transport_details.
(ii) After receiving transport_details, Special_carrier confirms to Middleman the availability of transportation for intermediate (transport_confirmation).
(iii) After receiving order_special_transport, Middleman receives production_status, does internal_checks, and waits for transport_confirmation.

- Example (8): [prepare_details]→[internal_checks]→[check]. Similar to the previous examples, the partners start by locally identifying relations that satisfy the derived assertions templates of Theorem 6, then apply a matching mechanism to check whether the additional interactions used for the derived assertions intersect and jointly fulfill the templates. It is noteworthy that the number of additional interaction activities required for the derived assertions is superior to the number required in Theorem 5. Despite that, Theorem 6 provides more relaxed assumptions compared to Theorem 5 as it does not restrict activity B from occurring before activity A. Theorem 6 still prevents B from happening between m1 and m3. The following assertions are the decomposition results of Example (8):

1. \( \text{Supplier : } \)
   \( \text{request_details} \rightarrow \text{prepare_details} \rightarrow \text{production_status} \rightarrow \text{transport_details} \rightarrow \text{waybill_intermediate} \)
2. \( \text{Special_carrier : } \)
   \( \text{request_details} \rightarrow \text{check} \rightarrow \text{transport_details} \rightarrow \text{waybill_intermediate} \)
3. \( \text{Special_carrier : } \)
   \( \text{transport_details} \rightarrow \text{transport_confirmation} \rightarrow \text{check} \)
4. \( \text{Middleman : } \)
   \( \text{production_status} \rightarrow \text{internal_checks} \rightarrow \text{transport_confirmation} \)

Note that all previous theorems consider loops and multiple occurrences of each of the activities composing the global compliance rule GCR. Indeed, in a process model that includes loops or multiple instance patterns, an activity may be executed multiple times at different points in time in the context of one single process instance. As such, each derived assertion including such repetitive activity should be satisfied for all its occurrences. Although this issue has been addressed in all previous theorems (see proofs), it resulted in additional decomposition complexity not required for loop-free processes. Therefore, we propose a simpler decomposition method for the "between" pattern, which may be applied solely to loop-free processes.

**Theorem 7 (Between Pattern (without loops)).**

Let A, B and C be three activities \( A \rightarrow C \rightarrow B \) if A and B occur and B occurs after A, then C shall occur in between.

- (1): \( A \rightarrow \{ M_1 \} \rightarrow M_2 \)
- (2): \( M_2 \rightarrow \{ M_1 \} \rightarrow B \)
- (3): \( M_1 \rightarrow C \rightarrow M_3 \)

Then: If the conjunction of formulas (1) \( \land (2) \land (3) \) evaluates to true, \( A \rightarrow C \rightarrow B \) is true as well.

**Proof Theorem 7 (Between Pattern (without loops)).**

1. \( \forall a: (x(a, A) \rightarrow \exists m_1, \exists m_2 : (x(m_1, M_1) \land x(m_2, M_2) \land (a < m_1 < m_2)) \)
2. \( \forall b: (x(b, B) \rightarrow \exists m_3, \exists m_2 : (x(m_3, M_3) \land (m_3 < m_1 < b)) \)
1 \( \land (2) \) \( \forall a \forall b : (x(a, A) \land x(b, B)) \rightarrow (x(m_1, M_1) \land x(m_2, M_2) \land x(m_3, M_3) \land (a < m_1 < m_2) \land (m_3 < m_1 < b)) \)

First Author et al.: Preprint submitted to Elsevier
$m_1 < m_2 \land (m'_2 < m_3 < b)$

As there are no loops over $A, B$ and corresponding $M$ messages, then $M_2$ can occur only once within one process instance. Consequently, $m_2 = m'_2$.

(1) $\land$ (2) $\vdash (\forall a, b, (A, A) \land (x(b, B)) \rightarrow (x(m_1, M_1) \land x(m_2, M_2) \land x(m_3, M_3) \land (a < m_1 < m_2 < m_3 < b))$

$\vdash (\forall a, b, (A, A) \land (x(b, B)) \rightarrow (x(m_1, M_1) \land x(m_3, M_3) \land (a < m_1 < m_3 < b))$

$\vdash (\forall a, b, (A, A) \land (x(b, B)) \rightarrow (x(m_1, M_1) \land x(m_2, M_2) \land x(c, C) \land (m_1 < c < m_3))$

$\exists c, x(m_2) \land (a < m_1 < c < m_3 < b)$

Theorem 8 (Requires transitivity).

Let $A$ and $B$ be two activities or interactions such as $A \land B$: if $A$ occurs then $B$ should occur (before or after, $\forall a, x(a, A) \rightarrow \exists B, x(b, B)$).

Let $A, B, M$ be three activities or interactions such that:

(1) $\vdash A \rightarrow M$

(2) $\vdash M \rightarrow B$

If (1) $\land$ (2) evaluates to true, then $A \rightarrow B \lor B \rightarrow A$ evaluates to true.

Proof 8 (Requires transitivity).

(1) $\vdash (\forall a, x(a, A) \rightarrow \exists m : x(m, M) \land (a < m))$

$\vdash (\forall m, (x(m, M) \rightarrow \exists b : (x(b, B)) \land (m < b)) \lor (\forall m, (x(m, M) \rightarrow \exists b : (x(b, B)) \land (b < m))$

$\vdash (\forall m, (x(m, M) \rightarrow \exists b : (x(b, B)) \land (m < b)) \lor (b < m))$

$\vdash (\forall a, x(a, A) \rightarrow \exists m : (x(m, M) \land (a < m)) \lor (\forall m, (x(m, M) \rightarrow \exists b : (x(b, B)) \land (m < b)) \lor (b < m))$

Note that this theorem also considers loops and multi-instance patterns. The illustration of Theorem 8 is similar to the rightwards and leftwards transitivity examples.

4. Algorithm for Decomposing Global Compliance Rules

At design time, checking a GCR that solely refers to interactions and/or public activities can be achieved by applying contemporary compliance checking techniques (cf. (29)) either on the choreography model or the public process models of the involved partners. By contrast, if a GCR refers to private activities of different partners, it becomes impossible to check its correctness as partners must not view the private process model parts of the other partners and,
Verifying Compliance in Process Choreographies

therefore, cannot identify the dependencies between the private activities involved in the GCR. To cope with this issue, we suggest decomposing the GCR into a set of assertions of which each can be checked locally by the corresponding partner. The decomposed rules then reproduce the behavior of the original GCR. Decomposition in compliance checking has been exploited by (60), but only at the process model level in order to achieve performance gains for the compliance checks. The article at hand proposes to decompose the GCR to distribute the compliance checks to the partners for maintaining the confidentiality of their private tasks. This section focuses on the decomposition algorithms and explains the steps to derive assertions by applying the theorems introduced in Section 3.

Figure 10 provides a high-level description of the steps required by partners involved in a GCR to identify a valid decomposition. Algorithm 1 provides a more detailed view on how this can be achieved in practice with a particular focus on compliance rules that include one antecedence pattern.

![Figure 10: Decomposition Process](image)

Given a GCR, the decomposition process starts by selecting a leader among the partners involved in the GCR. The leader will be responsible for identifying the pattern corresponding to the GCR (e.g., rightward chaining pattern or between pattern). This is trivial and can be accomplished with a simple exact graph matching algorithm (e.g., comparing node types and connectors). Once the pattern is identified, several decomposition theorems may be applicable. For example, in the case of the between pattern, Theorems 5, 6, and possibly 7 (if the processes are loop free) may be applied. The leader will then select and apply a theorem, derive the assertion templates accordingly, and send each of them to the corresponding partner—this step can be easily automated. An assertion template, in turn, is a derived assertion output from the theorem, where the actual interactions (i.e., message exchanges) have not yet been defined. For example, for \textit{Middleman}, \texttt{get\_permission\_of\_authority} → \{M\} (where M shall be an activity interacting with \textit{Special\_carrier}) is a derived assertion template of the global compliance rule \texttt{get\_permission\_of\_authority} → \{\texttt{safety\_check}\}, as M has not been defined yet.
Next, each partner will try to identify an assertion template instance that conforms with the derived assertion template— an instance of an assertion template corresponds to a template with actual activities. Order_special_transport is a valid option in this example as it interacts with Special_carrier fulfilling the template constraint (i.e., the template instance corresponds to \texttt{get_permission_of_authority}\texttt{-order_special_transport}). This can be automated by having each partner responsible for an assertion template iterating over the message exchanges in its private process model. Depending on the assertion template structure, one or several message exchanges may be selected for constructing an assertion instance candidate. The latter must conform with the assertion template. Moreover, it needs to be ensured that the process in question is compliant with it. Existing design-time compliance checking techniques can be employed in this regard \cite{3; 4; 35; 6}.

Several assertion instance candidates can be identified for the same partner, which may increase the probability of finding a collective solution among all partners. Afterwards, partners either collectively enter a negotiation phase and exchange their assertion instance candidates, or rely on the leader to collect all proposals and run a matching algorithm that selects assertion candidates, which replicate the templates derived by the decomposition. Indeed, two assertion templates may require that they use the same message exchange. Therefore, the matching algorithm will select the assertion instance candidates of different partners that have the same message exchange in common (using function \(\nu\) or \(\phi\) to ensure that the mapping is correct). While having the leader collecting the assertion proposals and doing the matching can be more efficient and reduce the communication overhead between partners, conducting the negotiation in a distributed manner reduces trust assumptions.

Note that it is possible to run the entire process in a distributed manner, without need for a leader. In this case, all partners will have to run the matching algorithms for identifying the GCR pattern. Moreover, they have to agree on the decomposition theorem to be applied (e.g., using a majority vote) and collectively execute the matching of assertion instances. If a matching solution is found, each partner will use the selected assertion instance for future run-time checking. Unless a solution is found, the next applicable theorem will be explored in the same way. If no solution could be found after trying all applicable decomposition theorems, synchronization messages become necessary for enabling distributed run-time checking of the GCRs. At run-time, no additional communication with other partners is needed for checking the GCR, unless a violation occurs. Similar to assertion and local compliance rules monitoring, each partner is responsible for complying with the derived assertions. This can be enforced using post-auditing processes by the respective legal entities, e.g., WHO in the case of Covid-19.

Algorithm 1 realizes GCR decomposition as set out in Definition 2. It assumes that each node of the GCR is assigned to one partner being responsible for it. Further on, we assume the input GCR to be consistent and satisfiable (for dealing with unsatisfiable and inconsistent rules we refer interested readers to \cite{11}). In the following, we first explain Algorithm 1 step by step and then illustrate the entire algorithm along Example 1 (see below).

Starting from the \(A\) node (cf. Def. 2), Algorithm 1 walks outwards through all other nodes of the GCR. Thereby, the visited parts are copied and become assertions. Wherever the algorithm walks over a connector between two nodes \(n\) and \(s\), which are assigned to different partners \(\rho(n)\) and \(\rho(s)\), the GCR is split at this position as this dependency cannot be evaluated by a single partner. Next, the algorithm tries to replicate the connector where the GCR was split through (transitive) message exchanges between both affected partners by applying the transitive relationships from Section 2. Therefore, sets \(n^\star\), \(s^\star\), and \(\Theta\) are calculated. Depending on the pattern of \(s\) (cf. Def. 2), \(n^\star\) and \(s^\star\) contain the messages succeeding or preceding \(n\) and \(s\), respectively. Note that these calculations have to be accomplished in a decentralized manner by \(\rho(n)\) and \(\rho(s)\) themselves as \(n\) and \(s\) may be private tasks. Next, \(\Theta\) combines those messages of \(n^\star\) and \(s^\star\) that can be combined.

If \(s\) is a \(C\) node (i.e., \(s\) must follow \(n\)), \(\Theta\) contains message tuples \((m_1, m_2)\) that ensure that \(n\) is always followed by \(m_1, m_1\) by \(m_2\) (unless \(m_1 = m_2\)), and \(m_2\) by \(s\). Any pair \((m_1, m_2) \in \Theta\) can then be used to complement the created assertions, i.e., \(m_1\) becomes a placeholder for \(s\) within the assertion of \(\rho(n)\), whereas \(m_2\) replaces \(n\) for \(\rho(s)\).

Regarding \(X\) nodes (i.e., \(s\) must not follow \(n\)), all pairs of messages \((m_1, m_2) \in \Theta\) ensure that \(n\) is preceded by \(m_1\) in any case, and \(m_1\) is preceded by \(m_2\) (unless \(m_1 = m_2\)), whereas \(s\) never follows \(m_2\). Finally, for \(X\) nodes an occurrence of \(s\) after \(n\) allows ignoring the rule. Hence, \(X\) nodes result in pairs \((m_1, m_2)\) such that \(m_1\) may only occur after \(n\) and \(m_2\) may only occur after \(m_1\) (unless \(m_1 = m_2\)). However, there should be at least one case in which \(m_2\) is followed by \(s\) (i.e., \(s\) is not always preceded by \(m_2\)).

Finally, all assertions of the same partner, which depend on the same \(A\) message, are merged to reduce the number of assertions. Remaining assertions without consequences are removed as they result from the processing of \(X\) nodes, but have not been merged in the previous step. Remember that ignoring \(X\) nodes is allowed as this makes rules even more strict.
Algorithm 1: GCR decomposition DECOMPOSE(gcr)

- Global compliance rule \( gcr = (N, p, \rho, \text{type}, \text{pattern}) \)
- Choreography model \( \gamma \), and \( M \) as the set of all partners’ message nodes.
- We assume that \( \rho \) also returns the partner private model of a node \( n \).

```plaintext
select the only \( a \in N \) with \( \text{pattern}(a) = \square \)
initialize queue \( Q \leftarrow \{a\} \)
create (incomplete) Assertion \( A_n \leftarrow \emptyset \) for the partner associated with \( \rho(a) \)

foreach \( (n \leftarrow \text{removeHead}(Q)) \) do

- If \( (n \in M) \) then
  - If \( \text{pattern}(n) = \{\square\} \) then extend \( A_n \) with \( \epsilon \)
  - Else
    - If \( \text{pattern}(n) = \{\bigcirc\} \) then extend \( A_n \) with \( \epsilon \)
    - Else
      - If \( \text{pattern}(n) = \{\lsquare\} \) then extend \( A_n \) with \( \epsilon \)
      - Else
        - If \( \text{pattern}(n) = \{\rtriangledown\} \) then extend \( A_n \) with \( \epsilon \)

- If \( \text{pattern}(n) = \{\triangledown\} \) then
  - If \( \text{pattern}(n) = \{\square\} \) then extend \( A_n \) with \( \epsilon \)
  - Else
    - If \( \text{pattern}(n) = \{\bigcirc\} \) then extend \( A_n \) with \( \epsilon \)
    - Else
      - If \( \text{pattern}(n) = \{\lsquare\} \) then extend \( A_n \) with \( \epsilon \)
      - Else
        - If \( \text{pattern}(n) = \{\rtriangledown\} \) then extend \( A_n \) with \( \epsilon \)

- If \( \text{pattern}(n) = \{\lsquare\} \) then
  - If \( \text{pattern}(n) = \{\square\} \) then extend \( A_n \) with \( \epsilon \)
  - Else
    - If \( \text{pattern}(n) = \{\bigcirc\} \) then extend \( A_n \) with \( \epsilon \)
    - Else
      - If \( \text{pattern}(n) = \{\lsquare\} \) then extend \( A_n \) with \( \epsilon \)
      - Else
        - If \( \text{pattern}(n) = \{\rtriangledown\} \) then extend \( A_n \) with \( \epsilon \)
```

Verifying Compliance in Process Choreographies

First Author et al.: Preprint submitted to Elsevier
Example 1. Let us apply Algorithm 1 to GCR C3 (cf. Fig. 11) from the running example that we introduced in Section 1 (cf. Figs. 1 - 4). Let the responsibilities be $\rho$(Safety Check) = Special Carrier, $\rho$(Get permission of authority) = Middleman, and $\rho$(Transport intermediate) = Special Carrier. After assigning responsibilities, Algorithm 1 starts with $[A]$ node Transport intermediate and creates a new assertion for the Special Carrier who is responsible for this activity. Then the Safety check is discovered and added to the assertion, since it belongs to the same partner. In turn, another partner (i.e., Middleman) is responsible for activity Get permission of authority. Hence, the algorithm cuts the respective connector and creates a new assertion for the respective partner. Next, Special Carrier and Middleman determine $n$ and $s$ with $n = \{\text{Waybill, T. Details, Req. Details, Order ST}\}$ and $s = \{\text{Order ST}\}$ to calculate those message pairs $\Theta = \{(\text{Waybill, Order ST}), \ldots, (\text{Order ST, Order ST})\}$ that can be used to transitively replicate the connector where the GCR was split. Finally, the algorithm places the selected messages into both assertions in such a way that the correctness of the original rule is preserved through the (leftwards) transitivity of eCRGs. Note that the Special Carrier could use message Waybill instead as (Waybill, Order ST) $\in \Theta$ holds.

For the same GCR, it is possible to infer several decomposition alternatives, depending on which interactions are used to find a transitive control flow relationship between the nodes of the GCR. It is also possible that no direct link can be identified between two partners’ GCR nodes (i.e., there is no interaction between these two partners). As such, interactions with intermediary partners can be used to find an indirect link (i.e., transitive interactions). As aforementioned, if no transitivity is identified between the GCR nodes of two partners (even not through intermediary partners), it becomes necessary to exchange additional execution data between the partners involved in the GCR, by, for example, adding sync messages. Sync messages are a specific type of messages communicated between partners to inform about the state of a given task (e.g., terminated, started, not executed). Although sync messages are not preferred as they expose private data about the exact execution time of a private task, they become necessary when the GCR cannot be decomposed into assertions, i.e., no transitive relations can be identified.

In the following, we discuss the complexity of the GCR decomposition in Algorithm 1. Results on checking regulatory compliance in general have been provided in (59). The first and second loops iterate over the nodes of the compliance rule. If we consider that two nodes can only have one flow connector, the number of required operations will be $n + n - 1$, otherwise $n(n - 1)$. In both cases complexity corresponds to $O(n^2)$. The first $if$ statement is $O(1)$, whereas the else statement calculates $n$, $s$ and $\theta$ each with a worst case complexity of $O(n^2)$. The second inner loop has the same complexity as the first inner loop. The third nested inner loop iterates over partners and compare assertions within the same partner with a number of operations equal to $n \times (m \cdot \frac{n-1}{2})$, which gives a complexity of $O(n^3)$. Finally, the last inner loop has a complexity of $O(n)$. Obviously, the overall worst case complexity of the algorithm is polynomial $O(n^4)$; i.e., outer loop combined with the third nested inner loop.

5. Verifying GCR Decomposition

The GCR decomposition algorithms from Section 4 are based on the theorems we have presented and proven in Section 3. Although these theorems support most control flow (i.e. behavior) compliance patterns known from literature (56; 19), they cannot cover every possible scenario. There may be two reasons for this: (i) either the structure of a GCR is not covered by Theorems 1–8 or (ii) none of the proposed decompositions is applicable. In both cases, it might not only become necessary to find a novel decomposition of a GCR, but also to verify the latter, i.e., to prove the correctness of the decomposition. One approach to accomplish this would be to apply the eCRG semantics and to formally
prove correctness (cf. Section 3). However, this is far from being trivial. Therefore, we introduce Algorithm 2 that enables the automated verification of GCR decompositions based on eCRG model checking.

**Algorithm 2:** Verification of Decompositions (Assertions \(A_1, \ldots, A_n\), GCR \(gcr\))

1. Let \(A\) be a function that translates an eCRG into a corresponding finite-state automaton
2. \(M \leftarrow \bigcap_{1 \leq i \leq n} A(A_i)\)
3. \(R \leftarrow M \cap \neg A(gcr)\)
4. If \(R = \emptyset\) then
   5. //Decomposition is correct
   6. return true
   7. else
      8. //Decomposition is incorrect
      9. return any arbitrary trace through \(R\) as counter example.

The main idea of Algorithm 2 is to interpret a GCR decomposition as declarative process model and to verify whether it solely allows for execution traces that comply with the original GCR. Thus, techniques that are known from the verification of declarative process models (50; 52) can be applied: First, all assertions \(A_1, \ldots, A_n\) of the decomposition are translated into finite state automata \(A(A_1), \ldots, A(A_n)\). Their intersection \((\bigcap_{1 \leq i \leq n} A(A_i))\) corresponds to an automaton that only accepts traces that comply with every assertion. In turn, \(\neg A(gcr)\) denotes the automaton that accepts solely traces violating the original GCR. If the intersection of these two automatons is empty, the decomposition is correct as it only allows for traces that do not violate the original GCR and, thus, comply with it.

\[
(\bigcap_{1 \leq i \leq n} A(A_i)) \cap \neg A(gcr) = \emptyset \Rightarrow (\bigcap_{1 \leq i \leq n} A(A_i)) \subseteq A(gcr)
\]

For any choreography \(y\), whose partners ensure \(A_1, \ldots, A_n\), we can now directly conclude:

\[
A(y) \subseteq (\bigcap_{1 \leq i \leq n} A(A_i)) \Rightarrow A(y) \subseteq A(gcr), \text{ i.e. } y \text{ complies with } gcr
\]

6. Implementation

The presented approach is implemented as part of the C³Pro framework⁶, which deals with change and compliance in process choreographies (21). The framework provides sophisticated functions for defining, propagating and negotiating changes in the context of process choreographies. Furthermore, it comprises a modeling component as one of its core components for editing and changing public and private process models as well as process choreography models. This component further enables the visualisation of change propagations. In the context of the present work, the three-layer architecture of the framework (21) (i.e., process modeling, change, and execution) was extended with additional components for dealing with process compliance. In detail, these new components include (i) an eCRG modelling tool, (ii) an automated generator of compliant choreographies, (iii) a model checker, and (iv) a GCR decomposition tool.

Figure 12 depicts the main components of the C³Pro framework. The compliance (CME) and process modeling (PME) environments allow defining and editing compliable process choreography models (39; 35) and decomposing global compliance rules. Compliability was introduced as “a semantic correctness criterion to be considered when designing interaction models. It ensures that interaction models do not conflict with the set of imposed global compliance rules” (39). At design time, it is ensured that the created choreography models are compliant with the defined compliance rules. Using both PME and CME, it becomes possible to parameterize and automatically generate compliable choreographies, which then can be used for testing and simulation purposes. A user, therefore, can specify the number and patterns of the GCRs as well as the parameters of the process and choreography models (e.g., number of private and public tasks, number of partners and interactions, or number and types of the control flow patterns that shall be covered by the processes) (6). Although the generated models represent synthetic processes without real-world semantics (i.e., these models do not reflect actual use cases such as a manufacturing collaborative process), they may

⁶http://www.wst.univie.ac.at/communities/c3pro/
serve as a support for simulation and research work evaluation, e.g., model executions can result in distributed logs of synthetic data, which are useful for evaluating the efficiency of specific mining techniques. In the context of this work, this tool can be used to test the feasibility and applicability of the decomposition process on more complex choreographies and corresponding GCRs. Currently, the automated generator tool only supports four basic compliance patterns. However, other GCR patterns can be directly inferred from the models and be used for testing. The tool is integrated in the C3Pro framework and can be tested. A data set of automatically generated models and the corresponding GCRs are made available in the same repository. Finally, the change editor allows defining and editing changes of process models and compliance rules, respectively.

The Compliance Management Service represents the main extension to C3Pro related to this work, and handles the defined compliance rules and implements the theorems as well as the GCR decomposition algorithm (cf. Section 4). As process execution engine, the Cloud Process Execution Engine is utilized. Most functions of the C3Pro framework are provided as a RESTful service, which enables unified access from any client being able to communicate via HTTP. Finally, the Compliance Management Service serves as a pluggable middleware that may be used to integrate other process execution engines.

For testing the framework, we edited BPMN 2.0 choreography and collaboration models using Signavio and exported them to the C3Pro framework as XML files. Examples are extended with GCRs, which are then decomposed into derived assertions using Algorithm 1. To this endeavor, mainly the CME, PME and the compliance management service were used.

In addition, the C3Pro framework was extended with a novel eCRG model checker that was published on github. Its command line interface enables the specification and verification of both global and local compliance rules (GCR and LCR) as well as process models and choreographies. In particular, the eCRG model checker supports the verification

---

First Author et al.: Preprint submitted to Elsevier
Verifying Compliance in Process Choreographies

- GCR decompositions, i.e., it allows verifying whether GCRs can be concluded from a given decomposition,
- local compliance, i.e., it allows verifying whether a single process model complies with a given compliance rule (CR), and
- global compliance, i.e., it allows verifying whether a process choreography complies with a given GCR.

Moreover, the eCRG checker enables the automated decomposition of tree-structured GCRs with a single antecedent.

In order to verify GCR decompositions and the various kinds of compliance respectively, the eCRG model checker translates global and local compliance rules as well as process models and choreographies into automaton, which are then combined and intersected. Depending on whether the resulting automaton is empty or not, the verification has been successful or a counter example trace has been produced. The eCRG model checker has been written in Java 8 on top of the dk.brics.automaton framework10.

7. Applicability

This section demonstrates and discusses how the presented decomposition algorithm can be applied in real-world settings. Here, a GCR may be imposed on process choreographies by external sources, e.g., considering regulatory documents such as the GDPR or standards such as ISO norms (63). A GCR may also reflect internal compliance rules expressing, for example, implicit dependencies between the partners that are crucial for (re-)scheduling the process activities for one partner or across multiple partners in the choreography. The visibility of activities and compliance rules in real-world settings depends on the contractual situation and the roles of the partners in the choreography. In supply chains in automotive domain, for example, an Original Equipment Manufacturer (OEM) might demand insights into certain specifics of the private processes of its suppliers and the connected (internal) compliance rules.

7.1. Use Cases

In the supply chain example presented in the Section 1, GCR C3 (cf. Fig. 2) reflects an externally imposed GCR on safety in manufacturing and logistics processes. GCR C1, in turn, might reflect an internal quality assurance rule that is solely verified by the Manufacturer, but is also made visible to the other partners in order to, e.g., create trust.

The real-world use case from manufacturing depicted in Fig. 13 demonstrates how the decomposition algorithms can be employed to lift implicit (data) connections to explicitly modeled assertions. The use case covers a process choreography between Partner 1 (i.e., a car manufacturer), Partner 2 (doing injection molding), and Partner 3 (i.e., the electro plater that coats parts in a correct color scheme). The choreography is designed and implemented using the CPEE (Cloud Process Execution Engine)11. Figure 13 shows the public activities of all partners, e.g., activity place order for Partner 1 and private activities, e.g., activity wait for order completion for Partner 1. The public activities send or receive messages, e.g., activity place order sends a message received by activity receive order. Note that the scenario abstracts from the details of the public and private activities, which are modelled as sub-processes activities. The underlying sub-processes are of different complexity, i.e., they might contain decisions and loops as well. The complex activity wait for order completion, in particular, comprises a set of sub-activities and is signifying the scheduling between the activities of the different partners.

During the design of the choreography the partners specified implicit connections, i.e., dependencies between (private) activities that are not covered by message exchanges and express mostly data dependencies. For example, activity wait for order completion (private, Partner 1) implicitly depends on the data produced by activities prepare for manufacturing, manufacturing of parts, and quality control (all private, Partner 2).

These implicit connections refer to two main “functions” of the manufacturing setting, i.e., (i) resource planning and (ii) quality control.

(i) Proper resource planning is part of the contract between the partners. There are implicit rules regarding how fast Partner 2 has to react to an order. This depends on assumptions how fast the stock drops for Partner 1. This

---

10https://www.brics.dk/automaton/

11https://cpee.org/
Verifying Compliance in Process Choreographies

Figure 13: Manufacturing Use Case

manifests as follows: If activity place order (Partner 1) occurs, then activity resource planning Partner 2 has been done before (i.e., resource planning data received) and activity resource planning (Partner 2) was based on activities put parts to stock and deliver until stock is low (Partner 1). Understanding this as a compliance task, we can say that when the above activity information matches, the compliant ordering can be ensured.

The question is how such implicit connections can be checked without revealing information on the private activities. Here, the presented decomposition algorithm can help. The idea is to express the implicit connections by GCR and verify them based on assertions. Take, for example, the implicit connection between private activities place order (Partner 1) and resource planning (Partner 2). We can formulate this implicit connection as GCR $C_1 : \text{place order} \rightarrow \text{resource planning}$

Using Algorithm 1, $C_1$ can be decomposed into the following assertions:

- $A^1_{C_1} : \text{place order} \rightarrow m_1$
- $A^2_{C_1} : m_1 \rightarrow \text{resource planning}$

Note that doing so, the implicit connection is lifted up to an explicit one by sending message $m_1$.

(ii) Consider now the more complex GCR covering the overall quality control that involves all three partners. Partner 1 has to do the final inspection, Partner 2 has to ensure the quality of the injection molded parts (no cracks, no holes), and Partner 3 has to ensure the quality.
Verifying Compliance in Process Choreographies

It is assumed that data for checking quality individually has been delivered whenever an order is finished. In this case, activity \textit{wait for order completion} by Partner 1 yields all information about the quality of the injection molded parts and the electroplating process, whereas during activity \textit{check electro-plated parts} by Partner 1 all additional information about the molding process is available. Overall, if activity \textit{check electro-plated parts} (Partner 1) occurs, then it has to be checked whether or not activities \textit{electro-plate parts} and \textit{quality control} by Partner 3 were executed. Before that, for activity \textit{wait for order completion}, activities \textit{prepare for manufacturing} (e.g. machine calibration data, material information), \textit{manufacturing of parts}, and \textit{quality control} by Partner 2 were executed. If all of the above information has been received, the manufacturing process was compliant, i.e., all required steps seem to have taken place.

7.2. Discussion

In the introduction, the following research question was stated:

\textbf{RQ: How to verify GCRs in a decentralized setting of a process choreography where no central coordinator with complete knowledge on the private and public tasks of all partners exists?}

In the following, we discuss how far the article at hand has addressed RQ and which open questions still remain. For this purpose, we sketch the end-to-end application of the decomposition algorithm along the following steps:

1. Check whether the GCR can be verified at choreography level, i.e., solely referring to interactions.
2. Check whether the GCR can be verified at the public process of one partner.
3. Check whether the GCR can be verified on the public processes of at least two partners: partners have to check for the absence/presence of GCR-related activities and activity orders based on choreography and interactions if possible. Otherwise, verification has to be postponed to the runtime by additionally synchronizing activities or compliance has to be verified in an ex post way based on logs if available.
4. Otherwise: The GCR refers to the private processes of one or several partners and a decomposition has to be applied.

As private activities and their dependencies are not visible to all collaborators, parts of the decomposition algorithm are executed locally by all partners involved in this GCR in order to identify possible transitive relations between their corresponding private activities and possible public activities, or interactions that replicate the connector where the GCR was split. This results in multiple derived assertion alternatives, which are then aggregated to alternatives from other partners in order to find a combination that recreates the original rule as described in Section 4 (cf. Example 1). Once the GCR is decomposed and the corresponding assertions are derived, each partner locally checks its derived assertions at runtime.

Overall, RQ has been addressed in breaking down the problem of GCR verification on distributed processes into the steps outlined above. Moreover, a sophisticated decomposition algorithm for GCR that refers to private activities of one or multiple partners has been provided. This enables distributed compliance verification for the supply chain and manufacturing use cases discussed in Section 7.1.

\textbf{Limitations and open questions:} This paper focuses on structural compliance, i.e., a GCR solely refers to control flow patterns. Compliance patterns that deal with, for example, data and resources (cf. (61)) are future work and will add substantially to the complexity of the approach. Moreover, we have applied our approach to a use case from the manufacturing domain. However, additional studies in other domains, such as healthcare and logistics, become necessary to evaluate the generalizability and broad applicability of the approach. In addition, the presence of \textit{XOR} branches in the processes (where sending of messages on these branches is optional) does not affect the correctness of the decomposition as long as the processes are \textit{compliable} with the original GCR (39). As aforementioned, we assume the soundness of the different process models (i.e., consistency and compatibility) and their compliability to the original GCR. This means that original GCRs are correctly specified, and the decomposition enables their checking in a distributed way. In this case, transitivity ensures correct decomposition of GCR even at the presence of XOR branches. If no transitive relations are identified, sync messages are required. Further on, in the end-to-end approach outlined above, Step 3 still offers the challenge on how to check GCR on public processes of multiple partners.
8. Related Work

The work presented in this article can be positioned at the interface between process choreographies and business process compliance. Section 8.1 summarizes basic works from these two research fields, whereas Section 8.2 discusses approaches that address issues at the interface between them.

8.1. Basic Research Fields

Section 8.1.1 gives backgrounds on process choreography research, whereas Section 8.1.2 summarizes basic works dealing with business process compliance.

8.1.1. Process Choreography

Process choreography research has mainly dealt with the modeling of process choreographies and the verification of correctness properties. For this purpose, specific choreography modeling languages like Let’s dance, Interaction Petri nets, and BPMN choreography diagrams are proposed, which support the modeling of collaborative process behavior. A particular focus of existing works has been put on correctness properties of choreography models (e.g., realizability), which have been intensively studied in literature (17; 16)–for an overview we refer interested readers to (62).

8.1.2. Business Process Compliance

Business process compliance, in turn, has been investigated for more than a decade and several surveys exist (e.g., (4; 24)). Contemporary approaches have focused on compliance rule languages, including visual notations (3; 40; 38), logic-based formalisms (45; 43), and Event Calculus (49). Moreover, several approaches enable compliance checking at both build- and run-time (e.g., (4; 44; 40)) or cover different process perspectives of compliance rule checking such as behavior, data, time, and resources (58; 40). Finally, characteristic patterns for business process compliance are proposed by (19).

8.2. Interface between Process Choreography and Process Compliance

There exist several approaches that address issues at the interface between process choreography and process compliance. Section 8.2.1 discusses centralized and distributed approaches for checking compliance in multi-party processes (i.e., process choreographies). In turn, approaches that map global contracts (i.e., sets of global compliance rules) to compliable process choreographies are presented in Section 8.2.2. The conformance between process choreography and local partner processes are considered in Section 8.2.3. Finally, issues related to business process compliance in the context of dynamically evolving business partner networks are discussed in Section 8.2.4.

8.2.1. Compliance Checking in a Process Choreography – Centralized vs. Distributed Approaches

Compliance checking mechanisms assuming a trusted party are proposed by (27). In (26) the same authors present a service-oriented approach that relies on a central integration platform in order to enable cross-organizational service interactions, while at the same time meeting global compliance rules. As opposed to our work, this approach relies on a central component (i.e., the integration platform) to ensure that global compliance rules can be checked.
Distributed approaches that rely on IoT technology are proposed by ([33]) advocates compliance checking in a distributed process (i.e., process choreography) as crucial, but it cannot be assessed in how far the approach deals with the restricted visibility and availability of process information as we do. In prior work, we have introduced the criterion of compliability ([39]) that captures the ability of a choreography to comply with a given set of compliance rules at all and how to check it ([35]). The approach presented in ([37]) enables checking the effects of changes on the compliance in process choreographies based on dependency graphs between global and local compliance rules as well as assertions. Finally, ([22]) provides an overview on the challenges, related approaches, and possible solutions at the interplay of compliance, change, and choreographies.

Distributed approaches that rely on IoT technology are proposed by ([51]; [48]). The approach suggested by ([51]) considers the flow of physical objects between the parties of a multi-party process. In particular, this approach exploits the sensing capabilities of smart devices to improve process compliance checking. For this purpose, commitments define mutual contractual relationships between parties in a declarative way and drive the configuration of smart devices, which check their satisfaction and, in case of misalignment, inform the concerned parties timely.

This multi-party process compliance monitoring approach is conceptually enhanced by ([48]) through IoT-enabled artifacts. This approach proposes a decentralized solution switching from control- to artifact-based monitoring, where physical objects can monitor their own conditions as well as the process activities in which they participate, i.e., compliance monitoring is distributed among the physical artifacts interacting with the global process. To instruct these smart objects, BPMN process models are translated into a set of artifact-centric process models, rendered in Extended-Guard-Stage-Milestone (E-GSM) notation. In particular, this work shows that artifact-based modeling approaches have a high potential in respect to multi-party process management involving physical objects, which has not been the focus of our work.

Finally, ([46]) discusses legal, organizational, human-centered, technical and economic challenges to be tackled in the field of business process compliance when enacting the (cross-organizational) business processes on the Ethereum blockchain. For example, at the implementation level, the immutability of illegal content or the error-proneness and zero-defect tolerance of smart contracts raise challenging issues in this context. Although this work does not deal with a concrete compliance verification approach, it indicates directions for future research on process compliance when using blockchain infrastructures for enacting multi-party business processes.

8.2.2. Mapping Global Contracts to Process Choreographies

Contract languages allow specifying obligations, permissions and prohibitions in business contracts, which govern the interactions between business partners. ([28]) provides means to model corresponding contract constraints. An early approach that extends choreographies with such contract constraints is provided by ([5]). This approach transforms the contract constraints into expressions of a choreography language, i.e., contract terms are translated into choreography expressions that govern the global process (i.e. choreography) to ensure compliance. In particular, it is shown how cross-organizational business processes can be monitored and enforced according to business contract specifications through the transformation of the contract definition to constraints on (global) process behavior. However, this approach is less powerful than ours as it tightly couples compliance constraints with choreography models, which aggravates the evolution of both choreography model and contract constraints. Besides, this approach does not consider local compliance checking (i.e., locally checking assertions derived from the decomposition of global compliance rules), which limits its applicability at the presence of more complex compliance requirements.

([31]) advocates Dynamic Condition Response (DCR) Graphs for decomposing global contracts into local processes. More precisely, ([31]) shows how a timed DCR Graph can be used to describe the global contract for a timed multi-party process (i.e., choreography), which can then be distributed as a network of communicating timed DCR Graphs (i.e. local processes) describing the local contract for each party. As opposed to our work, this approach relies on a declarative process modeling approach with a focus on discrete time deadlines.

8.2.3. Conformance between Process Choreography and Local Partner Processes

Several proposals have been made to ensure conformance between choreography (i.e., the global process) and the local processes of the involved business partners. In ([1]), conformance checking of the event logs of local processes against a given choreography model is addressed. As such an event log is not available at design time, ([43]) relies on a graph transformation tool–GROOVE (GRaphs for Object-Oriented Veriﬁcation)–to automatically verify that a local process of a partner involved in a choreography complies with the globally speciﬁed behavior of that choreography. LTL semantics of the choreography model is employed and token semantics of the local process model, which is expressed in terms of a BPMN collaboration diagram, is used to verify conformance.
Verifying Compliance in Process Choreographies

(9) relates the theory of contracts with the notion of choreography conformance, i.e., it is checked whether an aggregation of services correctly behaves according to a high level specification of their possible conversations. For this purpose, a method based on the composition of choreography projection and contract refinement is presented that allows verifying that a service with a given contract can correctly play a specific role within a choreography. Finally, (14) presents an approach for ensuring conformance between a set of BPMN collaboration diagrams (i.e., local process models) and a BPMN choreography diagram (i.e., choreography model).

As opposed to these approaches, our decomposition-based method verifies the compliance of a choreography model with global compliance rules and regulations that cover multiple process perspectives. However, conformance between the choreography and the participating partner processes can be considered as a prerequisite of our approach.

8.2.4. Ensuring Compliance in Dynamically Evolving Partner Networks

(64) assumes that the partners in a business networks try to provide wrong information and, hence, introduce the notion of accountability. Compliance requirements also need to be met in dynamic business networks (12; 13). In such a network, the partners may join and leave the collaboration dynamically and tasks over which compliance rules may be specified then have to be distributed or delegated to new partners or be backsources by network participants in order to avoid compliance issues. In (12; 13), a conceptual model for aligning the compliance requirements in a business network with the monitoring requirements they induce on the network participants, particularly when the network changes or evolves, is presented. Various techniques (e.g., task delegation and in-house back sourcing) for ensuring the consistency between the monitoring and compliance requirements as well as metrics for evaluating the status of a collaboration in respect to compliance monitorability are discussed. Obviously, this approach lacks a process perspective, but is complementary to our work with a focus on business network changes and their effects on compliance requirements.

9. Conclusions

The interplay between interoperability and business process compliance poses a tremendous challenge on companies. In this problem space, the work at hand addresses the question on how to verify global compliance rules (GCR), i.e., rules that span multiple partners in a multi-party process (i.e., process choreography), in a decentralized manner where certain tasks of one partner process might not be visible to the other partners due to confidentiality reasons. The presented approach focuses on the decomposition of a GCR such that the decomposed parts, i.e., assertions, can be checked by the partners locally. Consequently, compliance verification is shifted from a global to a decentralized manner.

The presented decomposition approach addresses research question RQ, which we introduced in Section 1. In particular, the presented decomposition algorithms exploits transitivity properties of the GCR for finding the correct decompositions. The correctness is formally proven. Moreover, the complexity of the decomposition algorithm is formally analyzed and also illustrated based on specific scenarios. The feasibility of the decomposition algorithm is shown based on a prototypical implementation, including a model checker for ensuring decomposition correctness. The applicability of the approach is demonstrated through a use case from the manufacturing domain.

Future work targets at two directions, (1) GCR language and (2) applications. First, we want to extend the decomposition based on the eCRG formalism, as used in this work, to arbitrary GCR and adapt the decomposition to other compliance rule languages such as Declare (55), PENELOPE (25), or BPMN-Q (3). Second, further applications of the approach include healthcare as interoperability and compliance are “strategic imperatives” in this domain. Overall, the presented approach provides a fundamental brick in enabling process collaborations between different partners by infringing neither their privacy nor any regulations.

Acknowledgment

This work is jointly supported by COMET SBA-K1 and the Austrian Research Promotion Agency (FFG) via (i) project number 874019, and (ii) the "Austrian Competence Center for Digital Production" (CDP) under contract number 85418. We thank Juergen Mangler for his input on the manufacturing use case.
Verifying Compliance in Process Choreographies

References


