Compliance Checking of Collaborative Processes for Sustainable Collaborative Network

Oyepeju Oyekola, Lai Xu, Paul Devrieze

Oyekola O., Xu L., de Vrieze P. (2021) Compliance Checking of Collaborative Processes for Sustainable Collaborative Network. In: Camarinha-Matos L.M., Boucher X., Afsarmanesh H. (eds) Smart and Sustainable Collaborative Networks 4.0. PRO-VE 2021. IFIP Advances in Information and Communication Technology, vol 629. Springer, Cham. https://doi.org/10.1007/978-3-030-85969-5_27

Compliance Checking of Collaborative Processes for Sustainable Collaborative Network

Oyepeju Oyekola, Lai Xu, Paul de Vrieze

Computing and Informatics, Bournemouth University, Poole BH12 5BB
Bournemouth, United Kingdom
{ooyekola,lxu,pdvrieze}@bournemouth.ac.uk

Abstract. Coronavirus pandemic has changed our lives and is likely to have a lasting impact on our economic development, i.e., industry and services. Most organisations must change their businesses and services to comply with the strategies and rules published by the governments of different countries for providing agility, sustainability, and resilience in the current situation. Non-compliance can result in an organisation paying a considerable sum of money in fines and litigation. In Collaborative Networks 4.0 (CN4.0), the importance of compliance is even more evident as its issue becomes more complicated when it involves collaborative processes due to its design principles for decentralized decision-making. The Collaborative Processes in CN 4.0 imply the collaborative business process and their relevancy in industry 4.0, i.e., the collaborative processes through Enterprise Resource Planning (ERP) and Manufacturing Execution System (MES). In this paper, we adopt two motivating use cases, define some of the regulatory requirements that govern the execution of each process, and then evaluate each process with the current compliance checking approaches. Based on this, we identify the challenges of compliance checking of collaborative processes, formalized as requirements needed to support the compliance checking of collaborative processes at design and running time, respectively. This paper further explores how the FIWARE architecture supports the automated compliance checking solution of collaborative processes in industry 4.0.

Keywords: Collaborative Processes, Collaborative Networks, Compliance, FIWARE, Business process, Industry 4.0

1 Introduction

Compliance is a big deal in today's business world, costing organizations a considerable sum of money in fines or litigation in case of non-compliance. As a result, compliance checking has become an inevitable step for organizations. The term compliance checking in this paper means the process of checking whether a business process complies with applicable policies and regulations [1]. The importance of compliance checking is even more evident as its issues become more complicated when it involves collaborative processes. The Collaborative Processes in CN 4.0 imply collaborative business processes and collaborative processes in the context of

industry 4.0. The current trend in digital transformation and market demand has presented an environment where organizations establish business collaboration between diversified and geographically distributed organizations to achieve a shared goal quickly and cost-effectively [1]. This concept has also created an environment for Small and Medium Enterprises (SMEs) to collaborate and compete with top-rated organisations. Achieving compliance in such a dynamic and networked environment is complex and challenging due to its design principle for decentralized decision-making. For instance, Collaborative processes present a unique attribute, such as the need to conform with security and privacy requirements, the need to comply with the regulatory requirement as a cross border process, the need to support data flow among partners, as well as the need to conform to the frequent changes in policies and regulations continuously, presents a unique challenge.

Most works on compliance checking are mainly structured for a single organisation process using different approaches and techniques. In contrast, compliance checking for collaborative processes is still sparse in the literature. Few works like [2], [3] that address the compliance checking of collaborative processes still lack full support to address the different phases of the process life cycles, i.e., control, data, time, and resource perspectives at both designs and run time[1]. Considering this, we justify the need to support the automated compliance checking of collaborative processes with varied regulatory requirements at all phases of the process life cycle at both design and runtime. Having such an automated compliance solution helps to reduce cost, avoid starting from scratch, wasting time and resources in creating new processes each time policies or regulations change.

To achieve compliance in such a dynamic environment, first, this paper adopts two motivating use cases to interpret the concept and complexities of the current compliance approaches in supporting compliance checking in collaborative processes. Second, we identify the challenges as requirements needed to support compliance checking of collaborative processes at both design and running time. Third, since the paper considers the compliance of collaborative processes in industry 4.0, we propose designing the compliance checking solution based on FIWARE architecture.

The rest of the paper is described as follows: section 2 presents two motivating use cases and their applicable policies and regulations. Section 3 uses the motivating use cases to explain some challenges in expressing compliance rules in collaborative processes. Finally, in section 4, a conceptual architecture is provided to design a solution that incorporates the identified challenges based on FIWARE.

2 Motivating Use Cases

This section presents two motivating use cases and their applicable policies and regulations that include internal policies, external regulations, and contractual obligations among partners. Section 2.1 describes the Collaborative Business Process (car insurance case), and Section 2.2 describes the collaborative process between the business process and manufacturing processes in the context of industry 4.0 (Car Assembly case).

2.1 Car Insurance Case

The car insurance case is adapted from the original work [4]. The collaborative business process involves five different partners, as shown in **Fig 1**. The process starts with the policyholder who owns the insurance policy and reports any damage to the issued car. Euro Assist is the company that registers the claim received from the policyholder via the telephone and encourages approved garages. AGFIL is the insurance company that underwrites the car policy and decides whether the reported claim is valid or not. If the claim is valid, AGFIL will make payment to all parties involved. Lee Consulting Services (CS) works on behalf of AGFIL and manages the day-to-day emergency service operation. Lee CS access and determine whether the car requires an assessor after the assigned Garage estimated the repair cost, i.e., an assessor would be assigned to assess the damage of the car only when the repair cost exceeds a certain amount. They control how quickly garages will receive payment, as all invoices received from the Garage are sent through Lee CS, and further present the invoice to AGFIL to process the payment while ensuring that repair figures align with industry norms. The approved garages are then responsible for repairing the car after Lee CS has agreed upon the repair. The repair work must be carried out quickly and cost-effectively.

Table 1 summarizes related policies and different requirements reflect in the car insurance case. For each requirement mentioned in Table 1, we analyzed what the current compliance checking approach could potentially address and its limitations in expressing some of the requirements.

Table 1. Policy requirement for car insurance

ID.	*Compliance Requirement*	*Sources*	*Categories*
Rq.1	The Garage must receive payment for all invoices within a specific period.	Contractual Obligation	Control, process time
Rq.2	AGFIL must check the policy's validity, and if it is invalid, it must be left a void.	Internal policy, Contractual Obligation	Control, Data
Rq.3	Each partner process must conform to the principle of privacy, and data access must be granted only on a justifiable need to complete a specific task.	GDPR, Contractual Obligation	Data

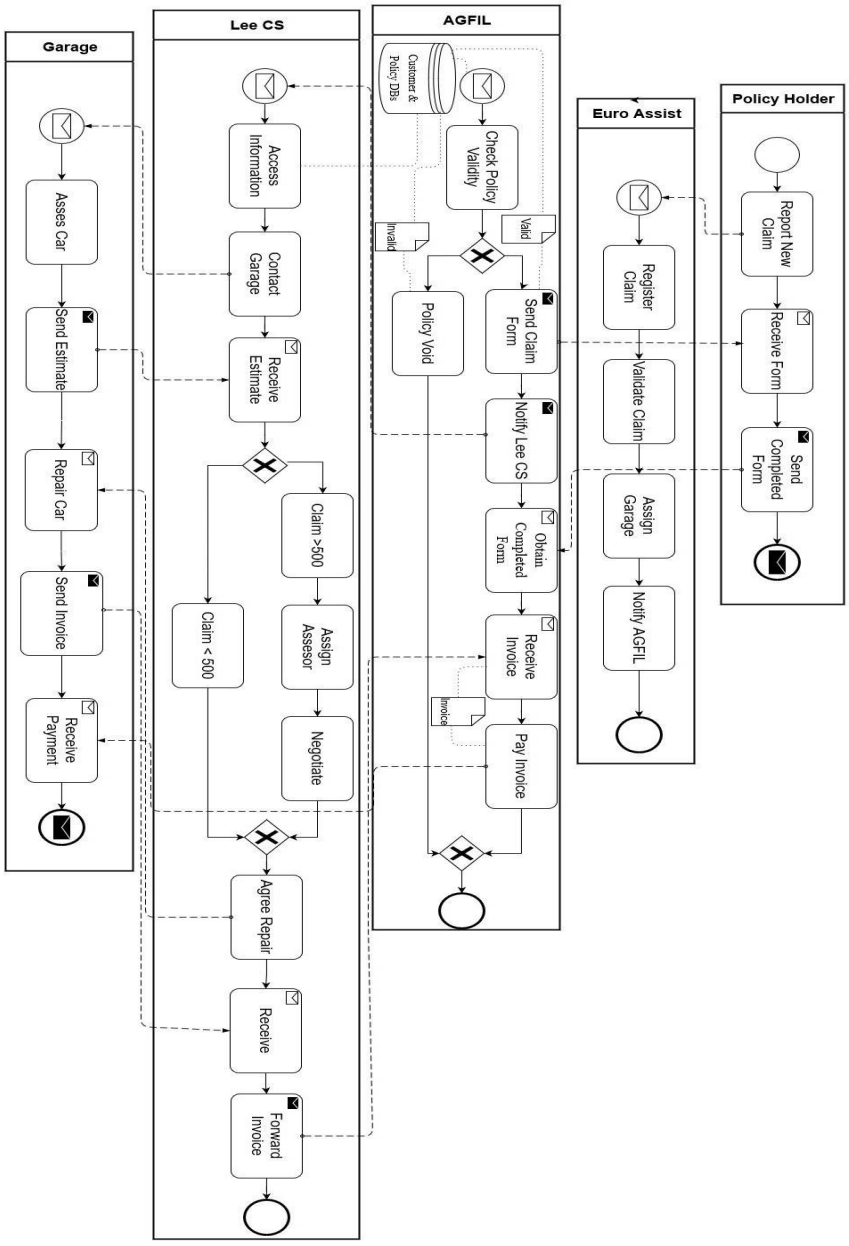

Fig 1. Car Insurance Case

2.2 Car Assembly Case

The car assembly process case is adapted from [5]. The assembly process of these cars requires a collaborative process involving mixed actor types (human and robot) to produce different types of cars with different configurations based on each customer preference assembled in the same production line. Compared to conventional factories, where humans and robots are separated in workspaces to prevent humans from entering a hazardous area, the robotic system's operating state could pose a danger to humans [6]. The process has significantly changed with technological advancement in achieving flexible, efficient, and intelligent manufacturing, i.e., the concept of Industry 4.0, bringing about new forms of collaborative networks. This change has brought about humans and robots working together on the same production line, where the safety situation on the shopfloor is controlled by sensors and possibly signals in a dangerous situation. The car assembly process must comply with several rules and regulations. These include the organization's internal policy and industry regulations, such as the International Standard ISO 10218 that incorporate safety in industrial robotic environments described in **Table 2.**

Table 2. Policy and Regulatory Requirement for Car Assembly case

ID.	*Compliance Requirement*	*Sources*	*Categories*
Rq.4	The process must comply with the safety standards and regulations	External Regulations - ISO 10218	Control, Resources
Rq.5	The process must meet up customer demands within a specified time.	Internal policy	Control, process time

3 General Findings and Idea

This section uses the motivating use cases described in section 2 to further interpret the concepts and complexities of the compliance checking of collaborative processes. For each requirement mentioned in **Table 1** and **Table 2**, we analyze what the exciting compliance checking approach could potentially address and its challenges in expressing some of the compliance rules in collaborative processes.

Car Insurance Requirement
For **Rq1,** since the collaborative processes involve multi partners, activities in such a process involve a high level of dependency and response between each partner activity. Any break in the precedence and response between activities is a violation. For example, if Garage does not receive the payment within the set time, then it is ideal to know which partner(s) is(are) the potential violator during the process execution. The compliance requirements require the activities of the different partners in the collaboration, which becomes impossible to check as each partner's private

activity cannot be viewed. And as a result, identifying the potential violator, in this case, might be tricky as any of the partners could be the potential violator. Expressing this type of rule is challenging as we cannot envisage that this violation will occur or when it will occur at runtime until it happens. The existing approaches do not support the preliminary specification of the future state of an action.

Rq.2, the existing compliance checking approach can check the conformance of this rule using data flow rules and conditional rules [7]. The requirement can be described such that the activity "Policy void" will only be executed when the data object "Policy" is in the state "Invalid" as a result of the execution of activity "Check policy validity." Thus, it ensures that a specific condition must always hold at the time an activity is executed.

Rq3 involves regulations with GDPR (General Data Protection Regulation) that require compliance with data privacy and addresses data transfer within the EU area. In the car insurance case, policyholder data is being accessed and processed between different partners. The reality is that each partner in the collaboration can be in different countries within the EU, and their ways of treating and managing customer data may be different. This means the same business function process can be specified in various forms in different countries. Conforming to privacy requirements in such instances remains challenging. The current work on access control and authorization mechanism [8], [9], [10] does not adequately address the existing complex and dynamic privacy requirements in collaborative processes environment. Therefore, checking data accessibility compliance needs to be context-aware. For example, at design time, the collaborative processes should be modeled as of which capabilities an actor should have to perform the task, which rights to access the data, how long the data can be access, what can be accessed when it can be accessed, and which part of the database can be accessed. At runtime, the roles should not allow access to specific data when they do not perform the activity. For instance, Lee CS should only be granted access to a single record per session of time a policyholder's details are needed to execute their tasks. This idea is a fundamental change from the traditional access control and authorization mechanisms that grant and authorize more access beyond what may be required and violate the data privacy principle.

Car Assembly Requirement

For **Rq.4, s**ince tasks are assigned to both humans and robots, it is necessary to check whether the assigned task to each actor is the right decision considering the safety, viability, or resource accessibility. For instance, when a task is scheduled to be executed by a human and robot simultaneously, a complete detailed description of the machine's condition and environment must be specified at design time and constantly monitored during execution, i.e., at runtime.

For **Rq.5,** each actor in the car assembly process can execute different tasks. These tasks must follow a strict schedule that must work flawlessly to meet customer demands on time. The delay in delivery schedule can tarnish the company's reputation and long-term customer relationship. Delay in delivery schedule can arise for different reasons. For instance, in a situation where the human actor assigned to complete a task is unavailable or in the event of machine failure, a task meant to be executed by a robot actor is passed to a human actor to perform manually. As such,

there is a possibility that the completion time will take longer than already planned, resulting in unplanned downtime and costs for the entire production line.

Based on **Rq**1-5, supporting collaborative process variability is essential and required; it makes it challenging to specify compliance constraints and collaborative process models. So, at design time, we can specify necessary and sufficient conditions for triggering certain activities. This implies that several deviations from the abstracted process can be specified at design time and allow the process model to be instantiated at the running time.

Also, time compliance needs to consider process variants i.e., dependency of activities, access rights, and different roles. The time compliance for the different process instances cannot always be constant. For example, when actors suddenly become unviable or safety conditions are not satisfied, the time compliance needs to be reflected. Accessibilities of resources may also be specified as temporal rules to support the control flow of the collaborative process model.

4 Proposed Solution based on FIWARE Architecture

With industry 4.0, business processes are collaborated among different factories and organizations to achieve flexible and effective handling of demands and the entire production life cycles. The collaborative processes are executed in a process execution environment, an integration system among the activities of ERP systems (i.e., ordering, inventory…), and MES (i.e., production planning, production) or other manufacturing systems [11], [12]. The process integration and collaboration through MES and ERP system require checking the compliance of predefined processes at design time, i.e., designing each process to comply with different rules before execution and continuously monitor process instances during execution. And since FIWARE offers scalable, flexible, and simple architecture that effectively manages dynamic collaborations, cost, product, and production life cycle [13], [14]. Then, to achieve compliance in industry 4.0, FIWARE architecture is adopted for the proposed compliance checking solution. The conceptual architecture describes how FIWARE could be extended to support the compliance checking of collaborative processes in industry 4.0, incorporating both design and runtime compliance checking, respectively.

The proposed Collaborative Process Compliance Checking solution based on FIWARE architecture is presented in **Fig 2**, consisting of three main layers. The lower layer entails the information systems, i.e., Manufacturing Execution Systems (MES), ERP system, design-time compliance checking module, CPS system, robots, equipment, (IoT) sensors in the shop floor. The second layer consists of the FIWARE Generic Enablers modules such as the FIWARE context broker, IDM & Access Control, IDAS IoT agents, Real-time media processing, different adapters, shopfloor map, mashup platform, runtime execution monitoring, database, and 3rd organizations. Lastly, the top layer includes the interfaces and dashboards for real-time monitoring.

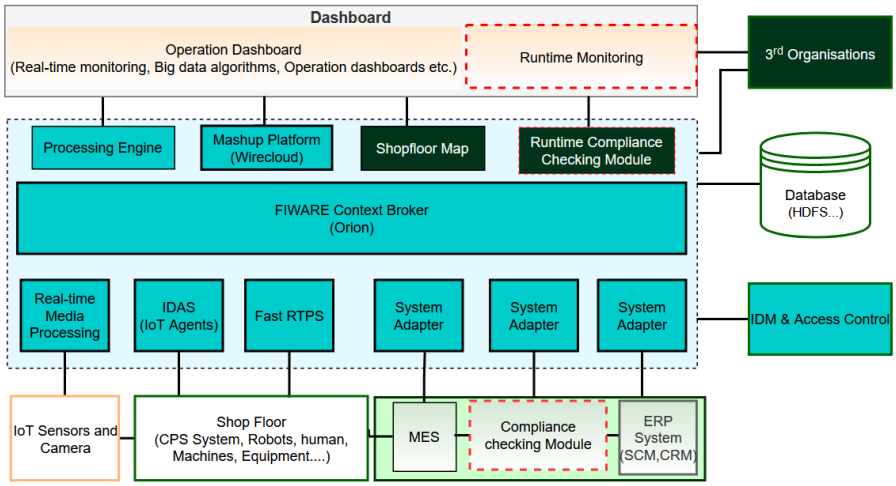

Fig. 2. Collaborative Process Compliance Checking Architecture based on FIWARE.

The proposed compliance check module (see the dashed box at the lower layer of **Fig 2)** is designed to handle the design time-related compliance checking and running time authorization before and during execution. The compliance checking module will be part of the process engine for integrating business management (ERP) and manufacturing operations (MES).

At design time, there are three primary modules involved in achieving compliance. The first module is the **Modeling and Specification module** and is further divided into three sub-modules. **(i)** The modeling of the manufacturing processes integrating the ERP system, MES, shop floor, and human interface using BPMN 2.0 populated by humans and various automated systems at the lower layer. This will include specifying several deviations from the abstracted process **(ii)** the elicitation and specification of compliance requirements sourced from internal and external regulations as well as contractual obligations among partners; then formalize these requirements into compliance constraints using a formal language that is expressive enough to capture all the requirements correctly. **(iii)** The compliance verification supports the process model and constraints; it serves as inputs for constraints and process models during the verification and storing verification results and feedback. The second module is the **Verification Service module** invoked during verification by submodule **(iii)** through an API. The Verification Service module consists of a process verification engine which employs different techniques and mechanism, like the simulation technique, compliance verification algorithms and the Process-Driven Access Control and Authorization (PDAC) mechanism [15]. The third module is the **Feedback and Reporting module**, which involves giving intelligent, appropriate, and comprehensible feedback to the end-user if any violations are detected.

After compliance has been checked at design time, the complaint process will start to initiate process instances as defined by the ERP, and MES then sends instructions to the shop floor as specified in the process model. But there is no certainty that the corresponding running process instance will be compliant during this time due to

human and machine-related errors [1]. This implies that after checking the compliance at design time and the actual execution of a process is initiated, it is crucial to constantly monitor the running process to detect any inconsistencies or deviant behavior. Therefore, a dedicated process engine will be used to track the system's behavior and occurrences of specific events during the process execution; The Runtime compliance checking module (see the dashed box at the middle layer of **Fig 2**) checks and identifies the undesired process behavior by comparing the actual behavior of the process instance with the expected behavior and alerts the end-users for any violations. The identified violations will then be displayed on the dashboard (see the dashed box at the top layer of **Fig 2**). The end-users then take appropriate measures actions to rectify the violations in case any violation is detected.

5 Conclusion and Future Works

Collaborative network 4.0 provides a rich concept to reshape industry digitalization. In this paper, the requirements to achieve compliance with collaborative processes at both design and running time are identified. The conceptual architecture for collaborative process compliance checking is presented. The development and implementation of our compliance checking solution are based on the FIWARE architecture and provides a service for Industry 4.0. Despite the different approaches of checking compliance in the literature, existing approaches are not sufficient enough to support the requirements imposed by the challenges of collaborative processes. Our ongoing work includes formalizing the process model and regulatory requirements using formal languages that are expressive enough to capture all the required requirements described in section 3 correctly. Then use techniques such as process simulation, algorithms, and PDAC to check for compliance. Lastly, we plan to implement the proposed compliance checking solution at both design and running time.

Acknowledgments. This research is part of the FIRST project that has received funding from the European Union's Horizon 2020 research and innovation programme, the Marie Skłodowska-Curie grant agreement No. 734599.

References

1. Oyepeju, O., L. Xu. Verification and Compliance in Collaborative Processes. In *Boosting Collaborative Networks 4.0: 21st IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2020*,.pp. 213-223. Springer, Valencia, Spain,(2020)
2. Bischoff, F., W. Fdhila, and S. Rinderle-Ma. Generation and transformation of compliant process collaboration models to BPMN. in International Conference on Advanced Information Systems Engineering. Springer. (2019).
3. Fdhila, W., Rinderle-Ma, S., Knuplesch, D. and Reichert, M. Change and compliance in collaborative processes" IEEE International Conference on Services Computing. Pp. 16-169. (2015).

4. Xu. L. A multi-party contract model. SIGecom Exchange. Pp.13-23. DOI: https://doi.org/10.1145/1120694.1120697. (2004).
5. Vanderfeesten, I., and P. Grefen, "Business process management technology for discrete manufacturing," in BETA publication: working papers, Technische Universiteit Eindhoven, (2015).
6. Robla-Gómez,S., V. M. Becerra, J. R. Llata, E. Gonzalez-Sarabia, C. Torre-Ferrero and J. J. I. A. Perez-Oria, "Working together: A review on safe human-robot collaboration in industrial environments," *IEEE Access,* vol. 5, pp. 26754-26773. (2017).
7. Awad, A., Weidtich, M., and Weske, M., "Specification, Verification and Explanation of Violation for Data-Aware Compliance Rules," in Service-Oriented Computing, 7th *International Joint Conference, ICSOC-ServiceWave*, pp. 24-27., (2009).
8. Wolter, C., and A. Schaad, "Modeling of task-based authorization constraints in BPMN," in *International Conference on Business Process Management*, (2007).
9. Gautam, M. Jha, S., Sural, S., Vaidya, J., Atluri, V. "Poster: Constrained policy mining in attribute-based access control," in *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, (2017).
10. Jin, X., R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering DAC, MAC and RBAC," in *IFIP Annual Conference on Data and Applications Security and Privacy*, (2012).
11. Erasmus, J, Vanderfeesteen, I., Traganos, K. and P. Grefen, "The Case for Unified Process Management in Smart Manufacturing," in *IEEE 22nd International Enterprise Distributed Object Computing Conference*, (2018).
12. Jaskó, S., A. Skrop, T. Holczinger, T. Chován, and J. Abonyi, "Development of manufacturing execution systems in accordance with Industry 4.0 requirements: A review of standard-and ontology-based methodologies and tools.," *Computers in industry,* vol. 123, p. 103300, (2020).
13. Sang, G.M, de Vrieze, P. and Yuewei, B. "Towards Predictive Maintenance for Flexible Manufacturing Using FIWARE," in *Dupuy-Chessa S., Proper H. (eds) Advanced Information Systems Engineering Workshops. CAiSE 2020. Lecture Notes in Business Information Processing*, 2020.
14. F. Catalogue, "FIWARE," 2020. [Online]. Available https://www.fiware.org/developers/catalogue/.. [Accessed 12 April 2021].
15. Kasse, JP, L. Xu, P. de Vrieze, and Y. Bai, "Process-Driven Access Control and Authorization Approach," in *Fourth International Congress on Information and Communication Technology*, (2020).