Choreographic Automata: A Case Study in Healthcare Management

Published Version:
Pal, S., Lanese, I., Clo, M. (2024). Choreographic Automata: A Case Study in Healthcare Management. GEWERBESTRASSE 11, CHAM, CH-6330, SWITZERLAND : Springer Science and Business Media Deutschland GmbH [10.1007/978-3-031-62697-5_1].

Availability:
This version is available at: https://hdl.handle.net/11585/997979 since: 2024-12-03

Published:
DOI: http://doi.org/10.1007/978-3-031-62697-5_1

Choreographic Automata: A Case Study in Healthcare Management

Sourabh Pal[1][0000−0001−6604−387X], Ivan Lanese[1][0000−0003−2527−9995], and Luca Cisbani[2]

[1] Olas Team, University of Bologna/INRIA, Bologna, Italy
{sourabh.pal2,ivan.lanese}@unibo.it
[2] Area ICT e Transizione digitale dei servizial cittadino - Direzione Generale Cura della Persona, Salute e Welfare - Regione Emilia Romagna, Italy
luca.cisbani@regione.emilia-romagna.it

Abstract. Choreographic models in general, and Choreographic Automata (CA) in particular, can be used to analyze and validate communicating systems. We applied CAs to a case study in healthcare management, the procedure for accreditation and authorization of public and private healthcare structures in the Emilia Romagna region (Italy). We formalized the procedure first using BPMN as intermediate step, and then using CAs. The tool Corinne showed a few issues in the formalized model, but it turned out that such issues were due to too strict requirements posed by the underlying theory. Upon weakening the requirements of Corinne with support for dynamic join from the literature, the case study was successfully validated.

Keywords: Choreographies · Healthcare management · Modeling · Communicating systems.

1 Introduction

Choreographic models are gaining popularity in the design and implementation of distributed systems in different domains [1] e.g., healthcare systems [2]. Choreographic approaches are used to holistically describe the interactions among components in message-passing systems (MPS), and enable to ensure by construction relevant communication properties such as deadlock-freedom. Choreographies provide two complementary views, i.e., the *global view* and the *local view*. The global view is the abstract description of the entire system, i.e., it consists of all the participants and describes their interactions from a global viewpoint. On the contrary, the local view represents the behavior of a specific participant and the message exchanges involving this participant. The global view is useful to design a system, while local views are more relevant in the implementation phase. Given a global view, it is possible to automatically generate local views enacting the global behavior.

In this paper, we will use Choreography Automata (CAs) [3], which combine the choreographic approach with the visual representation and the mathematical theory of finite state automata. We will apply CAs to a case study from healthcare administration, namely the procedure for accreditation and authorization of public and private healthcare structures in the Emilia Romagna region (Italy).

Since the case study we consider is defined in natural language, formalising it directly as CA is not easy. We found a suitable intermediate step in the Business Process Modelling Notion (BPMN) [4]. BPMN is a semi-formal graphical notation for describing business processes, and it is more flexible than CAs. Such flexibility allows for more easy modeling and easier interaction with domain experts. Then, one can refine the BPMN description to derive a CA, more suitable for the automatic analysis of communication properties.

For the analysis, we will exploit the tool Corinne [5, 6], which allows one to analyze CAs represented in the DOT format [7]. On the one hand, this will allow us to verify that the protocol considered in the case study satisfies relevant communication properties. On the other hand, this will allow us to verify also whether the expressive power of CAs and the related analysis techniques are suitable for applications in such a setting. Actually, our analysis showed that the theory implemented in Corinne (and aligned with most of the theories for choreographies in the literature, such as the ones surveyed in [8]) is too rigid, signaling as errors behaviours that are not problematic in practice. Indeed, it requires that if a participant is involved in some branch of a protocol, then it should be involved in all the branches. The rationale for this is that if a branch in which the participant is not involved is taken, then the participant is left waiting, possibly forever. However, in practice, participants are not waiting for interaction, but just react if they receive a request. In order to support and recognize as correct such behaviors, we extended Corinne with support for late join [9], which allows a participant to enter a conversation only if required to do so, e.g., only in some branch of a choice.

2 Case Study: Natural Language Description

Design and development of distributed communication systems is very complex. Therefore, researchers and practitioners consider the choreography approach suitable to verify the communication properties of distributed systems to avoid issues such as deadlocks at the design level of the software development [10, 11]. The key purpose of choreographies is to enact the principle of correctness-by-construction [10]. We will apply the choreographic approach to a case study on healthcare management. Health is a fundamental right of the individual. The Emilia-Romagna region provides regional health care services to protect the fundamental rights of their citizens. The Emilia-Romagna region ensures the quality, safety, and transparency of health services through the process of authorization and accreditation [12], defined by The Regional Law of 6 November 2019, n. 22 [13] for authorization and accreditation of public and private health structures.

The healthcare authorization procedure aims at ensuring the quality of healthcare services and assistance to the citizens. The authorization guarantees the structural, organizational, technological, and safety requirements of the patients in the public and private healthcare facilities in the Emilia-Romagna region in Italy. The authorization to operate the healthcare infrastructure is issued by the Mayor of the municipality. In contrast, the accreditation gives organizations, healthcare structures, and professionals, already in possession of healthcare authorization, the status of "subject suitable for providing services on behalf of the National Health Service". It provides for the possession of additional requisites that refer to the quality of health care and the related evaluation methods. It is granted by the Regional Coordinator of Authorization and Accreditation with subsequent verification of the Technical Accreditation Body aimed at ascertaining the possession or maintenance of the requirements. We have identified three protocols in this process, namely regional coordination for authorization and accreditation, authorization of health services, and accreditation of health services. In this case study, we will focus on the regional coordination for authorization and accreditation which assists in providing consistency and homogeneity in the exercise of the functionalities of authorization and accreditation processes. Thirteen participants are involved in this protocol, described below:

- General Directorate of Health (GDH): The highest authority in the process of authorization and accreditation, it instructs the other sub-ordinate participants to perform their tasks to ensure consistency between the authorization and accreditation, to maintain the organization rationalization, and to maintain the homogeneity to perform the functions.
- Regional Government (RG): It identifies the Regional Coordinator for authorization and accreditation among the managers of the services of the management to ensure homogeneity and consistency in the process.
- Regional Coordinator (RCOO): It is the main authority to conduct the different functions of healthcare organizations to issue authorization and accreditation.
- Authorization Commission (AC): It establishes itself in the public health departments of the local health unit to ensure the homogeneity in the assessment of authorization and it also identifies the priority of criteria to carry out checks for the authorization.
- General Manager of Health (GMH): It checks the issues of the healthcare organization for continuation of the accreditation to revoke or suspend all or part of the accreditation based on the seriousness of the issues found.
- Local Health Authority (LHA): It is the healthcare organization that is seeking authorization and accreditation.
- Registry Structure (RS): It stores the data for the accreditation and it provides the data upon request of RCOO.
- Technically Accrediting Body (OTA): It performs the accreditation checks to ensure impartiality, transparency, and autonomy in the activities of the management.
- OTA Manager (OTAM): It is a manager expert in assessing the quality of the healthcare management system.

- Evaluators (EV): They are qualified and trained professionals from the public and private national health services that are situated within the OTA to pursue the technical assessment of the accreditation.
- Expert Technicians (ET): They perform further technical investigations on the OTAM report for the accreditation.
- Regional Council (RC): On the proposal of the OTAM, the RC decides how to manage the EV.
- Verification Groups (VG): It coordinates with the OTA for the accreditation.

In a distributed communicating system, all the participants interact through message passing. In our case study, the RCOO will grant accreditation to the public or private LHA based on the verification of the OTA. The GDH notifies the RG to identify the RCOO among the managers of services and management. Subsequently, the GDH provides resources to the RCOO to perform their functions and it also instructs the RCOO to pursue verification of specific functions to evaluate the LHA for further continuation of the accreditation. The RCOO accomplishes coordination with the AC to check whether existing authorized healthcare authorities maintain prerequisites and additional requisites criteria to maintain the quality of healthcare. It also prepares plans for issuing, renewing, and monitoring accreditation and proposes it to the GDH. Moreover, it mandates the OTA to conduct verification to check whether existing authorized LHA are maintaining the prerequisites to provide safe health facilities. Besides, the OTA delegates the actual checks to an OTAM. The OTAM prepares the verification report of the healthcare institute and it also conducts further technical investigation on the report from the experts, such as EV and ET. Thereafter, the OTAM sends the report to the RCOO. The RCOO prepares the proposal for renewal, refusal, or issuing of the accreditation based on that report and submits it to the GDH to take the necessary action on the LHA.

3 BPMN Model of Case Study

Since the specification of our case study, described in the previous section, is given in natural language and hence necessarily informal, transforming it directly into a choreographic model is complex and error-prone. Therefore, we decided to model the protocol using a BPMN model, which is closer to the informal specification since they both focus on participants, activities and processes, while choreographies focus on message passing. However, moving to BPMN allows to move from informal to semi-formal specification, and to explicit introduce choices and message passing communications, key to then move to choreographies. The fact that BPMN representation is graphical and closer to the specification also allows more easy discussion with domain experts to ensure that the model actually captures the intended protocol. As a second step, we then converted the BPMN model into a choreography automaton to enable the verification of the correctness of its structure and behavior. We transformed the natural language description of the healthcare system into the BPMN model manually.

BPMN is a semi-formal specification with a wide variety of expressive and flexible features to ease the representation of complex systems. This section will present a fragment of our case study, available in Figure 1, to give to the reader an intuitioon about the transformation of our case study from natural language to BPMN specification. The whole case study model is available in [?]. The BPMN model consists of different participants [14] that represent a specific role or entity that is involved in a business process. Each participant has its own internal processes, and participants collaborate through the passing of messages. In our example in Figure 1, we present six participants ,namely RC, RCOO, OTA, OTAM, EV, and ET. The process diagram describes the details of a business process involving them. Moreover, it is the visual representation that gives a clear understanding of the flow of information and the sequence of activities of the business process. In the presented case study, we present the process diagram of the participant OTAM.

The participants communicate among themselves through the transfer of messages. Therefore, the *message event* (double circle containing an envelope) indicates the sending or receiving of a message from the current process to another process or participant. The OTAM is first involved in the protocol when the OTA appoints it for carrying out the accreditation checks. Therefore, the OTA notifies the OTAM to conduct checks on the previous authorization for accreditation through the message event.

A process is a collection of multiple tasks: in BPMN a single activity within a process is called a *task*. The OTAM, after receiving notification from the OTA, performs task **Request for Resources**, where the OTAM requires the RCOO to provide resources to perform its functions. Thereafter, the RCOO provides the required resources to the OTAM via a **Provide Resources** message. In BPMN, an *Exclusive Gateway or XOR Gateway* (diamond containing an X) is a decision gateway used to model a point in the process where the flow can take one of several mutually exclusive paths. The decision about which path to take is based on the evaluation of conditions associated with each outgoing sequence flow. The OTAM, after getting resources from the RCOO, checks whether the list of EVs exists. If it does not exist then it first creates the list of EVs to **Perform Technical Investigation**. In the case of the EVs already exist, needs to **Perform Technical Investigation** for accreditation or needs to **Update Evaluators** for assistance with the technical investigation for the accreditation. Here, we use an exclusive gateway to represent the choice of the path. The detailed explanations of the two paths are as follows:

- **Perform Technical Investigation:** The OTAM carries out the technical investigations, and expresses the technical judgment of competence by verifying the possession and maintenance of the accreditation requirements.
- **Update Evaluators List:** The OTAM holds and updates the list of EVs.

In the case of the technical investigation for the checks of authorization and accreditation, the OTAM needs assistance from experts such as EV and ET sequentially, as follows:

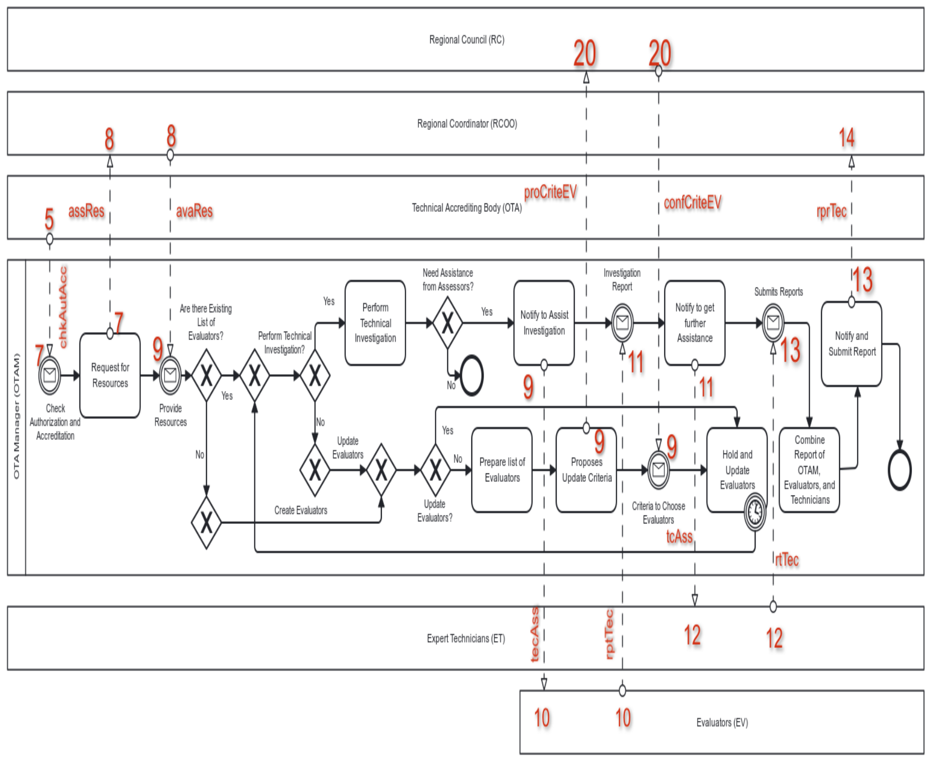

Fig. 1. BPMN: a fragment of our case study.

1. The OTAM performs the checks by making use of the EV. The OTAM **Notify to Assist Investigation** to the EV. The EV perform the technical investigation and submit to the OTAM the technical **Investigation Report** of checks of accreditation.
2. The OTAM, after receiving the investigation report from the EV, needs to perform further investigation with the assistance of the ET. Therefore, it **Notify to Get Further Assistance** to the ET. ET assists and **Submits Reports** to the OTAM.

The OTAM **Combine Report of OTAM, EVs, and ET** after performing all necessary checks for authorization and accreditation. Thereafter, it **Notify and Submit Report** to the RCOO and terminate the process. In the case of the **Create and Update Evaluators**, it performs the tasks sequentially i.e., **Prepare List of Evaluators**, **Proposes Update Criteria**, **Update Evaluators**. Moreover, the list of EVs gets updated periodically.

4 Choreography of the Case Study

We use Choreography Automata (CAs) [3] to model the message-passing behavior of our case study. This will allow us to verify the correctness of such behavior. The key concept of choreographic approaches is to describe the interactions among participants from a global viewpoint. In CAs, finite state automata are used, and a transition of the automaton models a message passing communication. More precisely, the interaction among two participants is represented as a label $A \to B : m$, where participant A sends message m to participant B, which in turn receives it [3]. In this section, we will discuss the transformation of our case study from BPMN model to CA.

We present the choreography automaton of our case study in Figure 2. To ease the comparison with the BPMN model, identifiers of states from the CA as well as labels of the transitions are also reported in the BPMN diagram, in red. Remember however that only part of the BPMN model is in Figure 1, while the whole model is in []. Let us start the description from the top. GDH proposes RG to identify a RCOO $GDH \to RG : fndCor$ to maintain consistency, organizational rationalization, and homogeneity of authorization and accreditation. Further, the GDH notifies the RCOO that resources have been assigned $GDH \to RCOO : assRes$ to execute the authorization and accreditation procedure. Moreover, the GDH requires the RCOO to perform the required functions $GDH \to RCOO : perFunc$ for accreditation. Afterward, the RCOO may take 4 alternative actions:

1. (loop involving state 6) to request the GDH for consultation to prepare a monitoring policy $RCOO \to GDH : chkPol$, which will trigger a reply from the GDH confirming the consultation $GDH \to RCOO : confChkPol$;
2. (leftmost path) to ask the AC to check an existing authorization $RCOO \to AC : chkAut$ of some healthcare structures for further continuation. The protocol will end with the response authorization report $AC \to RCOO : rptAut$ message to the RCOO;

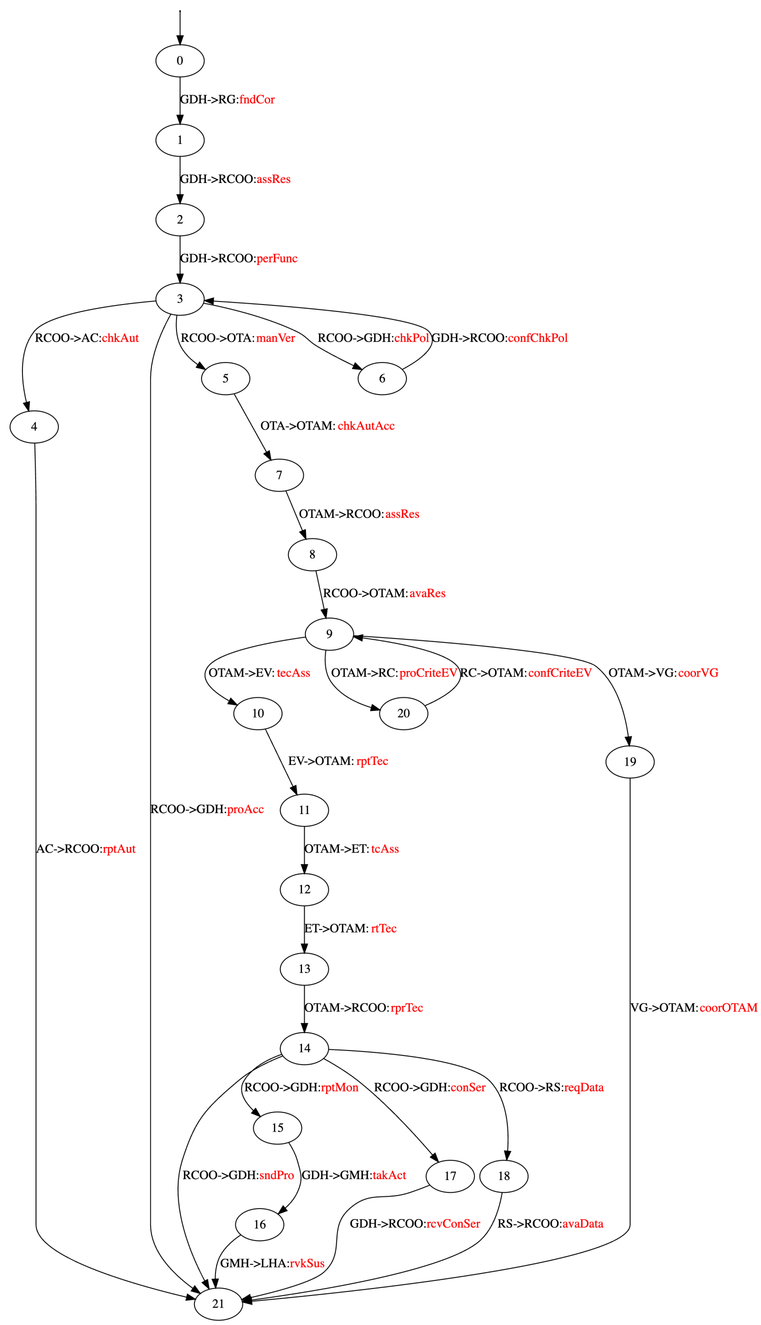

Fig. 2. Choreography Automaton for Regional Coordination for Authorization and Accreditation.

3. (transition to the final state) to propose to the GDH the regional planning for issuing, renewing and monitoring accreditation $RCOO \to GDH : proAcc$, ending then the protocol;
4. (transition to state 5) to ask the OTA to start the actual procedure for accreditation $RCOO \to OTA : manVer$.

In this last case, the OTA notifies the OTAM to check authorization and accreditation $OTA \to OTAM : chkAutAcc$ for checking the quality of the healthcare management systems of healthcare authorities (this starts the part represened in BPMN in Figure 1). The OTAM requests the RCOO to assign the corresponding resources $OTAM \to RCOO : assRes$, and the RCOO makes such resources available $RCOO \to OTAM : avaRes$ to the OTAM. Afterward, the OTAM may take 2 alternative paths: (1) (loop involving state 20) To manage the list of EVs: while this procedure is quite complex it is mostly local to the OTAM, hence we only have a loop composed by a pair of interactions, where the OTAM sends to the RC the proposal $OTAM \to RC : proCriteEV$ message about the criteria to manage the EVs, and the RC answers to the OTAM with message $RC \to OTAM : confCriteEV$ to confirm the proposed evaluation criteria; or else (2) the OTAM asks the EV for technical assistance with message $OTAM \to EV : tecAss$ and EV reply with a technical report $EV \to OTAM : rptTec$.

In the last case, after receiving the technical report from the EV, the OTAM performs a similar message exchange with the ET (messages $OTAM \to ET : tcAss$ and $ET \to OTAM : rtTec$). Note that from the informal specification it is not clear whether the two message exchanges should be sequential as in our model or concurrent. We will come back to this topic in the discussion. Further, the OTAM sends to the RCOO the results of the investigation with message $OTAM \to RCOO : rprTec$. The RCOO may react in 4 ways: (a) It requests the RS to give access to the data $RCOO \to RS : reqData$ relating to the operating methods to monitor its implementation and RS gives access to the data with $RS \to RCOO : avaData$ message by ending the protocol, or (b) It requests to the GDH to coordinate with the services related to the health matters with $RCOO \to GDH : conSer$ message and GDH responses to the RCOO with $GDH \to RCOO : rcvConSer$ message to end the protocol, or (c) It notifies to the GDH with $RCOO \to GDH : rptMon$ message of monitoring healthcare report based on the OTA report which further analyzes by the GDH and based on the seriousness of the violation of the requisites of the healthcare notifies to the GMH with message $GDH \to GMH : takAct$ to take necessary action whether to suspend or revoke the accreditation and inform to the LHA with message $GMH \to LHA : rvkSus$ whether the accreditation of that particular authority is revoke or suspended and end the protocol, or else (d) it notifies to the GDH with message $RCOO \to GDH : sndPro$ proposal for grant, renew, refusal, suspension, and revocation of the accreditation based on the report receive from the OTA and end the protocol.

5 Experimentation

We represented our case study in the form of Choreography which is a formal method used to represent the interactions, communication, and message-passing among different participants in distributed systems or concurrent systems. This choreography-based model is used for the specification of the communicating systems to represent how different participants coordinate and communicate with each other. More specifically, this model can be utilized in different ways i.e., specification of global and local behavior, understanding the communication protocols in distributed systems, system correctness for concurrency and parallelism, and standardization of distributed systems. We analyze the verification of behavioral properties such as deadlock freedom of g-choreographies of our case study in this paper. The correctness of our case study was verified using the choreography methodology based on well-formedness [3]. The well-formedness ensures that the communicating systems are well-behaved provided that they satisfy some conditions of the q-span. A pair (π, π') of pre-candidate q-branches of CA is a q-span if

1. either π and π' are cofinal, with no common node but q and the last one;
2. or π and π' are candidate q-branches with no common node but q;
3. or π and π' are a candidate q-branch and a loop on q with no other common nodes.

A communicating system will be well-formed if it satisfies the following two conditions of the above q-span:

– **Well-branchedness:** A c-automaton CA is well-branched if for each state q in $det(CA)$ and $A \in P$ sender in a transition from q, all of the following conditions must hold:
  1. all transitions from q involving A, have sender A;
  2. for each transition t from q whose sender is not A and each transition t' from q whose sender is A, t and t' are concurrent;
  3. for each q-span (σ, σ') where A chooses at and each participant $B \neq A \in P$, the first pair of different labels on the runs $\sigma \downarrow_B$ and $\sigma' \downarrow_B$ (if any) is of the form with $(CB?m, DB?n)$ with $C \neq D$ or $m \neq n$.
– **Well-sequencedness:** A c-automaton CA is well-sequenced if for each two consecutive transitions $q \xrightarrow{A \to B : m} q' \xrightarrow{C \to D : n} q''$ either
  - They share a participant, that is $\{A, B\} \cap \{C, D\} \neq \emptyset$, or
  - They are concurrent, i.e. there is q''' such that $q \xrightarrow{C \to D : n} q''' \xrightarrow{A \to B : m} q''$

Therefore, a synchronous communicating system, when represented as a choreographic automaton, is well-formed if it satisfies the above conditions. If these conditions are satisfied then the system is guaranteed to be deadlock-free (as well as to enjoy other behavioural properties). There is an available tool named Corinne [5] to verify the correctness of a synchronous communicating system using the approach above. We used this tool to analyse our case study in this paper. We conduct our experimentation regarding the well-formedness of our case study to verify the deadlock freedom of the distributed message-passing system. The well-formedness is the conjunction of the well-sequencedness and well-branchedness. We consider the above-mentioned theory as our baseline approach to identify the well-formedness of our case study. We use the Corinne tool to analyze the well-formedness of our case study. To simplify the analysis, we also slightly extended the tool. In case the system contains many violations of the conditions, Corinne only showed the first one. We extended the tool so that all the violations of the well-formedness were shown in a single execution.

Our case study satisfied well-sequencedness, but not well-branchedness, since in some cases a participant was involved only in some branches of a choice, and did not occur at all in others. This is flagged as an issue by Corinne, but it is allowed in some related theories such as dynamic theory of well-branchedness i.e., asserted choreography automata [9] because Corinne is implemented based on the baseline theories of well-formedness to validate the correctness of the systems. We will explore the above-mentioned baseline theories in our case study and identify the reason for successful or failure of the Corinne tool in our proposed case study because the Corinne is implemented based on the baseline theories. The analysis of well-sequencedness and well-beanchedness is detailed below:

Well-Branchedness (1^{st} Condition): A communicating system is well-branched if each participant of a q-state works as either sender or receiver. More specifically, if a participant works as both sender and receiver then the q-state is not well-branched. In our case study in Fig. 2, there are no transitions from a q-state where a participant works as both sender and receiver. We can consider some of the q-branches from the q-states 3 and 7 for the analysis of our study. The analysis of the 1^{st} Condition of the Well-Branchedness from q-state 3 and 7 is given below:

- **Fron q-state 3:** There are four possible transitions from the q-state 3 i.e., $3 \rightarrow 4$, $3 \rightarrow 5$, $3 \rightarrow 6$, and $3 \rightarrow 21$. The participants work as sender {RCOO} and as receiver {AC, OTA, GDH}. There are no common participants among the participants of the sender and receiver which means that the participants are solely involved as either sender or receiver. Therefore, it is well-branched from the q-state 3.
- **Fron q-state 7:** There is only one possible transition from the q-state 7 i.e., $7 \rightarrow 8$ because q-state 7 is singleton [9]. The participants work as sender {OTAM} and as receiver {RCOO}. Both participants are different which means the participants from the sender and receiver are not the same. Therefore, it is well-branched from the q-state 7.

In our case study, there are no participants who work as both sender and receiver as mentioned in the above example. Hence, our case study satisfied the 1^{st} Condition of the Well-Branchedness. We have shown two examples of it above for two conditions i.e. for the single transition from a q-state and multiple transitions from a q-state. Both cases satisfied the baseline condition of the well-branchedness. Therefore, it also satisfies this condition at the Corinne tool.

Well-Branchedness (2^{nd} Condition): A communicating system is well-branched if all transition from a q-state has the same sender participant. There could be single or multiple transitions from a q-state. In the case of a single transition from a q-state, there must be only one participant who works as the sender. Additionally, in case of multiple transitions from a q-state, there must be one sender participant for all transitions. We can consider two q-states 14 and 19 from our case study in Fig. 2 for our analysis below.

- **Fron q-state 14:** There are multiple transitions from the q-state 14. There are four possible transitions from the q-state 14 i.e., $14 \rightarrow 15$, $14 \rightarrow 17$, $14 \rightarrow 18$, and $14 \rightarrow 21$. The participant work as sender for all the transitions is {RCOO}. Therefore, there is only one sender participant for multiple transitions from a q-state. Hence, this is well-branched from the q-state 14.
- **Fron q-state 19:** There is only one transition from the q-state 19 i.e., $19 \rightarrow 21$. The participant works as the sender for the transitions from the q-state 19 is {RC}. Therefore, there is only one sender participant for the single transition from a q-state due to the singleton properties of q-state 19, because there is only one transition from the state. Hence, this is well-branched from the q-state 20.

In our case study, no multiple participants are working as senders from the transition from a q-state. We have shown two examples of it above for two conditions i.e. for the single transition from a q-state and multiple transitions from a q-state. Both cases satisfied the baseline condition of the well-branchedness. Therefore, our case satisfies the 2^{nd} Condition of the Well-Branchedness. Therefore, it also satisfies this condition at the Corinne tool.

Well-Branchedness (3^{rd} Condition): A communicating system is well-branched if the receiver of the transition or message is not the same in the first pair of transitions for the runs of a q-span. This condition gives the error to our case study in the Corinne tool. Hence, the baseline theories of the 3^{rd} Condition of the Well-Branchedness condition could not satisfy our case study in the Corrine tool. We will analyze and discuss the reason behind not satisfying the baseline theories below. We will consider three q-spans from the q-states 3, 9, and 14 in Fig. 2 of our case study for the analysis below.

- **Fron q-state 3:** We can consider the two runs of the q-span from the q-state 3, i.e., $\sigma_1 = \{3, 6, 3\}$ and $\sigma_2 = \{3, 4, 21\}$ which satisfy the condition 2 of the q-span. Now, the transition between the first q-state of σ_1 and the second q-state σ_2 (i.e., $3 \rightarrow 4$) is $RCOO \rightarrow AC : chkAut$. The sender participant in this transition is RCOO which is the same for the first pair of transitions in the runs of this q-span i.e., in $3 \rightarrow 6$ and $3 \rightarrow 4$. Thereafter, the transition of the $3 \rightarrow 6$ and $3 \rightarrow 4$ are $RCOO \rightarrow GDH : chkPol$ and $RCOO \rightarrow AC : chkAut$ respectively. The receiving participants and messages for both transitions are not the same with respect to the receiving participant of the transition $3 \rightarrow 6$ i.e., GDH. Hence, the discussed q-span is not well-branched due to the participant GDH in the baseline theory of the 3^{rd} condition of the well-branchedness. We will further analyze whether our case study becomes well-branch in the case of the dynamic theory of well-branchedness i.e., asserted choreography automata. The RCOO is the common participant in the partition $3 \rightarrow 6$ and $3 \rightarrow 4$ from the q-stare 3. Moreover, RCOO is fully-aware because the first interaction of σ_1 and σ_2 are $RCOO \rightarrow GDH : chkPol$ and $RCOO \rightarrow AC : chkAut$ respectively which is not equal. Moreover, the branches σ_1 and σ_2 are part of the candidate q-branch because there is only one cycle in σ_1 and there are no cycles in the case of σ_2. Hence, this is well-branched with respect to asserted choreography automata.

– **Fron q-state 9:** We can consider the two runs of the q-span from the q-state 9, i.e., $\sigma_1 = \{9, 19, 21\}$ and $\sigma_2 = \{9, 10, 11, 12, 13, 14, 17, 21\}$ which satisfy the condition 1 of the q-span. Now, the transition between the first q-state of σ_1 and the second q-state σ_2 (i.e., $9 \rightarrow 10$) is $OTAM \rightarrow EV : tecAss$. The sender participant in this transition is OTAM which is the same for the first pair of transitions in the runs of this q-span i.e., in $9 \rightarrow 19$ and $9 \rightarrow 10$. Thereafter, the transition of the $9 \rightarrow 19$ and $9 \rightarrow 10$ are $OTAM \rightarrow VG : coorVG$ and $OTAM \rightarrow EV : tecAss$ respectively. The receiving participants and messages for both transitions are not the same with respect to the receiving participant of the transition $9 \rightarrow 19$ i.e., VG. Hence, the discussed q-span is not well-branched due to the participant VG in the baseline theory of the 3^{rd} condition of the well-branchedness. We will further analyze whether our case study becomes well-branch in the case of the dynamic theory of well-branchedness i.e., asserted choreography automata. The OTAM is the common participant in the partition $9 \rightarrow 19$ and $9 \rightarrow 10$ from the q-stare 9. Moreover, OTAM is fully-aware because the first interaction of σ_1 and σ_2 are $OTAM \rightarrow VG : coorVG$ and $OTAM \rightarrow EV : tecAss$ respectively which is not equal. Moreover, the branches σ_1 and σ_2 are part of the candidate q-branch because there are no cycles in σ_1 and σ_2. Hence, this is well-branched with respect to asserted choreography automata.
– **Fron q-state 14:** We can consider the two runs of the q-span from the q-state 14, i.e., $\sigma_1 = \{14, 21\}$ and $\sigma_2 = \{14, 18, 21\}$ which satisfy the condition 1 of the q-span. Now, the transition between the first q-state of σ_1 and the second q-state σ_2 (i.e., $14 \rightarrow 18$) is $RCOO \rightarrow RS : reqData$. The sender participant in this transition is RCOO which is the same for the first pair of transitions in the runs of this q-span i.e., in $14 \rightarrow 21$ and $14 \rightarrow 18$. Thereafter, the transition of the $14 \rightarrow 21$ and $14 \rightarrow 18$ are $RCOO \rightarrow GDH : sndPro$ and $RCOO \rightarrow RS : reqData$ respectively. The receiving participants and messages for both transitions are not the same with respect to the receiving participant of the transition $14 \rightarrow 21$ i.e., GDH. Hence, the discussed q-span is not well-branched due to the participant GDH in the baseline theory of the 3^{rd} condition of the well-branchedness. We will further analyze whether our case study becomes well-branch in the case of the dynamic theory of well-branchedness for late join of participant. The RCOO is the common participant in the partition $14 \rightarrow 21$ and $14 \rightarrow 18$ from the q-stare 14. Moreover, RCOO is fully-aware because the first interaction of σ_1 and σ_2 are

$RCOO \to GDH : sndPro$ and $RCOO \to RS : reqData$ respectively which is not equal. Moreover, the branches σ_1 and σ_2 are part of the candidate q-branch because there are no cycles in σ_1 and σ_2. Hence, this is well-branched with respect to asserted choreography automata.

We analyze some of the errors of the Corinne tool which occur due to the third condition of the well-branchedness. The reason of this error is that the Corinne tool is implemented based on the baseline theories of the well-branchedness but these errors do not occur in the case of the theories of well-branchedness of asserted choreography automata.

Well-Sequencedness: A communicating system is well-sequenced whenever there are two consecutive transitions whose sets of participants are not disjoint or there should be an alternative path where the two transitions are swapped. In our case study in Fig. 2, there are no consecutive transitions with disjoint sets of participants which satisfies the first condition of the well-formedness. The second condition of well-formedness is the concurrent transitions in case of multiple transitions from a participant but our system does not have any concurrent transitions. Let's consider q to be the state of c-automata in Fig. 2. We can consider some of the q-branches from the q-state for the analysis of our study between the q-states 2 to 5 and 14 to 21. Some possible branches of the q-state 2 and 14 are given below:

1. $\pi_a : 2 \xrightarrow{GDH \to RCOO : perFunc} 3 \xrightarrow{RCOO \to GDH : chkPol} 6 \xrightarrow{GDH \to RCOO : confChkPol} 3 \xrightarrow{RCOO \to OTA : manVer} 5$
2. $\pi_b : 14 \xrightarrow{RCOO \to RS : reqData} 18 \xrightarrow{RS \to RCOO : avaData} 21$
3. $\pi_c : 14 \xrightarrow{RCOO \to GDH : conSer} 17 \xrightarrow{GDH \to RCOO : rcvConSer} 21$

There have always been common participants for each two consecutive transitions in the q-branch π_a. It has three consecutive transitions such as $2 \to 3 \to 6$, $3 \to 6 \to 3$, and $6 \to 3 \to 5$ with common participant $\{GDH, RCOO\}$, $\{GDH, RCOO\}$, and $\{RCOO\}$ respectively. Therefore, the q-branch π_a is well-sequenced because it satisfies the first condition of the well-sequencedness. Additionally, there are no concurrent transitions in our case study. For instance, the q-branches π_b and π_c are the two different q-branches between q-states 14 and 21 but this is not a concurrent transition. This does not satisfy the condition of the concurrency because the transition between $14 \to 18$ (i.e., $RCOO \to RS : reqData$) is not equal to the transition between $17 \to 21$ (i.e., $GDH \to RCOO : rcvConSer$) and the transition between $14 \to 17$ (i.e., $RCOO \to GDH : conSer$) is not equal to the transition $18 \to 21$ (i.e., $RS \to RCOO : avaData$). Therefore, although there are multiple branches from a q-state in our case study that is not concurrency. Hence, the second condition of the well-sequencedness is not applicable. But the π_b and π_c satisfy the first condition of the well-sequencedness because consecutive transitions $14 \to 18 \to 21$, and $14 \to 17 \to 21$ with common participants $\{RCOO, RS\}$, and $\{GDH, RCOO\}$ respectively. Our choreographic model satisfies the baseline condition of well-sequencedness. Therefore, the Corrine tool-based verification of the correctness of well-sequencedness satisfies our choreographic model.

We have identified that our case study is well-sequenced but not well-branched in the case of the baseline theories of well-formedness. Although it satisfies the first and second conditions of the well-branchedness of the baseline theories but it does not satisfy the third condition of the well-formedness due to dynamic participants in the different branches of the q-span. Therefore, we conducted further analysis to verify whether our case study satisfies well-branchedness in the dynamic theories of well-formedness for the third condition of well-branchedness. We have found that our case study can be well-formed based on the dynamic well-formed theories.

6 Conclusion, Related and Future Work

In this paper, we have analysed the well-formed properties of the choreographic approach of communicating systems on the accreditation and authorization of the Healthcare Management System in the Emilia Romagna region of Italy. We consider the theories proposed by Barbanera et. al [3] as our theories by considering the baseline theory for the purpose of verification of the well-formedness because of two reasons i.e., 1) we use the available Corinne tool for the verification of the well-formedness which is implemented on the baseline theories. 2) As per our knowledge, this is the first available proposed theory of the well-formedness which excites us to utilize it to verify the well-formedness of our case study. The well-formedness is the conjunction of the well-branchedness and well-sequencedness. The results show that baseline theories satisfy the first and second conditions of the well-branchness and well-sequencedness. In contrast, it didn't satisfy the third condition of well-formedness due to the diverse participants and branches in the choreographic model of our case study. In order to support and recognize as correct such behaviors, we extended Corinne with support for late join, which allows a participant to enter a conversation only if required to do so.

Related Work. The distributed communication system brings complexity to the communicating protocols. The approach of specification and formalization was introduced to reduce the complexity and improve the quality of the communication systems. The model of communication protocols based on the finite-state machine is to ensure that communication protocols maintain the desired properties to make the protocols well-formed [16]. The interaction among the whole distributed communication system can be presented as the global specification of the message-passing system i.e., conversation protocols which which are non-deterministic Büchi automata whose labels resemble our interactions [17]. The representation of the choreographic model from the BPMN model is convenient to provide and represents complex and elaborate functionalities.

Future Work. Future Work. The main motivation for our work is to verify whether the previously proposed well-formedness [**?**] choreography model is enough to verify the correctness of the communication system with the assistance of the Corinne tool. We have identified the following possible future extensions of our work:

– **Late Join:** We have identified from our case study that the new creation of the participants as part of the protocol [?] is ignored in the proposed theory. In the case of our case study in Figure 1, the EVs is created later during the communication among the participants. In such circumstances, there are possibilities of losing the communication message because the sender participant does not know whether the receiver participant exists. The available theories of the choreographies do not consider such situations. This needs to be further investigated whether such conditions are feasible for the synchronous communication system.
– **No Acknowledgement:** There are many situations where the protocol continues to participate without receiving the acknowledgment. We found from the healthcare management document that many participants continue to transmit the messages without receiving the acknowledgment. For instance, in Figure 2 the GDH sends the message to the RG in the transition between $0 \rightarrow 1$ but GDH does not receive any acknowledgment from the RG. This needs to be further investigated whether such conditions are feasible for the synchronous communication system.
– **Projection:** We did not perform any analysis on the Projection or the local choreographic model. An interesting future development could be the further analysis of the local choreographic model to investigate whether there are any impacts and differences between global and local choreographic models during the verification.

Creation of participants as part of the protocol

No ack after proposal of creation of RCOO? Ok for synchronous? Not mentioned in the documentation

References

1. Coto, A., Barbanera, F., Lanese, I., Rossi, D., and Tuosto, E. (2022, October). On formal choreographic modelling: a case study in EU business processes. In International Symposium on Leveraging Applications of Formal Methods (pp. 205-219). Cham: Springer International Publishing.
2. Mario Bravetti, Marco Carbone, Thomas T. Hildebrandt, Ivan Lanese, Jacopo Mauro, Jorge A. Pérez, Gianluigi Zavattaro: Towards Global and Local Types for Adaptation. SEFM Workshops 2013: 3-14
3. Barbanera, F., Lanese, I., and Tuosto, E. (2020, June). Choreography automata. In International Conference on Coordination Languages and Models (pp. 86-106). Cham: Springer International Publishing.
4. Barjis, J.: The importance of business process modeling in software systems design. Science of Computer programming 71(1), 73–87 (2008)
5. Orlando, S., Pasquale, V. D., Barbanera, F., Lanese, I., and Tuosto, E. (2021, October). Corinne, a tool for choreography automata. In International Conference on Formal Aspects of Component Software (pp. 82-92). Cham: Springer International Publishing.
6. Corinne-3 URL https://github.com/lanese/corinne-3
7. DOT URL https://graphviz.org/doc/info/lang.html

8. Hans Hüttel, Ivan Lanese, Vasco T. Vasconcelos, Luís Caires, Marco Carbone, Pierre-Malo Deniélou, Dimitris Mostrous, Luca Padovani, António Ravara, Emilio Tuosto, Hugo Torres Vieira, Gianluigi Zavattaro: Foundations of Session Types and Behavioural Contracts. ACM Comput. Surv. 49(1): 3:1-3:36 (2016)
9. Gheri, L., Lanese, I., Sayers, N., Tuosto, E., and Yoshida, N. (2022). Design-by-contract for flexible multiparty session protocols. In 36th European Conference on Object-Oriented Programming (ECOOP 2022). Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
10. Kavantzas, N., Burdett, D., Ritzinger, G., Fletcher, T., Lafon, Y., and Barreto, C. (2005). Web services choreography description language version 1.0. W3C candidate recommendation, 9, 290-313.
11. Autili, M., Inverardi, P., and Tivoli, M. (2014). Automated synthesis of service choreographies. IEEE Software, 32(1), 50-57.
12. Healthcare authorization and accreditation. URL https://salute.regione.emilia-romagna.it/ssr/strumenti-e-informazioni/autorizzazione-e-accreditamento/autorizzazione-e-accreditamento-sanitario)
13. Legge regionale 06 novembre 2019, n. 22. URL https://demetra.regione.emilia-romagna.it/al/articolo?urn=er:assemblealegislativa:legge:2019;22)
14. Adamo, G., Borgo, S., Di Francescomarino, C., Ghidini, C., Guarino, N., and Sanfilippo, E. M. (2017). Business processes and their participants: An ontological perspective. In AI* IA 2017 Advances in Artificial Intelligence: XVIth International Conference of the Italian Association for Artificial Intelligence, Bari, Italy, November 14-17, 2017, Proceedings 16 (pp. 215-228). Springer International Publishing.
15. Tuosto, E., and Guanciale, R. (2018). Semantics of global view of choreographies. Journal of logical and algebraic methods in programming, 95, 17-40.
16. Brand, D., and Zafiropulo, P. (1983). On communicating finite-state machines. Journal of the ACM (JACM), 30(2), 323-342.
17. Fu, X., Bultan, T., and Su, J. (2004). Conversation protocols: a formalism for specification and verification of reactive electronic services. Theoretical Computer Science, 328(1-2), 19-37.