

Choreography Automata: A Case Study in Healthcare Management

Sourabh Pal¹, Ivan Lanese¹, Massimo Clo²

¹ University of Bologna/INRIA, Italy

² Salute e Welfare - Regione Emilia Romagna, Italy

June 20, 2024

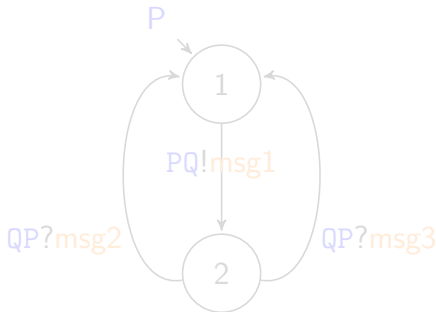
Outline

- ▶ Introduction to Choreography Automata
- ▶ Case Study: Objective and Approach
- ▶ Case Study: Models and Analysis
- ▶ Lessons Learned

Communicating Systems

A Communicating System is a set of Communicating Finite-State Machines (CFSMs), which are labeled with **receive(?)** and **send(!)** operations

A machine M_P

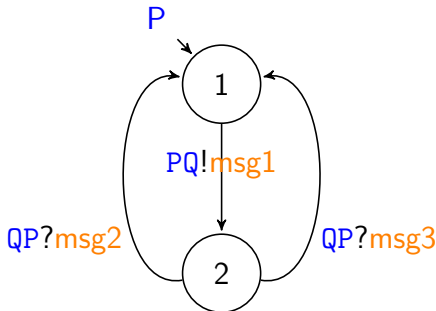


- ▶ M_P can send **msg1** to machine M_Q ;
- ▶ Then, either **msg2** or **msg3** can be received from M_Q ;
- ▶ and so on....

Communicating Systems

A Communicating System is a set of Communicating Finite-State Machines (CFSMs), which are labeled with **receive(?)** and **send(!)** operations

A machine M_P

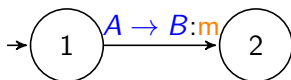


- ▶ M_P can send $msg1$ to machine M_Q ;
- ▶ Then, either $msg2$ or $msg3$ can be received from M_Q ;
- ▶ and so on....

Choreographic Representation of Communicating Systems

$$A \rightarrow B : m$$

Interactions as main building blocks.

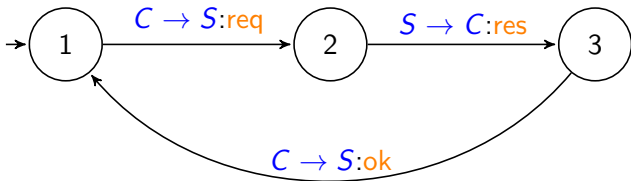


We use interactions to label transitions of automata.

Choreography Automaton - Informal

A Choreography Automaton (C-Automaton) is a finite state automaton whose transitions are labelled by interactions.

It can be projected on a Communicating System, and if the C-Automaton is well-formed then the projected Communicating System enjoys nice properties such as deadlock freedom.



Case Study

Regional Coordination for Authorization and Accreditation of public or private Healthcare Institutes in the health services in the Emilia-Romagna region in Italy.

Protocol needed to ensure Healthcare Institutes can actually operate.

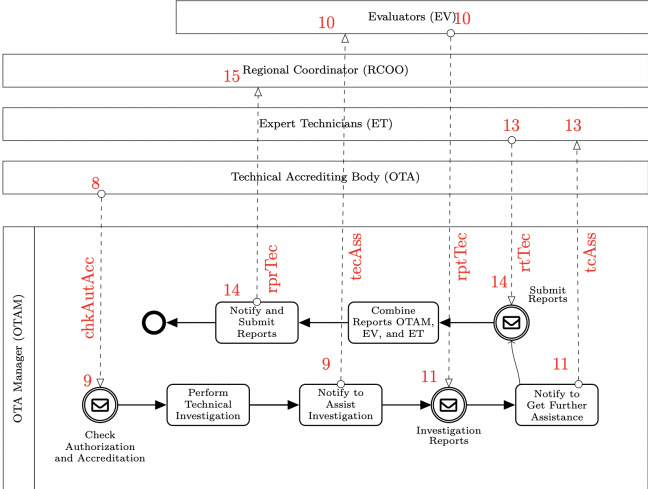
Objective

- ▶ Verify the **correctness of communications** of the Communicating System projected from the **C-Automaton**
- ▶ The projected system is correct if the C-Automaton is **Well-Formed**
- ▶ Well-Formed: Well-Branched \wedge Well-Sequenced
 - ▶ Well-Branched
 - ▶ When there is a choice, a single participant decides;
 - ▶ All the other participants are eventually made aware of the choices made (unless they behave the same).
 - ▶ Well-Sequenced
 - ▶ Parallelism of interactions with no common participant must be made explicit by interleaving them in all possible orders;
 - ▶ Two consecutive transitions are EITHER concurrent OR have a common participant.

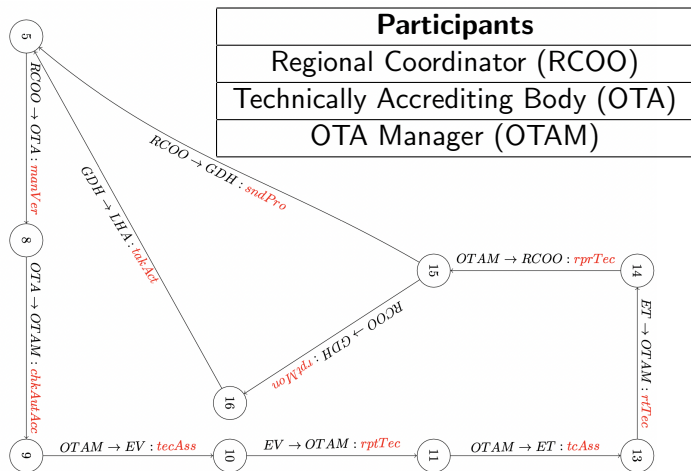
Approach

- ▶ We started from a natural language description of the protocol (a regional law);
- ▶ **BPMN:** Transform the natural language description to BPMN Collaboration Diagram (manually);
- ▶ **Choreography Automaton:** Transform the BPMN Collaboration Diagram into C-Automaton (manually);
- ▶ **Correctness:** Verify Well-Formedness (automatically using Corinne Tool).

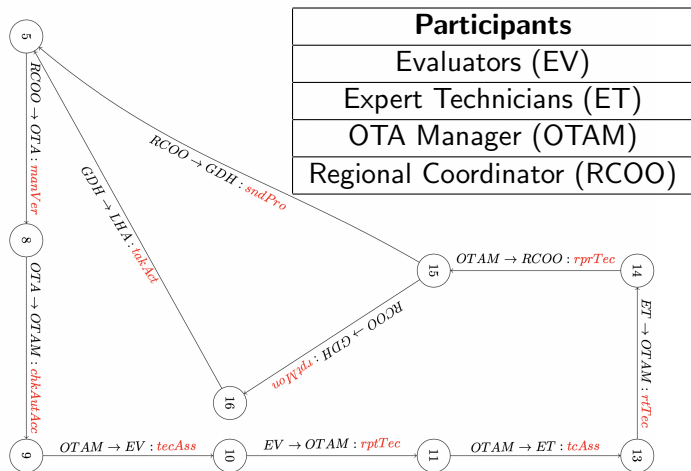
BPMN-Collaboration Diagram: A Fragment of Case-Study



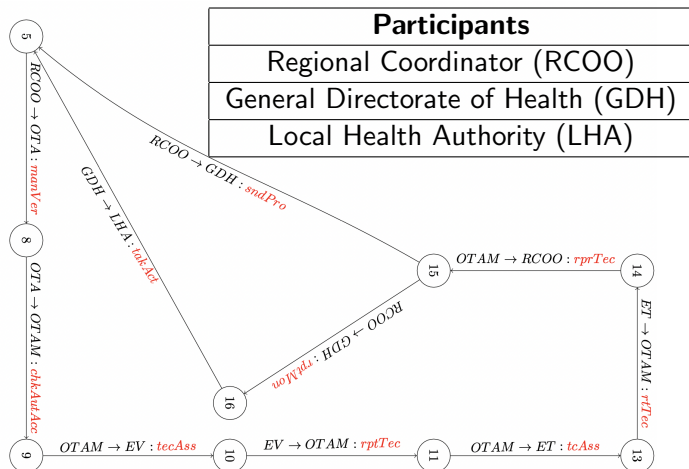
CA for Regional Coordination for Authorization and Accreditation



CA for Regional Coordination for Authorization and Accreditation



CA for Regional Coordination for Authorization and Accreditation



Analysis

- ▶ The check of well-formedness executed by Corinne reported a number of issues;
- ▶ Upon manual check, they all turned out to be false positives;
- ▶ No real issue found on the protocol;
- ▶ But got lot of useful feedback for Corinne and choreographic analysis in general.

Lessons Learned (1)

- ▶ **Gap between Laws and Choreographies:**
 - ▶ Laws describe the roles and responsibilities of the Participants. The message-passing information is mostly implicit and not detailed.
 - ▶ The intermediate step in terms of BPMN helps to bridge the gap.
 - ▶ BPMN is also useful to interact with domain experts.

Example

Regional Law 22 from November 06, 2019, Article 13.3

The OTA carries out the following functions in relation to accreditation:

- a) carries out the technical investigations [...];
- b) carries out the activities referred to in letter a) also making use of the EV included in the list referred to in article 14 and of ET of recognized competence. The overall results are transmitted to the RCOO for the relevant obligations;

Lessons Learned (2)

- ▶ **Late Join (also called Selective Participation):**
 - ▶ Some participant may be involved only in some branches of a protocol. (S)he reacts to requests of other Participants and (s)he is not involved in all the executions.
 - ▶ Late Join not supported by Corinne, this causes many false positives.
- ▶ **Parallel Protocols:**
 - ▶ An actor carries on multiple protocols at the same time.
 - ▶ Showing all the possible interleavings would made the diagram unreadable.
- ▶ **Creation of New Participants:**
 - ▶ During protocols new roles are created to perform tasks, which did not exist when the Choreography started.
 - ▶ It would be interesting to model this aspect.

Future Work

- ▶ Extend C-automata and Corinne to tackle the problems above;
- ▶ Automate the extraction of C-automata from BPMN;
- ▶ Further validate the approach on other case studies.

Thank you for your attention.