Please read me: Fundamental Principles and Details required to participate in the experiment

Task description

Imagine the following scenario: You are responsible to analyse and handle recorded business process executions which were reported as anomalous by an automatic anomaly detection system. For this you will need to a) identify which parts of the executions are anomalous and b) determine what kinds of anomalies have taken place to c) select appropriate solutions which enable to react on all the identified anomalies (e.g., by redesigning a business process model). Note, in this experiment we will *only* address the first two aspects [i.e., aspect **a)** and **b)**].

To participate in the experiment please perform the following steps:

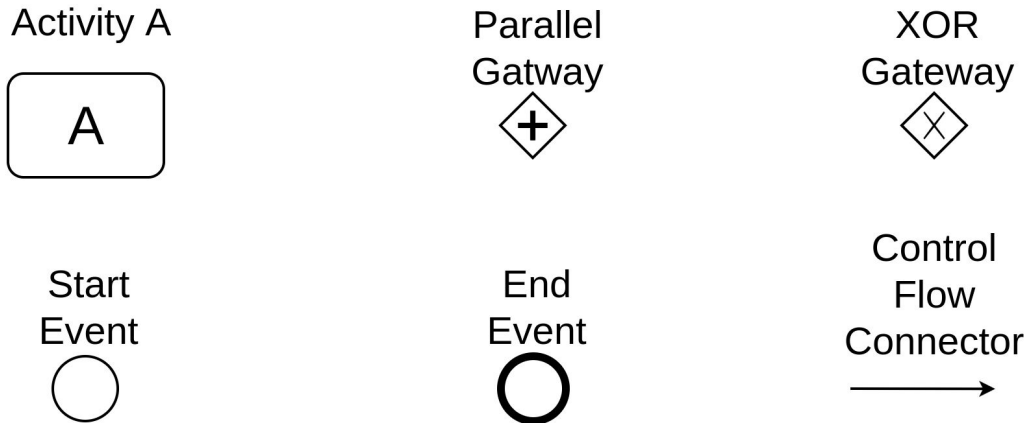
1. (Preparatory) Quickly read up on the task and fundamental principles related to business processes, traces, and logging. Note, all the necessary details are laid out in the following pages.
2. (On site, during the experiment) Quickly study the available documentation of the two business process models which will be utilized throughout the experiment.
3. (On site, during the experiment) Analyse the given anomalous process execution traces and spot as many anomalous process execution events (or missing events) as possible.

Fundamental Principles

In the following we will describe the fundamental principles required to read and understand the documentation and details given to you throughout the experiment.

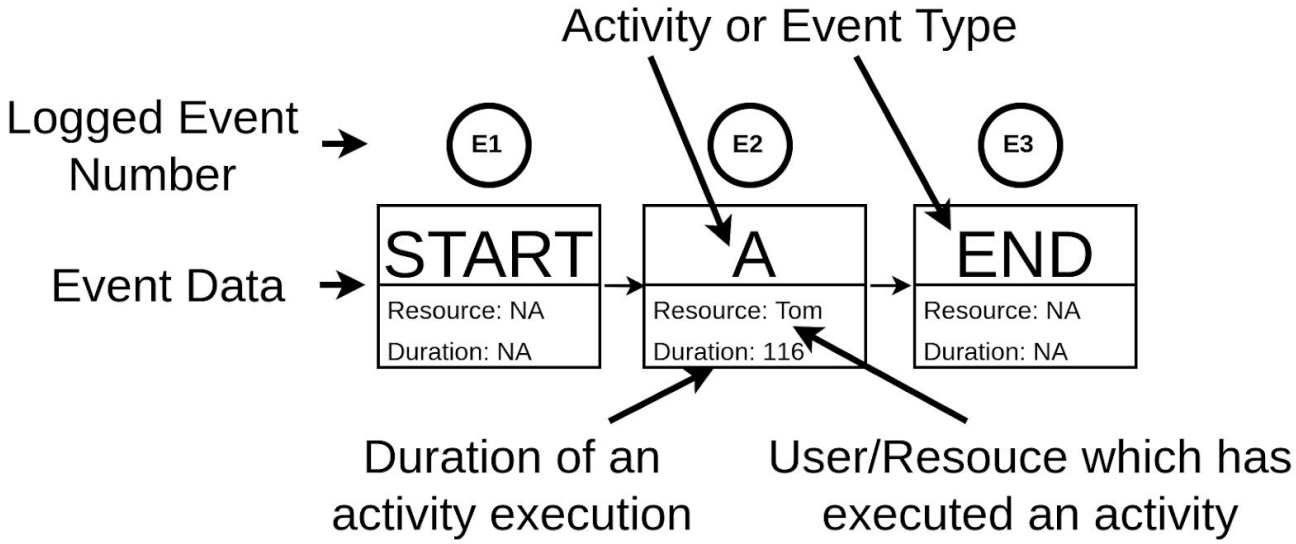
Utilized Notations - Business Process Model and Notation (BPMN)

The given process models are modelled using BPMN. In the following you will see all notation elements (and their purpose) which are utilized throughout this experiment to model business process models.



Utilized Notations - Logged (Recorded) Business Process Execution Trace

While participating in the experiment you will need to understand and analyse a number of recorded (logged) business process executions (i.e., execution traces). Such traces are always representing complete business process instance executions, i.e., they are holding all execution events which were recorded for a specific process instance execution from its start to its termination. Such traces are depicted based on the following notation:



Anomaly Types

While participating in the experiment you will observe three types of anomalies, which can be “hidden” in each process execution trace provided to you. Note, you can assume that each trace contains at least one anomaly as it was reported by the process execution security system as being anomalous (this does not apply to the benign traces for process model 2 which you can assume as being anomaly free - additional information will be given throughout the experiment).

- **Control Flow** (anomalies related to activities/events and their order/occurrence)
  - *Missing Activity:* Typically, a specific activity/event should be part of a non-anomalous instance execution, but the respective activity execution event is missing in the anomalous execution trace (e.g., while normally activity B should follow on activity A the activity B execution event is not contained in the trace).
  - *New Activity:* A new activity which should not be part of the business process execution was observed (e.g., normally a trace should only consist of execution events for activity A and B but this time it also contained an execution event for activity C).
  - *Swapped Activity:* While the correct activities were executed, their order was unusual (e.g., while normally activity B should follow on activity A this order was reversed in the anomalous trace based on the given activity execution events).
- **Resource** (anomalies related to the users and resources which execute a specific activity)
  - *Binding of Duty (BoD):* Two activities must always be executed by the **same** resource, for example, for consistency reasons.
  - *Separation of Duty (SoD):* Two activities must always be executed by **separate** resources, for example, to prevent misuse.
  - Note: Each relevant execution event holds the resource/user which has executed the respective activity.
- **Time** (anomalies related to the temporal execution behaviour of two or more activities)
  - Frequently a temporal relation between activity executions can be observed. For example, when activity A is executed faster than average activity B is executed faster too. Time related anomalies would violate this kind of relations (e.g., activity A was executed faster while activity B was executed slower).

Anomaly Detection Support

For this experiment we will assume that process modelling experts are supported in three different ways by today's process execution anomaly detection systems while dealing with anomalous process executions.

- **First:** It is assumed that the anomaly detection system will only inform the expert that a specific process model execution trace is anomalous - without providing any additional information about the identified anomalous and suspicious execution events.
- **Second:** In comparison, the second approach will highlight specific parts (i.e., execution events) of a recorded process execution (i.e., an process execution trace) to indicate that those parts are benign, likely related to an anomaly, or almost certainly related to an anomaly.
- **Third:** Finally, the third approach will provide additional information and hints about the typical process execution behaviour which was violated by a given anomalous trace (e.g., which behaviour was expected vs. which behaviour was observed based on the anomalous execution trace - in the form of simple IF/THEN rules).

Note, additional details and explanations about each of the three approaches will be given to you during the experiment.