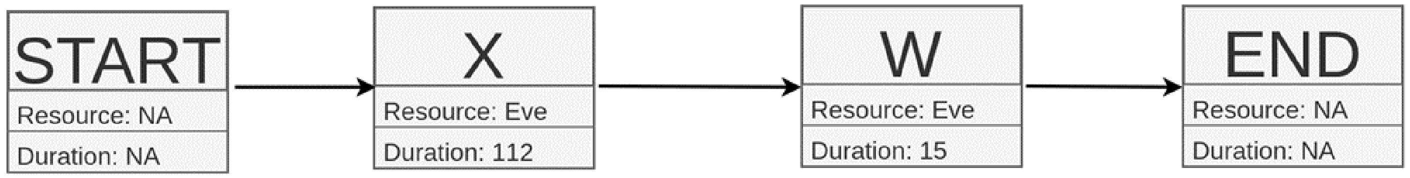
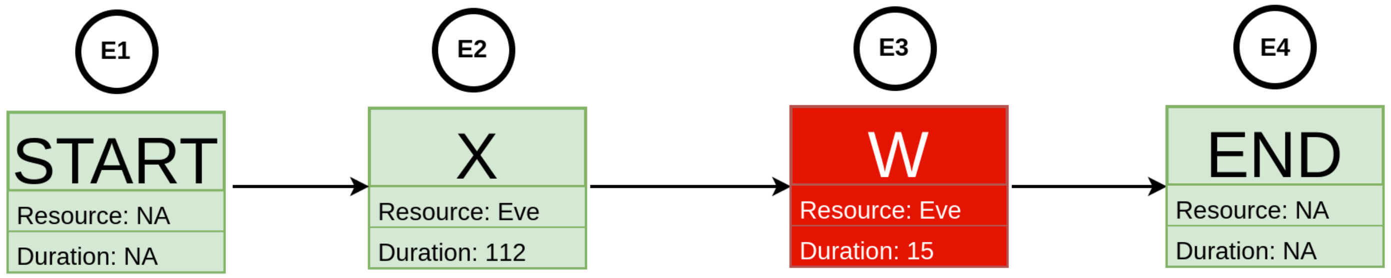
## Discussion of the first approach: No Anomaly Detection Support

The first approach will only depict the process execution trace which was identified as being anomalous.



## Discussion of the second approach: Anomaly Detection Highlights

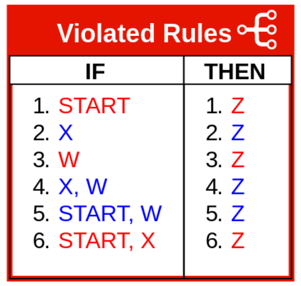
The second approach marks events as green (cf., E1 below) if it was found that this event is most likely ***not* related** to an anomaly. In comparison, events marked in a red colour (cf., E3 below) are most likely **related** to an anomaly. Finally, some events are marked in a blue colour. For such events, **no final conclusion** could be drawn about the anomaly state, i.e., in certain situations the observed behaviour could be benign while in others it could be anomalous. So, it is up to the experts (you) to decide if it is related to an anomaly or not. Note, no additional details will be available, i.e., a bright red coloured event can be related to one (or multiple) anomaly types (control, resource, temporal) - which one applies must be deduced by you.



## Discussion of the third approach: Anomaly Detection Rules/Hints

This approach enriches the second approach by adding hints/rules to each event which provide additional information about the aspects which motivated the classification of that event as anomalous. All hints about potential anomalies will be represented as rules consisting out of an IF and THEN part. Hence, whenever the IF part occurs we assume that also the THEN part should occur. If this is not the case (i.e., if the IF part is satisfied but the THEN part is not) then some suspicious/anomalous behaviour was found which indicates the occurrence of an anomaly. Note, while the IF part can take multiple aspects (preconditions) into account the THEN part always only represents a single aspect.

- **Significance**: The rules will be depicted using two significance levels. Rules which are written in a red colour are ***very* significant** and should always be supported by a process execution (strong rules). Rules written in a blue colour are *less* significant (weak rules) and are also sometimes violated by executions which were found to be benign (i.e., non-anomalous executions). An example for both rule types is given by the Figure on the right (for example, rule 1 would be strong and rule 2 would be weak). Note, this follows the same concept then the second approach (red indicates that most likely an anomaly has occurred while blue indicates that potentially an anomaly has taken place).



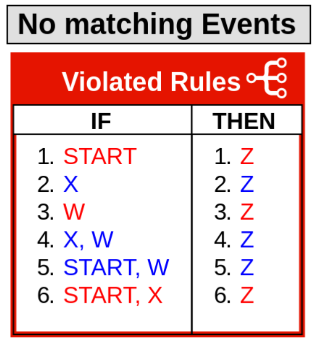
Violated Rules

| IF | THEN |
|---|---|
| 1. START<br>2. X<br>3. W<br>4. X, W<br>5. START, W<br>6. START, X | 1. Z<br>2. Z<br>3. Z<br>4. Z<br>5. Z<br>6. Z |

- **Violated rules**: Only hints/rules will be depicted which were violated by the respective trace. So, the depicted rules are most likely indicating that an anomaly related to the THEN part has taken place (i.e., when the IF part has taken place but the THEN part is not supported by a trace then this indicates an anomaly related to the THEN part, such as, an execution of an activity was expected but was not observed in the trace.)

**In the following example you can see all three types of hints:**

- **Control Flow Rules**: Represents that IF a specific activity was executed THEN another activity should be executed afterwards. Note, the execution of the THEN activity needs to occur after the IF activity at an arbitrary position before the termination of the respective trace/instance.
  - **No matching events**: If possible expected but missing (or violated) behaviour (the related rule visualizations, resp.) will always be located right next to the event which is addressed in the THEN part of the affected rules. However, if the respective event/activity (which would be related to the THEN part) is missing (e.g., an activity should occur, but it did not) then the respective rules are summarized below a "*No matching Events*" Header. This situation can only occur for control flow rules.
  - **Example based on the first rule:** If the START event has occurred then the execution of activity Z should take place between the START and the termination of the process instance (i.e., after the execution of "START" an execution of "Z" should be found in the trace). If this is not the case an anomaly has been found, i.e., an execution of activity Z is missing. Additional example: For the third rule an execution of activity Z should take place after the execution of activity W.

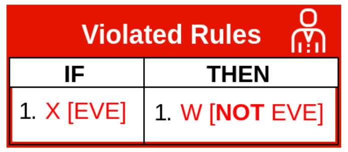


**No matching Events**

Violated Rules

| IF | THEN |
|---|---|
| 1. START<br>2. X<br>3. W<br>4. X, W<br>5. START, W<br>6. START, X | 1. Z<br>2. Z<br>3. Z<br>4. Z<br>5. Z<br>6. Z |

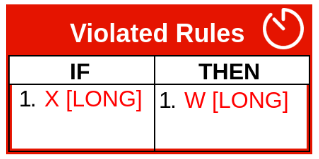
- **Resource Rules**: Represents that IF and activity was executed by a specific user/resource THEN the execution of another activity must be performed by the same (BoD) or a different (SoD) user/resource.
  - **Example:** If activity X was executed by user EVE then activity W should not be executed by EVE too SoD. However, this rule was violated as activity W was in fact, also, be executed by EVE (i.e., this rule indicates a SoD violation).



Violated Rules

| IF | THEN |
|---|---|
| 1. X [EVE] | 1. W [**NOT** EVE] |

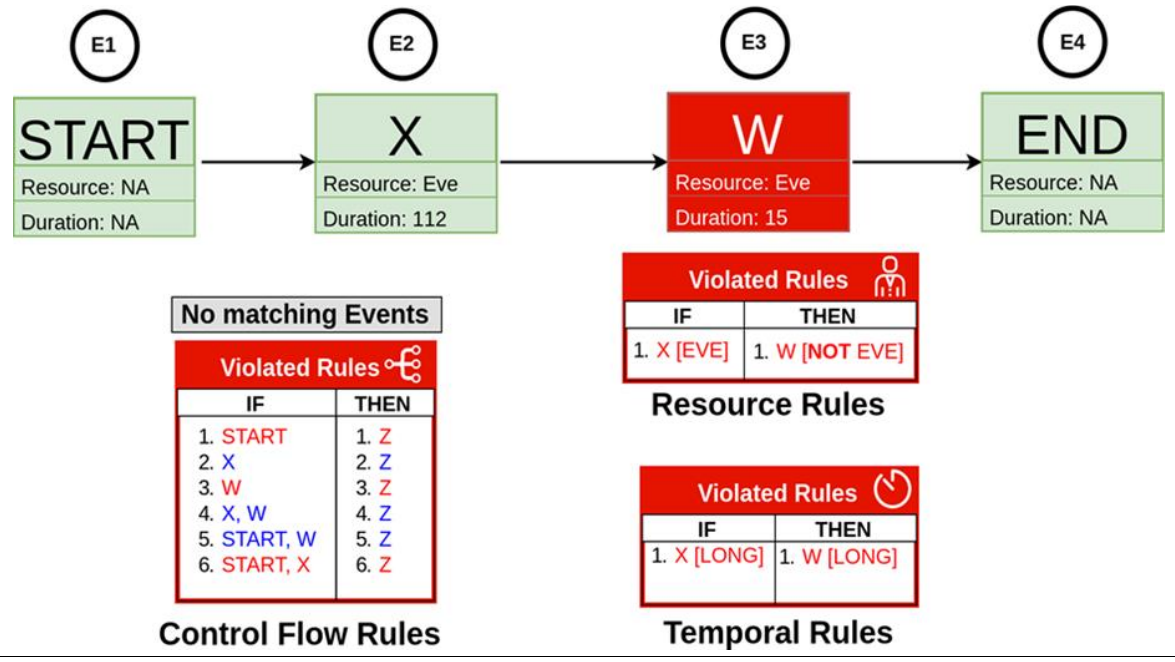
- **Temporal Rules**: Activity execution durations are classified as FAST, AVERAGE, or LONG.
  - FAST: The execution is faster than the average execution of that activity.
  - AVERAGE: The execution is similar to the average execution duration of that activity.
  - LONG: The execution takes longer than the average execution duration of that activity. Related rules, for example, depict that IF an activity is executed, e.g., faster on average THEN another activity is executed, e.g., longer than average.
  - **Example:** If the execution of activity X takes longer than average then the execution of activity W should also take longer than an average execution of W. However, here the execution of W is completed very quickly which violates this rule and indicates an anomaly.



Violated Rules

| IF | THEN |
|---|---|
| 1. X [LONG] | 1. W [LONG] |

**Larger example/composition of exemplary rules and a trace:**



**No matching Events**

Violated Rules

| IF | THEN |
|---|---|
| 1. START<br>2. X<br>3. W<br>4. X, W<br>5. START, W<br>6. START, X | 1. Z<br>2. Z<br>3. Z<br>4. Z<br>5. Z<br>6. Z |

**Control Flow Rules**

Violated Rules

| IF | THEN |
|---|---|
| 1. X [EVE] | 1. W [**NOT** EVE] |

**Resource Rules**

Violated Rules

| IF | THEN |
|---|---|
| 1. X [LONG] | 1. W [LONG] |

**Temporal Rules**