# Attributes description: enriched event log of an incident management process

**Claudio A. L. Amaral**[1], **Marcelo Fantinato**[1], **and Sarajane M. Peres**[1,*]

[1]University of São Paulo, São Paulo, 038280-000, Brazil
[*]sarajane@usp.br

## Abstract

In this document, we present the descriptions of the attributes which compose an enriched event log of an incident management process extracted from an instance of the *ServiceNow*$^{TM}$ platform used by an IT company. The log is made available in two versions: *(a)* [`incident_event_log_01.csv`] the log as it was used in the experiments for time completion prediction as described in our paper[1] and *(b)* [`incident_event_log_02.csv`] an improved log with event labels standardization. This log is composed by 24,918 cases (incidents) and 141,712 events and it was extracted from Mar-2016 to Feb-2017. Information was anonymized for privacy.

## Citation Request

If you publish some work based on this event log, please make the appropriate citations to our work as best suited the context of your work. If your experiments are not related to ours, just cite the paper[1] as the first one to use this event log. If you have downloaded this event log from any academic repository, please refer to the corresponding citation policy.

## Attributes description

- Control Attributes:
  - *number*: incident identifier with the same number as total cases;
  - *incident state*: attribute with eight levels controlling incident management process transitions from opening until closing the case;
  - *active*: boolean attribute indicating if record is active or closed/canceled;
  - *reassignment_count*: number of times incident has changed group or support analysts;
  - *reopen_count*: number of times incident resolution was rejected by caller;
  - *sys_mod_count*: number of incident updates until that moment;
  - *made_sla*: boolean attribute to incident exceeded target SLA or not;
- Identification and Classification Attributes:
  - *caller_id*: user identifier affected;
  - *opened_by*: user identifier that reported the incident;
  - *opened_at*: incident opening date and time;
  - *sys_created_by*: user identifier that registered the incident;
  - *sys_created_at*: incident creation date and time;
  - *sys_updated_by*: user identifier that made update and generated current log record;
  - *sys_updated_at*: log update date and time;
  - *contact_type*: categorical field with values indicating how incident was reported;
  - *location*: location identifier of place being affected;
  - *category*: description of the first level of service being affected;
  - *subcategory*: description of the second level of service being affected – related to first level;

  - *u_symptom*: description about user perception of service availability;
  - *cmdb_ci*: (confirmation item) identifier (not mandatory) referencing homonyms relation and used to report item being affected;
  - *impact*: description of the impact caused by incident. Values are: 1–High; 2–Medium; 3–Low;
  - *urgency*: description to the urgency asked by user for incident resolution. Values are same as *impact*;
  - *priority*: priority calculated by system based on *Impact* and *urgency*;

- Support, Diagnosis and Other Attributes:
  - *assignment_group*: identifier referencing the relation *Group* (database relational model in *ServiceNow*$^{TM}$) describing support group in charge of incident;
  - *assigned_to*: user identifier in charge of incident;
  - *knowledge*: boolean attribute indicating whether a knowledge base document was used to resolve incident;
  - *u_priority_confirmation*: boolean attribute indicating whether *priority* field was double checked;
  - *notify*: categorical attribute indicating whether notifications was generated for this incident;
  - *problem_id*: identifier referencing homonyms relation describing problem identifier associated with this incident;
  - *rfc*: (chance request) identifier referencing homonyms relation describing change request identifier associated with incident;
  - *vendor*: identifier referencing homonyms relation describing vendor in charge of incident;
  - *caused_by*: relation with RFC code responsible by the incident;
  - *close_code*: resolution code of the incident;
  - *resolved_by*: user identifier who resolved the incident;
  - *resolved_at*: incident resolution date and time;
  - *closed_at*: incident close date and time;

The attributes *sys_created_by*, *sys_created_at*, *sys_updated_by* and *sys_updated_at* are audit log attributes extracted from the audit system offered by *ServiceNow*$^{TM}$. In fact, the last two attributes were derived from such an audit system. All other attributes were extracted from a relational database related to the incident management system. The attributed *closed_at* is used to determine the dependent variable in the time completion prediction task. The attribute *resolved_at* is highly correlated with *closed_at*. In this event log, some rows may be have the same values (they are equal) since not all attributes involved in the real-world process are present in the log. Attributes used to record textual information were not placed in this log.

## References


**1.** do Amaral, C. A. L., Fantinato, M. & Peres, S. M. Attribute selection with filter and wrapper: An application on incident management process. In Ganzha, M., Maciaszek, L. & Paprzycki, M. (eds.) *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, vol. 15 of *Annals of Computer Science and Information Systems*, 679–682, DOI: http://dx.doi.org/10.15439/2018F126 (IEEE, 2018).