MANUAL FOR LOG COMPLIANCE PLUG-IN

INTRODUCTION

The log compliance plug-in analyses a set of log traces and identifies which of them are security-critical. The installation of the plugin will create a new menu, **LogCompliance,** which will contain a button **Conformance Analysis**. The button permits to start the analysis, the aim of which consist in finding critical deviations.

The document is organized as it follows: Section 1 describes how to install the plug-in into the STS-Tool. Section 2 describes the functionalities of the plug-in and how it works and how to complete an analysis.

In the document the font: "Tahoma" is used to highlight the name of the elements of the plug-in such as Buttons, Menus, Dialogs name, Views name, etc.

HOW TO INSTALL

The Log compliance plug-in is installed from STS-Tool[1]. The user can select from the menu **Help->Install New Software** (**Figure 1Error! Reference source not found.**) and select the plug-in **Log Compliance** from the list of the available plug-in (**Figure 2**). In order to run the plug-in, **SecBPMN2** plug-in is install automatically.

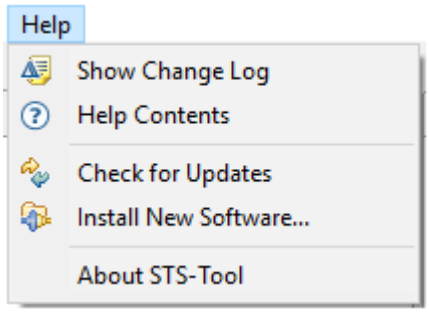

Figure 1 Install New Software menu

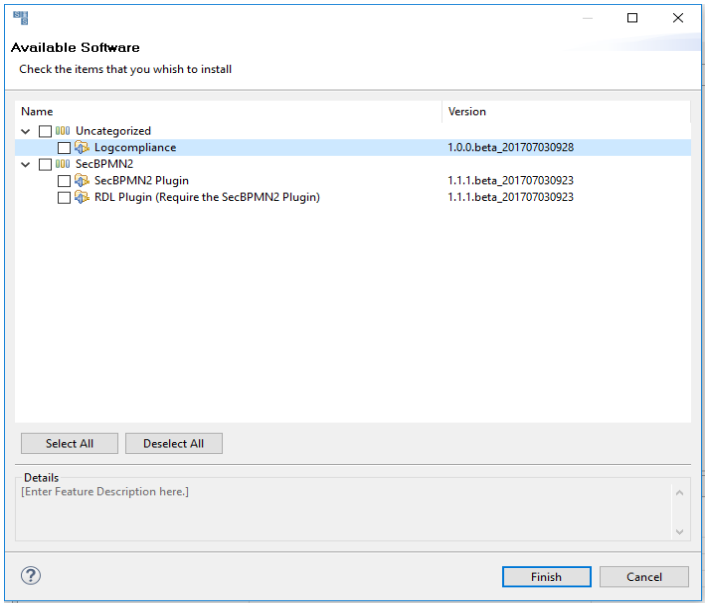

Figure 2 Available Software dialog

[1] STS-Tool :http://www.sts-tool.eu/

DESCRIPTION OF THE PLUG-IN

The main objective of the plug-in consists in analyzing lists of actions (called log traces) and identifying which of them deviated from a predefined execution set, defined with a business process, and may threat the security of an organization.

The plug-in performs a conformance analysis, that identifies the deviations in a set of log traces with respect to SecBPMN2 business process, and it determines which of them are security-ctitical, i.e., which log traces might threat the security of an organization. The conformance analysis requires a business process diagram, with the format of Business Process Model and Notation 2.0 (BPMN2.0) [1], and a log file, with the format of eXtensible Event Stream (XES) [2]. Once the plug-in is installed, a new button appears in **Analysis** menu: **LogCompliance**, shown in **Figure 3**. The button is only visible if there is a BPMN2.0 file open.

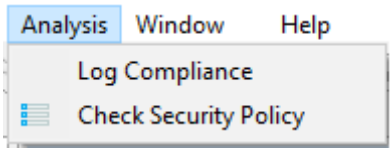

Figure 3 Analysis Menu

Before starting the analysis, users can choose witch algorithm will be used to identify the deviations of the log traces, using the following procedure:

a. The algorithm can be selected in the preferences menu in **Window-> Preferences -> Log Compliance -> Select Algorithm**. (**Figure 4**)
b. In **Figure 5**, there is the Preferences dialog, that permits to select an algorithm, use during the analysis. A default algorithm is set in order to start the analysis with an algorithm.

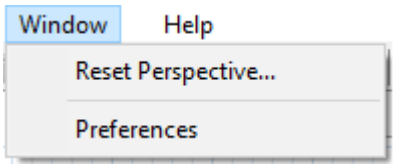

Figure 4 Window menu

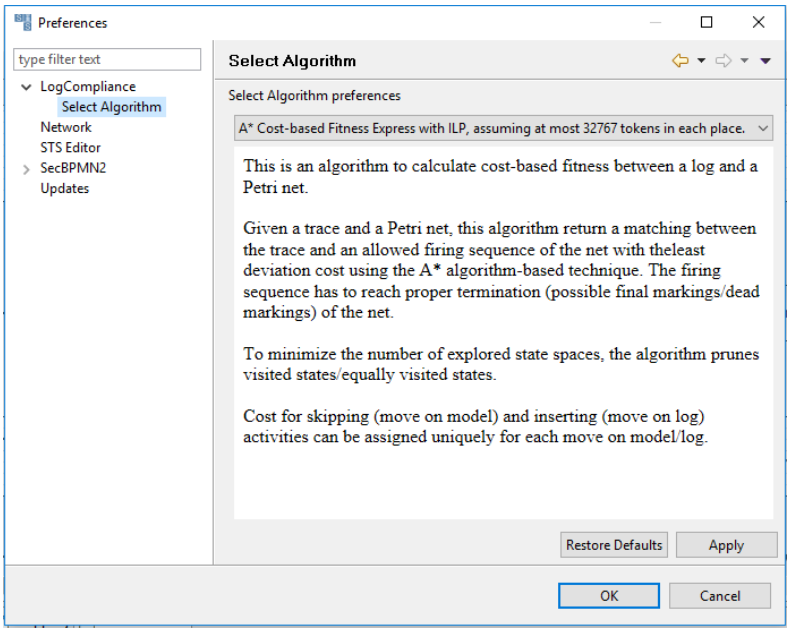

Figure 5 Preferences dialog

The Conformance Analysis is divided into three phases:

- the first phase, in which the user creates a SecBPMN2 diagram and starts the analysis;
- the second phase, in which the user has to import a log file and set parameters for the analysis;
- the third phase is fully automated done by the plug-in.

FIRST PHASE:

This phase consists in creating a SecBPMN2 business process and translating the business process diagram into a Petri Net.

1. The plugin requires a SecBPMN2 process that will be used as a template to check whether a log trace deviated. Therefore the very first step is the definition of a SecBPMN2 diagram, as specified in the SecBPMN2 plug-in manual[2].
2. After the creation of the SecBPMN2 diagram, the user has to start the analysis: open the SecBPMN2 file and click on the menu **Analysis -> Log Compliance** to start the analysis. (**Figure 3**). The plug-in creates a Petri Net Markup Language (PNML) [4] file, that contains the Petri Net generated from the SecBPMN2 diagram. The PNML file is save into the same folder of the SecBPMN2 file and is visible to the user. The user can open the file and see the generated petri net.

[2] SecBPMN2 plug-in User Guide and SecBPMN2 Modeling Language http://www.sts-tool.eu/manuals/

SECOND PHASE:

This phase start when the analysis is launched and it generates a Comma-separated values file (CSV) [3], in which are store the results of the analysis between the log and Petri net.

1. The plug-in requires a set of log traces a file with the format Extensible Event Stream (XES). If a XEX file is already present in the same folder of the SecBPMN2 diagram, with the same name of the diagram, the plug-in will automatically use the file. Otherwise, before the start of the analysis, the plug-in will ask the user a path to the XES file to import (**Figure 6**,**Figure 7**).

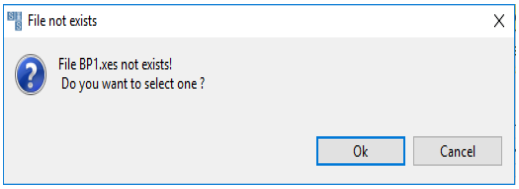

Figure 6 Import file message

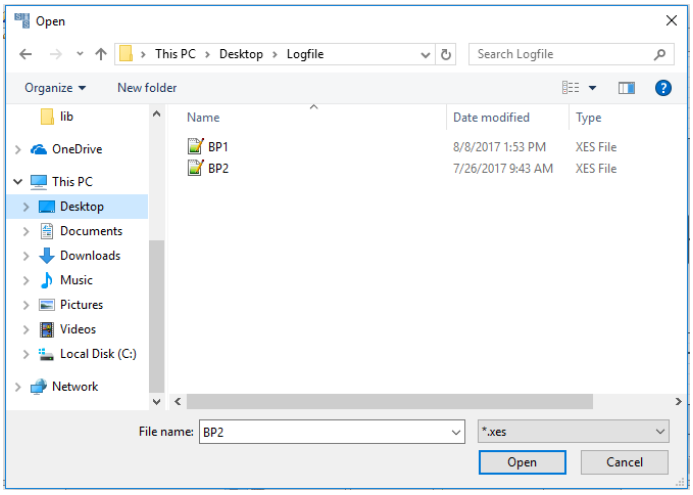

Figure 7 Import file dialog

2. The plug-in identifies the deviating log traces. The plug-in shows a Wizard Dialog, in Error! Reference source not found., in which offers to the user the possibility to:
    a. map the transitions in the Petri net model with the events in the trace of the log.
    b. set the cost of the moves using during the analysis.

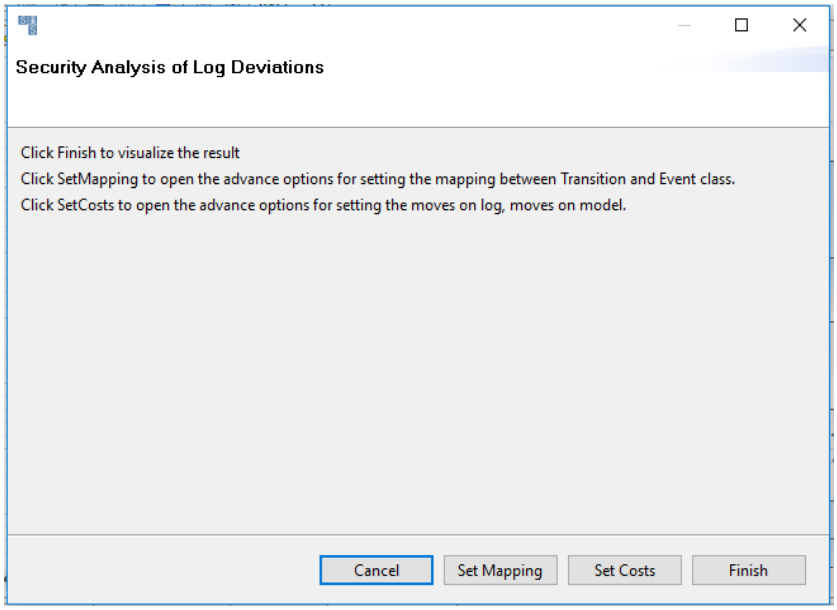

Figure 8 Security Analysis of Log Deviations Wizard dialog

The user can click the **Finish** button in order to use default values. Otherwise the user can access advance parameters by clicking **Set Mapping** button to customize the mapping between Transition and Event, or can click the button **Set Costs** to cistomize the cost of the different moves.

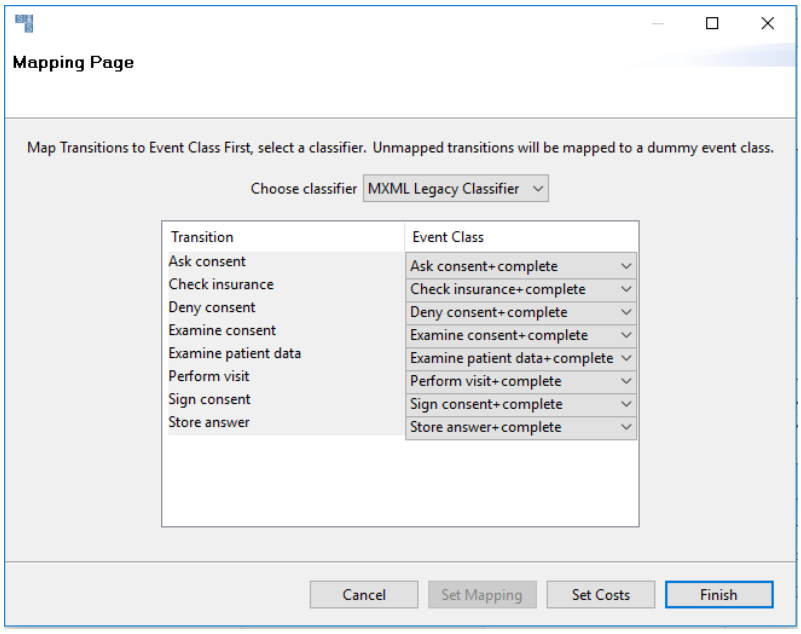

Figure 9 Mapping Page dialog

The **Mapping page** permits to the user to link the Transition of the Petri Net with the Event stored into the log file. The user can select a Classifier for the Event. When the user opens the mapping page he can go to set the costs or finish the analysis. (Figure 9)

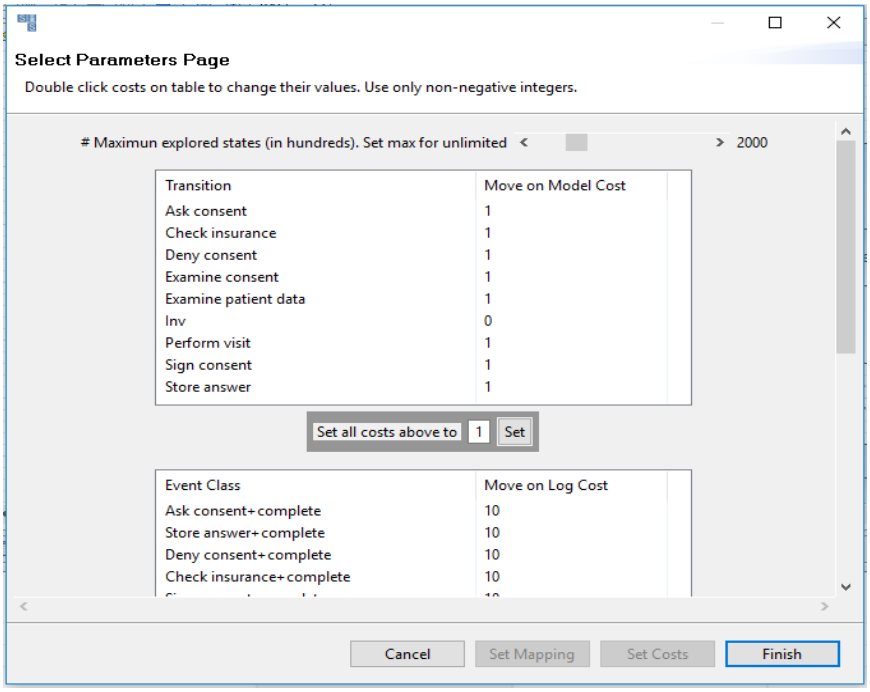

Figure 10 Select Parameters Page dialog

The **Select Parameters Page** permits to the user to set the cost of the move on model, move on log and synchronous move. The user, after setting the costs, can only finishes the analysis or cancels it. (**Figure 10**). When the Finish button is clicked the analysis is performed. and it creates a file with extension Comma-separated values (CSV) [3], that contains the result of the analysis, the file is save into the same folder of the SecBPMN2 file and with the same name.

3. When the analysis is finished the plug-in shows a dialog that illustrates all deviating log traces. **Figure 11** shows an example of the **Analysis Results dialog**. The dialog contains a recap of the number of traces analyzed, the different paths found, in which we can group the traces and how many of these paths deviate. There are two checkboxes: a checkbox that allows to visualize only the critical deviations, deviations these cause security problems, on the business process and a checkbox that allows to execute the analysis, with the handle of multiple executors for activities in the same lane/pool.

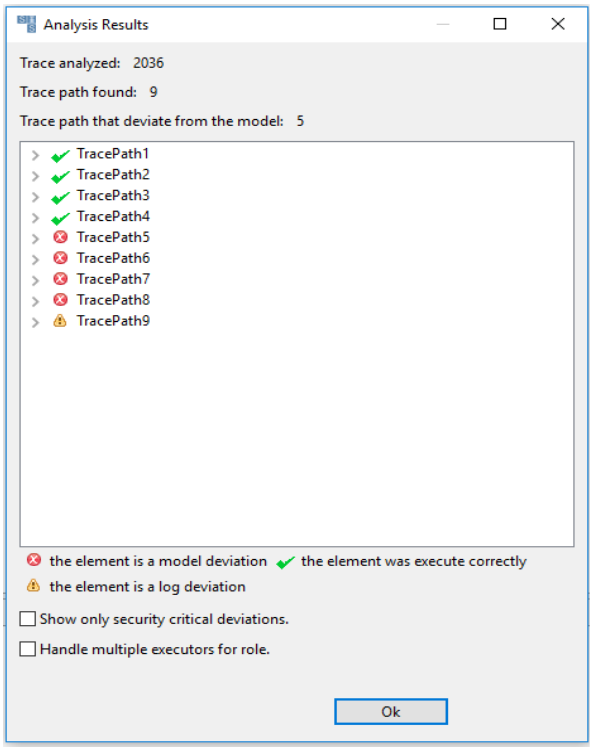

Figure 11 Analysis Results dialog

4. The user will have to click on **OK** to complete the analysis and generates the SecBPMN2 files of the Path that cause deviation. These files are used into the analysis of Security Policy to check if these files violate the Security Policy contained into the project folder.

THIRD PHASE:

The aim of this phase consists in visualizing the deviations contained into the CSV file on the business process diagram. The plug-in parses the CSV file and extracts all the traces groups. The plug-in, after that, transforms those log traces into a SecBPMN2 files and executes the Security Analysis, which identifies the security-critical deviations. After finish the analysis the plug-in shows the different results depending on the setting defined by the user:

1. If the checkbox, in the dialog in **Figure 11**, is checked: the plug-in shows only the critical deviations. In particular, the plug in shows a view **SecurityDeviations** (**Figure 12**), that contains a table with 4 columns: (i) the name of the SecBPMN2 file generate in the previous phase, (ii) the names of the security policy violated by the file, (ii) the button to show the identifiers of the traces with that trace path, (iv) the button that allows the user to highlight in the SecBPMN2 business process diagram, the log traces and where it deviated.

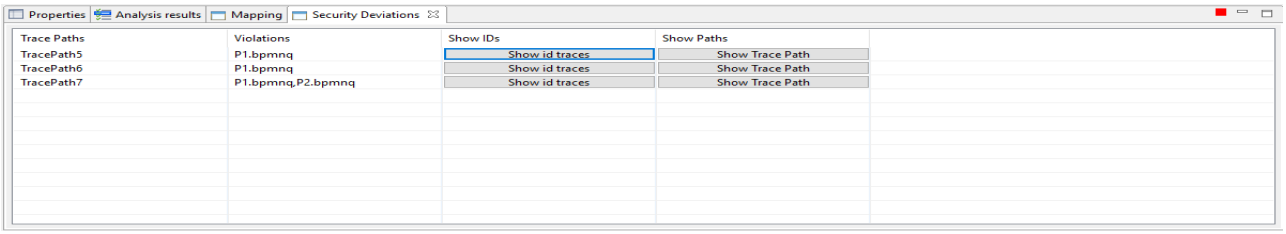

Figure 12 Security Deviations view.

2. If the checkbox, in the dialog in **Figure 11**, is not checked: the plug-in :
    a. highlights, in the SecBPMN2 business process diagram, the elements that caused the deviations on model (activity skipped) in red, and the deviations on log (activity insert) in purple.
    b. shows the **SecurityDeviations** view describes previously.
    c. shows the **Deviations** View (**Figure 13**), that contains a table with 4 columns: one column for the type of deviations (model or log), the second column for the name of the activities these are a **Task with Security risks,** the third column for the frequency of the activity be a deviation into the log file and the last for a button, **Show Traces**, that shows a list of traces, in which that activity deviates.
        i. Click on the button allows the user to selects a trace, from a list of trace, and show the path of that trace onto the business process diagram. (**Figure 14**)
        ii. User can also click on button, Show IDs, to see the ids of the traces that has this type of trace path. (**Figure 15**).

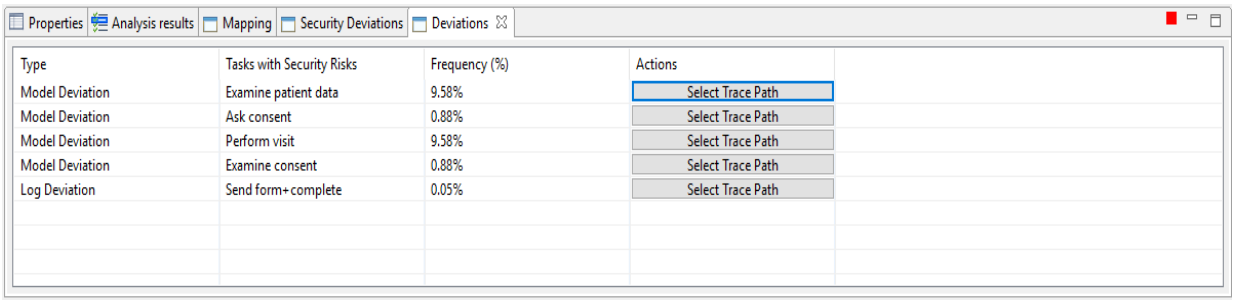

Figure 13 Deviations view

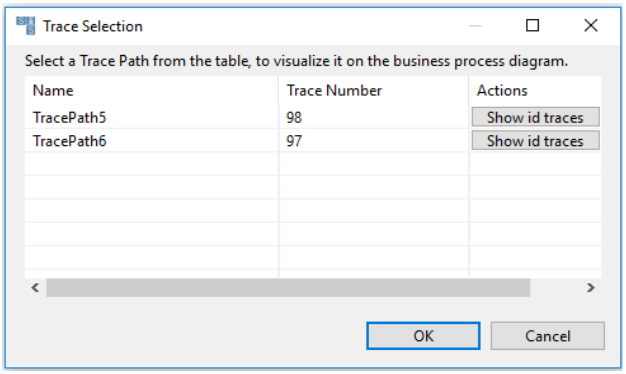

Figure 14 Trace Selection dialog

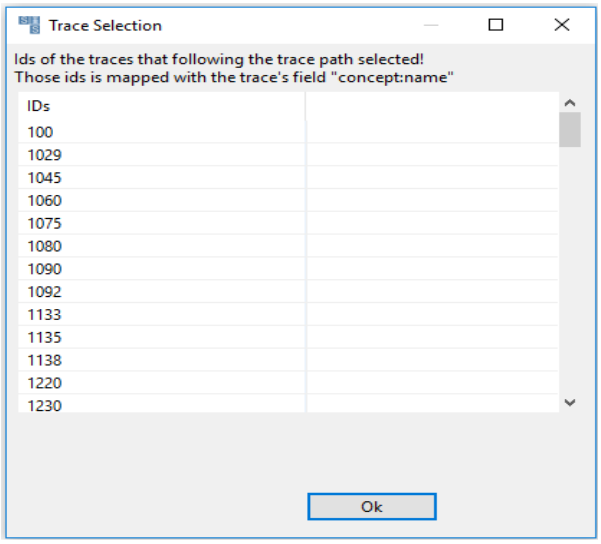

Figure 15 Show Trace ids dialog

FIGURES

Figure 1 Install New Software menu 1
Figure 2 Available Software dialog 1
Figure 3 Analysis Menu 2
Figure 4 Window menu 3
Figure 5 Preferences dialog 3
Figure 6 Import file message 4
Figure 7 Import file dialog 4
Figure 8 Security Analysis of Log Deviations Wizard dialog 5
Figure 9 Mapping Page dialog 5
Figure 10 Select Parameters Page dialog 6
Figure 11 Analysis Results dialog 7
Figure 12 Security Deviations view. 8
Figure 13 Deviations view 8
Figure 14 Trace Selection dialog 9
Figure 15 Show Trace ids dialog 9

REFERENCES

[1] "Business Process Model and Notation (BPMN)," OMG, 1 2011. [Online]. Available: http://www.omg.org/spec/BPMN/2.0/.

[2] IEEE Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams," in IEEE Std 1849-2016 , vol., no., pp.1-50, Nov. 11 2016

[3] Common Format and MIME Type for Comma-Separated Values (CSV) Files. [Online]. Available: https://tools.ietf.org/html/rfc4180.

[4] Petri Net Markup Language. [Online]. Available: http://www.pnml.org/papers.php