GRIF 2011

Module SIL

User manual

Version 31 January 2011

Table of Contents

1. Introduction

This module of GRIF is used for PFD computations. We will focus on the processing of Safety Instrumented Functions (SIF) on continuous process installations (safeties functioning in "on demand mode"). The computations carried out are safety computations; the top event is a non-detected dangerous failure of the SIS safety function.

The definitions and parameters used in this document are explained in the glossary (cf Section 8, “Glossary”)

2. Prerequisites and Installation

This chapter describes the procedure to follow before the software can be used. Because an external computation engine is used, certain prerequisites are necessary.

2.1. Prerequisites

The minimum hardware requirement is a Pentium IV (or more) with 512 MB memory. Works under Window XP, Vista and 7

2.2. Installation of TOTAL version without

TOTAL's version of the GRIF software does not require an installation procedure. You must unzip the GRIF 201X-Module SIL.zip in the directory of your choice. The path of directory must not contain any special characters such as: {,},[,],(,),$,%, etc.

In the following chapters, we will assume you have unzipped the file in C:\Programmes\Total\GRIF 201X-Module SIL\

2.3. Installation of retail version with installer and demonstration version

The retail version of software is provided with a file whose name is GRIF 201X.zip . Unzip the file (on your desktop for exemple), ans launch GRIF-Install-Win32.exe. A window will guide you through installation step. If you haven't purchase GRIF, please select demo at the end of inttallation.

In the following chapters, we will assume you have install GRIF in C:\Programmes\Total\GRIF 201X\

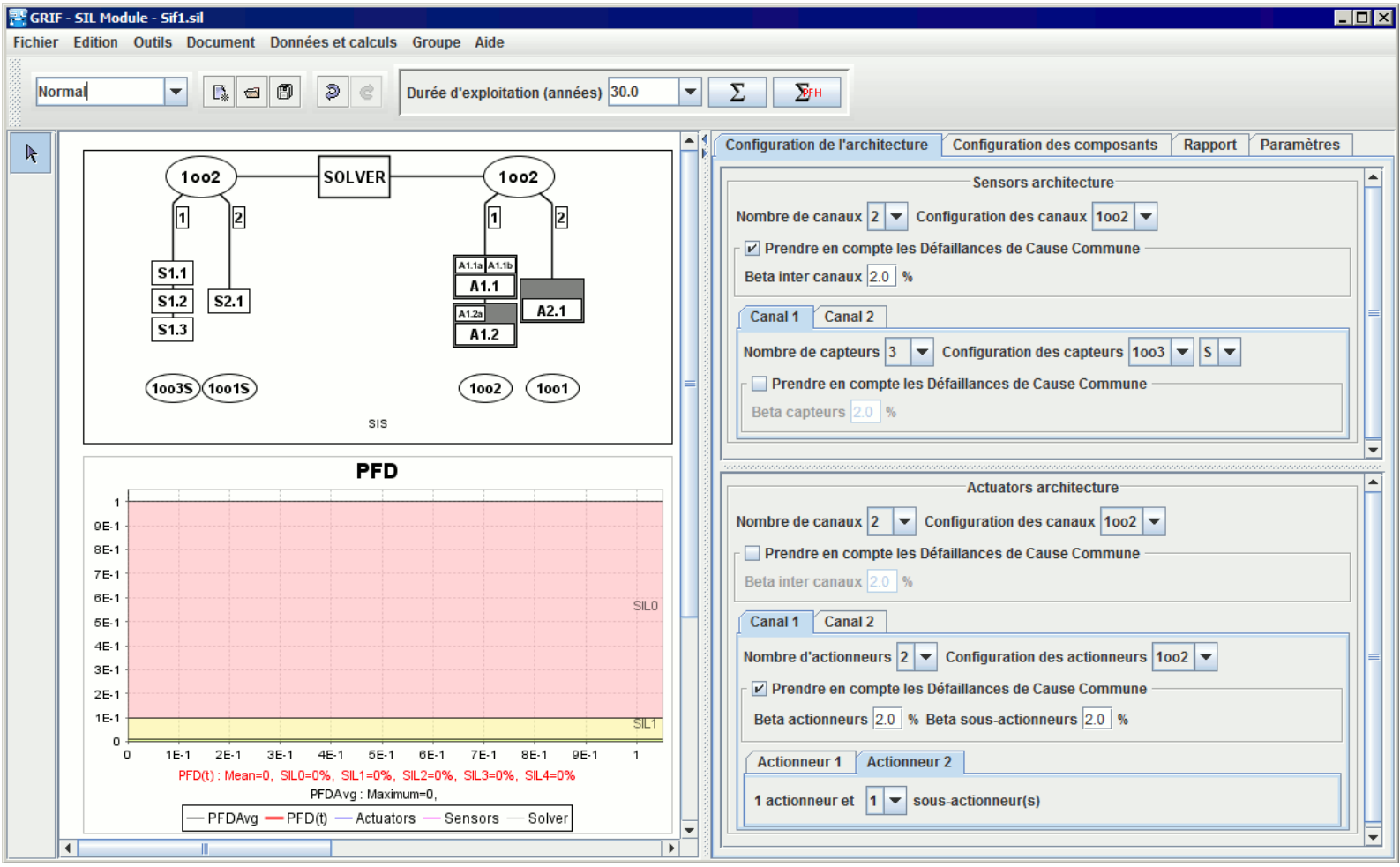
2.4. Saving

Data generated by GRIF are saved in "USER" directory. With Windows XP it is **C:\Documents And Setting \USER**, with Windows Vista and Windows 7 it is **C:\Users\USER**. The name USER is usually your name or your identification number with which you have openned your session on computer.

GRIF Module SIL saves its files in USER/GRIF/SIL/Application

2.5. Launching

The software is now ready for use. To launch the SIL module, double-click on SIL.bat qui is in directory where GRIF bas been installed. In retail version, you can also use the Start menu (Sofwares/Sdf/GRIF 201X).



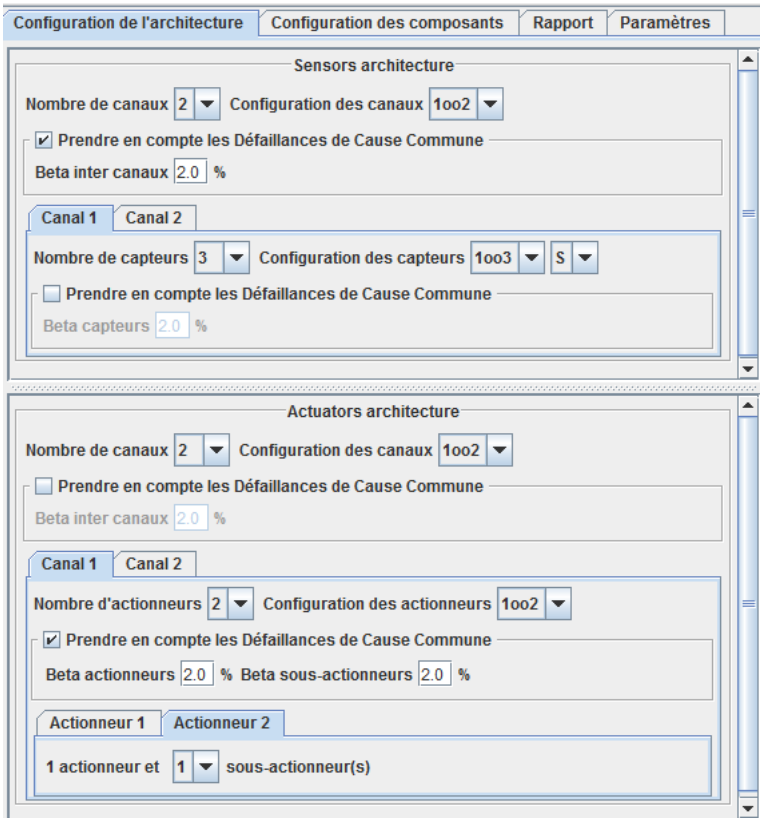
3. Selecting the SIS architecture

When module is launched, it contains a picture representing the architecture as well as an empty chart as no computations have yet been carried out.

In the tool-bar on the top of the window, the **Operating duration** area lets you specify the operating duration, and launch computation.

On the right, the **Parameters** tab contains the definitions of the model's parameters, the **Sensor(s)** tab is used to configure the safety loop's sensors, the **Solver** tab is used to configure the solver, the **Actuator(s)** tab is used to configure the actuators and the **Report** tab contains the information pertaining to the reports.

The **Configuration of architecture** tab enables to define architecture. Each modification made on the tab is visible on piture of architecture.



The top part of the tab : **Configuration of architecture** enables to define the configuration of sensor part. Possible choices are:

- **The number of chanels and the (logical) configuration between chanels**.
- **Taking Common Cause failure into account for all sensors**.
- **Number of components in each chanel and the configuration of these components in the chanel**.
- **Taking Common Cause failure into account for sensors of a chanel**.

The bottom of **Configuration of architecture** tab enables to define the configuration of sensor part. Possible choices are:

- **The number of chanels and the (logical) configuration between chanels**.
- **Taking Common Cause failure into account for all actuators**.
- **Number of actuators in each chanel and the configuration of these components in the chanel**.
- **For each actuator, the number of sub-actuators (0,1, or 2)**.

- **Taking Common Cause failure into account with a different Beta for actuators and for sub-actuators**.

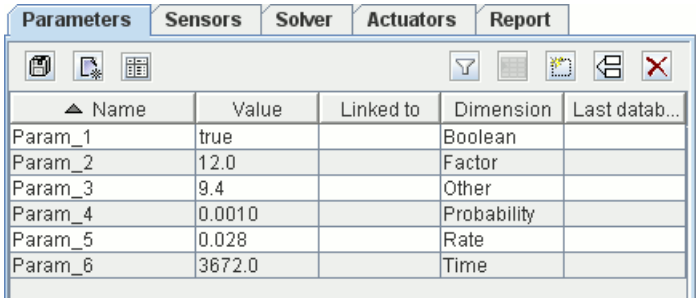
4. Editing the architecture

The objective is to specify the values particular to each element of the SIF being studied.

NB: In the following chapters, all the numerical values entered can be real numbers, where the decimal separator is a dot. It is possible to write them as such: 0.0000015 or in scientific notation: 1.5E-6

4.1. Editing the parameters

The parameters table contains all of the model's parameters.



Name	Value	Linked to	Dimension	Last datab...
Param_1	true		Boolean	
Param_2	12.0		Factor	
Param_3	9.4		Other	
Param_4	0.0010		Probability	
Param_5	0.028		Rate	
Param_6	3672.0		Time	

Each parameter is defined by the following:

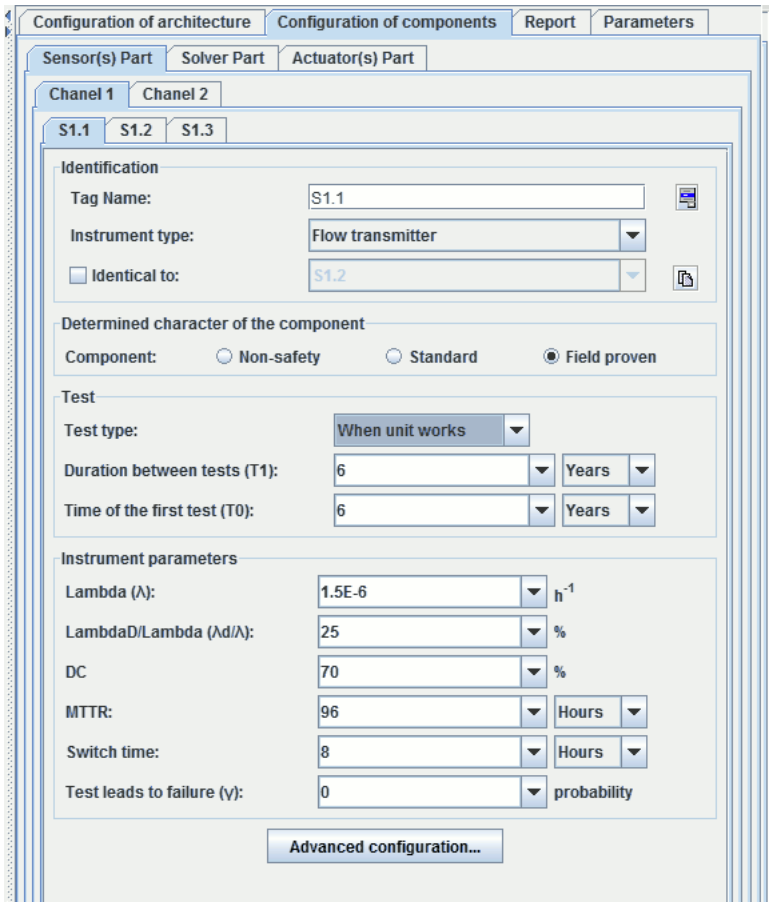
- **Name** : the parameter's name (unique).
- **Value** : the parameter's value (consistent with its dimension).
- **Linked to** : the identifier of the database to which the parameter is linked.
- **Dimension** : the parameter's dimension. It is selected from a drop-down menu: Boolean, factor, probability, rate, time, other.
- **Last database** : last database used to update the parameter.

The parameters can then be used to fill in the characteristics of the safety loop's components.

This table can be accessed using the tabs situated on the right but can also be opened in another window via the menu **Data and Computations - Edit parameters**.

4.2. Configuring the sensors

The sensors of the safety loop can be configured in the **Configuration of components**/**Sensor(s) Part** tab. Each sensor can be accessed separately in the sub-tabs **S1.1**, **S1.2**, etc. The first number (before the dot) is the chanel number, the second (after the dot) is the position in the chanel.



In the following paragraph, the sensor will be called "the component".

The component is configured using the following parameters:

- **Tag** : component's instrument tag on PID (e.g.: 10 PT 2034 for a sensor, or 10 UV 2034 for an actuator).
- **Instrument type** : type of instrument used. It is selected from a drop-down menu.
- **Identical to** : used to specify whether the component is identical to another component of the same type (i.e. a sensor when editing a sensor, another main actuator when editing a main actuator or another main or sub-actuator when editing a sub-actuator. The reference component is selected from a drop-down list. This functionality can only be accessed when the SIF comprises several components of the same type. If the checkbox is checked, only the **Tag** and **Instrument type** characteristics of the component can be edited (the others are identical to the reference component).
- **Copy another component's parameters** : enables you to copy the parameters of another component of the same type. This functionality can only be accessed when the SIF comprises several components of the same type. Only the characteristics **Tag** and **Identical to** are not copied. The components available are the same as those displayed for the functionality **Identical to**.
- **Modify the default parameters of the application** : enables you to manage the default parameters of the application and the document model system. Four actions can be chosen from the drop-down menu, displayed with a left click on the button:
  - **Save as default model** Save as default model. : saves the component's characteristics in the default model.

- **Re-intialyse to default values** 

: copies into the component the characteristics stored in the default model.
- **Save in a model file** 

: saves the component's characteristics in a model file, whose location must be specified. This file can be reused or sent to another person.
- **Use a model**

: copies into the component the characteristics stored in a model whose location must be specified.

- **Determined character of the component** : enables you to specify the component's determined character. The component is characterised by one of the three characters available **Non safety** : indicates that the component is operating in negative safety mode (energise to trip) and has no self-diagnostic system. **Standard** : indicates that the component is operating in positive safety mode (fail-safe) or is equipped with a self-diagnostic system. **Field-proven** : indicates that the component is operating in positive safety mode (fail-safe) and proven in use (or certified) and equipped with a self-diagnostic system (or implementation of regular proof tests) and has protected access safeguarding the settings of the internal configuration parameters.

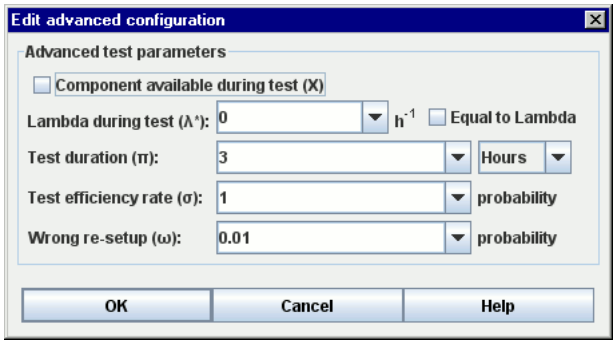
- **Test type** : enables you to specify the type of test used for the component. Two types of test can be selected from the drop-down menu:
  - **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
  - **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.

  Remark: it is also possible to specify that the component will undergo no periodic test.
- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).
- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.
- **LambdaD/Lambda (**$\lambda d/\lambda$**)** : proportion of dangerous failures among the total number of failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **MTTR (in h)** : mean time between detection of a failure and the repair of the component (Mean Time To Repair). The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.
- **Test leads to failure**γ **(Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 = no test causes any failure, 1 = 100% of the tests cause failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

- **Switch time parameter** : is the period of time during which the component causing the failure is disconnected from the system and replaced by a component in working order. This time is necessarily lower than the MMTR.

The advanced parameters of a sensor can be specified by left clicking on the **Advanced configuration button**.

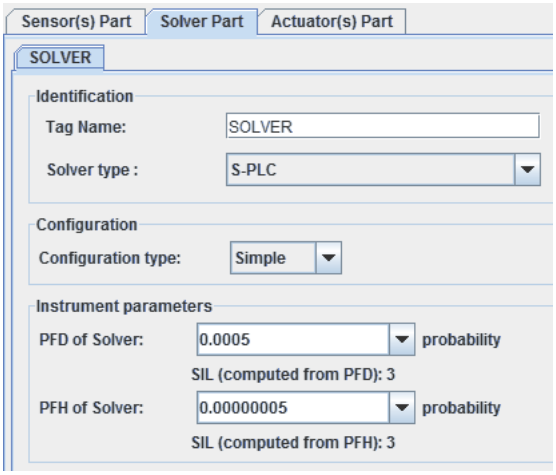


The advanced parameters of the sensor are as follows:

- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ du).
- **Test duration π (Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup ω (Omega)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being repaired by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

4.3. Configuring the solver

The solver of the safety loop can be configured in the **Solver** tab.



The solver is configured using the following parameters:

- **Tag** : solver's instrument tag on PID (e.g.: 10 ESD 06).

- **Solver type** : type of solver used. It is selected from a drop-down menu.

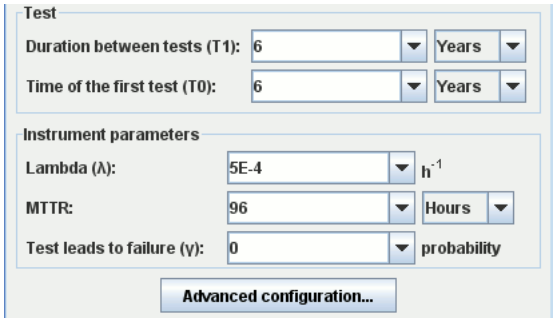
- **Configuration type** : specifies the solver's configuration type. Two types of configuration can be selected from the drop-down menu:
  - **Simple** : the solver is modelled by a constant law.
  - **Advanced** : the solver is modelled by a full periodic test law.

The parameters of the solver are described under **Instrument parameters**. They depend on the type of configuration which has been selected.

In the case of a simple configuration, the parameters are as follows:

- **PFD of solver** : probability that the solver will not work when triggered. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.
- **SIL (computed from PFD)** : automatically displays the solver's SIL computed based on the solver's PFD.
- **PFH of solver** : the PFH of the solver, given by manufacturer or by experience feedbacks.
- **SIL (computed from PFH)** : automatically displays the solver's SIL computed based on the solver's PFH.

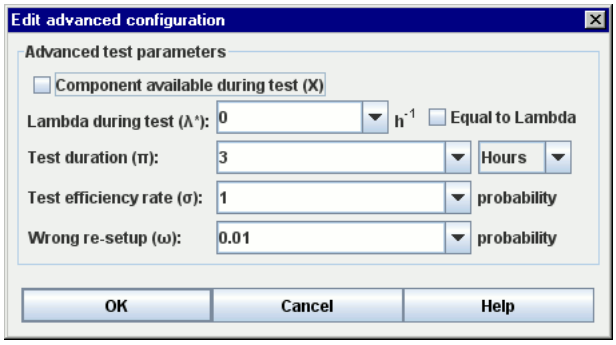
In the case of an advanced configuration, the parameters are as follows:



- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).
- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.
- **MTTR (in h)** : mean time between detection of a failure and the repair of the component (Mean Time To Repair). The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.
- **Test leads to failure** γ **(Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 = no test causes any failure, 1 = 100% of the tests cause failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

Other parameters can be accessed by left clicking on the **Advanced configuration ...** button (only for a solver configured in advanced mode).



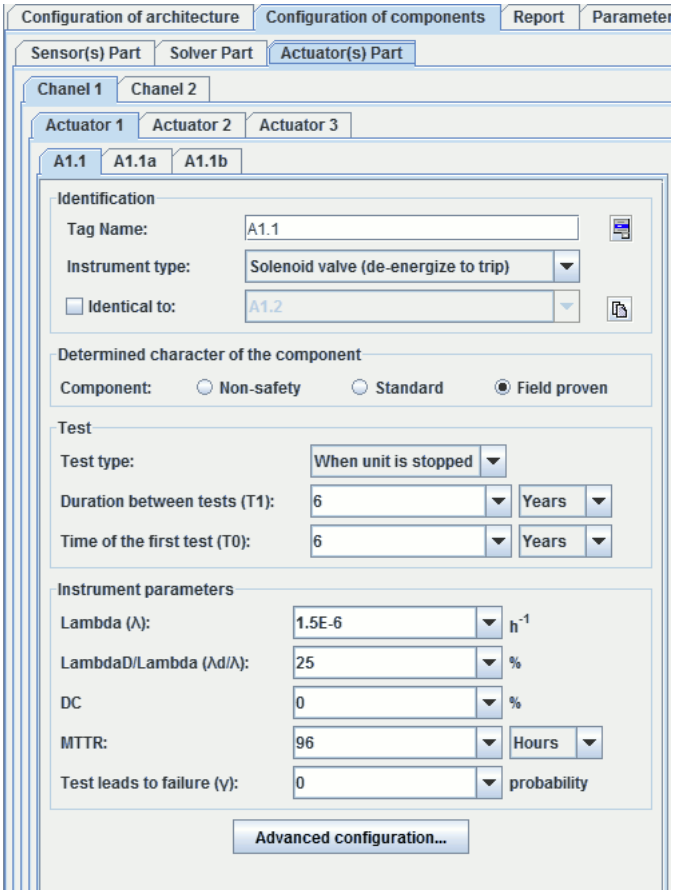
- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ du).
- **Test duration π (Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup ω (Omega)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being repaired by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

4.4. Configuring the actuators

The actuators of the safety loop can be configured in the **Configuration of componentsActuator(s) Parts** tab. The actuators can be classified as follows:

- **Main actuators** : they are set up in parallel and have 0, 1 or 2 sub-actuators.
- **Sub-actuators** : they are set up in series with their respective actuators. The sub-actuators of a same main actuator are set up in parallel.

each main actuator can be accessed separately in the sub-tabs **A1.1**, **A1.2**, ..., and each sub-actuator in the sub-tabs **A1.1a**, **A1.1b**, ...



In the following paragraph, the actuator (main or sub) will be called "the component".

The component is configured using the following parameters:

- **Tag** : component's instrument tag on PID (e.g.: 10 PT 2034 for a sensor, or 10 UV 2034 for an actuator).
- **Instrument type** : type of instrument used. It is selected from a drop-down menu.
- **Identical to** : used to specify whether the component is identical to another component of the same type (i.e. a sensor when editing a sensor, another main actuator when editing a main actuator or another main or sub-actuator when editing a sub-actuator. The reference component is selected from a drop-down list. This functionality can only be accessed when the SIF comprises several components of the same type. If the checkbox is checked, only the **Tag** and **Instrument type** characteristics of the component can be edited (the others are identical to the reference component).
- **Copy another component's parameters** : enables you to copy the parameters of another component of the same type. This functionality can only be accessed when the SIF comprises several components of the same type. Only the characteristics **Tag** and **Identical to** are not copied. The components available are the same as those displayed for the functionality **Identical to**.
- **Modify the default parameters of the application** : enables you to manage the default parameters of the application and the document model system. Four actions can be chosen from the drop-down menu, displayed with a left click on the button:
  - **Save as default model** Save as default model. : saves the component's characteristics in the default model.
  - **Re-intialyse to default values** Re-initialyse to default values. : copies into the component the characteristics stored in the default model.
  - **Save in a model file** Save in a model-file ... : saves the component's characteristics in a model file, whose location must be specified. This file can be reused or sent to another person.

- **Use a model**

: copies into the component the characteristics stored in a model whose location must be specified.

- **Determined character of the component** : enables you to specify the component's determined character. The component is characterised by one of the three characters available **Non safety** : indicates that the component is operating in negative safety mode (energise to trip) and has no self-diagnostic system. **Standard** : indicates that the component is operating in positive safety mode (fail-safe) or is equipped with a self-diagnostic system. **Field-proven** : indicates that the component is operating in positive safety mode (fail-safe) and proven in use (or certified) and equipped with a self-diagnostic system (or implementation of regular proof tests) and has protected access safeguarding the settings of the internal configuration parameters.

- **Test type** : enables you to specify the type of test used for the component. Two types of test can be selected from the drop-down menu:
  - **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
  - **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.

  Remark: it is also possible to specify that the component will undergo no periodic test.
- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).
- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

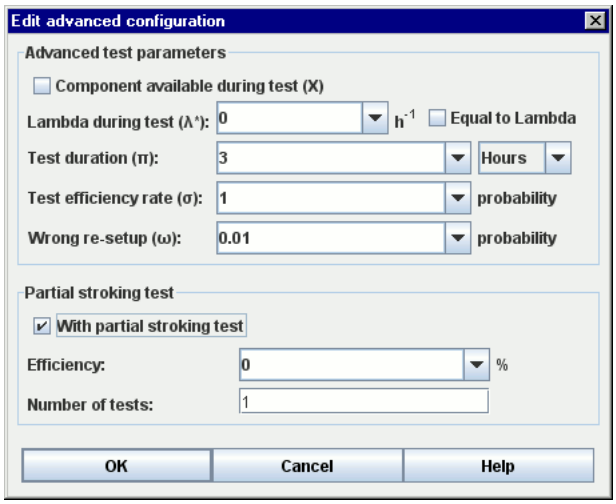
- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.
- **LambdaD/Lambda (**λ**d/**λ**)** : proportion of dangerous failures among the total number of failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **MTTR (in h)** : mean time between detection of a failure and the repair of the component (Mean Time To Repair). The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.
- **Test leads to failure**γ **(Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 = no test causes any failure, 1 = 100% of the tests cause failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

Important

NB about Sub-actuators

: Sub-actuators do not have a **Determined character of the component** characteristic. The section relating to this characteristic does therefore not appear when configuring the sub-actuators. As a rule, the sub-actuator has the same character as the one defined for its main actuator.

The advanced parameters of an actuator (main or sub) can be specified by left clicking on the **Advanced configuration** button.



The advanced parameters of the actuator are as follows:

- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ du).
- **Test duration π (Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup ω (Omega)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being repaired by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

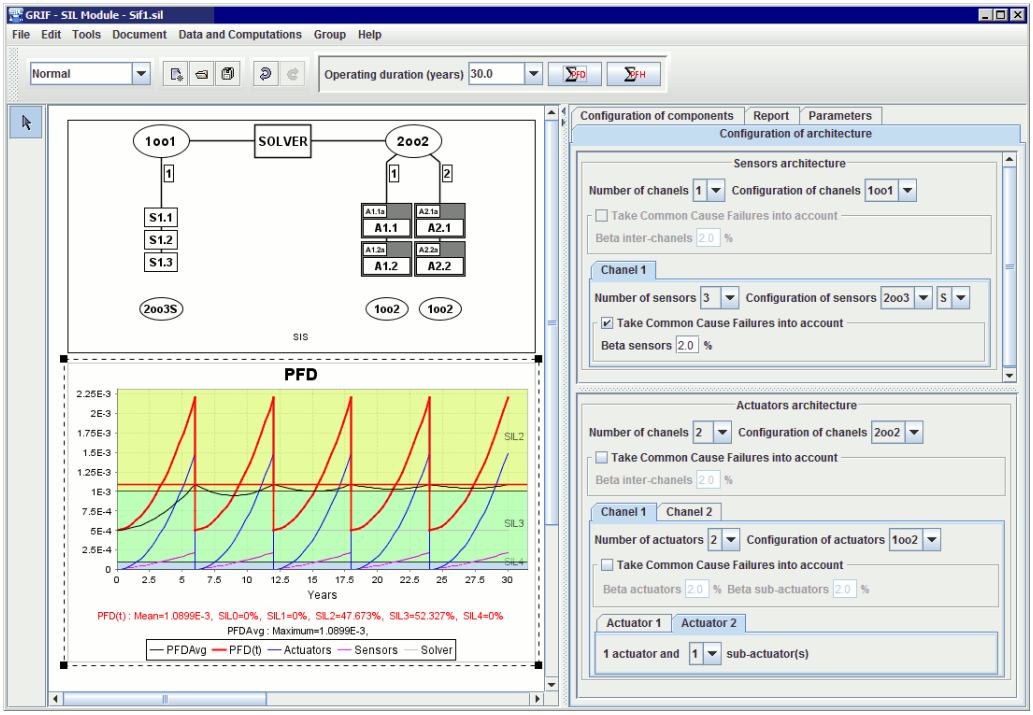
- **With partial stroking test** : if checked, specifies whether the component takes partial stroking tests into account, as for example the partial stroke testing of a valve gate.
- **Efficiency of partial stroking tests** , **Proportion of detected failure** :proportion of hidden failures detected during partial stroking tests (0-100%). 0% means no failure is detected, 100% means every failure is detected. The value of the efficiency can be edited manually or selected from a drop-down list displaying all the parameters with a Factor dimension. This characteristic is accessible only if the component takes partial stroking tests into account.
- **Number of tests** : number of partial stroking tests carried out between two full tests.

NB: Sub-actuators do not take partial stroking tests into account. There is therefore no Partial stroking test section in the sub-actuator configuration tab.

5. Computing the SIF's PFD

When all of the components have been configured, computations can be started. PFD Computations are launched via the menu **Data and Computations/Launch PFD computations** or by clicking on the  icon. PFH Computations are launched via the menu **Data and Computations/Launch PFH computations** or by clicking on the  icon.

The chart, which contained no information, has now been updated.



Reminder: The combination Control+Scroll wheel enables you to enlarge (zoom in) or reduce the window.

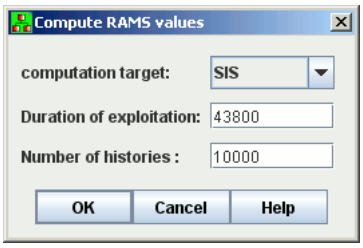
The x-axis represents the time in hours and the y-axis represents the probability of failure of the SIF when triggered, also called PFD. The chart ranges from 0 to 30 years by default but it is possible to modify this value as explained in the chapter on curves. There are 5 curves in the chart:

- **PFD(t) or PFH(t)** : the instantaneous value of the system's PFD/PFH.
- **PFD Avg or PFH** : the average value of the system's PFD/PFH.
- **Actuators** : the instantaneous value of the PFD/PFH of the actuator part of the system.
- **Sensors** : the instantaneous value of the PFD/PFH of the sensor part of the system.
- **Solver** : the instantaneous value of the solver's PFD/PFH.

The curves are located in one or several bands of colour. These bands represent the PFD ranges, which define the SIL:

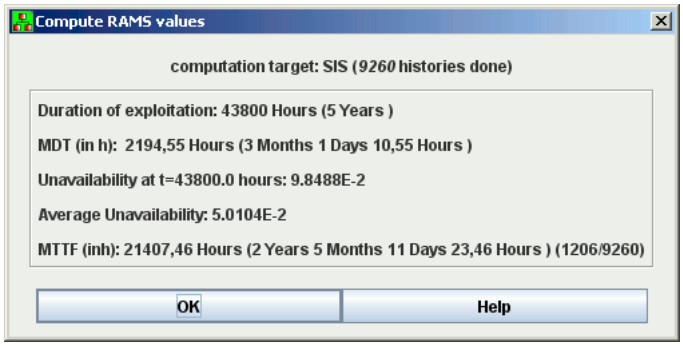
- **SIL 0** : instantaneous PFD $\in [10^{-1}; 1]$. PFH $\in [10^{-5}; +\text{infinity}]$.
- **SIL 1** : instantaneous PFD $\in [10^{-2}; 10^{-1}[$. PFH $\in [10^{-6}; 10^{-5}[$.
- **SIL 2** : instantaneous PFD $\in [10^{-3}; 10^{-2}[$. PFH $\in [10^{-7}; 10^{-6}[$.
- **SIL 3** : instantaneous PFD $\in [10^{-4}; 10^{-3}[$. PFH $\in [10^{-8}; 10^{-7}[$.
- **SIL 4** : instantaneous PFD $\in [0; 10^{-4}[$. PFH $\in [0; 10^{-8}[$.

For advanced users, a menu can be used to launch computations based on Monte-Carlo simulation. The computation is launched from the menu **Data and Computations / Computation of SDF values**. A window for configuring the simulation appears:



- **Computation target** : enables you to specify the target studied by the computations.
- **Duration of exploitation (in h)** : enables you to specify the period of time over which the simulation will be carried out.
- **Number of histories** : enables you to specify the number of histories played out.

The results obtained are values generally computed in dependability:



- **Duration of exploitation (in h)** : recalls the duration of exploitation entered previously.
- **MDT (in h)** : indicates the mean time between the occurrence of a failure and the re-start of the system (Mean Down Time). It is the average downtime.
- **Unavailability at t=xxx** : indicates the probability that the system will be unavailable at time t. Time t (xxx) is equal to the duration of exploitation.
- **Average unavailability** : indicates the mean unavailability over the duration of exploitation.
- **MTTF (in h)** : indicates the mean time between the start-up of the system and the occurrence of the first failure (Mean Time To Failure). It is the average time of operation before the first failure occurs. $\lambda = 1/$ MTTF for a component. There may be information between brackets: number of histories where a failure occurred/ number of histories played out; if there is no failure, there will logically be no time of first failure and the history will not be taken into account when computing the MTTF. This is why the number of stories used for computing the MTTF is indicated.

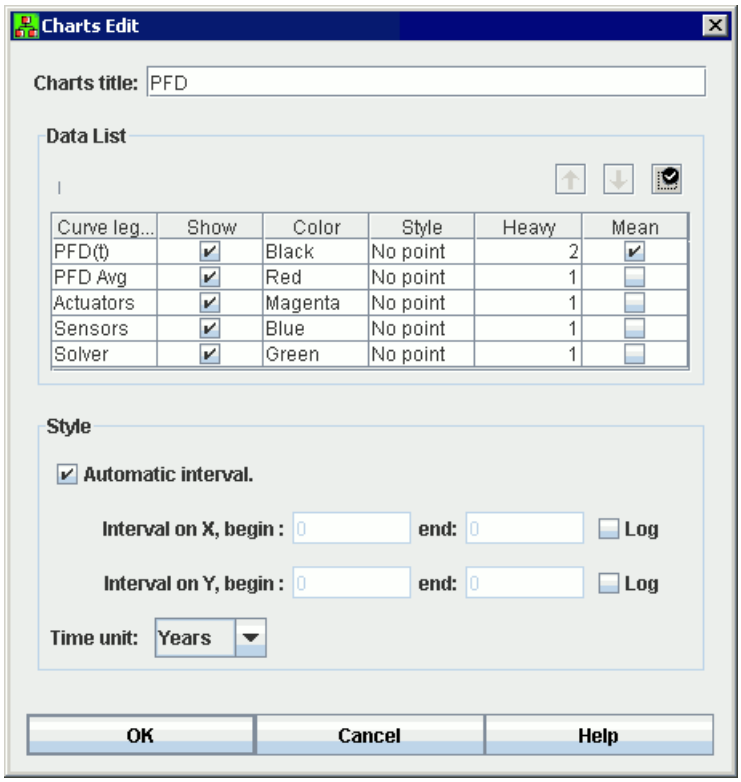
Depending on the end user of the software, this function may or may not be accessible.

6. Charts

Curves are drawn to study the results better. Five curves are available : PFDAvg(t), $PFD_{System}(t)$, $PFD_{Actuators}(t)$, $PFD_{Solver}(t)$, $PFD_{Sensors}(t)$.

6.1. Charts Edit window

The Charts Edit window is displayed when user double-click on charts.



This window is divided into several parts:

1. **Charts Title**: allows you to give a title to the graphic.
2. **Data List**: This part contains a three-column table listing the chart's different curves (name, description, display, curve colour, curve style, curve thickness).Several buttons are available above this table.
   - **Up** : moves the selected curve upwards in the list.
   - **Down** : moves the selected curve downwards in the list.
   - **Save as default model** : saves current chart setting as default setting for new documents.

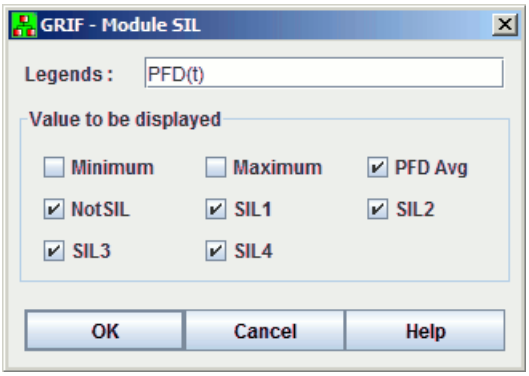
   For each curve, you can specify its colour, its style of points, its thickness and its display options.
3. **Style**: This part deals with displaying curves.
   - **Style type**: specifies the type of all the chart's curves (line or histogram). N.B: For histogram style, bars going outside drawing zone will be drawn with a gradient to warn user that he has to change intervals to see the entire bar.
   - **Intervals on X and Y**: Specifies the display interval for the X and Y axes (default interval or user-defined interval). This last function can, for example, be used to zoom in on the most interesting parts of the curve.

     The **log** check boxes are used to enable the logarithmic scale on the axis concerned. Important: 0 cannot be represented on a log scale, remember to give a strictly positive starting point (e.g.: E-10). If 0 is given, the log scale will start with an arbitrary value E-15.

When domain axe deals with time, you can choose time unit among : hours, days, months, years. Default display is "hours" because it is the usualy used unit for modeling. It's only available in SIL module.

6.2. Editing the curves

When a curve is edited (with a double-click on its name in list of curves), the curve edition window is displayed. The following window id displayed :



The window is divided into three parts:

- **Legends**: enables you to give a title to the curve.
- **Value to be displayed**: used to select the values which are to be displayed or not below the curve.

  For SIL curve (probability functions of times), available values are :
  - **NonSIL** : percentage of time spent in SIL 0.
  - **SIL 1** : percentage of time spent in SIL 1.
  - **SIL 2** : percentage of time spent in SIL 2.
  - **SIL 3** : percentage of time spent in SIL 3.
  - **SIL 4** : percentage of time spent in SIL 4.
  - **PFDMax** : the maximum instantaneous PFD over the period studied.
  - **PFDAvg** : the average of the PFD over the period studied.

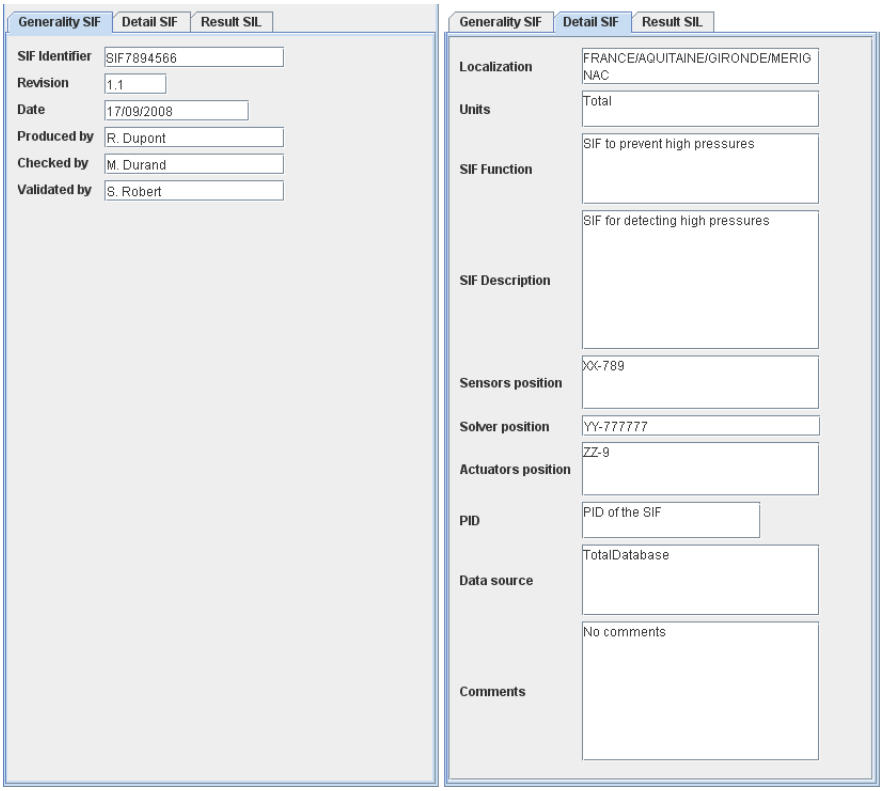
  For average probability curves (like PFDAvg), available values are :
  - **Minimum** : the minimum value of the average PFD over the period studied.
  - **Maximum** : the maximum value of the average PFD over the period studied.
  - **Mean** : the average value of the average PFD over the period studied (which is NOT the PFDAvg).

When the values are entered, just click on **OK** to close the windows.

7. Generating reports

7.1. Generality et detail

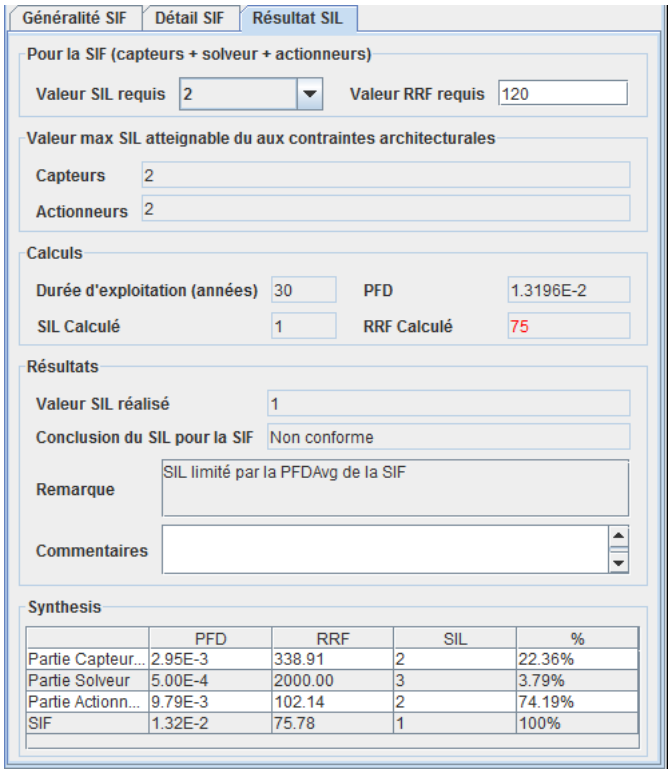
The PDF reports can be configured in the tab **Report** and its sub-tabs **Generality SIF**, **Detail SIF**:



- **SIF Identifier** : identifier of the SIF or report.
- **Revision** : revision index of the report.
- **Date** : date on which the report was issued.
- **Produced by** : name of the author of the report.
- **Checked by** : name of the checker of the report.
- **Validated by** : name of the person who validated the report

- **Localization** : specify the refinery, the platform, the plant.
- **Units** : specify the units, the sectors, the workshops, the project.
- **SIF Function** : function of the SIF (top event).
- **Description of the SIF** : description of the SIF.
- **Sensors position** : instrument tag of the SIF sensors.
- **Solver position** : name of the solver.
- **Actuators position** : instrument tags of the SIF actuators.
- **PID** : number of the PID.
- **Data source** : source of the data used in the computations (e.g.: TOTAL, EXIDA, OREDA, etc.).
- **Comments** : comments.

7.2. Result SIL



Result SIL tab do a synthesis of results. On the top of the tab you must specify the objectives to be reached :

- **Required SIL** : value of the SIL required for the SIF.
- **Required RRF** : value of the RRF required for the SIF.

Then the softwre reminds you the maximum reachable SIL of each part. (not available if many chanels)

- **Maximum reachable SIL for sensors** : maximum SIL which can be reached by the sensors due to architectural constraints.
- **Maximum reachable SIL for actuators** : maximum SIL which can be reached by the actuators due to architectural constraints.

The "Computation" part reminds the computed values

- **Operation duration** : The duration used to do computation.
- **PFD or PFH** : computed PFDAvg or PFH.
- **Computed SIL** : SIL obtained with computed PFD or PFH. Architectural contraints are not taken into account.
- **RRF Calculé** : RRF obtained with computed PFD or PFH.

Then the results part says if objectives are reached or not.

- **Achieved SIL** : SIL obtained for the SIF according to the PFD computation and architectural constraints.
- **Conclusion of SIL for the SIF** : conclusion (compliant or non-compliant).
- **Remark** : Remark generated by the software. It shows the part whose Max-SIL is limiting.
- **Comments** : Comments made by user.

At the end of the tab, a table shows you values for each part in order to identify the most important contributor.

7.3. Different reports

When all the computations have been carried out, two types of report can be generated:

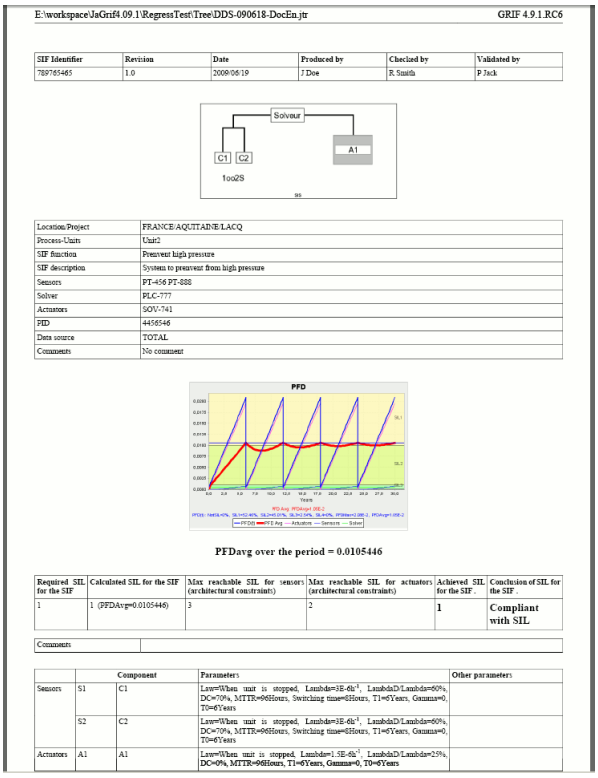
- **Internal PDF Report** : this type of report is very detailed. It includes all the information on the results obtained, the input parameters, etc.

- **External PDF Report** : this type of report can be circulated outside the site. It is a summary of the main results.

The language of the report (English or French) can be selected for each type of report.

the internal PDF report is generated from the menu **File/Create a report/Internal PDF report (en)** (report written in English) or from the menu **File/Create a report/Internal PDF report (fr)** (report written in French). The external PDF report is generated from the menu **File/Create a report/External PDF report (en)** (report written in English) or from the menu **File/Create a report/External PDF report (fr)** (report written in French). In all four cases, you must select the location where the PDF file is to be stored and click on save. When the report is generated, it is opened with the programme associated with the PDF format (generally Acrobat Reader).

Internal PDF report:



E:\workspace\JaGrif4.09.1\RegressTest\Tree\DDS-090618-DocEn.jtr GRIF 4.9.1.RC6

SIF Identifier	Revision	Date	Produced by	Checked by	Validated by
789765465	1.0	2009/06/19	J Doe	R Smith	P Jack

Location/Project	FRANCE/AQUITAINE/LACQ
Process-Units	Unit2
SIF function	Preserve high pressure
SIF description	System to preserve from high pressure
Sensors	PT-456 PT-888
Solver	PLC-777
Actuators	SOV-741
PID	4456546
Data source	TOTAL
Comments	No comment

PFDavg over the period = 0.0105446

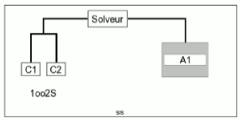
Required SIL for the SIF	Calculated SIL for the SIF	Max reachable SIL for sensors (architectural constraints)	Max reachable SIL for actuators (architectural constraints)	Achieved SIL for the SIF.	Conclusion of SIL for the SIF.
1	1 (PFDAvg=0.0105446)	3	2	1	Compliant with SIL

Comments	

	Component		Parameters	Other parameters
Sensors	S1	C1	Law=When unit is stopped, Lambda=3E-6h^{-1}, LambdaD/Lambda=60%, DC=70%, MTTR=96Hours, Switching time=6Hours, T1=6Years, Gamma=0, T0=6Years	
	S2	C2	Law=When unit is stopped, Lambda=3E-6h^{-1}, LambdaD/Lambda=60%, DC=70%, MTTR=96Hours, Switching time=6Hours, T1=6Years, Gamma=0, T0=6Years	
Actuators	A1	A1	Law=When unit is stopped, Lambda=1.5E-6h^{-1}, LambdaD/Lambda=25%, DC=0%, MTTR=96Hours, T1=6Years, Gamma=0, T0=6Years	

External PDF report:

SIF Identifier	Revision	Date	Produced by	Checked by	Validated by
789765465	1.0	2009/06/19	J Doe	R Smith	P Jack



Location/Project	FRANCE/AQUITAINE/LACQ
Process-Units	Unit2
SIF function	Prevent high pressure
SIF description	System to prevent from high pressure
Sensors	PT-456 PT-888
Solver	PLC-777
Actuators	SOV-741
PID	4456546
Data source	TOTAL
Comments	No comment

PFDavg over the period = 0.0105446

Required SIL for the SIF	Calculated SIL for the SIF	Max reachable SIL for sensors (architectural constraints)	Max reachable SIL for actuators (architectural constraints)	Achieved SIL for the SIF .	Conclusion of SIL for the SIF .
1	1 (PFDAvg=0.0105446)	3	2	**1**	**Compliant with SIL**

Comments	

	Component		Parameters
Sensors	S1	C1	Law=When unit is stopped, Lambda=3E-6h^{-1}, LambdaD/Lambda=60%, DC=70%, MTTR=96Hours, Switching time=8Hours, T1=6Years, Gamma=0, T0=6Years
	S2	C2	Law=When unit is stopped, Lambda=3E-6h^{-1}, LambdaD/Lambda=60%, DC=70%, MTTR=96Hours, Switching time=8Hours, T1=6Years, Gamma=0, T0=6Years
Actuators	A1	A1	Law=When unit is stopped, Lambda=1.5E-6h^{-1}, LambdaD/Lambda=25%, DC=0%, MTTR=96Hours, T1=6Years, Gamma=0, T0=6Years
Solver	SOLVER	SOLVEUR	Law=Constant, PFD solver=0.0005, SIL solver=3

8. Glossary

8.1. Format

All values can be entered in two different ways:

- **"Normal" notation** : the decimal separator is the dot, e.g. 0.0000015.
- **Scientific notation** : the decimal separator is the dot, e.g. 1.5E-6 which corresponds to 0.0000015.

8.2. Definition and explanation of the acronyms and parameters

- **Beta (β)** : proportion of common cause failures (in %).
- **CCF or DCC** : Common Cause Failure. When several identical elements are put in a system, there is always a probability that they will fail at the same time from a common cause (design problem, external phenomena for example). This is called a common cause failure.
- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected.
- **Detected** : applies to the equipment and means detected by diagnostic tests, periodic tests or human intervention (e.g. physical inspection and manual tests) or during normal operation.
- **DCS** : Distributed Control System
- **Determinate** : A component can be one of these 3 types : "Non Safety", "Standard" or "Field proven"
- **Duration between tests (T1)** : period of time between two proof tests of the component.
- **E/E/PE** : electrical/electronic/ programmable electronic. Technology based on electricity (E), and/or electronics (E) and/or programmable electronics (EP). NB. - This term designates all devices which work according to electrical principles.
- **Efficiency of partial stroking tests** , **Proportion of detected failure** :proportion of hidden failures detected during partial stroking tests (0-100%). 0% means no failure is detected, 100% means every failure is detected.
- **External PDF Report** : this type of report can be circulated outside the site. It is a summary of the main results.
- **Failure** : a functional unit ceases to accomplish its required function.
- **Internal PDF Report** : this type of report is very detailed. It includes all the information on the results obtained, the input parameters, etc.
- **Lambda** λ : failure rate of the component (h^{-1}).
- **Lambda during test** λ***** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda.
- **Lambda D (λ d)** : dangerous failures. Failure with the potential to put the safety system into a dangerous state or make it unable to carry out its function.
- **MDT (in h)** : indicates the mean time between the occurrence of a failure and the re-start of the system (Mean Down Time). It is the average downtime.
- **MTTF (in h)** : indicates the mean time between the start-up of the system and the occurrence of the first failure (Mean Time To Failure). It is the average time of operation before the first failure occurs. λ = 1/ MTTF for a component.
- **MTTR (in h)** : mean time between detection of a failure and the repair of the component (Mean Time To Repair).
- **Non-detected (Undetected)** : applies to the equipment and means non-detected by diagnostic tests, periodic tests or human intervention (e.g. physical inspection and manual tests) or during normal operation.
- **Number of tests** : number of partial stroking tests carried out between two full tests.
- **Operating duration (Years)** : means the foreseen operating industrial duration of the Safety Instrumented Function (SIF) installed on its process unit.
- **PFD** : Probability of Failure on Demand. Cf. Norm IEC61508. Can be defined as Unavailability
- **PFH** : Probability of Failure per Hour. Cf. Norm IEC61508. Can be defined as Unconditionnal Failure Intensity
- **Redundancy** : implementation in parallel of elements which have the same safety function so that the sub-system is more available.

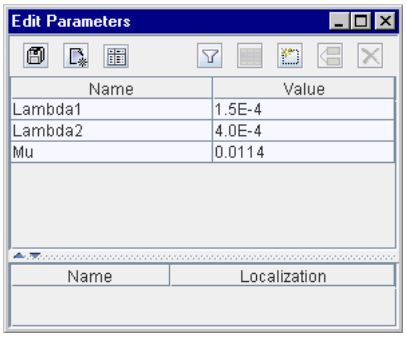
- **Repair rate μ (Mu)** : repair rate in $^{-1}$, whose symbol is (μ). This value is equal to 1/MTTR, for a repair time of 48h, Mu = 1/48 = 2.08E-2
- **R.R.F** : Risk Reduction Factor of the SIF
- **Safety function** : function to be carried out by an E/E/EP safety system, by a safety system based on another technology or by an external risk reduction device, designed to ensure or maintain the controlled system in a safe state with regard to a specific dangerous event.
- **SIF** : Safety Instrumented Function.
- **SIL 0** : instantaneous PFD ∈ $[10^{-1}; 1]$. PFH ∈ $[10^{-5}$; +infinity].
- **SIL 1** : instantaneous PFD ∈ $[10^{-2}; 10^{-1}[$. PFH ∈ $[10^{-6}; 10^{-5}[$.
- **SIL 2** : instantaneous PFD ∈ $[10^{-3}; 10^{-2}[$. PFH ∈ $[10^{-7}; 10^{-6}[$.
- **SIL 3** : instantaneous PFD ∈ $[10^{-4}; 10^{-3}[$. PFH ∈ $[10^{-8}; 10^{-7}[$.
- **SIL 4** : instantaneous PFD ∈ $[0; 10^{-4}[$. PFH ∈ $[0; 10^{-8}[$.
- **SIS** : Safety Instrumented System. Instrumented system used to carry out one or several safety functions. An SIS is made up of sensors, a logical processing system and actuators.
- **System** : set of elements which interact according to a specific model, an element, which may be another system called a sub-system. The sub-systems can themselves be either a command system or a controlled system made up of hardware, software and interacting with man.
- **S-PLC** : Safety-Programmable Logic Controller
- **Test duration π (Pi)** : period of time necessary for testing the component.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure).
- **Test leads to failureγ (Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 = no test causes any failure, 1 = 100% of the tests cause failures.
- **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
- **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.
- **Time of the first test (T0)** : time at which the first test of the component is carried out.
- **Vote with "D" type architecture** : the invalidity of the sensor triggers no action other than an alarm (availability).
- **Vote with "S" type architecture** : the invalidity of the sensor triggers the safety system (Safe).
- **Wrong re-setup ω (Omega)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being repaired by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.).

9. Appendix

9.1. Data Editing Tables

9.1.1. Description of the Tables

To create or modify data (parameters, variables, etc.), tables are available in the **Data and Computations menu**. All the GRIF 2011 data tables operate in the same manner.

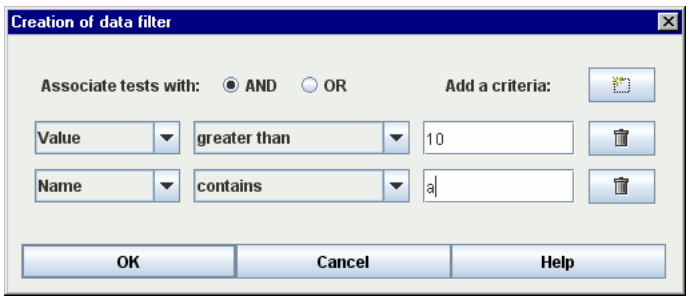


The data editing table/panel is divided into 3 parts:

- The top part containing the buttons.
- The main part containing the data table.
- The bottom part indicating what the selected data is used for.

	Saves the table in a text file.
	Opens the table in a text editor (that defined in the Options).
	Opens the column manager.
	When the **display selection** button is pressed, a click in the table leads to the selection in the input area.
	Displays the data filtering part.
	Multiple modifications made to all the selected data.
	Creates new data.
	Deletes the selected data (one or many).
	Enables data filtering or not.
	Defines the filter to be applied to the data.

Filtering allows you to display only what is necessary in a table. Several filtering criteria can be combined, as shown below:



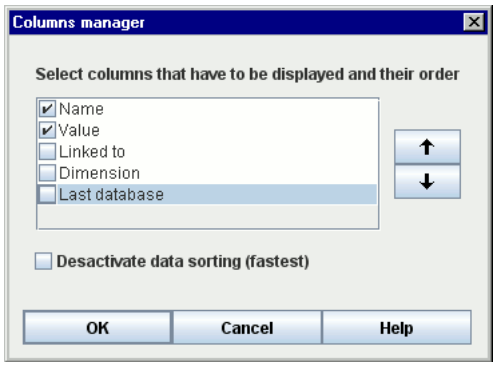
Select **AND** or **OR** to choose the type of association between each line (filter criterion). A line is a Boolean expression divided into 3 parts:

1. the first is the column on which the filter is used;
2. the second is the comparator;
3. the third is the value to which the data will be compared.

If the Boolean expression is true, the data will be kept (displayed); otherwise the data will be masked. When the filter is enabled its value is displayed between < and >.

The data in a column can be sorted by double clicking the header of this column. The first double click will sort the data in ascending order (small triangle pointing upwards). The second double click on the same header will sort the column in descending order (small triangle pointing downwards).

A table can contain many columns, some columns may be unnecessary in certain cases. The "linked to database" column is unnecessary when no database is available. It is thus possible to choose the columns to be displayed and their order. To do this, click right on a table header, or click the **Columns Manager** button, the following window opens:

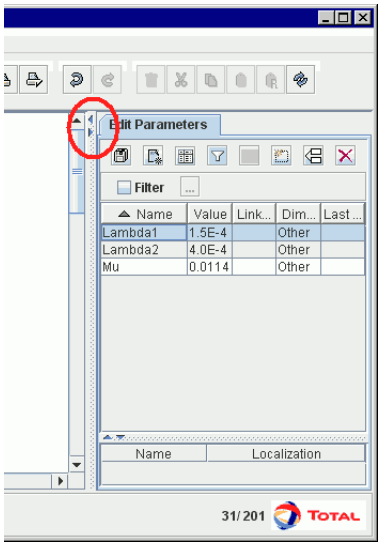


You can choose the columns to be displayed by selecting (or deselecting) the corresponding check boxes. The arrows on the right are used to move the columns up or down in the list to choose the order of the columns. The **Disable data sorting** check box disables the data sorting. This improves the application's performance with very complex models.

9.1.2. Arrangement of tables

As said before, tables are available in **Data and Computations** menu, In this case, each table is openned in a separate window.

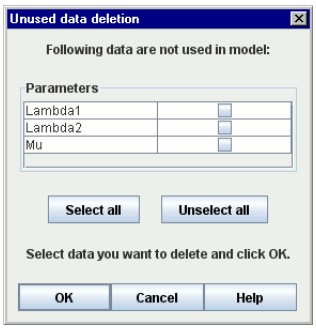
To decrease number of openned windows, tables are gathered in a tabbed pane at the right of the application. The pane can be "hiden" with the little arrows at the top of split-pane.



You can chose displayed tables with a right clic on the title of the tabs.

9.1.3. Table Cleaning

Data may not be used anymore, it can be used usefull to delete every unused data. To facilitate removal, use **Data and Computations / Unused data deletion** menu.



This window displays unused data. Select data you realy yan to delete and click OK.

9.2. Options of GRIF - SIL

Tools - Application Options menu opens a window containing the following tabs:

9.2.1. Executables

Executables tab enables to specify path to external executables :

- **Editor path** : Specifies text editor path.
- **Automatically open PDF files** : Specifies if PDF reports must be openned avec generation.
- **Style-sheet from XML to DocBook.** : Style-sheet allowing converting from XML report to docbook file.
- **Style-sheet from XML to HTML.** : Style-sheet allowing converting from XML report to HTML file.
- **Style-sheet from DocBook to PDF.** : Style-sheet allowing converting from docbook file to PDF file.
- **Moca-RPC path** : Specifies Moca version 12 path.
- **Javaw path** : Path of javaw.exe executable.
- **Style-sheet from XML to DocBook for internal SIL report.** : Style-sheet allowing converting from XML report to docbook file for internal SIL report.
- **Style-sheet from XML to DocBook for external SIL report.** : Style-sheet allowing converting from XML report to docbook file for external SIL report.

9.2.2. Database

Database tab enables to configure database connection :

- **Use DataBase connection for parameters** : Select if database must be use.
- **Name** : Database name will be put into parameter during its update. It enables to know from which database parameter has been lastly updated.
- **JDBC Driver** : Enter name of JDBC driver to be used(sun.jdbc.odbc.JdbcOdbcDriver, oracle.jdbc.driver.OracleDriver, ...).
- **Connection to database** : Database Url.
- **Connection options** : Connection properties.
- **Login** : Login to be used to connect to database.
- **Password** : Password to be used to connect to database.
- **SQL Request** : Request that have to be executed to retrieve data from database.
- **Name of "ID" field** : Name of field containing data ID.
- **Type of ID** : Type of ID field (INTEGER, FLOAT, VARCHAR(32), ...)
- **Name of "name" field** : Name of field containing data name.
- **Name of "value" field** : Name of field containing data value.
- **Name of "description" field** : Name of field containing data description.
- **Test Connection** : Name of field containing data description.

9.2.3. Language

Language tab enables to choice language :

- **Language** : Language changes are taken into account when option windows is closed.Available language are French and English.

9.2.4. Options

Options tab enables to tune application behavior :

- **Save working document options as default options in application** : Save options of current doc as application default options.
- **Application manage default options of documents. Apply defaut options to current document** : Apply -Application options- to current document.
- **Number of undo** : Specifies number of possible undo/redo.
- **Number of recent files** : Specifies number of files in recent files list.
- **Window display** : Enables separate tables (external) or linked tables (internal).
- **Columns to be resized in tables** : Enables to specify the columns on which space will be taken for resizing.
- **Use net protection key (Red)** : Check this box only if a network key is used (reg key).
- **Manage new names to avoid name conflict** : Tries to avoid name conflict, creating new objects whose name is unik (when pasting for example).
- **Synchronise view with tables** : Select objects in tables (on the right) when they are selected in view.
- **Synchronise view with explorer** : Select objects in explorer (on the left) when they are selected in view.

9.2.5. Graphics

Graphics tab enables to modify GUI look :

- **Element Zoom** : Changes graphics size.
- **Comment size** : Changes comment font size.
- **Activate smoothing for texts** : Activate anti-aliasing (smoothing) for texts, it can slow the display.
- **Activate smoothing for images** : Activate anti-aliasing (smoothing) for images, it can slow the display.
- **Activate tooltips** : Activate tooltip-system.

9.2.6. Digital format

Digital format tab enables to customize digits display :

- **Display of parameters** : Specifies the display of parameters (number of digits, ...).

9.2.7. Links

Links tab enables to change links display :

- **Label size** : Specifies label font size.
- **Link arrow width** : Specifies arrow width.
- **Link arrow height** : Specifies arrow height.

9.2.8. Curves

Charts tab enables to change charts drawing :

- **Set graphics borders** : Add borders to charts.
- **Set generic values borders** : Add borders to generic values under charts.
- **Display grid** : Display grid on curves area.
- **Display legends** : Display legends under curves.
- **Drawing zone transparency** : Activate curves area transparency.
- **Graphic transparency** : Activate charts transparency.
- **Title size** : Specifies charts title font size.
- **Generic values size** : Specifies generic values font size.
- **Point size** : Specifies point size on curves.
- **Coordinates size** : Specifies coordinates font size.
- **Legend size** : Specifies legends font size.
- **Max number of points** : Specifies maximum number of points to be drawn.
- **Max number of points to save** : Specifies maximum number of points to be saved.
- **Draw S.I.L** : Horizontal lines are drawn at E-1 E-2 E-3 E-4.
- **Save points in document** : Specifies if points of charts have to be saved in document.
- **Vertical abscise for histogram.** : Display coordinate of abscise verticaly.