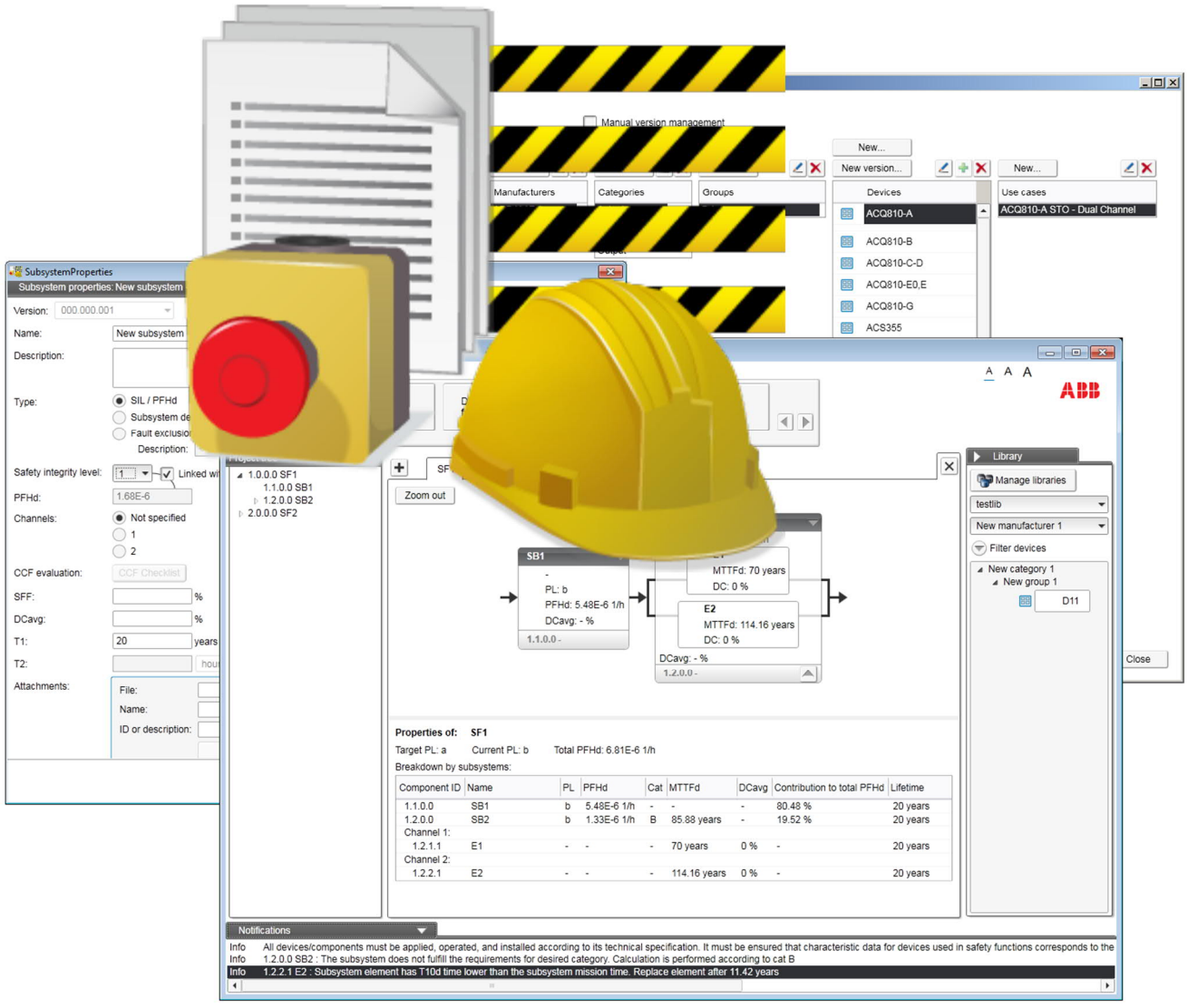
ABB Drives

# User's manual
# Functional safety design tool




Power and productivity
for a better world™

# User’s manual

Functional safety design tool

3AXD10000102417 Rev J
EN
EFFECTIVE: 2019-01-04

# Table of contents

# List of Figures

1

# Introduction to the manual

## What this chapter contains

This chapter introduces this manual.

## Target audience

The reader is expected to be familiar with functional safety, safety calculations and the international standards *ISO 13849-1* and *IEC 62061*. Also a basic knowledge of Microsoft Windows operating system is needed.

**Note:** Knowledge and correct application of the relevant standards and directives, in particular *ISO 13849-1* and *IEC 62061* are a requirement for using this tool. The tool is aimed to help the user with the calculations but appropriate knowledge is necessary in order to get proper results.

## Purpose of the manual

This manual describes the Functional safety design tool PC application and instructs how to use it in designing safety functions.

The same content as in this manual can be found also in the tool's help, which can be reached by selecting **Index** in the tool's **Help** menu

# Contents of the manual

The manual consists of the following chapters:

- *Introduction to the manual* introduces this manual.
- *Overview of Functional safety design tool* briefly lists the main features of the Functional safety design tool software and instructs how and where it can be run, and how to get help and additional information.
- *Installation and uninstallation of Functional safety design tool* describes how to install and uninstall the Functional safety design tool software.
- *Main user interface components* describes the main user interface components of Functional safety design tool PC application, including the menus.
- *Project steps* describes the steps needed to be fulfilled to complete a safety project.
- *Managing the libraries* describes how to manage the component libraries, how to create devices in libraries and how to import and export libraries.

# Related standards and directives

Referenced standards are listed in the table below.

| | Standard | Name |
|---|---|---|
| 1 | ISO 13849-1:2015 | Safety of machinery – Safety related parts of control systems – Part 1: general principles for design |
| 2 | IEC 62061:2015 (ed.1.2) | Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems |
| 3 | VDMA 66413:2012-10 | Functional Safety – Universal data format for safety-related values of components or parts of control systems |

## Copyright issues regarding the standards

In order to be fully compliant with the standards, some parts of the tool contain material, which is directly copied from the above mentioned standards.

We thank the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

We thank the Finnish Standards Association SFS for permission to reproduce Information from ISO International Standard ISO 13849-1:2015.

# Terms and abbreviations

| Term/abbreviation | Definition |
|---|---|

| | |
|---|---|
| Architecture | Specific configuration of hardware or software elements |
| $B_{10}$ | Number of cycles until 10 % of the components fail. |
| $B_{10D}$ | Number of cycles until 10 % of the components fail dangerously. |
| Cat | Category |
| CCF | Common cause failure |
| Dangerous failure | Failure that has the potential to cause harm or increase the risk. In single channel systems without diagnostics, a dangerous failure disables the safety function. |
| DC | Diagnostic coverage. Ratio between dangerous detected failure rate and dangerous failure rate. |
| HFT | Hardware fault tolerance |
| Lifetime | The period of time covering the intended use of the component. Also referred to as mission time. |
| $MTTF_D$ | Mean time to dangerous failure |
| $PFH_D$ | Frequency of dangerous failures (per hour, 1/h). |
| PL | Performance level |
| PLr | Required performance level. |
| RDF | Ratio of dangerous failures. Ratio between dangerous failure rate (λd) and total failure rate (λ). |
| SE | Subsystem element: Component in a subsystem. |
| SF | Safety function |
| SFF | Safe failure fraction. Fraction of the overall failure rate of a subsystem that does not result in a dangerous failure. |
| SS | Subsystem. A dangerous failure in any subsystem will disable the control function |
| SIL | Safety integrity level |
| SILCL | SIL claim limit |
| T1 | Proof test interval or lifetime, whichever is smaller. |
| T2 | Diagnostic test interval |
| λ (lambda) | General symbol for failure rate (1/h) |
| λd (lambda d) | Dangerous failure rate: Represents failures that have the potential to cause harm and increase risk. |

For complete and more extensive definitions see *ISO 13849-1* and *IEC 62061*.

## Certificate

TÜV Nord certificate for FSDT-01 is attached below.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-11074-01-00

TÜV NORD

# Certificate

**No. SEBS-A.145616/15, V1.1**

**TÜV NORD Systems GmbH & Co. KG hereby certifies to**

**ABB OY**
Hiomotie 13
00381 Helsinki
Finland

**that the**

**Functional Safety Design Tool**
**V1.2**

**meets the requirements listed in the below mentioned standards**

- **IEC 61508:2010; Part 3; Section 7.4.4; Qualified up to SIL 3**

**and is capable as a T2 Tool within safety developments according ISO 13849-1 up to PLe, IEC 61508 up to SIL 3 and IEC 62061 up to $SIL_{CL}$ 3 for the calculation of safety parameter and safety loop design.**

**Base of certification is the report SEBS-A.145616/15TB in the valid version.**

**This certificate entitles the holder to use the pictured Trusted Tool mark.**

**Valid until: 2020-11-24**
**File reference: 8112794766**

**Hamburg, 2017-08-16**

**Bianca Pfuff**

TÜV NORD
TÜV NORD Systems GmbH & Co. KG
Trusted Tool
Functional Safety Design Tool, V1.2
IEC 61508:2010 SIL3
SEBS-A.145616/15
Voluntary Certification

**Certification Body SEECERT**
**TÜV NORD Systems GmbH & Co. KG**
**Große Bahnstraße 31, 22525 Hamburg, Germany**

2

# Overview of Functional safety design tool

## What this chapter contains

This chapter briefly lists the main features of the Functional safety design tool software and instructs how and where it can be run, and how to get help and additional information.

## Functional safety design tool

Functional safety design tool is a 32-bit Windows application, which is a support tool for performing functional safety modeling, design, calculations and verification for machine functional safety. The tool is aimed to simplify the process of safety function design and verification according to standards *ISO 13849-1* and *IEC 62061* and to generate documentation to support compliance to the requirements of the mentioned standards and the European Machine Directive for safety.

**Note:** Knowledge and correct application of the relevant standards and directives, in particular *ISO 13849-1* and *IEC 62061* are a requirement for using this tool. The tool is aimed to help the user with the calculations but appropriate knowledge is necessary in order to get proper results.

**Note:** Although careful measures have been taken to ensure the correctness of the software, there is always a possibility for error. ABB does not warrant that the operation of the program will be uninterrupted or error free. ABB does not make any assurances with regard to the accuracy of the selections or any other output deriving from the use of software.

## Highlights

With Functional safety design tool, it is possible to do:

- Risk evaluation for estimation of required safety level (SIL/PL)
- Graphical safety function design
- Calculations according to *ISO 13849-1* and *IEC 62061*
- Inclusion of components from ABB product libraries
- Creation of component libraries
- Inclusion of third party components in calculations
- Generate reports for machine technical documentation

## Hardware and software requirements

- Computer hardware
  - IBM compatible PC
  - Pentium 2 GHz or a faster processor (recommended)
  - 1 GB RAM
  - At least 1 GB free hard disk space (2 GB with 64-bit)

- Software
  - Operating system Windows XP, Vista, Windows 7 (32 or 64 bit operating system) or Windows 8 (32 bit operating system)
  - Microsoft .NET Framework 4.0
  - Microsoft Office 2007 or above (for reporting functionality)
  - Adobe Reader (for reporting functionality)

3

# Installation and uninstallation of Functional safety design tool

## What this chapter contains

This chapter describes how to install and uninstall Functional safety design tool software.

## Determining the current Functional safety design tool version

To find out the version of Functional safety design PC tool, select **About Functional safety design tool** on the **Help** menu. The **About Functional safety design tool** dialog box containing the Functional safety design tool version is shown.

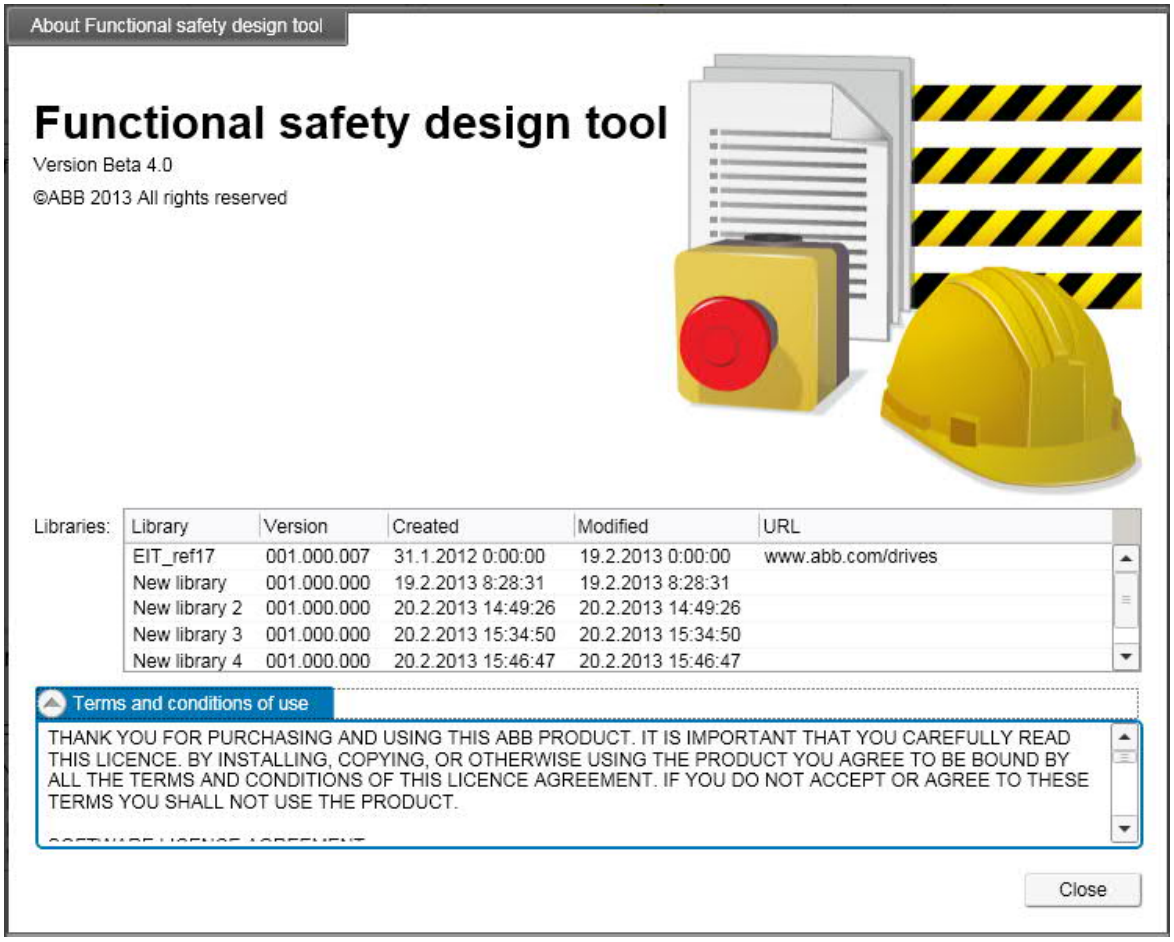



*Figure 1. About the product dialog box*

## Installing Functional safety design tool

It is recommended that you uninstall all previous versions of Functional safety design tool before installing a new version. Quit all applications before starting the installation.

1. Run the setup.exe file from the folder where you have the installation files for Functional safety design tool.
2. When the Functional safety design tool installation wizard window is shown, click the Next > button.

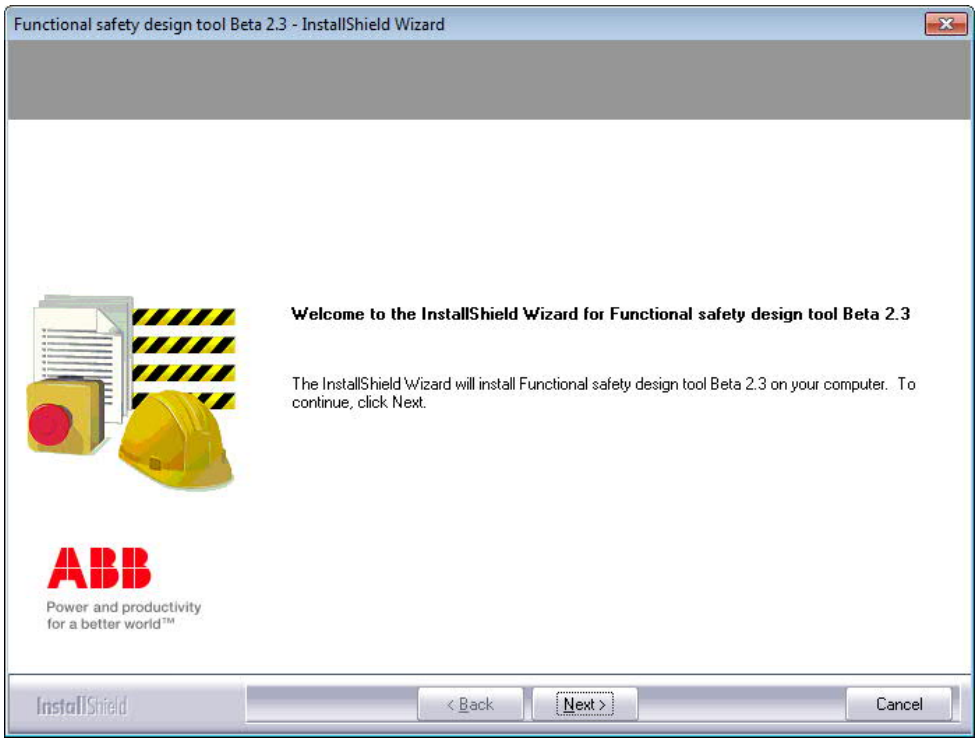



*Figure 2. Welcome to InstallShield Wizard for Functional safety design tool window*

3. In the next screen give the user information

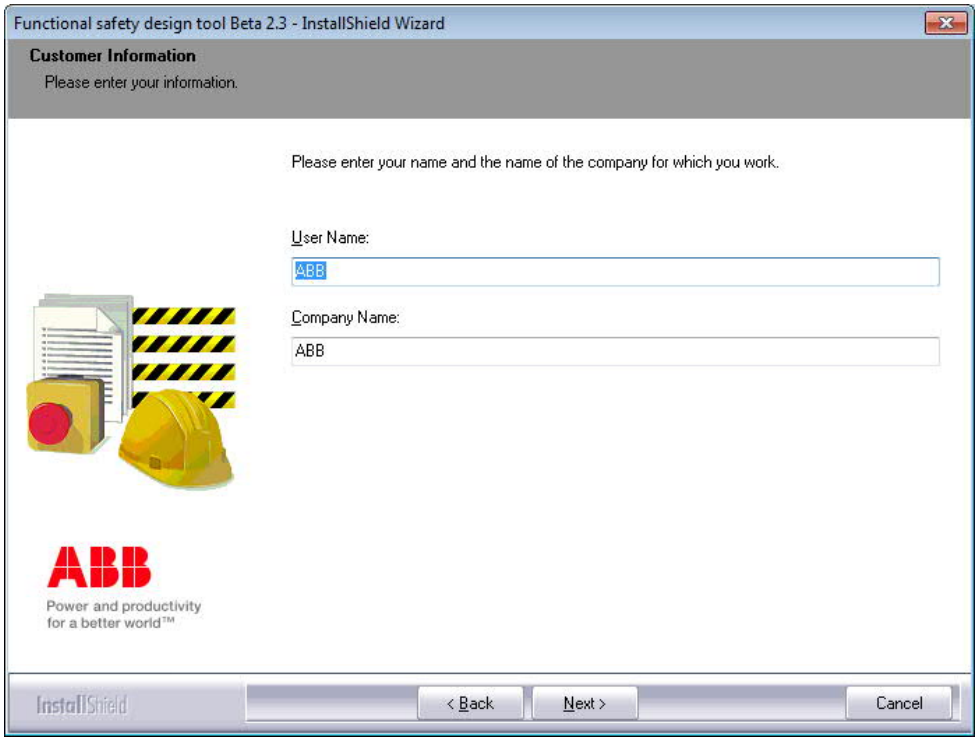



*Figure 3. Customer Information window*

4. Select the location of the installation folder and click the Next > button

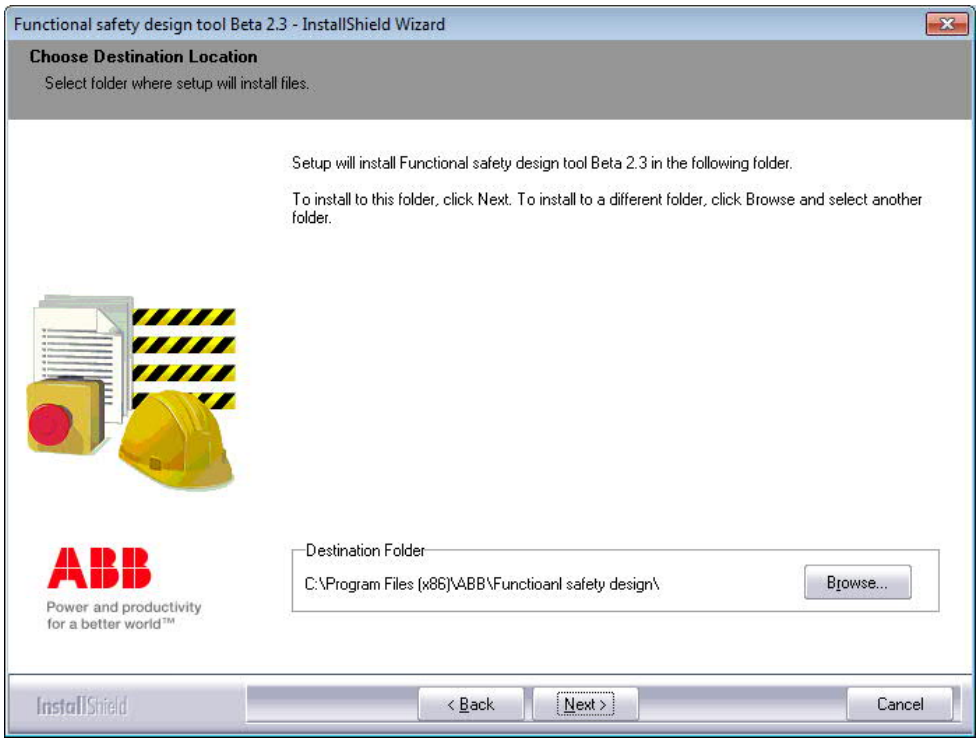



*Figure 4. Choose Destination Location window*

5. If everything is OK, click Install to start installation.

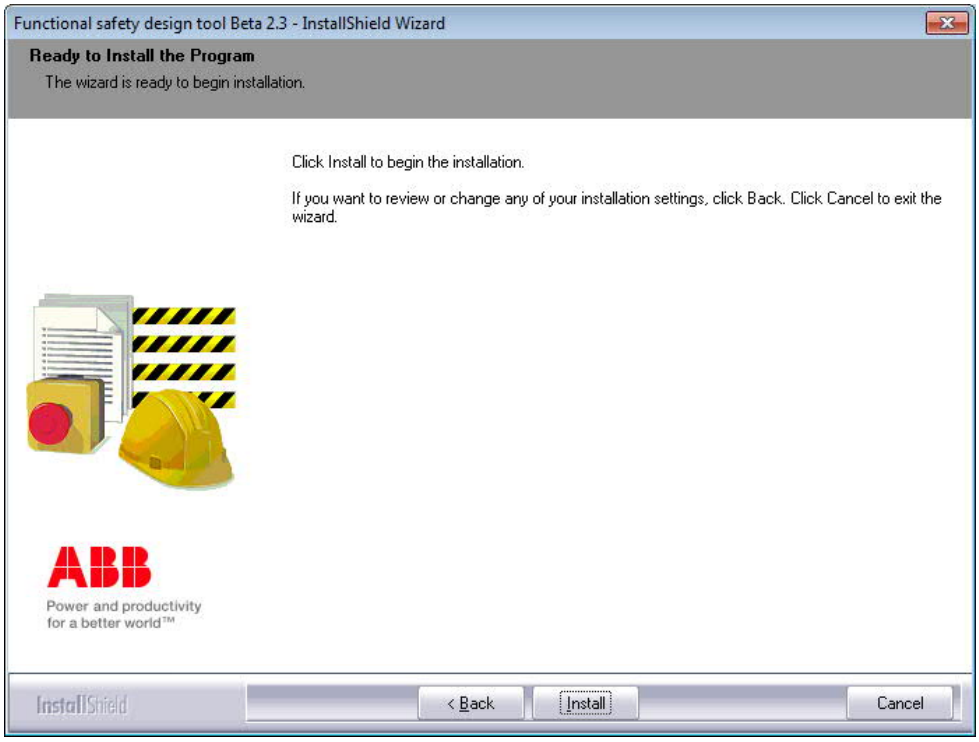



*Figure 5. Ready to Install the Program window*

6. The installation is complete. Click Finish and Functional safety design tool is now ready for use.

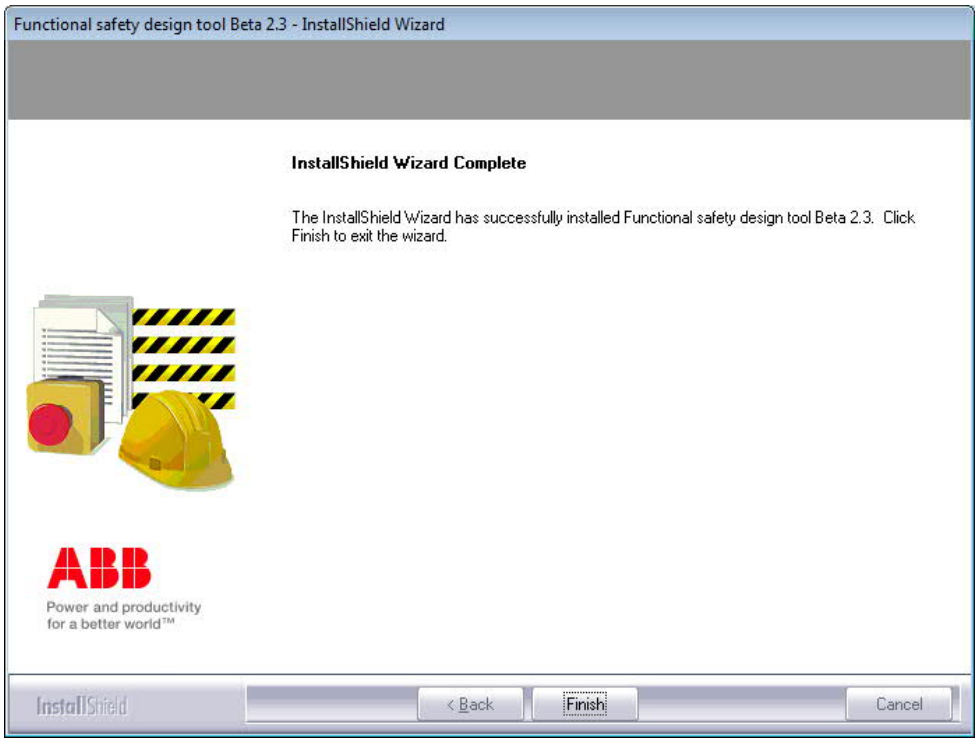



*Figure 6. Installation complete window*

# Uninstalling Functional safety design tool

**Note:** You must have administrator privileges to be able to complete the uninstallation.

1. In the **Add or Remove Programs** window of the Control Panel, click the **Change or Remove** icon and browse for Functional safety design tool in the Currently installed programs list, select it and click **Remove**.

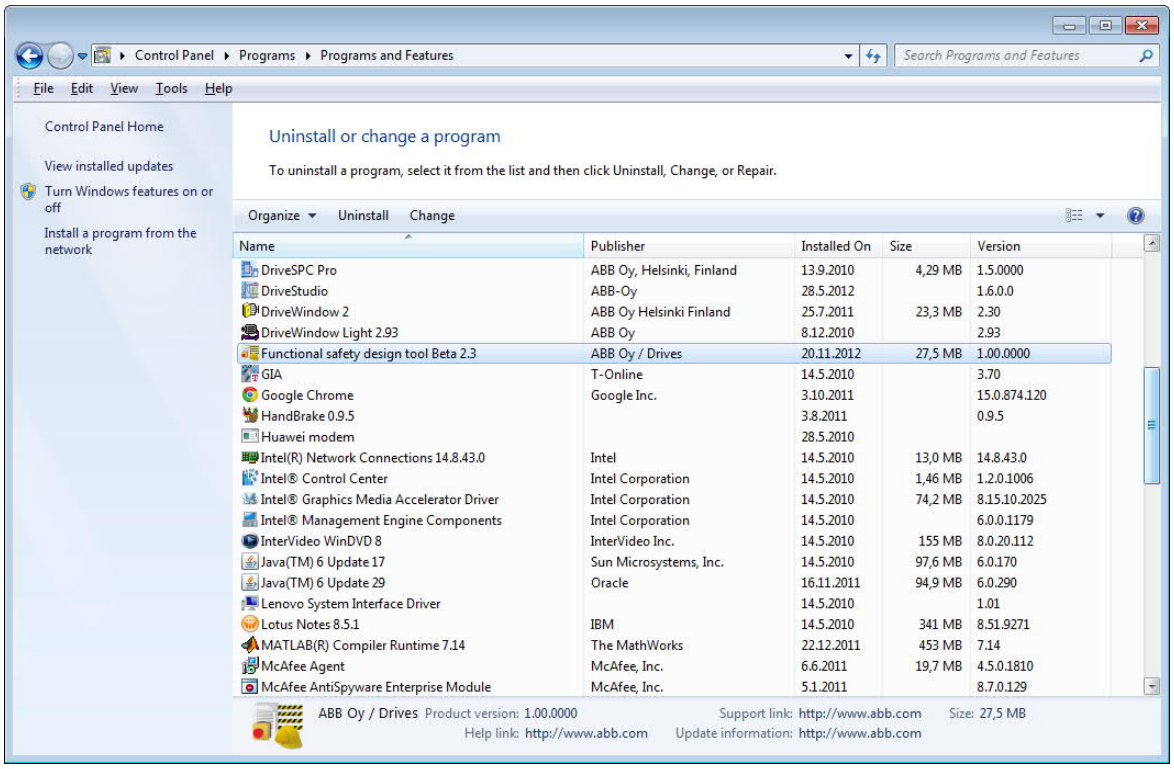



*Figure 7. Removing Functional safety design tool*

**Note:** In Win 7, the window is called Programs/Uninstall a program.

2. Click the **Yes** button to confirm that you want to remove the application.

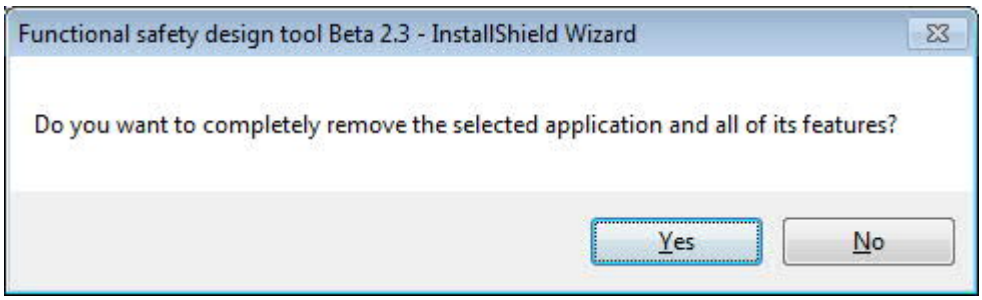



*Figure 8. Confirming the removal of Functional safety design tool*

3. When uninstall has completed, click the Finish button.

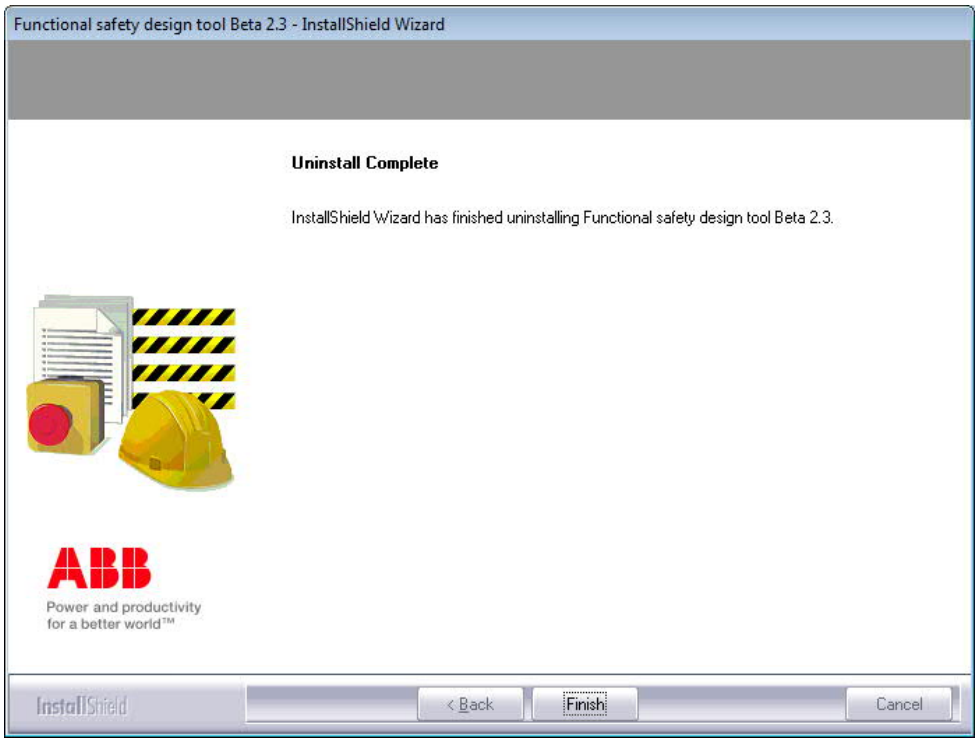



*Figure 9. Uninstall complete*

4

# Main user interface components

## What this chapter contains

This chapter describes the main user interface (UI) components and how to use them. The user interface is designed so that the need to use menus has been minimized. All main functions are available on the component level.

## Overview

The user interface consists of the following parts:

1. Title bar
2. Menu bar
3. Project panel
4. Workflow panel
5. Project tree panel
6. Work area
7. Library panel
8. Performance panel
9. Notifications panel

The Project tree, Library, and Notifications panels can all be expanded and collapsed. When expanded, they normally adjust their size to the current content but they can also be resized as desired.

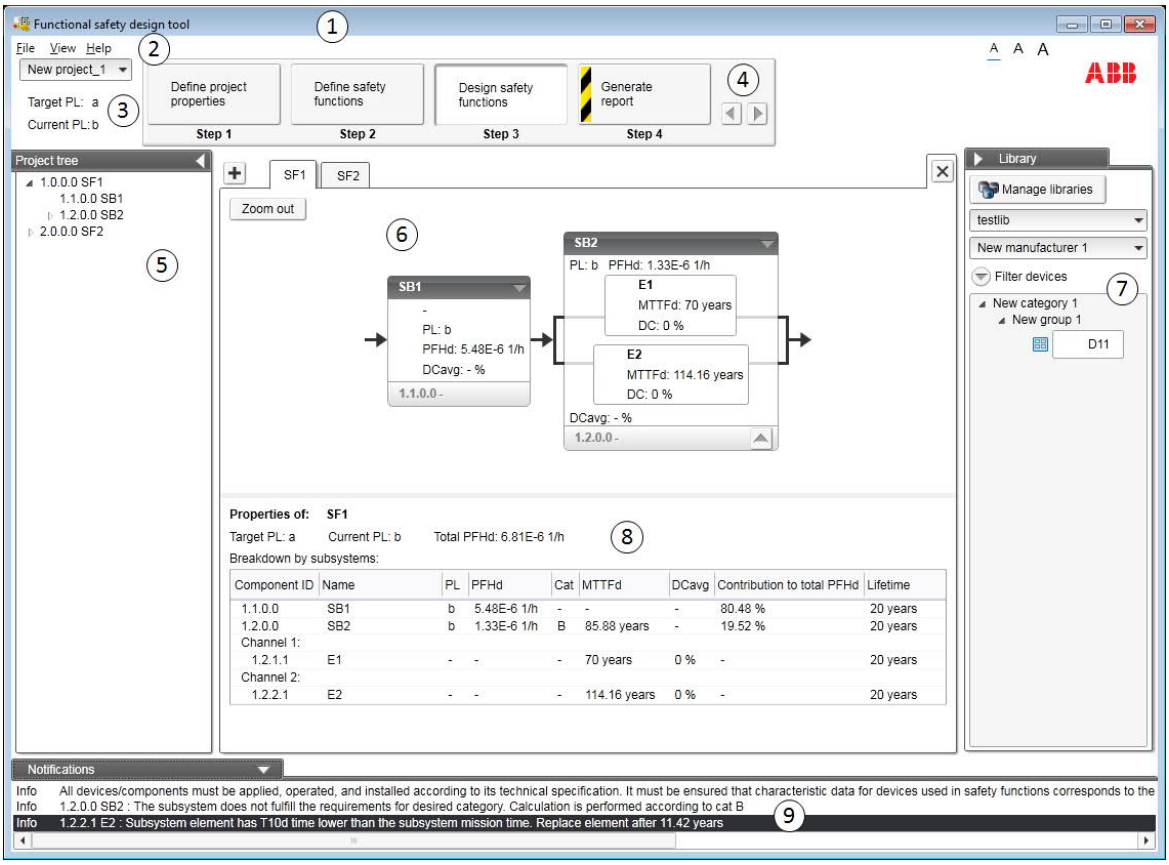



*Figure 10. Overview of the user interface*

## Title bar

The title bar is located at the top of the main window. It consists of the following parts:

- System menu icon
- Application name (Functional safety design tool)
- Minimize button which has the same function as Minimize in the System menu.
- Maximize/Restore Down button (the name depends on the status of the maximized window) which has the same function as Maximize or Restore in the System menu.
- Close button which has the same function as Close in the System menu.


*Figure 11. Title bar*

To reduce the main window to the taskbar or a sub-window to the bottom of the window area, click the **Minimize** button or go to **System menu –> Minimize**.

To enlarge the window to fill the available space, click the **Maximize** button or go to **System menu –> Maximize**.

To return the window to the size and position it had before it was maximized, click **Restore Down** button or go to **System menu –> Restore**.

You can also maximize or restore the window by double-clicking the title bar.

To move a window, drag it from its title bar. To move a dialog box, drag it from its title bar. If you have maximized or minimized a window, you cannot move it by dragging from the title bar.

To end your Functional safety design tool session, click the Close button. Before closing down, Functional safety design tool may:

- Prompt you to save the projects with unsaved changes
- Remind you of unfinished printing.

You can close Functional safety design tool by

- double-clicking the System menu icon
- selecting **Close** in the System menu
- selecting **Exit** in the File menu
- pressing the shortcut key Alt+F4.

### System menu

You can open the System menu by

- left- or right-clicking the System menu icon
- pressing the shortcut key Alt+space bar
- right-clicking within the non-button area of the title bar.

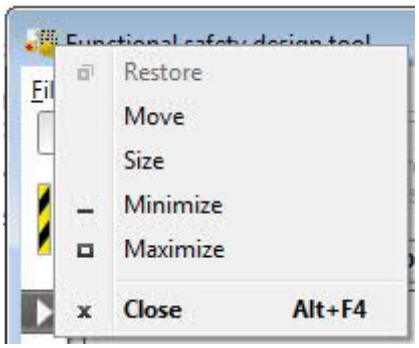



*Figure 12. System menu*

There are simple system menus at the dialog box level. You can open the System menu of a dialog box by

- clicking the **System menu** icon of the dialog box
- right-clicking within the non-button area of the title bar
- pressing the shortcut key Alt+space bar.

The System menu contains the following commands:

- **Restore** which has the same function as the Maximize/Restore Down button in the title bar when the window is maximized. The Restore command returns the window to its size and position that it had before it was maximized.

- **Move** which can be performed also by dragging the window from its title bar. After selecting the Move command from the System menu, it is possible to move the window with the arrow keys. To stop moving the window, press Enter. To cancel the move, press Esc.
- **Size** which can be performed also by dragging any of the sides or corners of the window. After selecting the Size command, it is possible to resize the window with the arrow keys. To stop resizing the window, press Enter. To cancel resizing, press Esc.
- **Minimize** which has the same function as the Minimize button in the title bar. The Minimize command reduces the window to the taskbar or to the bottom of the window area.
- **Maximize** which has the same function as the Maximize button in the title bar when the window has not been maximized. The Maximize command enlarges the window to fill the available space.
- **Close** has the same function as the Close button in the title bar. The Close command ends the Functional safety design tool session.

## Menu bar

The menu bar is located immediately below the title bar. It always contains the following drop-down main menus:

- File
- Edit
- View
- Help

To open a drop-down menu, click its name on the menu bar.

To execute a command from a menu, click its name on the menu. You can also use the arrow keys to navigate between the menus and within a menu. To execute a highlighted command, press Enter. To close a menu, press the Esc key. You can also use the shortcut keys to execute the commands.

### File menu

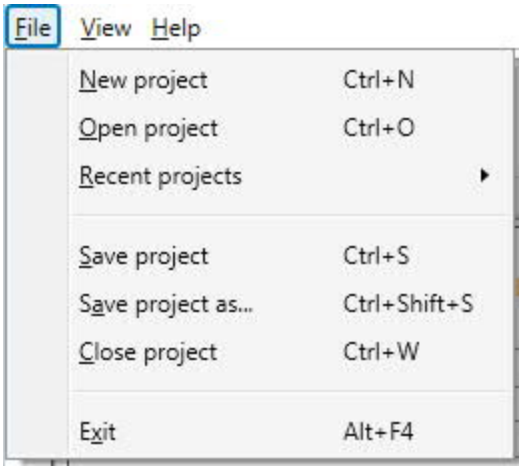



*Figure 13. File menu*

The menu contains the following commands:

- **New project** creates a new project. The keyboard shortcut is Ctrl+N.
- **Open project** opens a dialog for opening a previously saved project. The keyboard shortcut for the Open project command is Ctrl+O.
- **Recent projects** views a list of projects that have recently been opened to the tool.
- **Save project** saves the project to a file. The keyboard shortcut for the Save project command is Ctrl+S.
- **Save project as…** saves the project to a file with a new name. The keyboard shortcut for the Save project as… command is Ctrl+Shift+S.
- **Close project** closes the currently active project. The keyboard shortcut for the Close project command is Ctrl+W.
- **Exit** ends the Functional safety design tool session.

### View menu

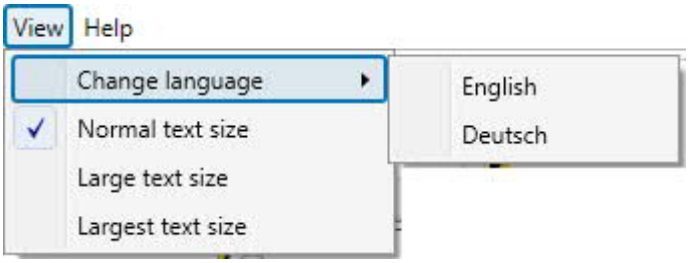



*Figure 14. View menu*

The menu contains the following commands:

- **Change language** for opening the list of available user interface languages.
- **Normal text size** for selecting the normal text size.
- **Large text size** for selecting the large text size.
- **Largest text size** for selecting the largest text size.

The font sizes can be also be changed with the following A-letter icons.


*Figure 15. A-letter icons for changing the font size*

### Help menu

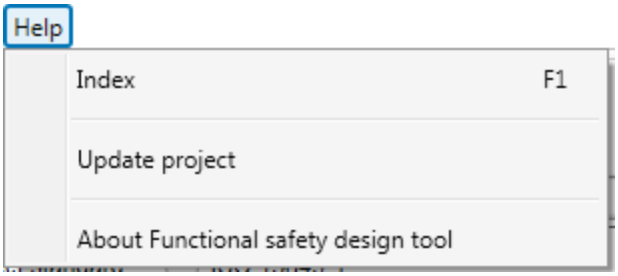



*Figure 16. Help menu*

The menu contains the following commands:

- **Index** or the F1 key opens the Functional safety design tool help.
- **Update project** updates the library components used in the currently active project, if newer versions of the components are available in the loaded libraries.
- **About Functional safety design tool** opens a window displaying the program information, version numbers and copyright text.

## Project panel

The project panel is located below the menu bar. It has a selection box for selecting the active project among the projects, which currently are open in the tool. It also shows, depending on the selected standard, the current and target PL or SIL for the currently selected safety function.

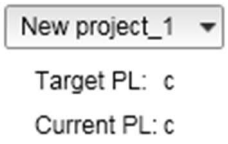



*Figure 17. Project panel*

## Workflow panel

The workflow panel indicates and guides the progress of the user in the workflow of the active project. Contents of the work area are changed according to which step is selected here. The user can either click the button of the desired step or use the Previous step or the Next step buttons. The current step is indicated by the pressed state of corresponding button.


*Figure 18. Workflow panel*

When starting a new project, the Step2, Step3, Step4, and the Next and Previous buttons are disabled until all required information has been entered in the previous step.

If a step contains components that require attention from the user or some information is missing, the warning stripe (see *Figure 20*) is shown on the corresponding step button.

## Project tree panel

The project tree shows the system that the user has built in the active project.

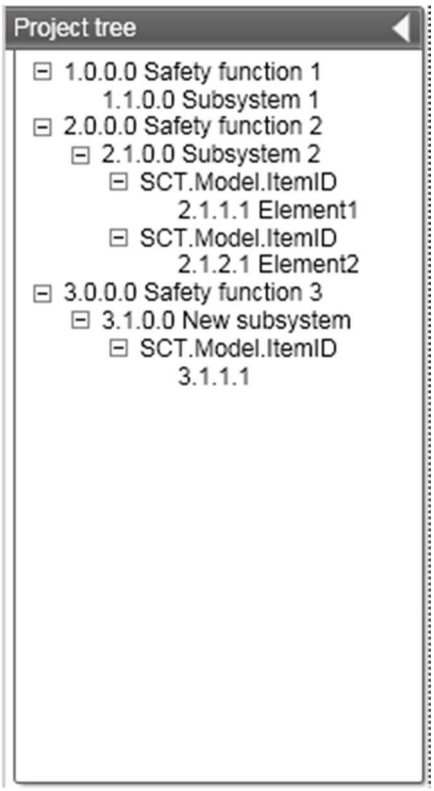



*Figure 19. Project tree panel*

The panel is collapsed by default. It can be expanded and collapsed by clicking the header. By default the panel scales to fit its contents but it can be resized by dragging the line separating it from the work area. The contents of the work area changes according to which item the user selects here.

## Work area

The views for different project steps are shown in the work area. The individual steps are described in more detail in chapter *Project steps*.

There are some basic principles used on the work area, which aim to help the user in defining the safety project.

- **The warning stripe** is shown on every item, which needs attention from the user. The reason for this need may be, e.g. that mandatory data is missing or the value is out of its range or in conflict with some other value in order to perform the calculation.

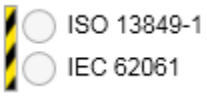



*Figure 20. Warning stripe*

- **Mandatory data** Each view has some data, which is mandatory. If mandatory data is missing or the value given is for some reason not accepted, the tool shows the warning stripe for the value and prevents the user from proceeding before the mandatory value is correctly defined.

## Library panel

The library panel contains component library items, which the user can drag and drop into the work area when designing the system in Step 3.

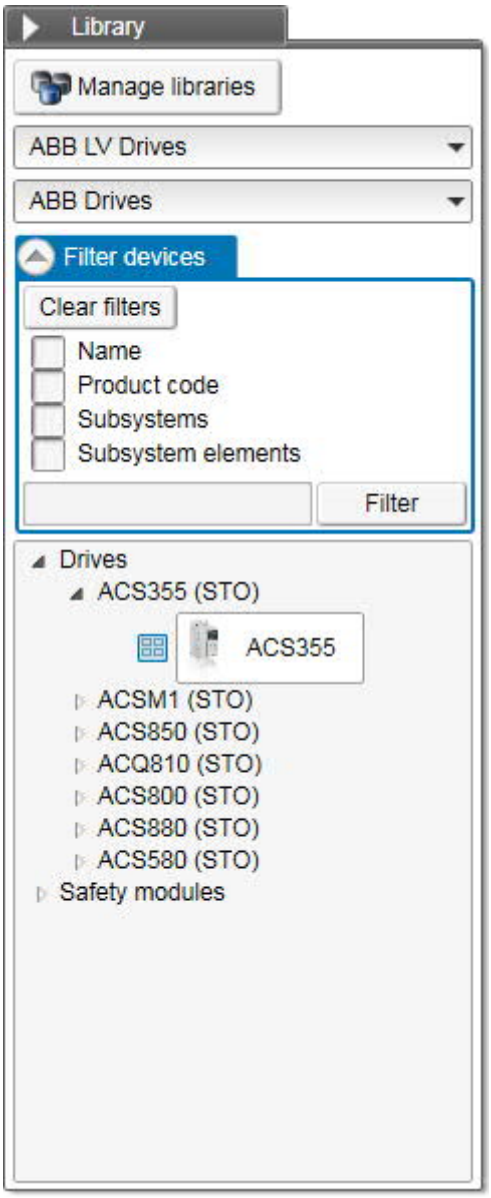



*Figure 21. Library panel*

One component library at a time is shown. Here are shown the components, which have data for the currently selected standard. User can filter the list by device name or product code. User can also select only the subsystems or subsystem elements to be shown. The library panel can be expanded and collapsed by clicking the header. By default the panel scales to fit in its contents but it can be resized by dragging the line separating it from the work area.

## Notifications panel

All items, which may require attention from the user, are reported on the notifications panel.

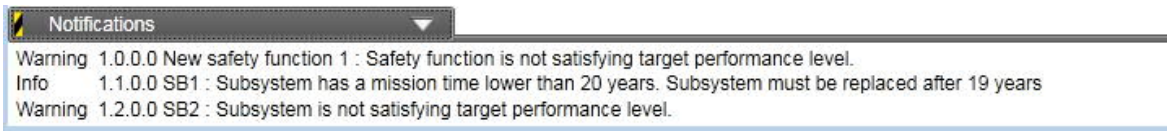



*Figure 22. Notifications panel*

The notifications panel can be expanded and collapsed by clicking the header. By default the panel scales to fit in its contents but it can be resized by dragging the line separating it from the work area. The warning stripe is shown on the panel header if the panel is collapsed and new notifications have appeared since the panel last time was expanded. The item, to which the notification affects to, is identified with its ID number and name.

There are two types of notifications:

- **Warning** is either a condition where the design does not fulfill the safety requirements or it is not possible to finish the calculations. Warning activates warning stripes.
- **Info** is information about a condition, which may be acceptable but the user shall still be aware of it. Info does not enable any warning stripes. It is only shown in notification panel.

5

# Project steps

## What this chapter contains

The tool workflow panel indicates the natural steps to perform in order to sufficiently specify a safety project. From the workflow panel the following steps are available:

1. Define project properties

   In this step the standard, which is used in project calculations, is selected. General information about this safety calculation project is given.

2. Define safety functions

   In this step the required PL or SIL level is defined for the safety function. General information about the safety function is given.

3. Design safety functions

   In this step the safety function is designed by including the appropriate components and filling in their safety data.

4. Generate report

   In this step the report content is defined and the report created.

Steps from 1 to 3 require mandatory and optional input from the tool user, whereas the last step, Step 4, gives the tool user the possibility to generate a report documenting the safety functions in the project. This chapter describes the user inputs, and options available for each of the available steps.

## Getting started

When the tool is launched, the user is first shown a dialog box, which presents key information about the installed version of the tool, as seen in *Figure 23*:

- Installed version of tool
- Currently imported and available product libraries

With the given checkbox, the Terms and conditions of use must be accepted before the user can proceed and start using the tool.

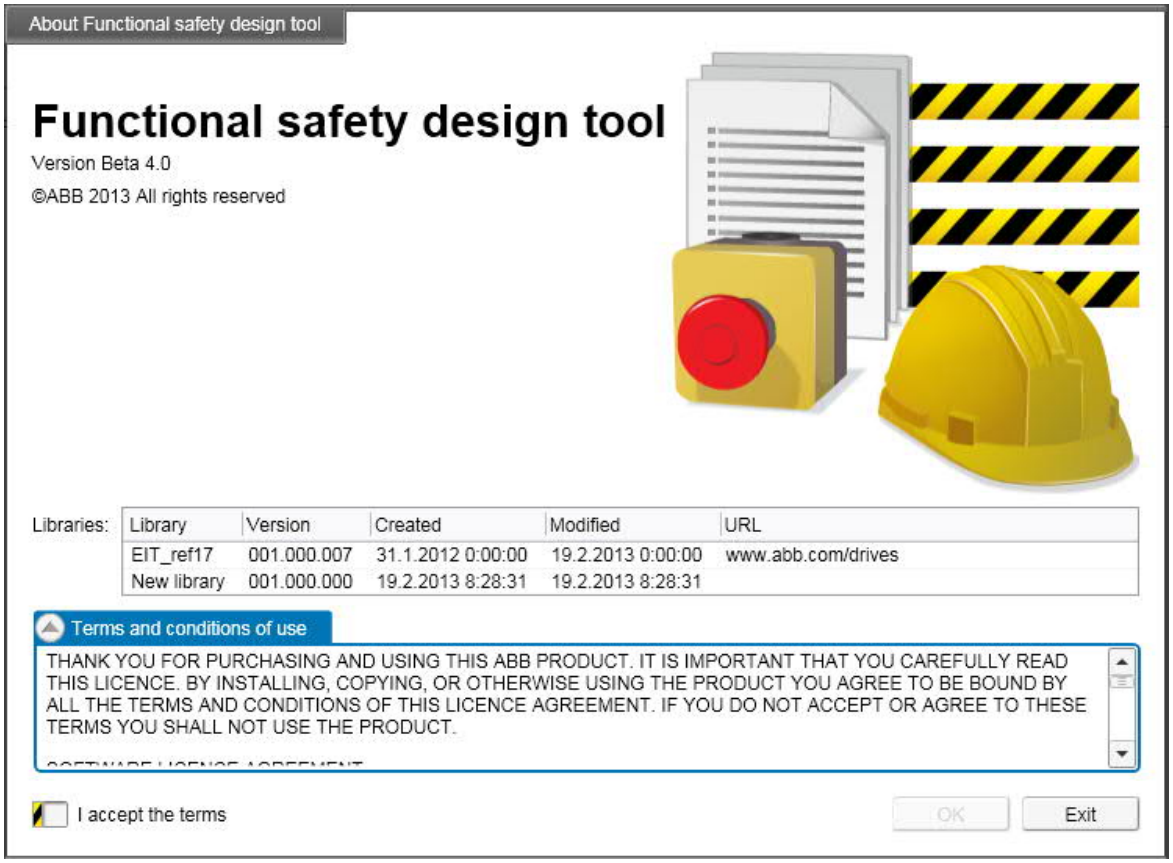



*Figure 23. Tool start up dialog and accepting the terms of tool usage*

After having accepted the terms a starting screen is shown, see *Figure 24*, giving the tool user the following options:

- **New project** creates a new and empty project.
- **Open file** opens a dialog for browsing and opening existing projects.
- **Open** opens the project, which is selected on the Recent projects list.

After selecting one of the options the tool will enter Step 1 of the project workflow.

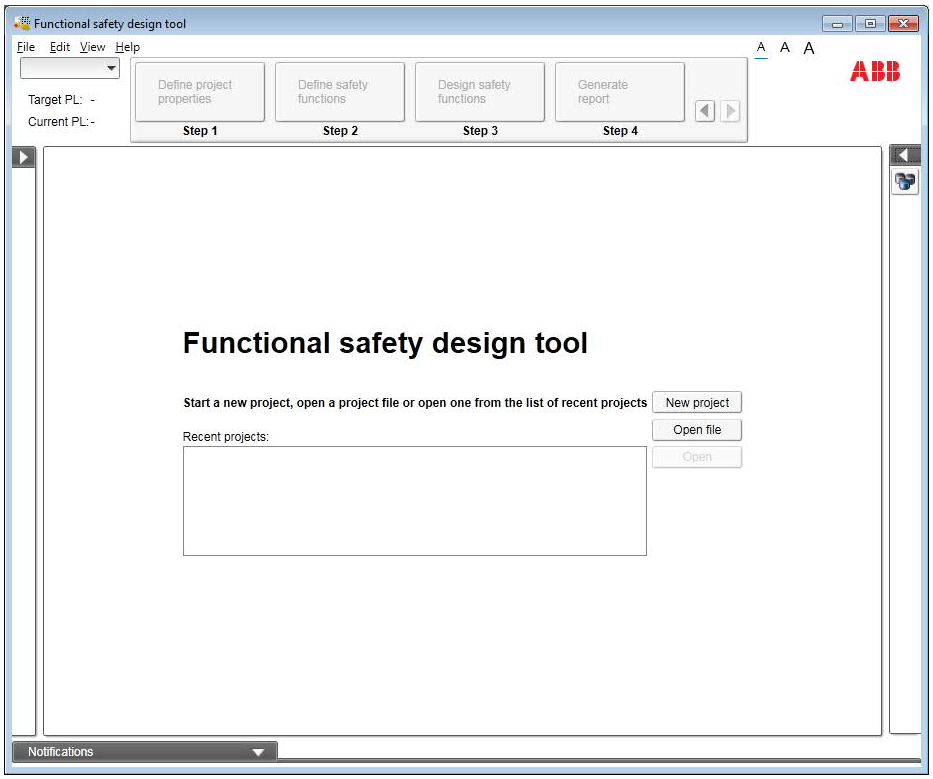



*Figure 24. Starting screen*

# Step 1 – Define the project properties

In Step 1 basic properties of the current project are specified, as shown in *Figure 25*.

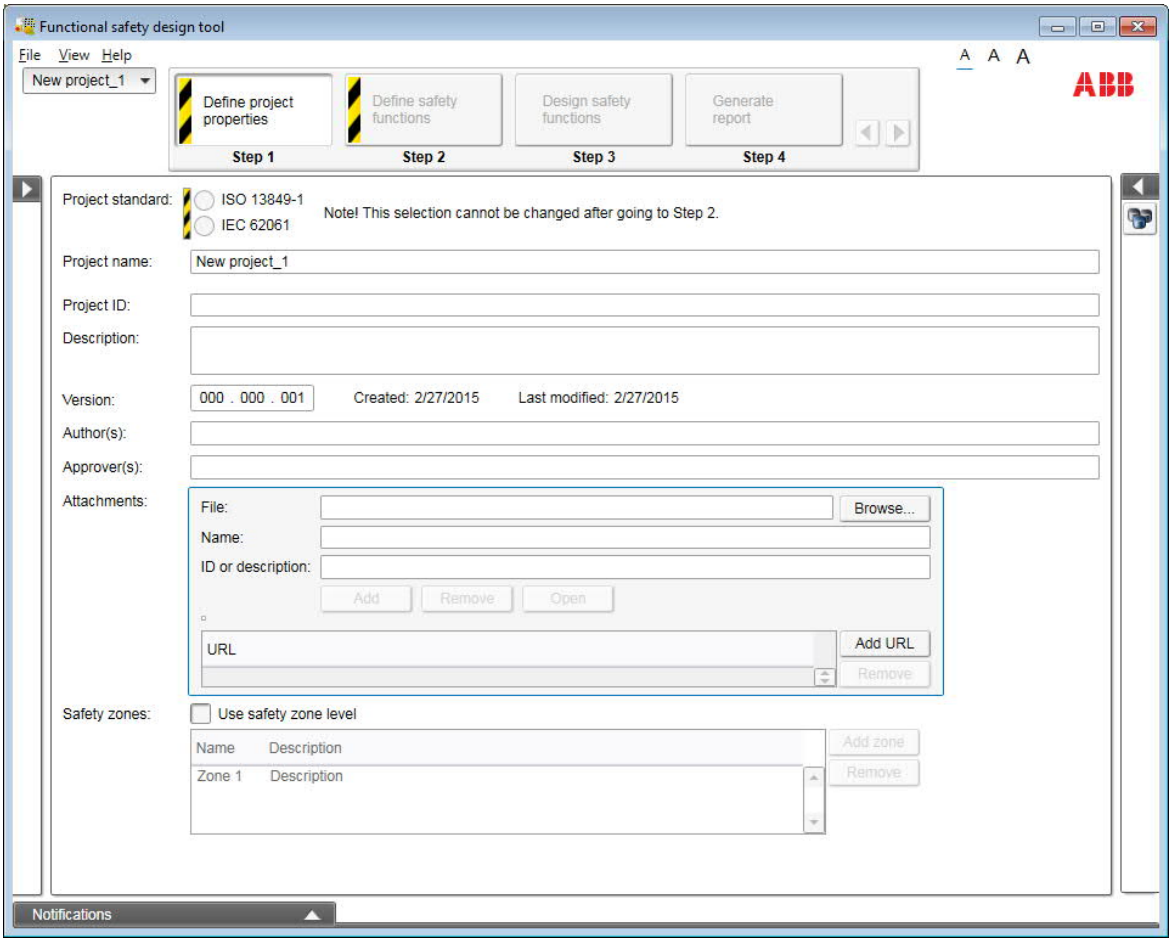



*Figure 25. Step 1: The project properties*

The mandatory inputs for Step 1 are:

- **Project standard** selection defines the standard, according to which the project is evaluated.

  **Note:** The calculations within one project are always done according to one standard. The standard selection cannot be changed after you have proceeded from Step 1 to Step 2.

- **Project name** must be defined. The tool suggests a default name.

The optional inputs for Step 1 are:

- **Project ID** is some unique identifier for the project.
- **Description** is where the project can be described in more detail.
- **Version** number of the project can be given here.
- **Author(s)** of project can be given.
- **Approver(s)** of project can be given.
- **Attachments** are any files needed to be attached to the project. Here you can also define URLs for useful web site links.

  - Click **Browse** to look for a file in an existing folder on the hard disks or enter the folder path and file name directly. The tool suggests a name for the attachment but the name can be changed if needed. The user can also give the attachment an ID or description. Click **Add** to add the attachment to the project. The attachments can be removed with the **Remove** button. Clicking **Open** opens the selected attachment in an appropriate application.
  - To add a web link to the project, click **Add URL** button and write the web site address in the list. To remove an URL, select it from the list and click **Remove**.
- **Safety zones**
  - The **Use safety zone level** option enables the user to group safety function into different safety zones.

    **Note:** If you remove a safety zone with the **Remove** button, also the safety functions defined under that zone will be removed.

When all mandatory data is specified for Step 1, the user is allowed to proceed to Step 2, Define safety functions, by selecting **Step 2**, or by utilizing the next step button **[>]**, which both become enabled, as all mandatory data for Step 1 has been specified.

## Step 2 – Define safety functions

A project can contain several safety functions, and depending on the setting in Step 1 the different safety functions can also belong to specific safety zones. For each project these safety functions need to be defined. *Figure 26* illustrates the define safety function step for an *ISO 13849-1* project.

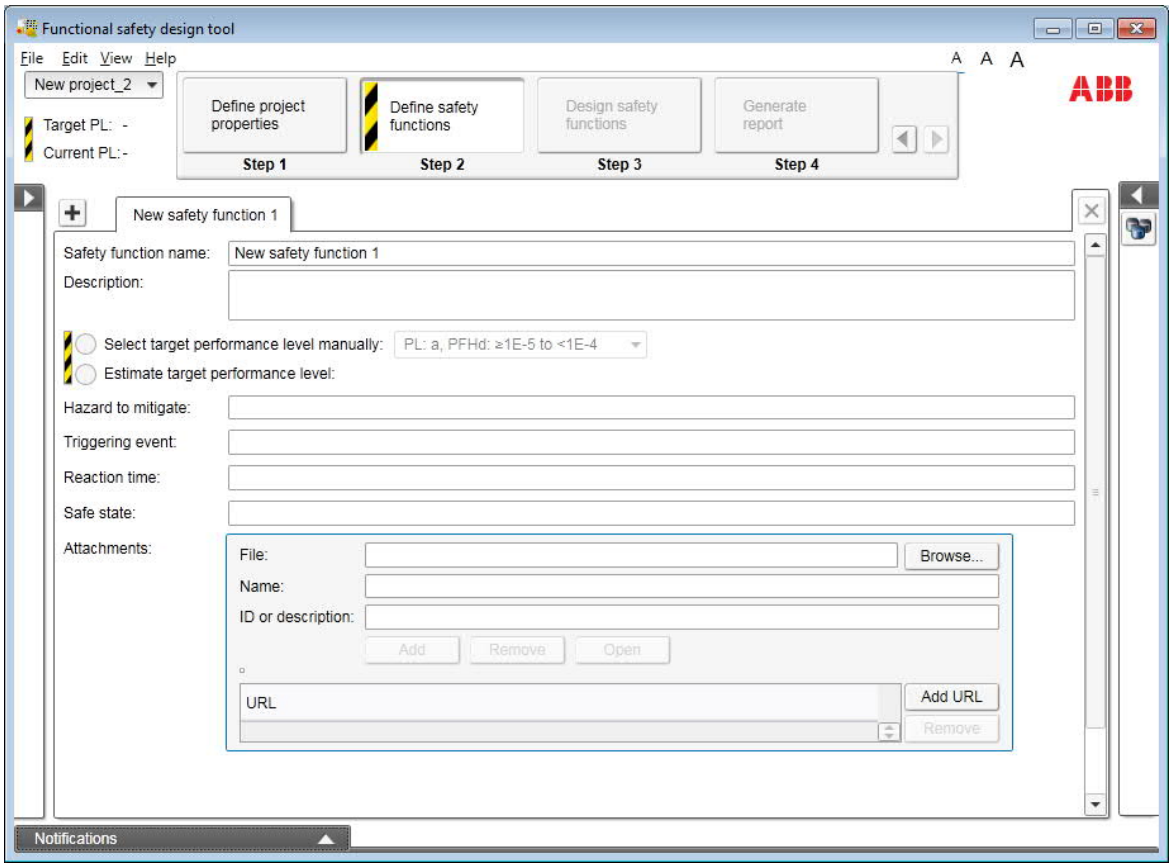



*Figure 26. Step 2: Define safety functions – ISO 13849 project*

The mandatory inputs for Step 2, *ISO 13849-1* projects are (See *Figure 26*):

- **Safety function name** shall be a unique name within a safety zone or if zones are not used within the project.
- Safety function target performance level:
  - **Select target performance level manually** allows the user to directly specify the required target performance level PLr for the safety function using the related pull down menu.
  - **Estimate target performance level** enables the user to determine the required performance level PLr according to method described in *ISO 13849-1*, Annex A.

Optional inputs for Step 2, *ISO 13849-1* projects are (See *Figure 26*):

- **Hazard to mitigate** allows the user to specify the purpose of the given safety function.
- **Triggering event** allows the user to describe the conditions required for activating the safety function.
- **Response time** allows the user to specify the response time of the safety function.
- **Safe state** allows the user to describe the safe state enforced by the safety function
- **Attachments** are any files needed to be attached to the project. Here you can also define URLs for useful web sites.
  - Click **Browse** to look for a file in an existing folder on the hard disks or enter the folder path and file name directly. The tool suggests a name for the attachment but the name can be changed if needed. The user can also give the attachment an ID

or description. Click **Add** to add the attachment to the project. The attachments can be removed with the **Remove** button. Clicking **Open** opens the selected attachment in an appropriate application.

- To add a web link to the project, click **Add URL** button and write the web site address in the list.

For *IEC 62061* projects *Figure 27* illustrates the **Define safety function** step.

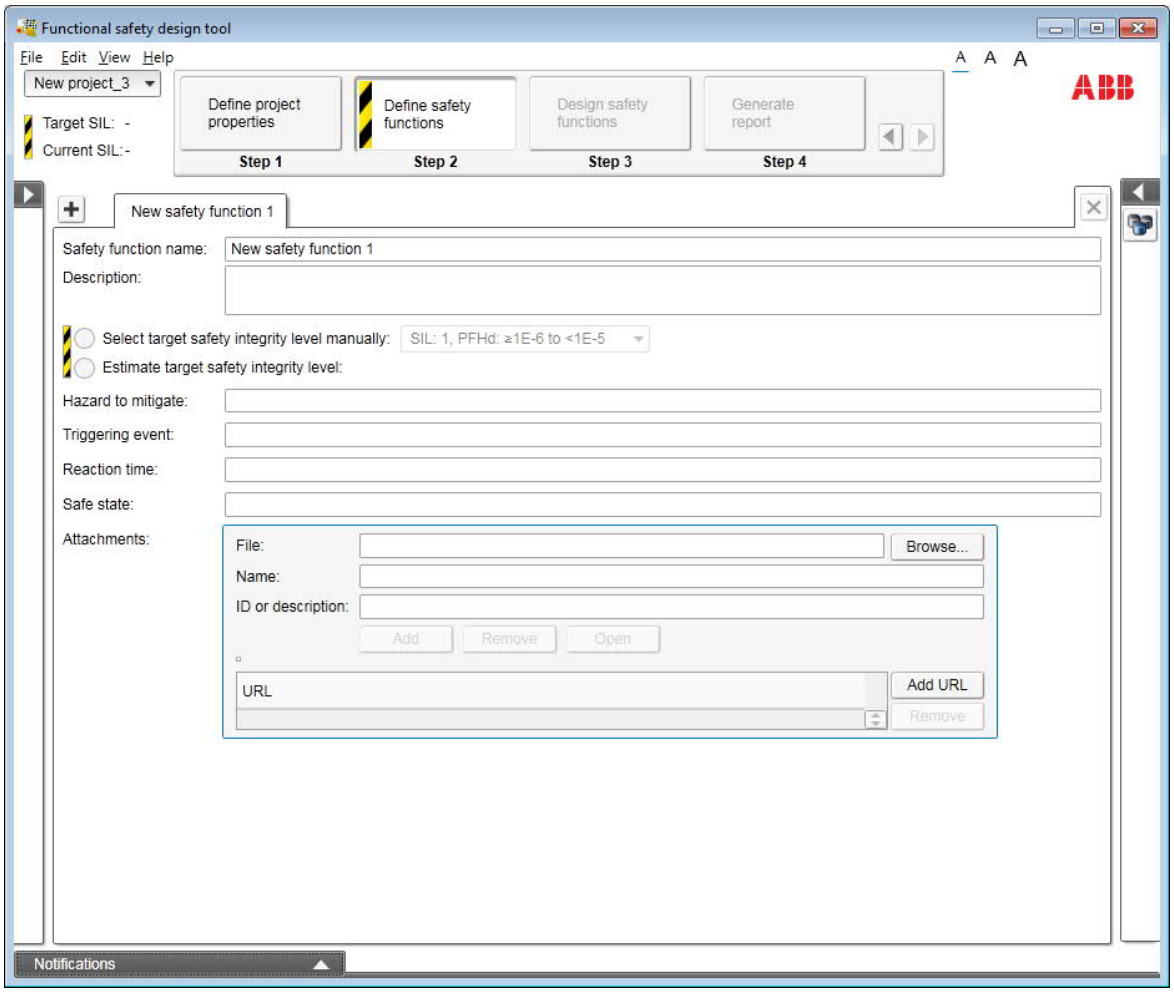



*Figure 27. Step 2: Define safety functions step – IEC 62061 project*

The mandatory inputs for Step 2, *IEC 62061* projects are (See *Figure 27*):

- **Safety function name** shall be a unique name within a safety zone or if zones are not used within the project.
- Safety function target SIL level:
  - **Select target safety integrity level manually** allows the user to directly specify the required target SIL level for the safety function using the related pull down menu.
  - **Estimate target safety integrity level** enables the user to do SIL assignment for the safety function according to method described in *IEC 62061*, Annex A.

Optional inputs for Step 2, *IEC 62061* projects are (See *Figure 27*):

- **Hazard to mitigate** allows the user to specify the purpose of the given safety function.
- **Triggering event** allows the user to describe the conditions required for activating the safety function.
- **Response time** allows the user to specify the response time of the safety function.
- **Safe state** allows the user to describe the safe state enforced by the safety function.
- **Attachments** can be any files needed to be attached to the project. Here you can also define the URL for useful web site links.
  - Click **Browse** to look for a file in an existing folder on the hard disks or enter the folder path and file name directly. The tool suggests a name for the attachment but the name can be changed if needed. The user can also give the attachment an ID or description. Click **Add** to add the attachment to the project. The attachments can be removed with the **Remove** button. Clicking **Open** opens the selected attachment in an appropriate application.
  - To add a web link to the project, click **Add URL** button and type in the web site address on the list.

For both *ISO 13849-1* and *IEC 62061* projects safety functions can be added by pressing the **[+]** button located at the top of Step 2 view, see *Figure 27*. You can select the currently active safety function from the tabs at the top of view. The currently active safety function can be deleted by applying the **[x]** button located at the top of Step 2 view.

When mandatory data is specified for Step 2, the user is allowed to proceed to Step 3, Design safety functions, by selecting **Step 3**, or by utilizing the next step button **[>]**, which both become enabled, as all mandatory data for Step 2 has been specified.

# Step 3 – Design safety functions

## Templates

Between Step 2 and Step 3 there is an intermediate step for each new safety function where safety function templates can be selected, as shown in *Figure 28*. The intermediate step appears in the tool work area.

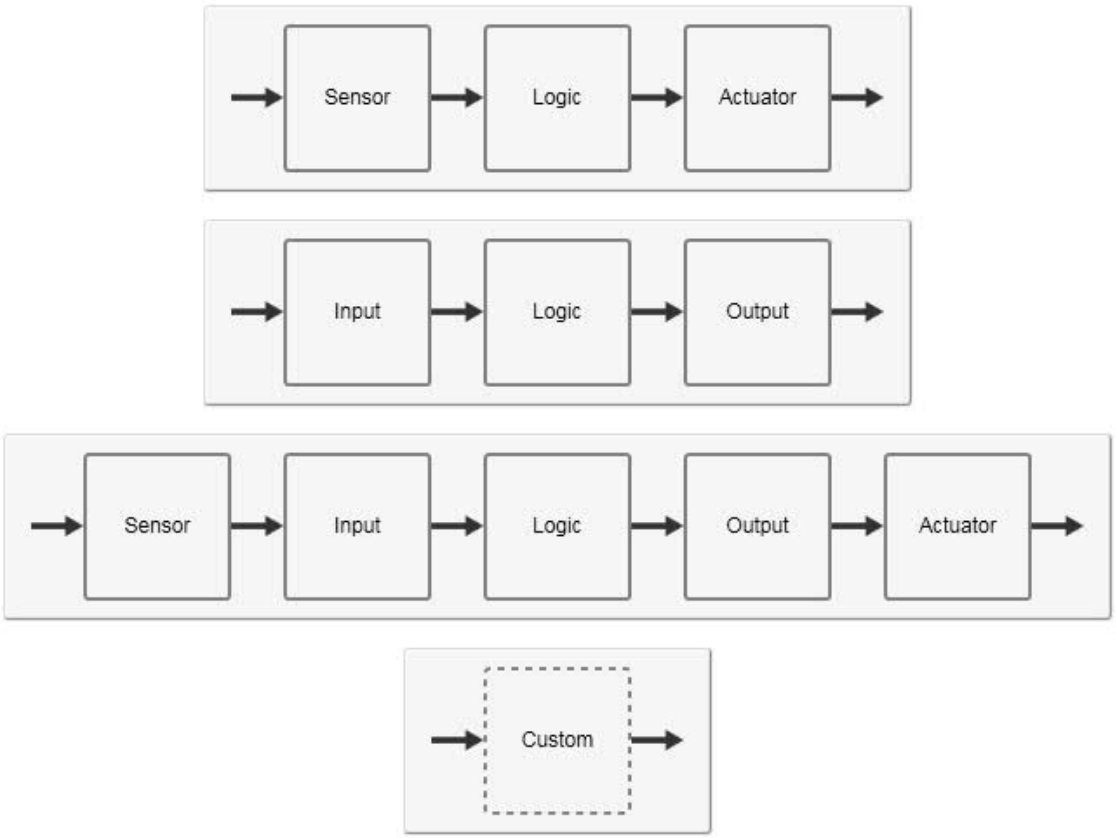



*Figure 28. Template selection for safety functions*

Available templates are:

- Sensor – Logic – Actuator
- Input – Logic – Output
- Sensor – Input – Logic – Output – Actuator
- Custom

The templates reflect the natural way to classify the subsystems in a chain of subsystems resulting in a complete safety function. If the user prefers not to use templates the **Custom** template may be selected, yielding an unconfigured subsystem that does not belong to any specific category. The template selection is similar for both *ISO 13849-1* and *IEC 62061* projects. The selected template appears in the work area and can be configured manually by the tool user, or configured by the dragging and dropping of components taken from available product libraries. The template offers guidance for safety function creation when using components from a library. When dragging a library component to a template the tool compares the functions defined for the component to the template blocks. You are allowed to drop the component into a template block when it has at least one use case with a function matching with the block. E.g. if a Sensor – Input – Logic – Output – Actuator template is used, a component, which has just “input” function defined can be dropped into the Sensor and Input blocks. Template blocks are at the subsystem level, so elements can be dropped into blocks regardless of their functions. It should be noted that with large safety functions the template block corresponding the library component may currently be outside the screen.

E.g. selecting the template **Input – Logic – Actuator** results in the template shown in *Figure 29*.


*Figure 29. Template Sensor – Logic – Actuator*

## Presentation of the safety functions

Functional safety design tool is a tool where safety functions are represented graphically as interconnected blocks, and where the building blocks are:

- **Subsystems** are the largest building blocks of a safety function. Subsystems are always serially connected.
- **Elements** are the smallest building blocks of a safety function. Elements are building blocks of subsystems. Elements inside subsystems are always organized according to designated architectures Cat B, Cat 1, Cat 2, Cat 3, or Cat 4 as described in *ISO 13849-1* for ISO projects, and according to architecture A, B, C and D for *IEC 62061* projects. Elements can be both serially and parallel connected.

*Figure 30* illustrates the work area and the graphical representation of the safety function. Subsystem SB3 is designed based on elements

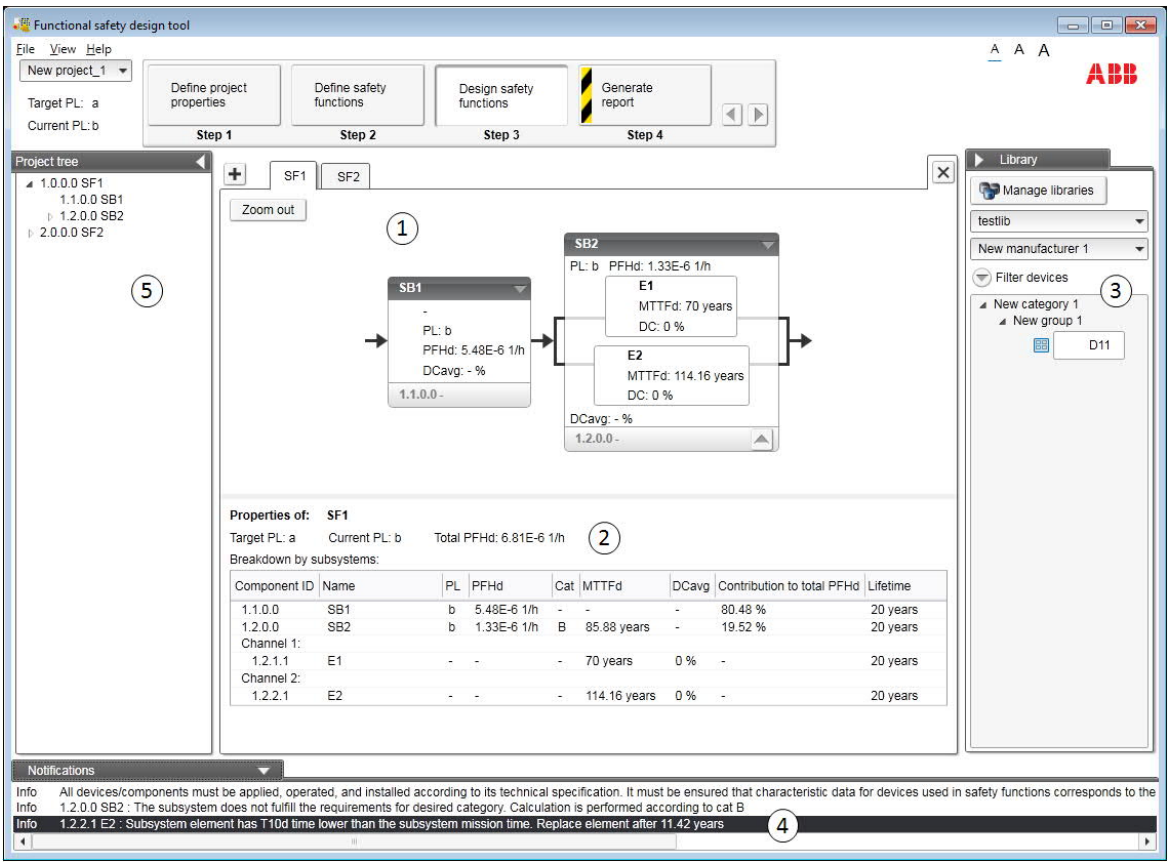



*Figure 30. Graphical representation of a safety function*

In *Figure 30* the following areas are identified:

1. Diagram area where the graphical representation of the safety function is drawn.
2. Performance panel where the calculation results and component configuration are listed. The performance panel is context dependent:

   Clicking in the work area outside a subsystem yields a list containing safety values for the current safety function, and also for the safety function building blocks.

   Clicking on the top bar of a subsystem yields a list containing the safety values and settings for the respective subsystem.

   Clicking on an element inside a subsystem yields a list containing safety values and settings for the respective elements.
3. Library panel where relevant component can be found and included into the work area by using drag and drop functionality.
4. Notification panel where critical messages and status information about the project can be found. Warnings are unacceptable conditions that must be solved. Info is given of a situation, which does not necessarily require actions, but of which the user should be aware.
5. Project panel where a hierarchical representation of the project can be found.

The values shown in performance panel depend on which standard, *ISO 13849-1* or *IEC 62061* is selected for the project.

When subsystems and elements are configured, the respective graphical block shows the top-level safety values inside the block. Subsystems and elements can be configured by selecting the relevant subsystem or element and pressing **Edit** in the performance panel or by selecting **Edit** from the component's context menu.

Subsystems and elements can be created manually or they can be taken from a library. When moving the mouse cursor over the diagram area, the blue fields indicate where elements and subsystems can be manually created or dropped from libraries, see *Figure 30*. Elements can only be placed inside subsystems. Manually created subsystems and elements must be configured with safety data.

Subsystems and elements are represented as shown in *Figure 31*.

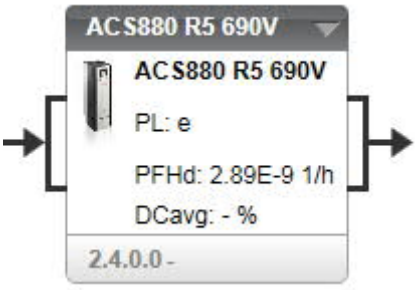



*Figure 31. Subsystem representation, ISO 13849-1 project*

For both subsystems and elements the options described below are available in their context menu. The context menu can be opened either by clicking the arrow in the top right corner of the subsystem block or by right-clicking the subsystem or element block.

- **Properties** selection brings the selected component's safety values and settings to the performance panel.
- **Edit** selection opens up subsystem or element property window for editing and configuration of subsystem or element.
- **Cut** selection cuts the subsystem or element.
- **Copy** selection copies the subsystem or element to clipboard.
- **Paste** selection allows user to paste in copied/cut subsystem or element.
- **Delete** selection deletes the relevant subsystem or element.

It is possible to add an icon for subsystems and elements. The used icon can be defined by pressing **Change icon** in the component's configuration window.

## Adding components to project area

### Drop areas

The project area contains specific areas, where the new components can be created. These areas show a blue rectangle when the mouse cursor is hovering above them. These areas for subsystems are shown in *Figure 32*. Respectively, *Figure 33* represents the areas for adding elements.

**Note:** In order to add elements, there needs to be a suitable subsystem first. A suitable subsystem is of the type: Subsystem designed with elements.


*Figure 32. Areas for adding subsystems*

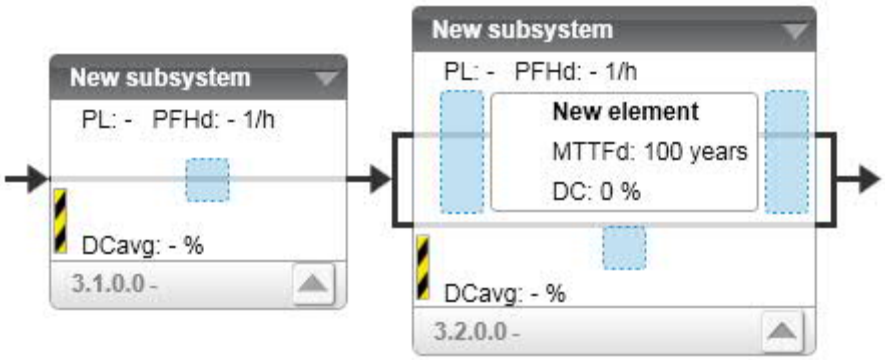



*Figure 33. Areas for adding elements*

## Options for adding components

You have three options for adding components to a safety function:

1. Create a completely new component. To do this, right-click any drop area, which opens a context menu with options to add the new component. Subsystems can be created also by right-clicking anywhere on empty space of the project area. The new subsystem is then created at the end of the safety function.
2. Paste a component. Right-click any drop area to open the context menu. The menu contains the option to paste the component if the clipboard contains a suitable component: a subsystem when clicking a subsystem drop area and similarly with elements. The component may be copied from any safety function from any project. The only requirement for the copied component to be pasted is that it is of the current standard. Subsystems can be pasted also by right-clicking anywhere on empty space of the project area. The subsystem is then pasted at the end of the safety function.
3. Drag a component from a library. Any subsystem can be dragged from a library and dropped to any subsystem drop area. Similarly, elements can be dragged and dropped to any element drop area. If you have selected a template, you can drop subsystems of with appropriate use case function to a block on the template. Elements can be dropped into any block on the template. When an element is dropped into a template block, the tool automatically sets the subsystem properties to the default values. Please note that when a library component is

used in a project, the version and the safety values of the component are saved with the project. Thus when the project is again opened, the values are retrieved from the project file. This is done in order to keep the project as designed regardless of the library updates. If you have a newer version of the library and want to get the newer safety values into use, use the **Update** project functionality from the **Help** menu. See chapter *Updating projects with new library data* for details.

# Configuration of subsystems and elements in ISO 13849-1 projects

## Configuration of subsystems in ISO 13849-1 projects

Subsystems in *ISO 13849-1* projects can be of the following types:

- **PL/PFH$_D$** type with which the top-level safety data is specified (see *Figure 34*).
- **Channel MTTF$_D$** type with which the subsystem MTTF$_D$ is specified (see *Figure 35*).
- **Subsystem designed with elements** type with which subsystem safety values are calculated based on the included elements (see *Figure 36*).
- **Output without reliability data** type which is only for mechanical, hydraulic or pneumatic components, which act as the output of the SRP/CS. With this type the subsystem safety values are calculated based on the reliability data (see *Figure 37*).
- **Fault exclusion** type with which the subsystem fault is excluded (see *Figure 38*).

The mandatory and optional data needed for configuration depend on the selected type. The different types are presented in the following chapters.

### PL/PFH$_D$ type

Mandatory subsystem configuration data for PL/PFH$_D$ type are (see *Figure 34*):

- **Name** of the subsystem.
- **Type** selected PL/PFH$_D$.
- **Performance level** (PL) shall be from a to e according to *ISO 13849-1*.
- **PFH$_D$** shall be equal or better than required for the specified PL level. The link between PL and PFH$_D$ can be deactivated if desired. If the link is used, the tool automatically sets a suitable PFH$_D$ value.
- **Lifetime** (mission time) of the subsystem shall be specified.

Optional data for PL/PFH$_D$ type are:

- **Category** Available selections are Cat B, 1, 2, 3 and 4 in accordance with the categories in ISO *ISO 13849-1*.
  - **Requirements** can be specified if the category is specified. If the requirements are specified, the user must explicitly confirm by using the category requirements checklist that all mandatory requirements needed for claiming a certain category are fulfilled.
- **CCF evaluation** If the category is specified and equals Cat 2 or higher the user can select to specify the CCF value for the subsystem. If the CCF is specified, its value must be equal or greater than 65 in order to claim Cat 2, 3, or 4.

- The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually.**

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

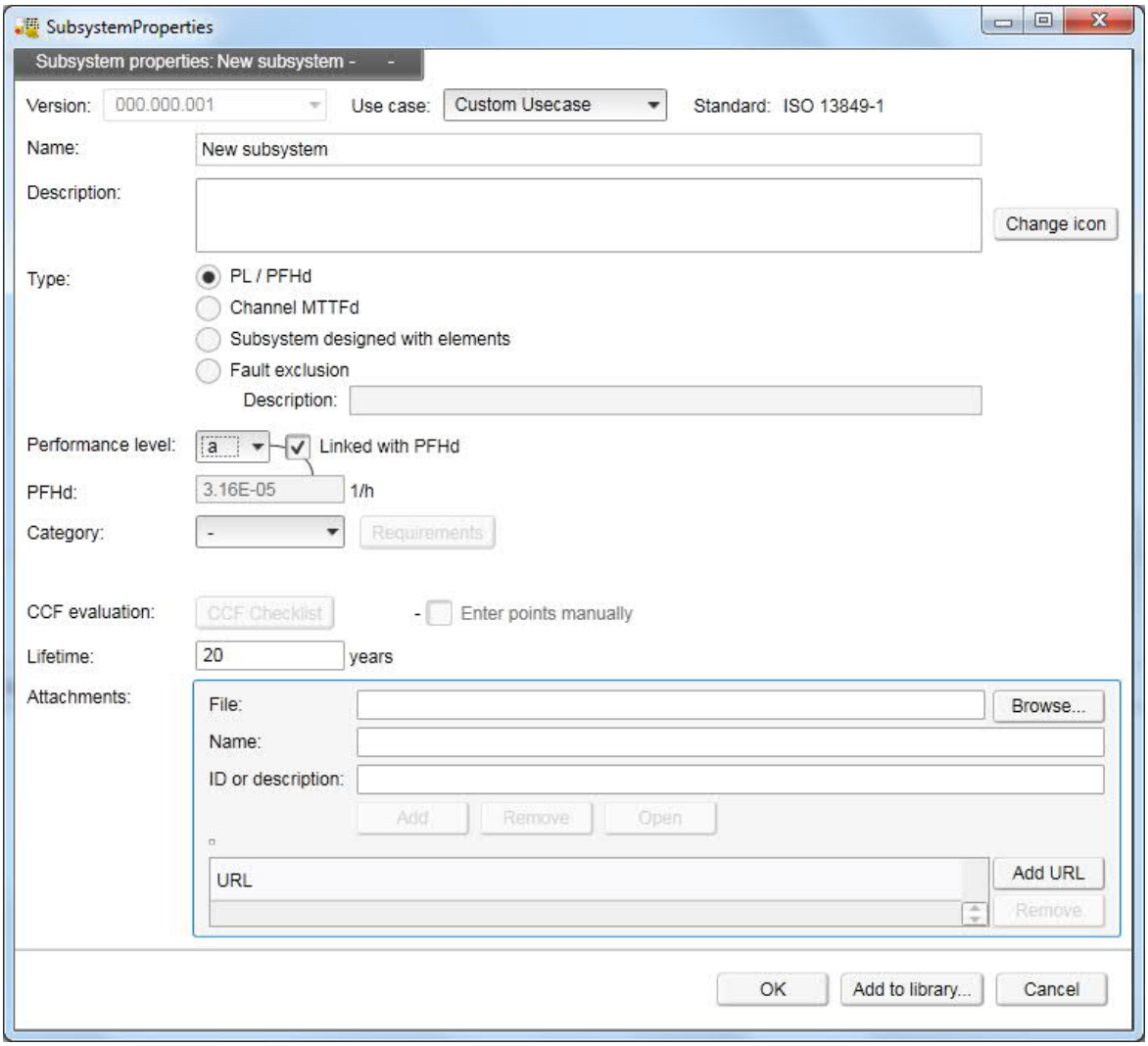



*Figure 34. Subsystem configuration window, ISO: PL/PFH$_D$ type*

## Channel MTTF$_D$ type

Mandatory subsystem configuration data for Channel MTTF$_D$ type are (see *Figure 35*):

- **Name** of the subsystem
- **Type** selected Channel MTTF$_D$
- **Category** Available selections are Cat B, 1, 2, 3 and 4 in accordance with categories in *ISO 13849-1*.
  - **Requirements** for claiming the selected category must be fulfilled. The user must explicitly confirm this by using the category requirements checklist.

    **Note:** If all mandatory requirements for the desired category are not confirmed to be fulfilled, the tool automatically reduces the category and performs the calculations according to the reduced category. At least such

requirements must be fulfilled that it is possible to find a category to reduce to. If this is not done, the tool prevents the user from proceeding.

**Note:** With category 2, selecting the less strict requirement for demand rate means that the component won't get as good $PFH_D$ value as otherwise.

- **CCF evaluation** If category equals Cat 2 or higher the user shall specify the CCF value for the subsystem. The CCF value must be equal or greater than 65 in order to claim cat 2, 3, or 4. If the CCF is lower than 65, the category is reduced accordingly.
  - The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually**.
- **$MTTF_D$** shall be specified for the subsystem
  - For category 4 subsystems extended $MTTF_D$ values are allowed. This is applied only for subsystems with effective category Cat 4.
- **DCavg** shall be specified for subsystems of Cat 2, 3, or 4.
- **Lifetime** (mission time) of the subsystem shall be specified.

Optional data for Channel $MTTF_D$ type are:

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

With the Channel $MTTF_D$ type the subsystem PL and $PFH_D$ are calculated based on the mandatory inputs.

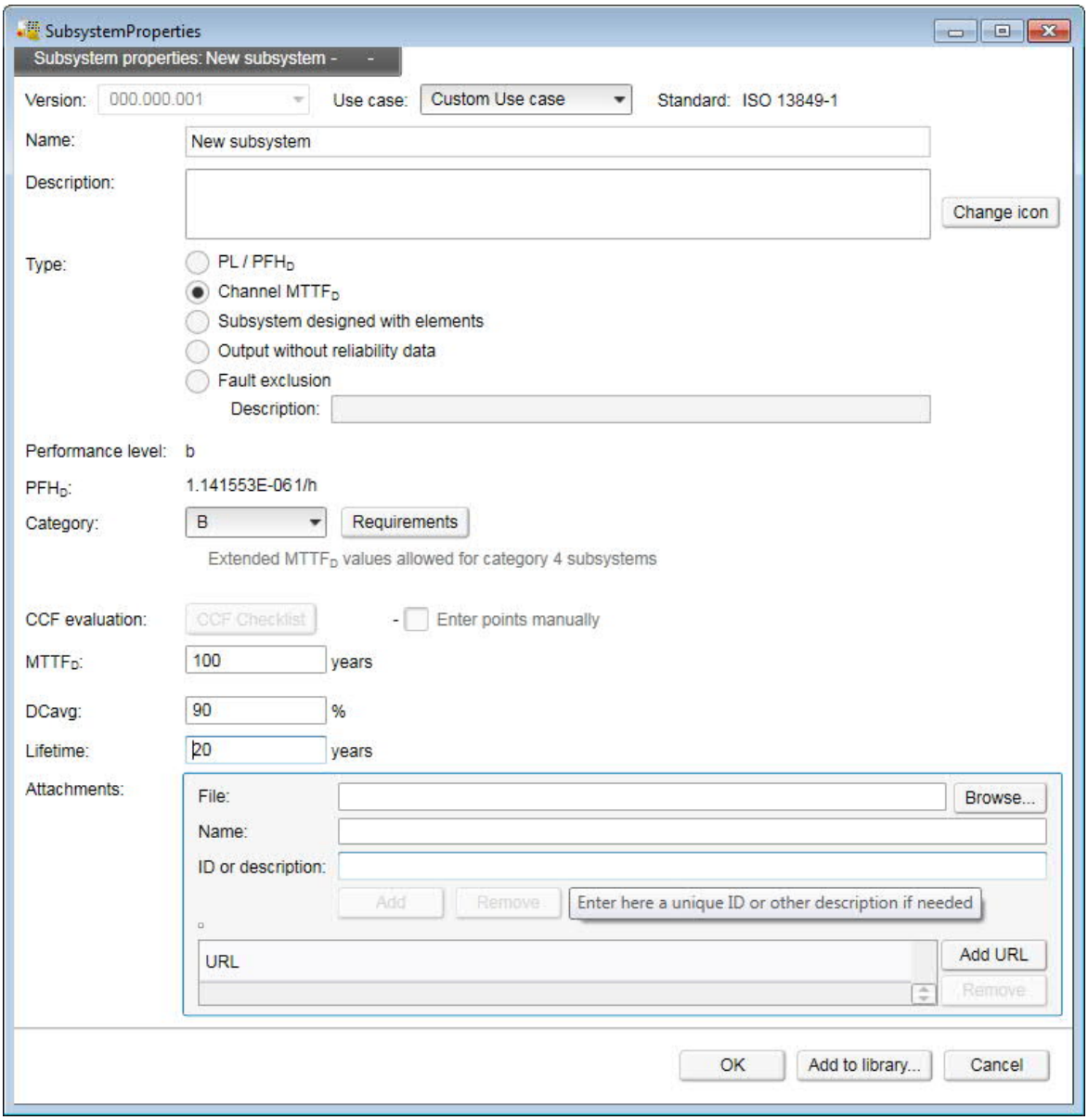



*Figure 35. Subsystem configuration window, ISO: $MTTF_D$ type*

## Subsystem designed with elements type

Mandatory subsystem configuration data for Designed with elements type are (see *Figure 36*):

- **Name** of the subsystem
- **Type** selected Subsystem designed with elements
- **Category** Available selections are Cat B, 1, 2, 3 and 4 in accordance with categories in *ISO 13849-1*.
  - **Requirements** for claiming the selected category must be fulfilled. The user must explicitly confirm this by using the category requirements checklist.

    **Note:** If all mandatory requirements for the desired category are not confirmed to be fulfilled, the tool automatically reduces the category and performs the calculations according to the reduced category. At least such

requirements must be fulfilled that it is possible to find a category to reduce to. If this is not done, the tool prevents the user from proceeding.

**Note:** With category 2, selecting the less strict requirement for demand rate means that the component won't get as good $PFH_D$ value as otherwise.

- **CCF evaluation** shall be specified for the subsystem if category equals Cat 2 or higher. The CCF value must be equal or greater than 65 in order to claim cat 2, 3, or 4.
  - The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually**

Optional data for Designed with elements type are:

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

With the Designed with element type the subsystem PL and $PFH_D$ are calculated based on mandatory inputs in the subsystem configuration window and based on included elements.

**Note:** The safety data PL and $PFH_D$ evaluation for this type of subsystem cannot be completed until elements are included and configured.

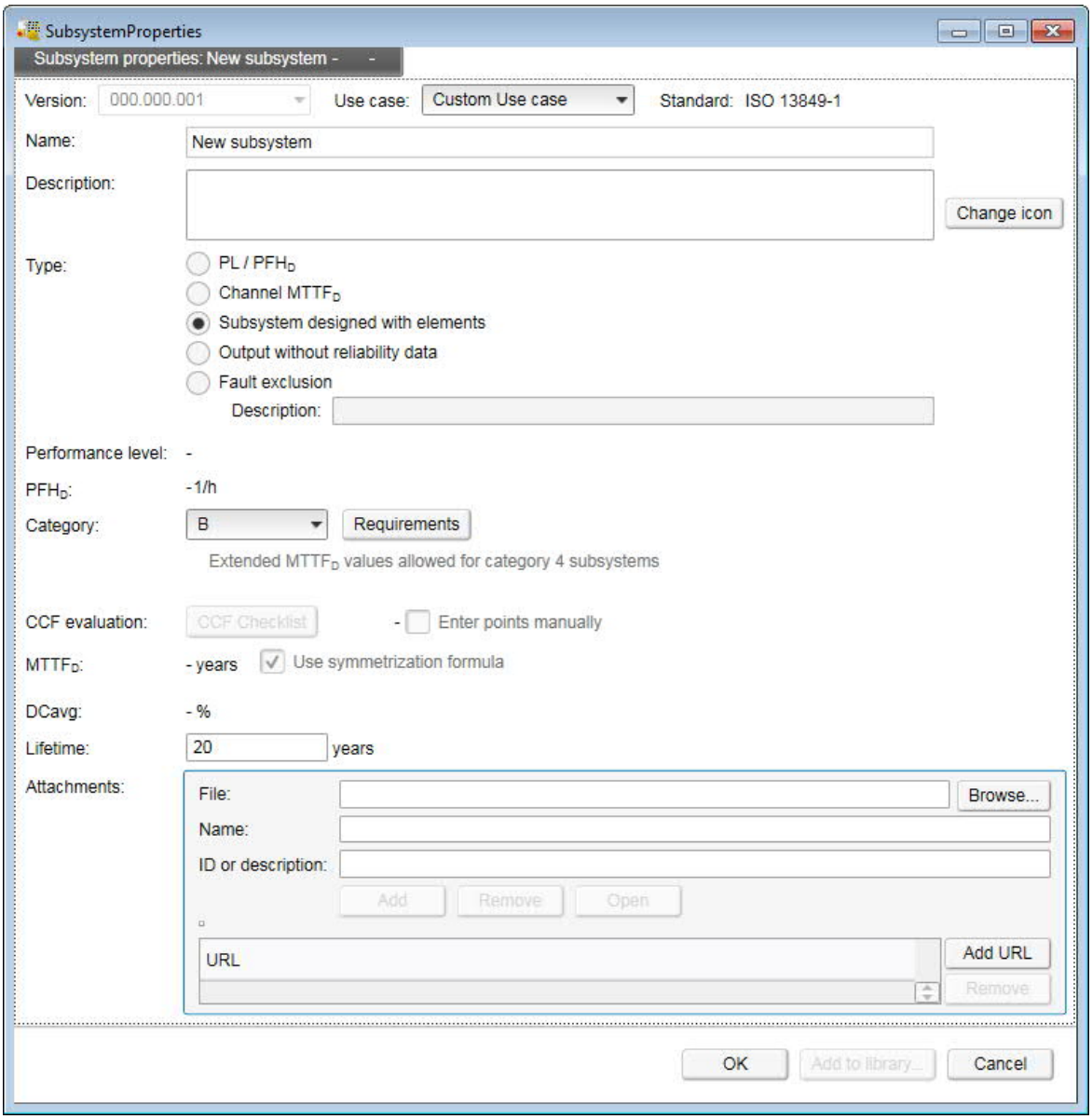



*Figure 36. Subsystem configuration window, ISO: Designed with elements type*

## Output without reliability data type

Mandatory subsystem configuration data for Output without reliability data type are (see *Figure 37*):

- **Name** of the subsystem.
- **Type** selected Subsystem designed with elements
- Confirmation that the component is used as the output part of the SRP/CS. This is required as this type is allowed only for outputs.
- **Category** Available selections are Cat B, 1, 2, 3 and 4 in accordance with categories in *ISO 13849-1*.
  - **Requirements** for claiming the selected category must be fulfilled. The user must explicitly confirm this by using the category requirements checklist.
- **CCF evaluation** shall be specified for the subsystem if category equals Cat 2 or higher. The CCF value must be equal or greater than 65 in order to claim cat 2, 3, or 4.

  - The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually**
- **DCavg** shall be specified for subsystems of Cat 2, 3, or 4.
- **Performance level** (PL) shall be from a to e according to *ISO 13849-1*.
  - The available PL levels depend on the selected category.
- **Lifetime** (mission time) of the subsystem shall be specified.

Optional data for Output without reliability data type are:

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

With the Output without reliability data type the subsystem $PFH_D$ is calculated based on the mandatory inputs.

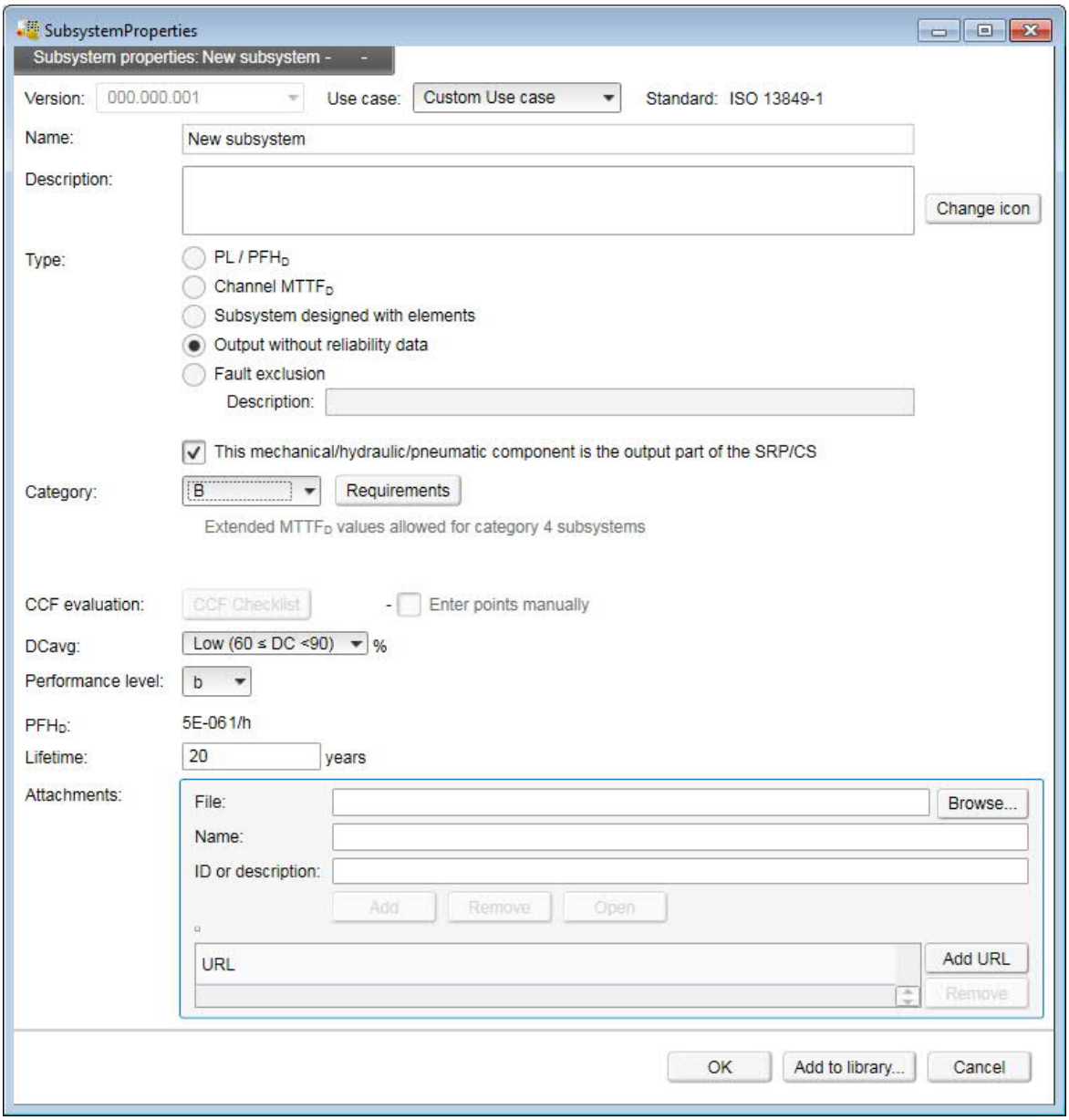



*Figure 37. Subsystem configuration window, ISO: Output without reliability data type*

## Fault exclusion type

Mandatory subsystem configuration data for Fault exclusion type are (see *Figure 38*):

- **Name** of the subsystem.
- **Type** selected Fault exclusion.
  - **Description** or fault exclusion rationale shall be stated. Standard ISO 13849-2 provides ruling for fault exclusions to be claimed.
- **Performance level** shall be from a to e according to *ISO 13849-1*.
- **Lifetime** (mission time) of the subsystem shall be specified.

Optional data for Fault exclusion type are:

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

**Note:** For fault excluded subsystems the $PFH_D$ is set equal to 0. When fault exclusion is claimed it means that no dangerous faults can occur with the subsystem in question.

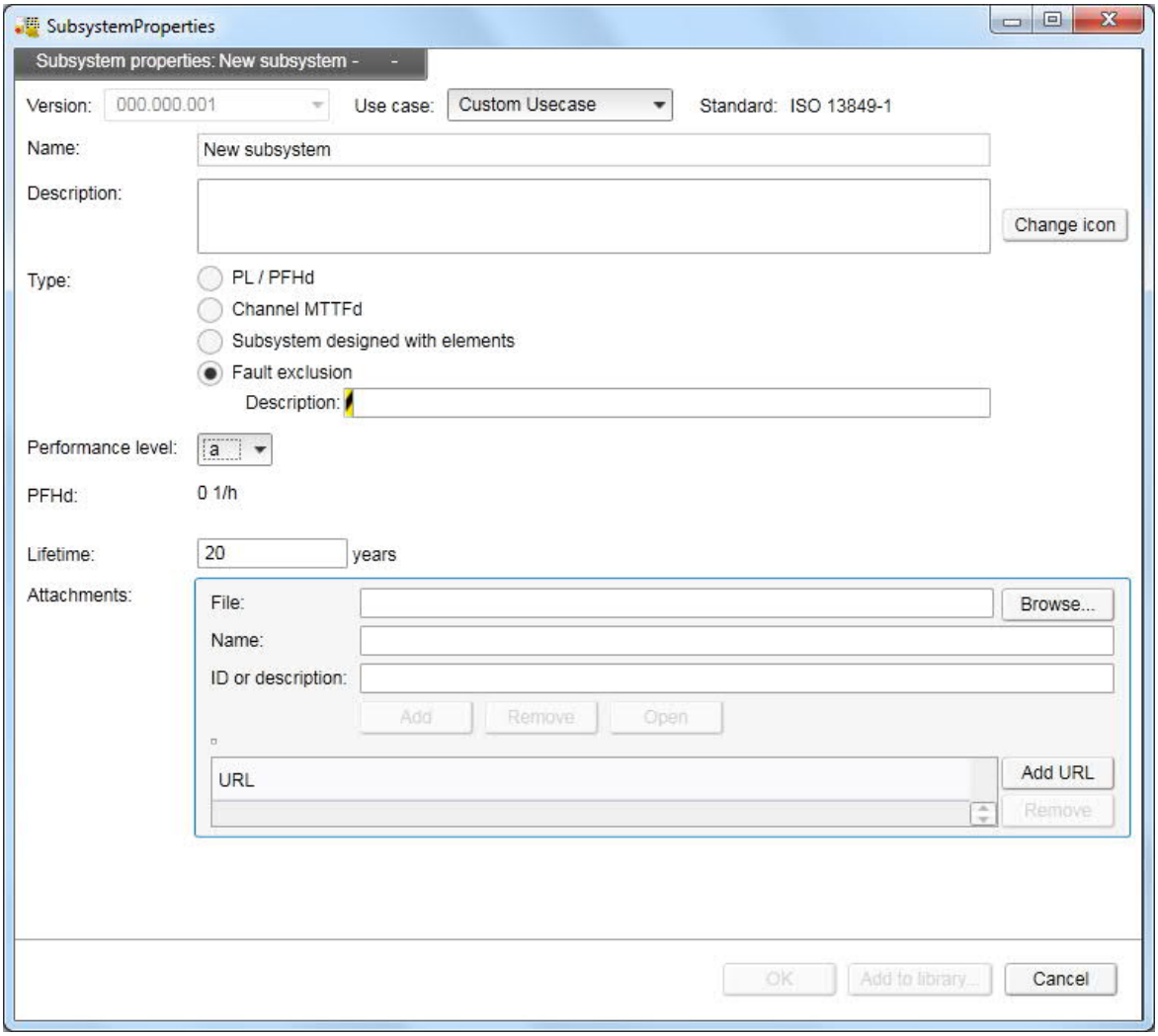



*Figure 38. Subsystem configuration window, ISO: Fault exclusion type*

## Configuration of subsystem elements in ISO 13849-1 projects

Subsystems elements (or just elements) in *ISO 13849-1* projects can be of the following types:

- **Non-wearing**, with which the $MTTF_D$ for the device can be specified directly (see *Figure 39*).
- **Wearing**, with which the elements $MTTF_D$ can be specified in terms of $B_{10D}$ values and the device's operation frequency (see *Figure 40*).
- **Fault exclusion** for elements where fault exclusion can be applied (*Figure 41*).

The mandatory and optional data needed for configuration depend on the selected type. The different types are presented in the following chapters.

### Non-wearing type

Mandatory element configuration data for Non-wearing type are (see *Figure 39*):

- **Name** of the element.
- **Type** selected Non-wearing type.
- **$MTTF_D$** shall be specified.
  - There are two ways to specify the $MTTF_D$: either by specifying the $MTTF_D$ directly or by specifying **MTTF** and **RDF**. In this latter case the tool calculates the $MTTF_D$ based on MTTF and RDF. If MTTF and RDF are both already specified and the user edits the $MTTF_D$, the tool calculates a new value for the MTTF. All three values shall be specified. Usual assumption is RDF = 50% if the ratio is unknown. See *ISO 13849-1*.
- **Lifetime** (mission time) of the element shall be specified.
- **DC** is the diagnostic coverage of the device.
  - DC can be found using the embedded **DC measure** checklist or specified manually.
  - Optionally the rationale for the DC can be specified in the related **Description** field. If the DC measure checklist is used, the rationale from the selected point in the list is automatically copied to the description.

Optional data for Non-wearing type are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

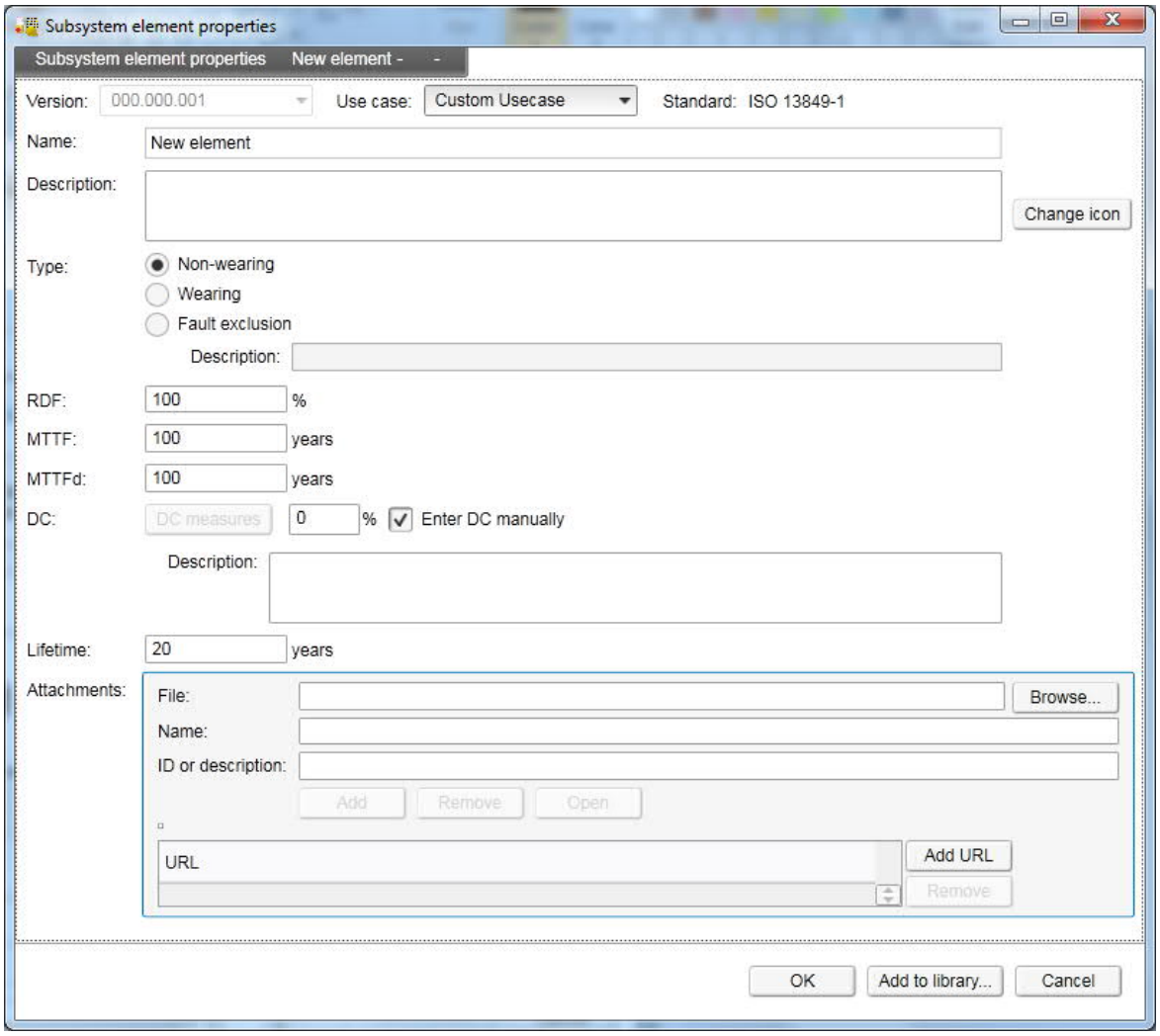



*Figure 39. Element configuration window, ISO: Non-wearing type*

## Wearing type

Mandatory element configuration data for Wearing type are (see *Figure 40*):

- **Name** of element.
- **Type** selected Wearing type.
- **$B_{10D}$** shall be specified.
  - There are two ways to specify the $B_{10D}$: either by specifying the $B_{10D}$ directly or by specifying **$B_{10}$** and **RDF**. In this latter case the tool calculates the $B_{10D}$ based on $B_{10}$ and RDF. If $B_{10}$ and RDF are both already specified and the user edits the $B_{10D}$, the tool calculates a new value for the $B_{10}$. All three values shall be specified. Usual assumption is RDF = 50% if the ratio is unknown. See *ISO 13849-1*.
- **nop** is the number of operations per year.
  - nop can be specified either by specifying the **operating days per year**, **operating hours per day**, and **time between operations** or, if the **Enter number of operations manually** is checked, by specifying directly the number of operations per the selected time unit.
  - **Note:** it is possible to add the component to a library also without defining a value for nop.

- **Lifetime** (mission time) of the element shall be specified.
- **DC** is the diagnostic coverage of the device.
  - DC can be determined by using the embedded **DC measure** checklist or it can be specified manually.
  - Optionally the rationale for the DC can be specified in the related **Description** field. If the DC measure checklist is used, the rationale from the selected point in the list is automatically copied to the description.

Optional data for Wearing type are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

$MTTF_D$ for the element is calculated based on mandatory inputs.

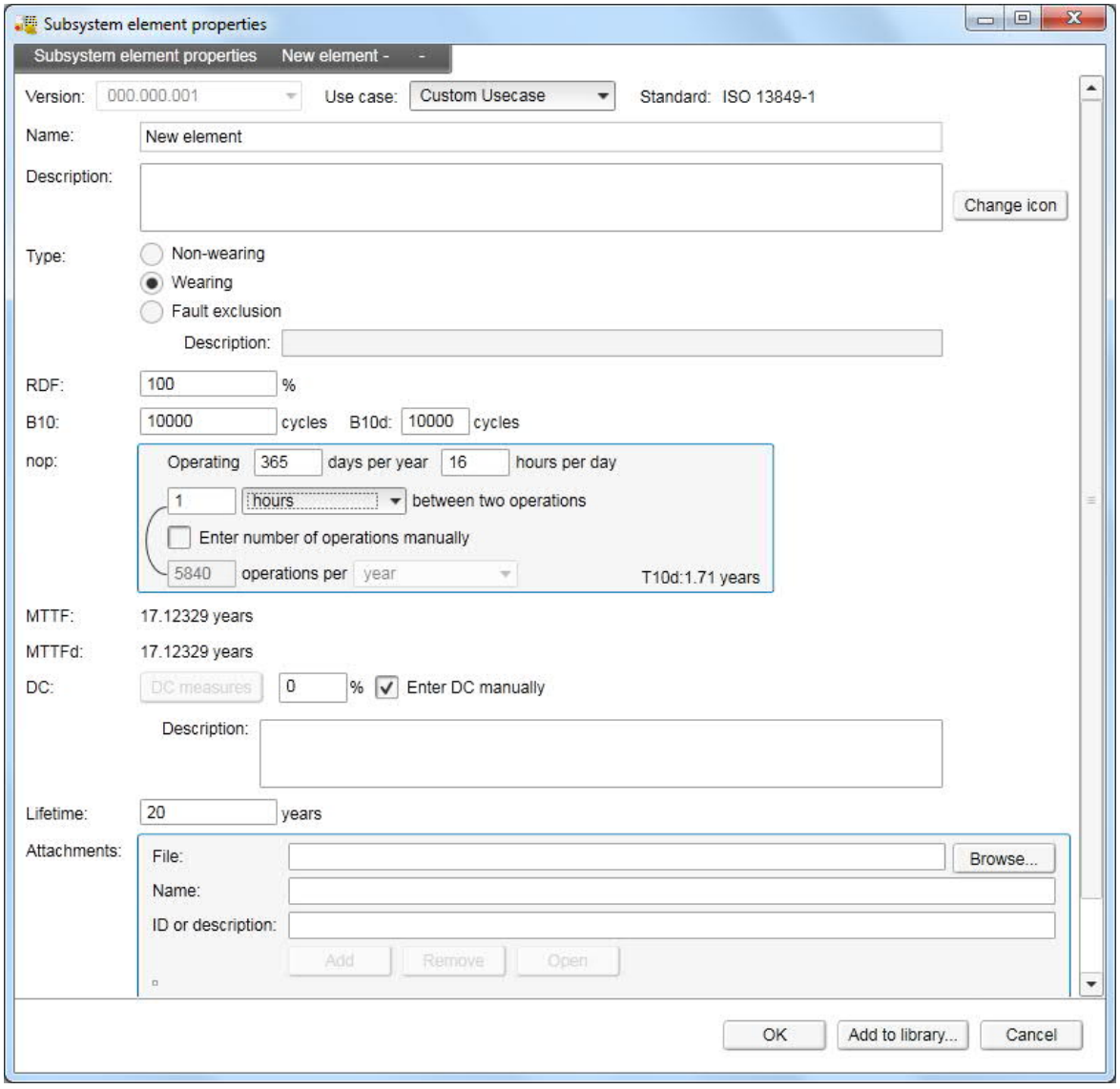



*Figure 40. Element configuration window, ISO: Wearing type*

## Fault exclusion type

Mandatory element configuration data for Fault exclusion type are (see *Figure 41*):

- **Name** of the element.
- **Type** selected Fault exclusion type.
  - Rationale for fault exclusion shall be specified in the respective **Description** field. Standard ISO 13849-2 provides ruling for fault exclusions to be claimed.
- **Lifetime** (mission time) shall be specified.

Optional data for **Fault exclusion** types are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

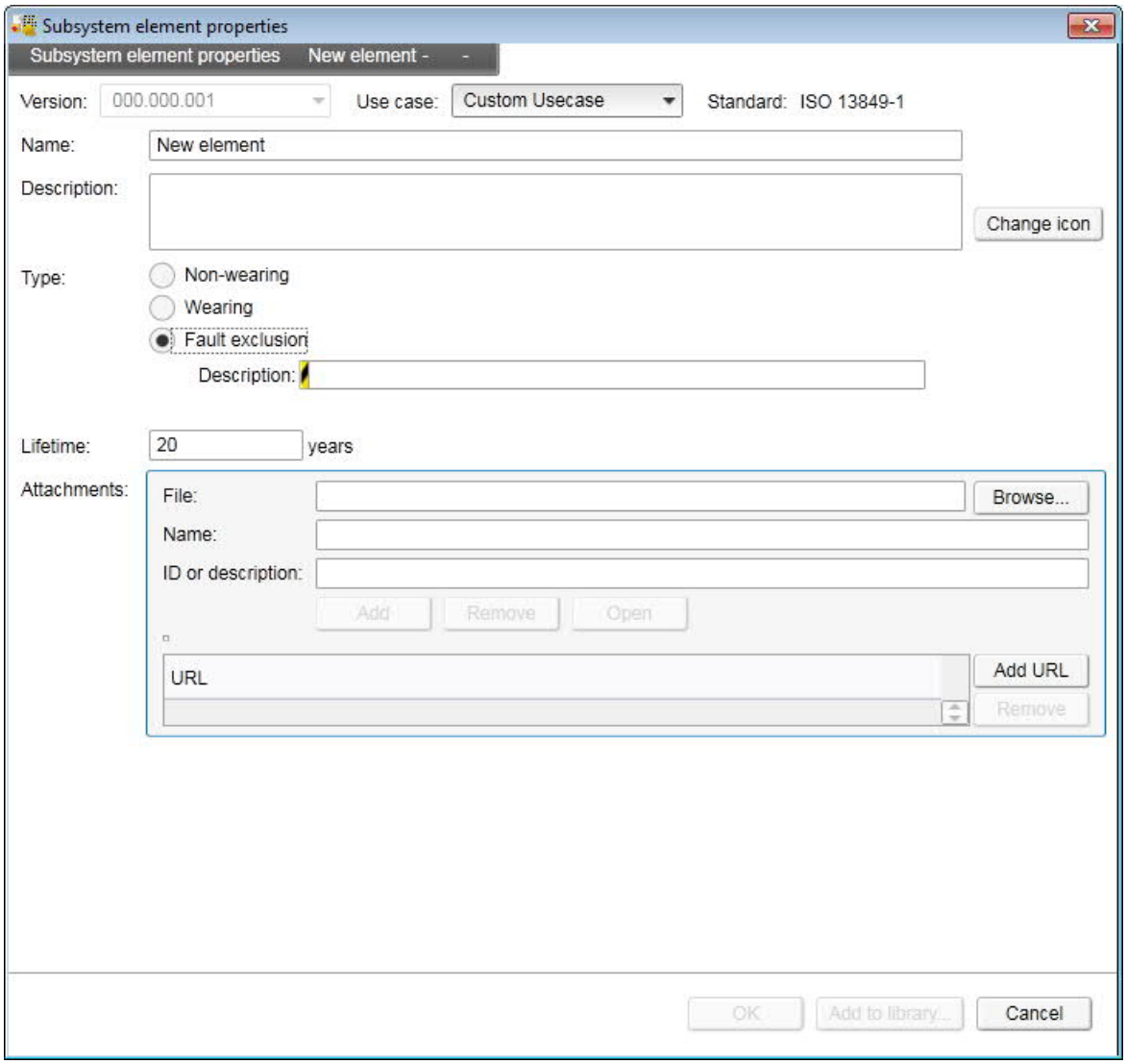



*Figure 41. Element configuration window, ISO: Fault exclusion type*

# Configuration of subsystems and elements in IEC 62061 projects

## Configuration of subsystems in IEC 62061 projects

Subsystems in *IEC 62061* projects can be of the following types:

- **SILCL/PFH$_D$**, with which the top-level safety data is specified (see *Figure 42*).
- **Subsystem designed with elements**, with which the subsystem safety values are calculated based on included elements (see *Figure 43*).
- **Fault exclusion**, with which the subsystem is fault excluded (see *Figure 44*).

The data needed for configuration depends on the type, and the different types are presented in the following chapters. Mandatory and optional data depends on the selected type.

### SILCL/PFH$_D$ type

Mandatory subsystem configuration data for SILCL/PFH$_D$ type are (see *Figure 42*):

- **Name** of the subsystem.
- **Type** selected SILCL/PFH$_D$.
- **SILCL** shall be from 1 to 3 according to *IEC 62061*.
- **PFH$_D$** shall be equal to or better than required for the specified SILCL level. The link between SILCL and PFH$_D$ can be deactivated if desired. If the link is used, the tool automatically sets a suitable PFH$_D$ value.
- **T1** is the proof test interval or lifetime of the subsystem (whichever is smaller) and it shall be specified.

Optional data for SILCL/PFH$_D$ type are:

- **Channels** Available selections are: Not specified, 1 or 2 in accordance with *IEC 62061*.
- **CCF evaluation** If two channel subsystem is specified the user can select to specify the CCF value for the subsystem. The CCF may be 1%, 2%, 5% or 10% in accordance with *IEC 62061*.
  - The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually.**
- **SFF** (safe failure fraction) is the percentage of the safe failures.
- **DCavg** is the average diagnostic coverage of the device. If left empty the tool assumes DCavg = 0. DCavg must always be less than or equal to SFF.
- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

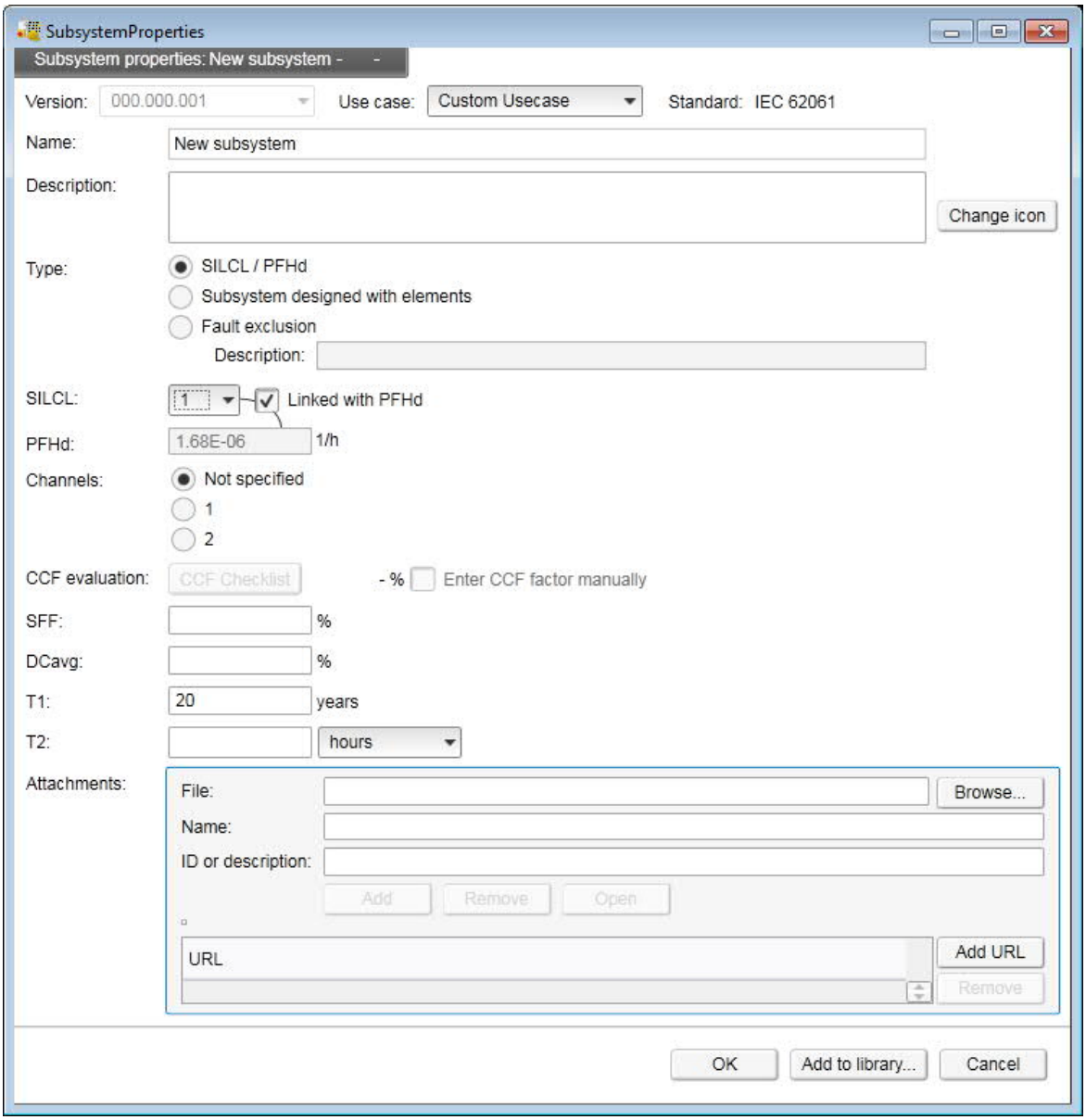



*Figure 42. Subsystem configuration window, IEC: SILCL/PFH$_D$ type*

## Subsystem designed with elements type

Mandatory subsystem configuration data for Designed with elements type are (see *Figure 43*):

- **Name** of the subsystem
- **Type** selected Subsystem designed with elements
- **Channels** Available selections are 1 or 2 in accordance with *IEC 62061*. Not specified cannot be selected for this type of subsystem.
- **CCF evaluation** If two channel subsystem is specified the user shall specify the CCF value for the subsystem. The CCF may be 1%, 2%, 5% or 10% in accordance with *IEC 62061*.
  - The CCF value for the subsystem can be evaluated by using the available **CCF checklist** or entered manually by selecting **Enter points manually**

- **T1** is the proof test interval or lifetime of the subsystem (whichever is smaller) and it shall be specified.
- **T2** of the subsystem shall be specified, if a two channel subsystem is specified and the diagnostics are utilized (DCavg > 0).

> **Note:** Since the DCavg cannot be defined until elements are specified, T2 is treated as optional until elements with DC > 0 are included. If T2 is left unspecified and elements with DC > 0 are included, the warning stripe on subsystem will be enabled, and T2 is made mandatory. User needs to enter subsystem configuration window and specify T2 in order to remove warning.

Optional data for Designed with elements type are:

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

With the Designed with element type the subsystem SILCL and $PFH_D$ are calculated based on mandatory inputs in the subsystem configuration window and based on included elements.

> **Note:** The safety data SILCL and $PFH_D$ evaluation for this type of subsystem cannot be completed until elements are included and configured.

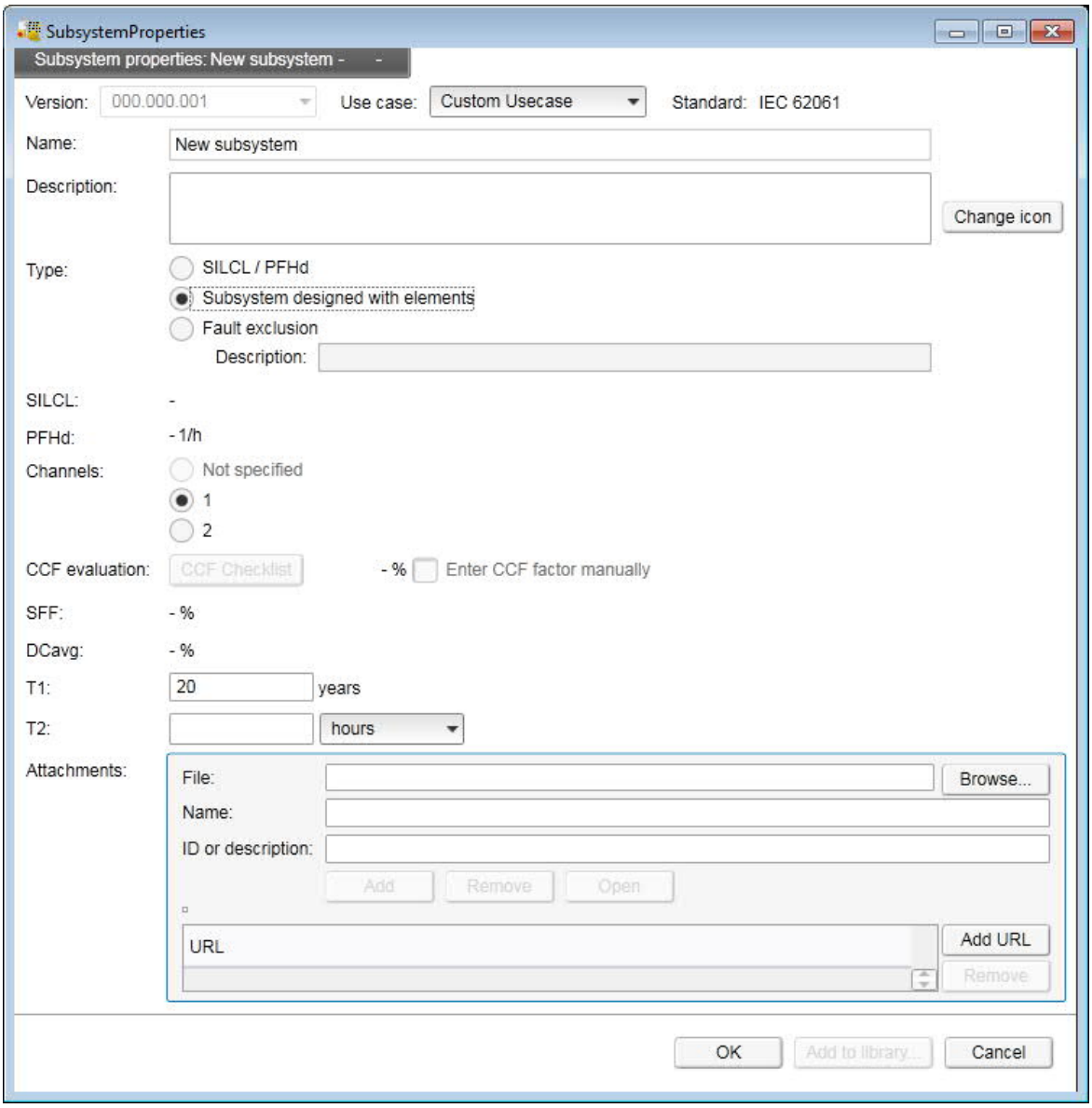



*Figure 43. Subsystem configuration window, IEC: Designed with elements type*

## Fault exclusion type

Mandatory subsystem configuration data for Fault exclusion type are (see *Figure 44*):

- **Name** of the subsystem.
- **Type** selected Fault exclusion.
  - **Description** or fault exclusion rationale shall be stated.
- **SILCL** shall be from 1 to 3 according to *IEC 62061*.
- **T1** is the proof test interval or lifetime of the subsystem (whichever is smaller) and it shall be specified.

Optional data for Fault exclusion type are:

- **Channels** Available selections are: Not specified, 1 or 2 in accordance with *IEC 62061*.

**Note:** If Channels = 1, maximum SILCL allowed is SIL 2. For Channels = Not specified, and channels = 2, all SILCL levels are allowed.

- **Description** can be used to describe the subsystem.
- **Attachments** can be added as well as URLs.

**Note:** For fault excluded subsystems the $PFH_D$ is set equal to 0. When fault exclusion is claimed it means that no dangerous faults can occur with the subsystem in question.

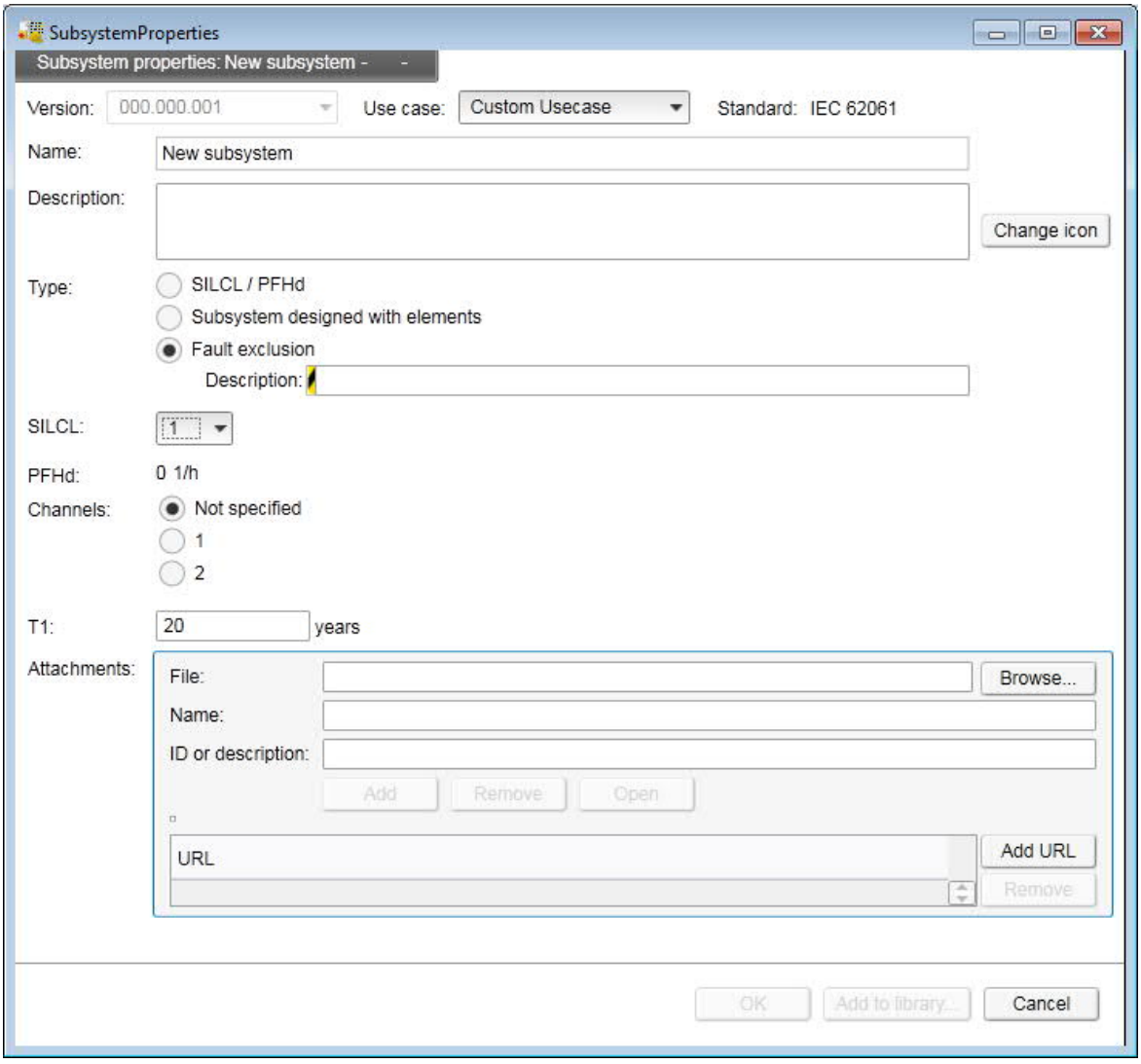



*Figure 44. Subsystem configuration window, IEC: Fault Exclusion type*

## Configuration of subsystem elements in IEC 62061 projects

Subsystems elements (or just elements) in *IEC 62061* projects can be of the following types:

- **Non-wearing**, with which the failure rate of dangerous failures, the λd, for the device can be specified directly (see *Figure 45*).
- **Wearing**, with which the element's λd can be specified in terms of $B_{10D}$ values and the device's operation frequency (see *Figure 46*).

- **Fault exclusion** for elements where fault exclusion can be applied (see *Figure 47*).

The mandatory and optional data needed for configuration depend on the selected type. The different types are presented in the following chapters.

### Non-wearing type

Mandatory element configuration data for Non-wearing type are (see *Figure 45*):

- **Name** of the element.
- **Type** selected Non-wearing type.
- **λd** (failure rate of dangerous failures) shall be specified.
  - There are two ways to specify the λd: either by specifying the **λd** directly or by specifying **λ** and **RDF**. In this latter case the tool calculates the λd based on λ and RDF. If λ and RDF are both already specified and the user edits the λd, the tool calculates a new value for the λ. All three values shall be specified.
- **T1** is the proof test interval or lifetime of the element (whichever is smaller) and it shall be specified.
- **DC** is the diagnostic coverage of the device. If left empty the tool assumes DC = 0.
  - DC can be found using the embedded **DC measure** checklist or specified manually.
  - Optionally the rationale for the DC can be specified in the related **Description** field. If the DC measure checklist is used, the rationale from the selected point in the list is automatically copied to the description.

Optional data for Non-wearing type are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

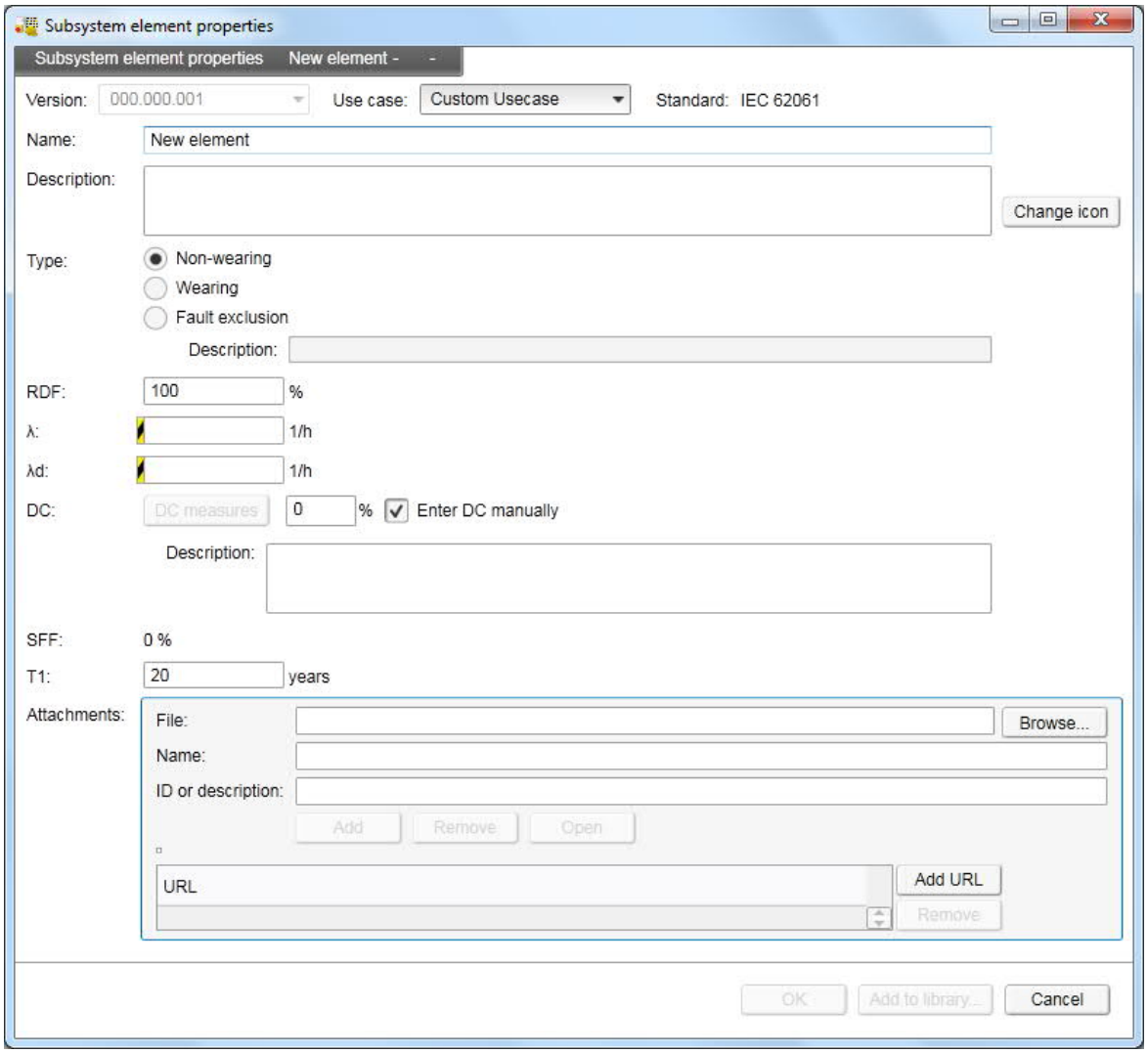



*Figure 45. Element configuration window, IEC: Non-wearing type*

## Wearing type

Mandatory element configuration data for Wearing type are (see *Figure 46*):

- **Name** of element.
- **Type** selected Wearing type.
- **$B_{10D}$** shall be specified.
  - There are two ways to specify the $B_{10D}$: either by specifying the $B_{10D}$ directly or by specifying **$B_{10}$** and **RDF**. In this latter case the tool calculates the $B_{10D}$ based on $B_{10}$ and RDF. If $B_{10}$ and RDF are both already specified and the user edits the $B_{10D}$, the tool calculates a new value for the $B_{10}$. All three values shall be specified.
- **nop** is the number of operations per year.
  - nop can be specified either by specifying the **operating days per year**, **operating hours per day**, and **time between operations** or, if the **Enter number of operations manually** is checked, by specifying directly the number of operations per the selected time unit.
  - **Note:** it is possible to add the component to a library also without defining a value for nop.

- **T1** is the proof test interval or lifetime of the element (whichever is smaller) and it shall be specified.
- **DC** is the diagnostic coverage of the device.
  - DC can be found using the embedded **DC measure** checklist or specified manually.
  - Optionally the rationale for the DC can be specified in the related **Description** field. If the DC measure checklist is used, the rationale from the selected point in the list is automatically copied to the description.

Optional data for Wearing type are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

λd for the element is calculated based on mandatory inputs.

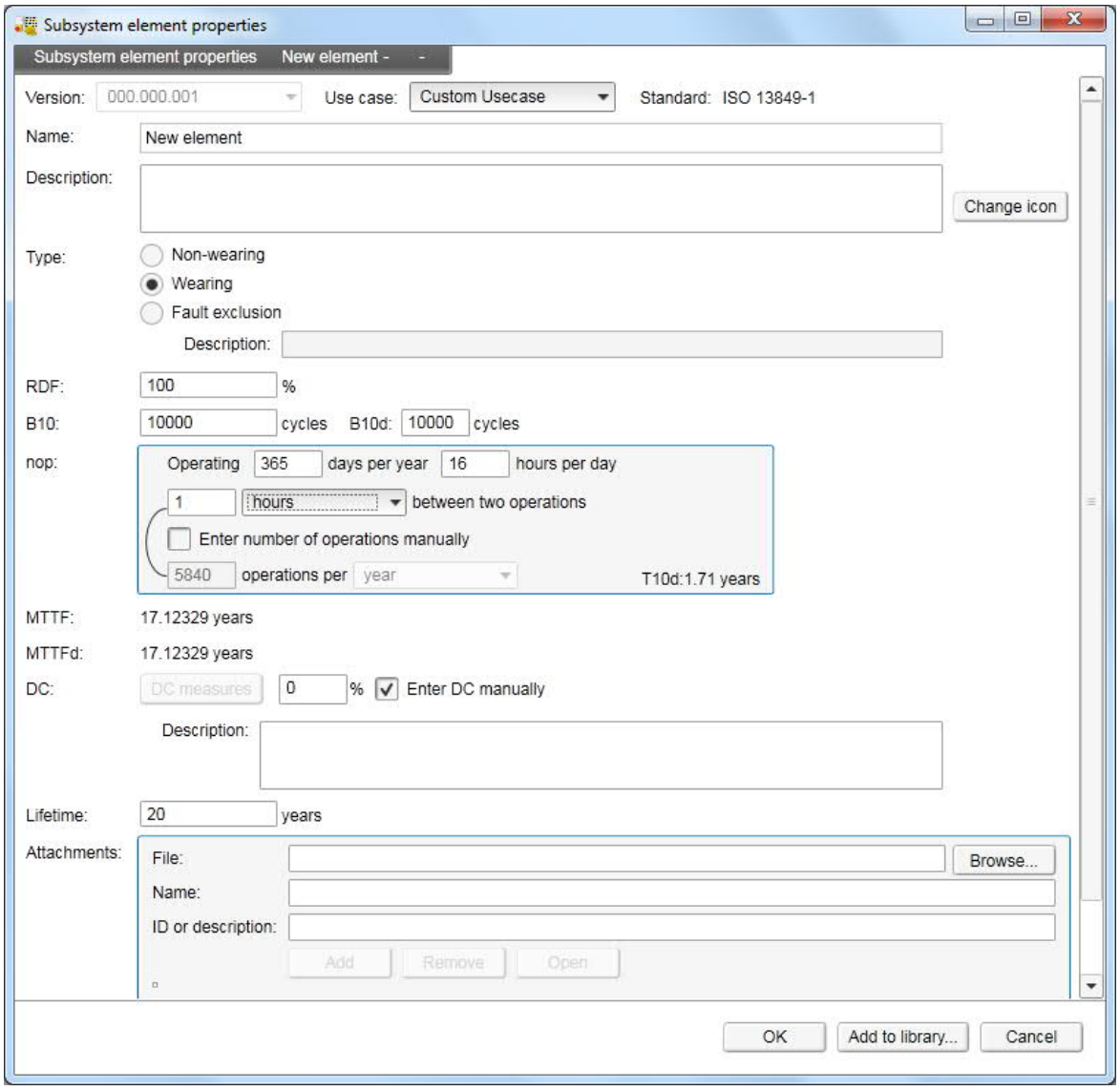



*Figure 46. Element configuration window, IEC: Wearing type*

### Fault exclusion type

Mandatory element configuration data for Fault exclusion type are (see *Figure 47*):

- **Name** of the element.
- **Type** selected Fault exclusion type.
  - Rationale for fault exclusion shall be specified in the respective **Description** field.
- **T1** is the proof test interval or lifetime of the element (whichever is smaller) and it shall be specified.

Optional data for **Fault exclusion** type are:

- **Description** can be used to describe the element.
- **Attachments** can be added as well as URLs.

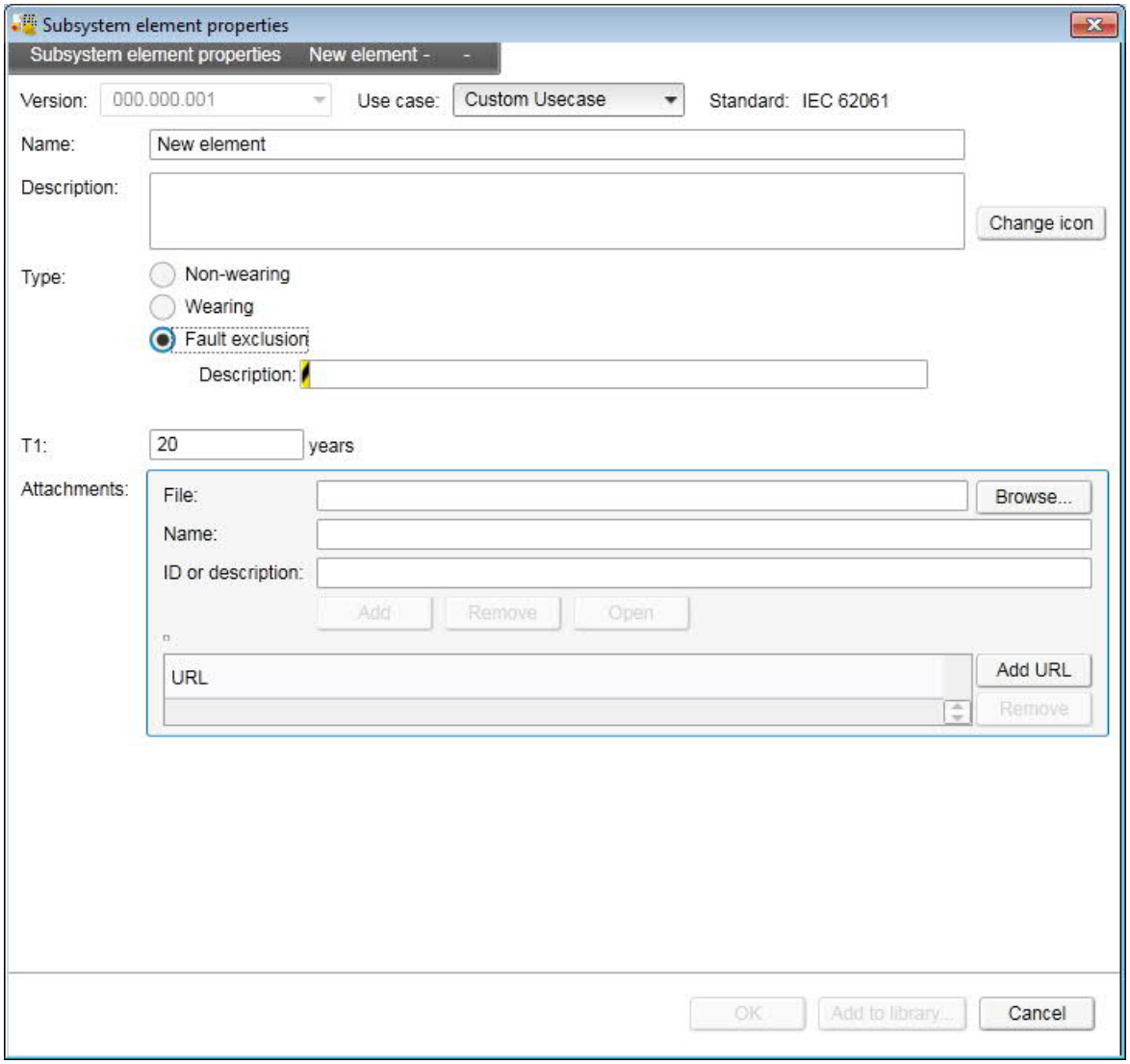



*Figure 47. Element configuration window, IEC: Fault exclusion type*

# Step 4 – Generate report

The last step with a project is to generate a report, which documents the project features. The following options are available for report handling:

- **Language** The current tool version supports reports in English and German.
- **Format** The current tool version supports reports in PDF format.
- **Content** included in the report can be manually modified with the checkboxes below. You can also save a set of selections with the **Save content preset** button and load it again with the **Load content preset** button. **Default content template** button selects all checkboxes.
- **Company header** can be the company's name etc. This is shown in the report footer.
- **Company address** is shown in the report footer.
- **Contact information** can be some other means to take contact. This is added to the report footer.
- **Company icon** is shown in the report header.

- **Preview** opens the report in the appropriate application based on the selection above.
- **Print** opens a print dialog for printing the report.
- **Save report** opens the save dialog for saving the report to a disc.

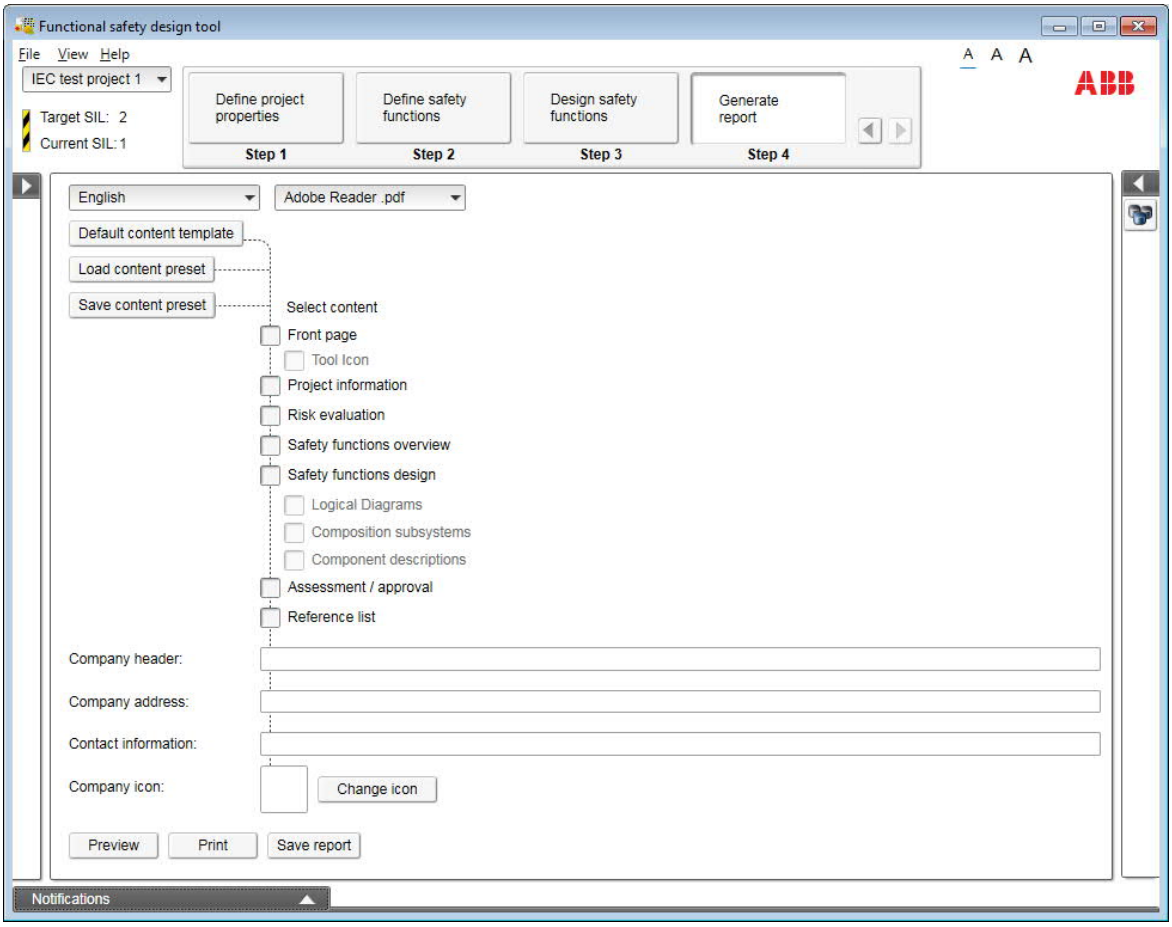



*Figure 48. Step 4: Generate report*

6

# Managing the libraries

## What this chapter contains

This chapter describes the component libraries and how to manage them. The procedures how to create, edit, import, export and update the libraries are described.

## Overview of the libraries

The component libraries are collections of devices with safety data. All libraries used in Functional safety design tool are converted to its own, ABB proprietary library format. Functional safety design tool also supports using the libraries, which are in the universal data format specified by VDMA (Verband Deutscher Maschinen- und Anlagenbau - German Engineering Federation) in *VDMA 66413*. These libraries can be imported to the tool. Libraries can also be exported from the tool in the ABB format in order to deliver the libraries to other users.

The data in the libraries is hierarchically organized. From top down, the hierarchy is:

- **Library** contains information about the library itself.
- **Manufacturer** describes the company, which offers the products. ABB proprietary library can contain several manufacturers' devices in one library. The universal format libraries contain data only for one manufacturer's products.
- **Category** defines the devices based on their logical function in a safety function (e.g. sensor, logic or output).

  **Note:** this category is not to be confused with the category of a subsystem used with standard *ISO 13849-1*.
- **Group** defines the devices based on their actual real world functionality (e.g. pressure mat, light curtain).
- **Device** includes the information about the physical device.

- **Use case** describes a particular usage of a device. The safety values of a device may vary depending on how the device is being used, thus the safety values are given under use cases.
- **The subsystem/element properties** contain the actual safety data, which defines the use case in the terms of functional safety.

## Library management main user interface

The library management has a main user interface view, from which all the functions are launched. This view contains some components common to many functions.

| Component | Description |
|---|---|
|   | New. Creates a new item for the selected hierarchy level. |
|   | New version. Creates a new version of the selected item. |
|  | Edit. Opens the selected item for editing. |
|  | Delete. Deletes the selected item. |
|  | Add new element. Adds a new element for the selected device. This button is only for the devices and is enabled only if the selected device is of Designed with elements type. |

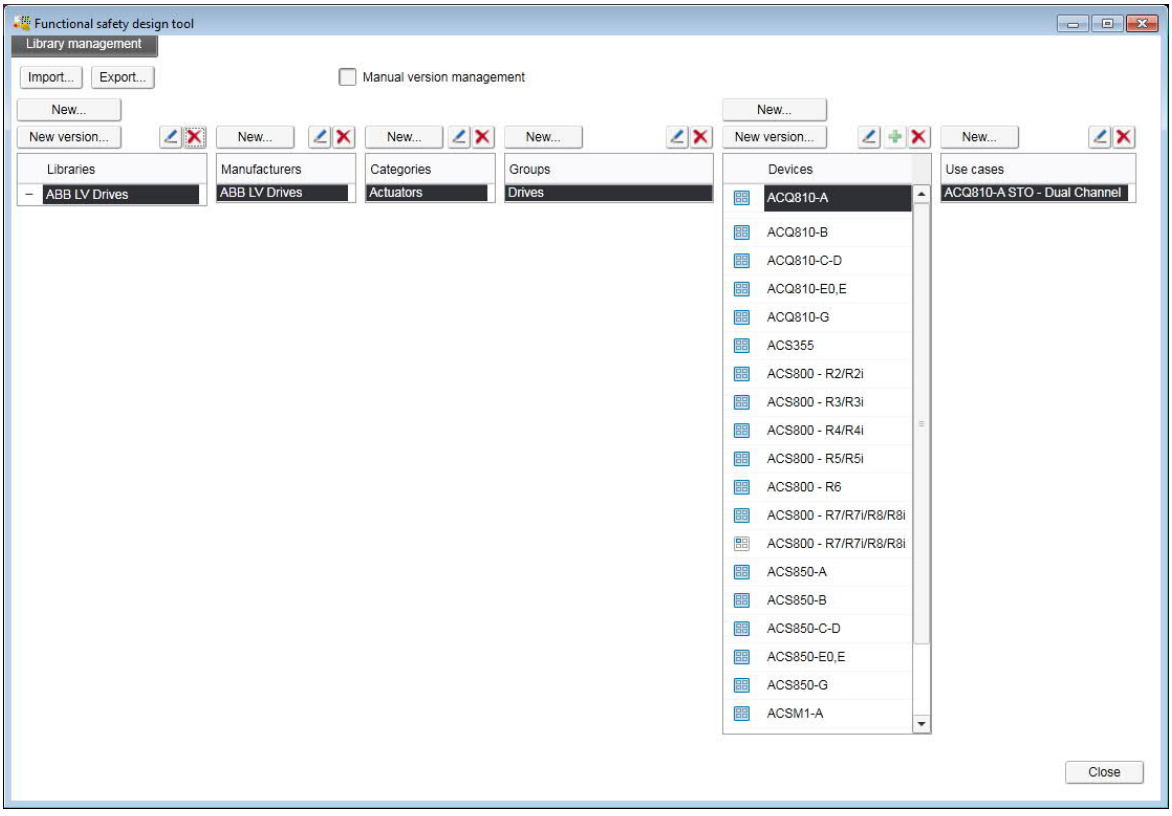



*Figure 49. The library management main view*

# Library data

## Library

A new library is created by clicking **New** above the **Libraries** list. This opens the Library properties dialog for entering the library data.

- **Library name** is mandatory data. Library name must be unique among the libraries, which are currently available for use in the tool – that is: the libraries in the Libraries list (which either have been imported to the tool or created in the tool).
- **Version** of the library can either be edited by the user or it is automatically set by the tool. See chapter *Library version handling* for details.
- **Language** selects the language of the library. When creating a new library English is shown by default but it can be changed. If a library contains texts for more than one language, the shown language can be changed here.
- **Author(s)** of the library can be given.
- **Approver(s)** of the library can be given.
- **Locked** checkbox locks the library. See chapter *Locking the libraries* for details.
- **URL** once you have filled in the URL, clicking on the URL field will open it in the browser. Click the **Edit URL** button if you need to edit the URL.
- **Description** can be used to give free form information about the library.

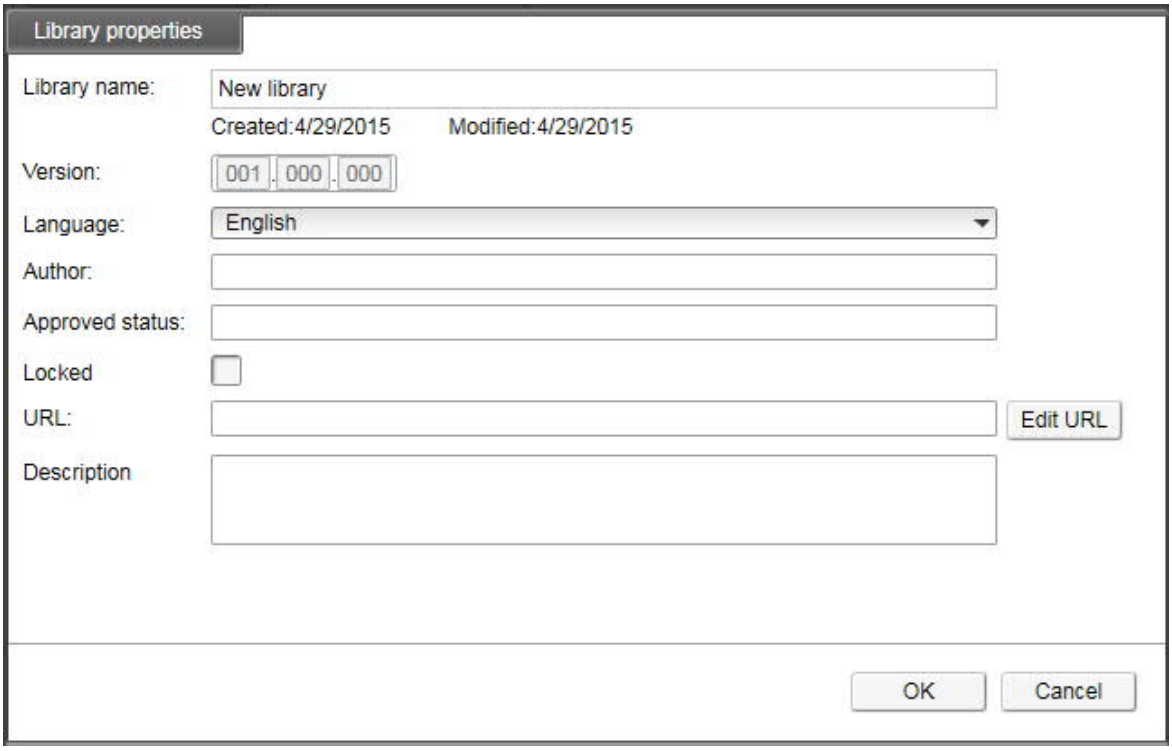



*Figure 50. The library properties*

## Manufacturer

To create a new manufacturer to a library, select the library to which the manufacturer shall be created and click **New** above the **Manufacturers** list. This opens the Manufacturer properties dialog, where you can define the properties of the manufacturer.

- **Manufacturer name** is mandatory data and must be unique within the library.
- **Description** can be used to give free form information about the manufacturer.
- **URL** once you have filled in the URL, clicking on the URL field will open it in the browser. Click the **Edit URL** button if you need to edit the URL.
- **Version** of the manufacturer can either be edited by the user or it is automatically set by the tool. See chapter *Library version handling* for details.

You can also set an icon for the manufacturer. In order to do this, click **Change icon** and select an image file to be used as the icon. The icon is shown in the size of 48 x 48 pixels. If the icon is larger than that, it will be resized to fit.

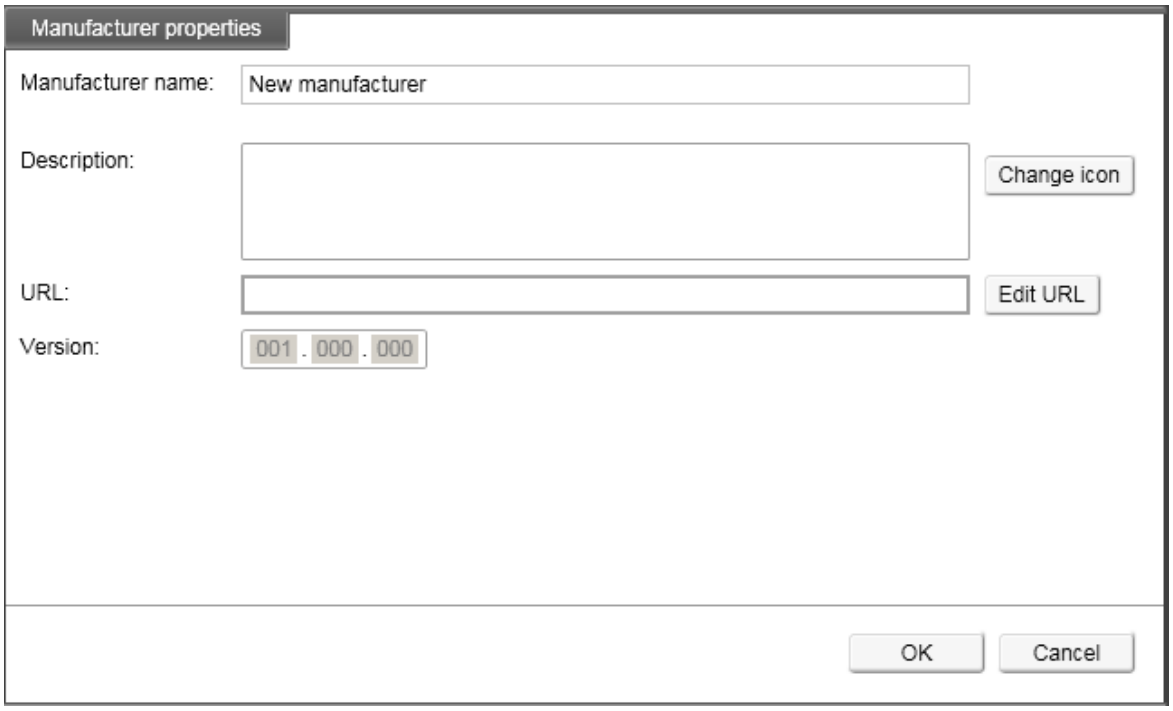



*Figure 51. The manufacturer properties*

## Category

To create a new category to a library, select the library and manufacturer under which the category shall be created and click **New** above the **Categories** list. This opens the Category properties dialog, where you can define the properties of the category.

- **Manufacturer** is by default the one that was selected in the library management main view but it can be changed here.
- **Category name** is mandatory data and must be unique within the manufacturer.


*Figure 52. The category properties*

## Group

To create a new group to a library, select the library, manufacturer and category under which the group shall be created and click **New** above the **Groups** list. This opens the Group properties dialog, where you can define the properties of the group.

- **Manufacturer** is by default the one that was selected in the library management main view but it can be changed here.
- **Category** is by default the one that was selected in the library management main view but it can be changed here.
- **Group name** is mandatory data and must be unique within the category.

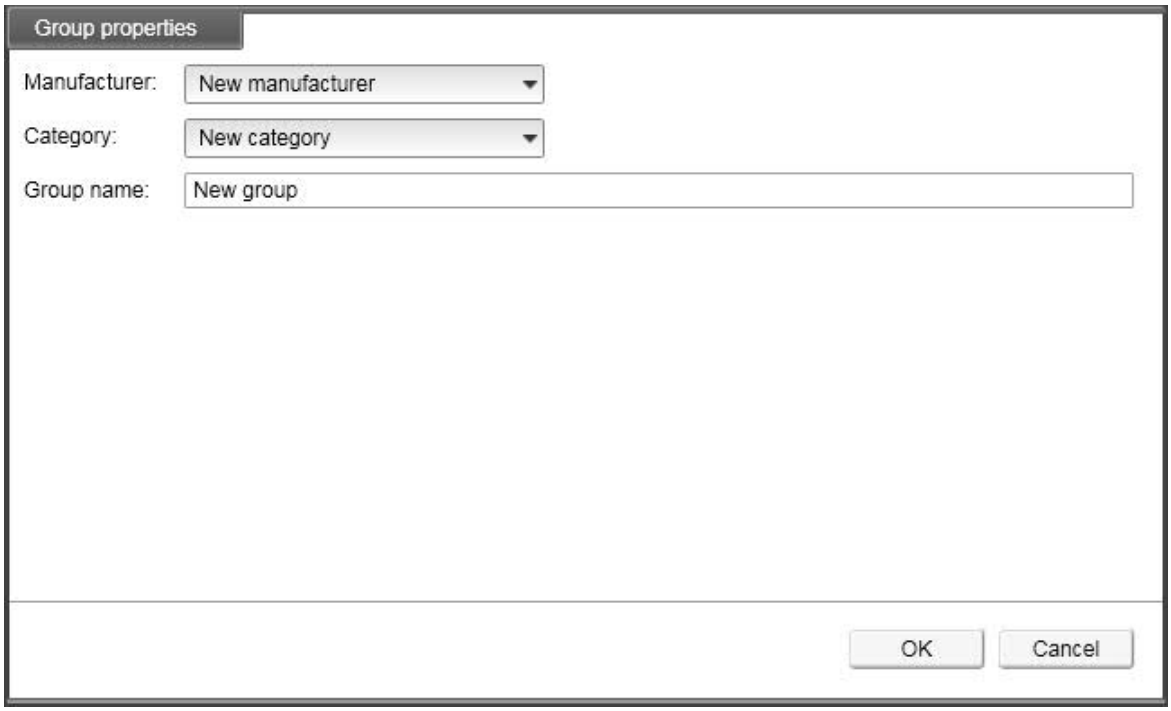



*Figure 53. The group properties*

## Device

To create a new device to a library, select the library, manufacturer, category and group under which the device shall be created and click **New** above the **Devices** list. This opens the Device properties dialog, where you can define the properties of the device.

- **Library** is by default the one that was selected in the library management main view but it can be changed here.
- **Manufacturer** is by default the one that was selected in the library management main view but it can be changed here.
- **Category** is by default the one that was selected in the library management main view but it can be changed here.
- **Group** is by default the one that was selected in the library management main view but it can be changed here.
- **Name** of the device is mandatory data.
- **Identifier** is mandatory data and must be unique within the manufacturer. After entering the name for the device, the tool inserts a default identifier, which is created based on the name. The user can change the identifier if needed.
- **Version** is the safety data version of the device in the library. It can either be edited by the user or it is automatically set by the tool. See chapter *Library version handling* for details.
- **Part number**
- **Revision** is the hardware or software version of the actual real world device.
- **Description** can be used to give free form information about the device.
- **Status** can be used to inform the user that this device version is no longer available.
- **Attachments** can be used to include the device documentation in the library
- **URL**

You can also set an icon for the device. In order to do this, click **Change icon** and select an image file to be used as the icon. The icon is shown in the size of 48 x 48 pixels. If the icon is larger than that, it will be resized to fit.

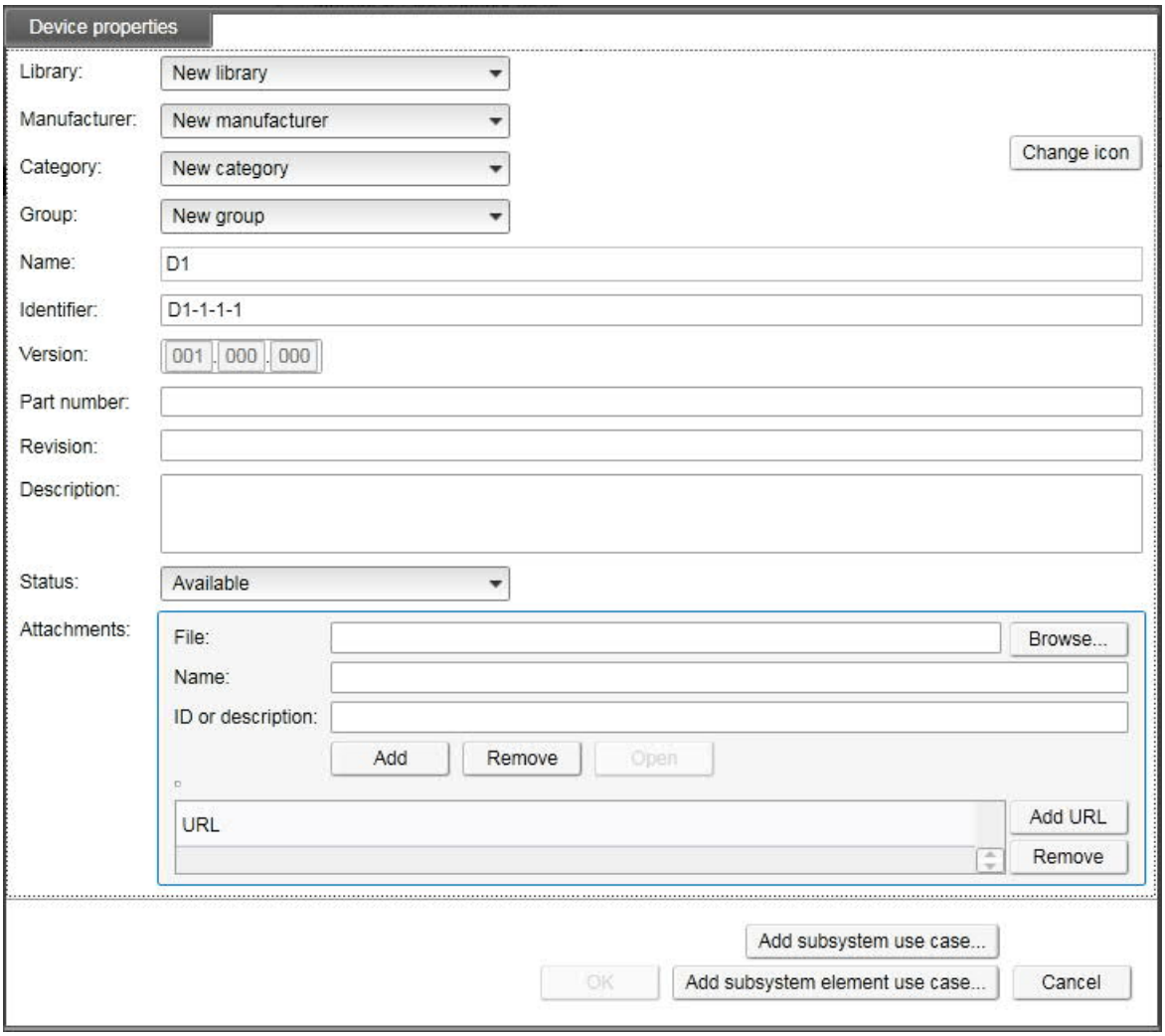



*Figure 54. The device properties*

When all mandatory device data has been defined, the **Add subsystem use case** and **Add subsystem element use case** buttons are enabled. Press the appropriate button to proceed to use case definition.

> **Note!** One device can contain either subsystem or element use cases, not both.

## Use case

A use case contains the safety values for one type of usage and is an entity consisting of three basically individual aspects:

1. **Use case properties** define the basic information about the use case itself: name, version, etc.

2. **ISO safety data** defines the safety values to be used when calculating the system's safety level by the *ISO 13849-1* standard.
3. **IEC safety data** defines the safety values to be used when calculating the system's safety level by the *IEC 62061* standard.

## Use case properties

To create a new use case for a device, select the device for which the use case is to be created click **New** above the **Use cases** list. This opens the Use case properties dialog, where you can define the properties of the use case.

- **Use case name** is mandatory data and must be unique within device.
- **Description** can be used to give free form information about the use case.
- **Input/Logic/Output Functions** can be used to define the use case's function. The function helps in the safety function design when using the templates.
- **Internal category** is information provided by the universal library. When importing a universal library, this value is set. After that the user is able to freely edit the value.
- **Version** is the version of the use case.

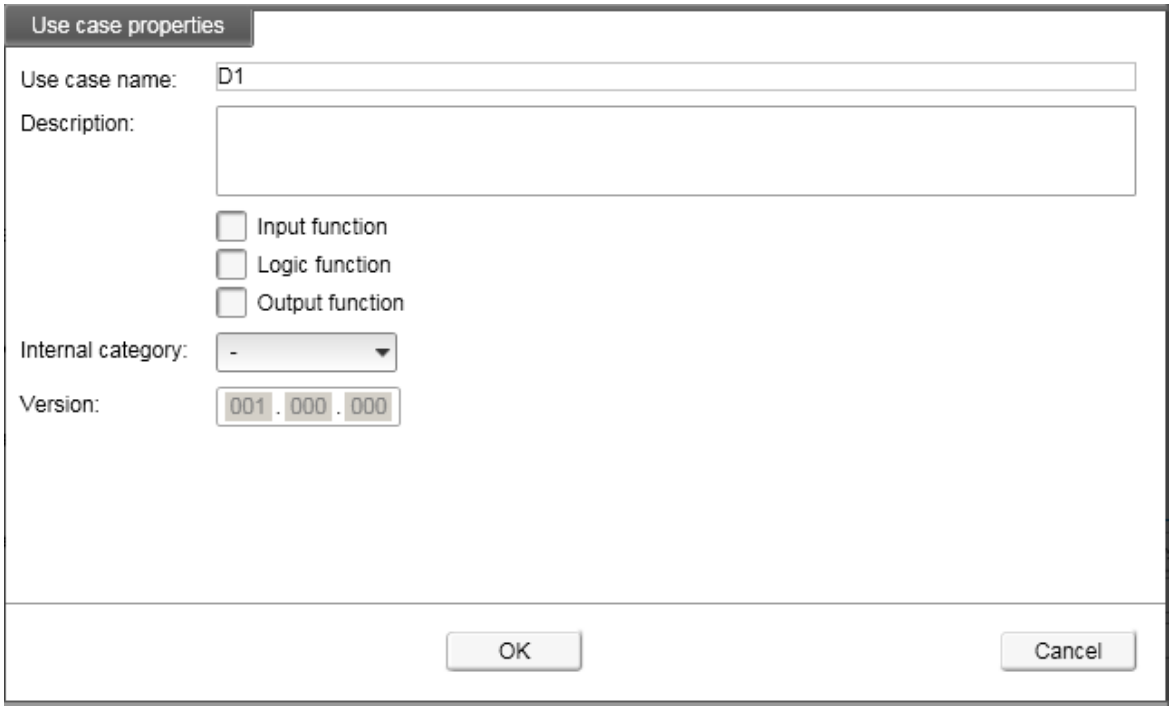



*Figure 55. The use case properties*

## The ISO and IEC safety values

The configuration windows for defining subsystems and subsystem elements are similar to those in the Step 3 in the project definition as far as the *ISO 13849-1* and *IEC 62061* safety values are concerned. For the details on these safety values, refer to the chapters *Configuration of subsystems and elements in ISO 13849-1 projects* and *Configuration of subsystems and elements in IEC 62061 projects*.

The configuration windows contain the following parts special for library management:

- **Version** shows the device version. This is valid also for library components when adding them to a project.
- **Use case** selection box is for selecting the use case, which is to be edited. When adding a library component to a project, the use case can be selected here.
- **Edit use case** button is for opening the use case property window for editing the selected use case.
- **New use case** button is for adding a new use case.
- **Delete use case** button is for deleting the selected use case.
- **Standard** selection box is for selecting the standard to be edited. For a library component, both *ISO 13849-1* data and *IEC 62061* data can be added. When adding a library component to a project, the project's standard is shown here.

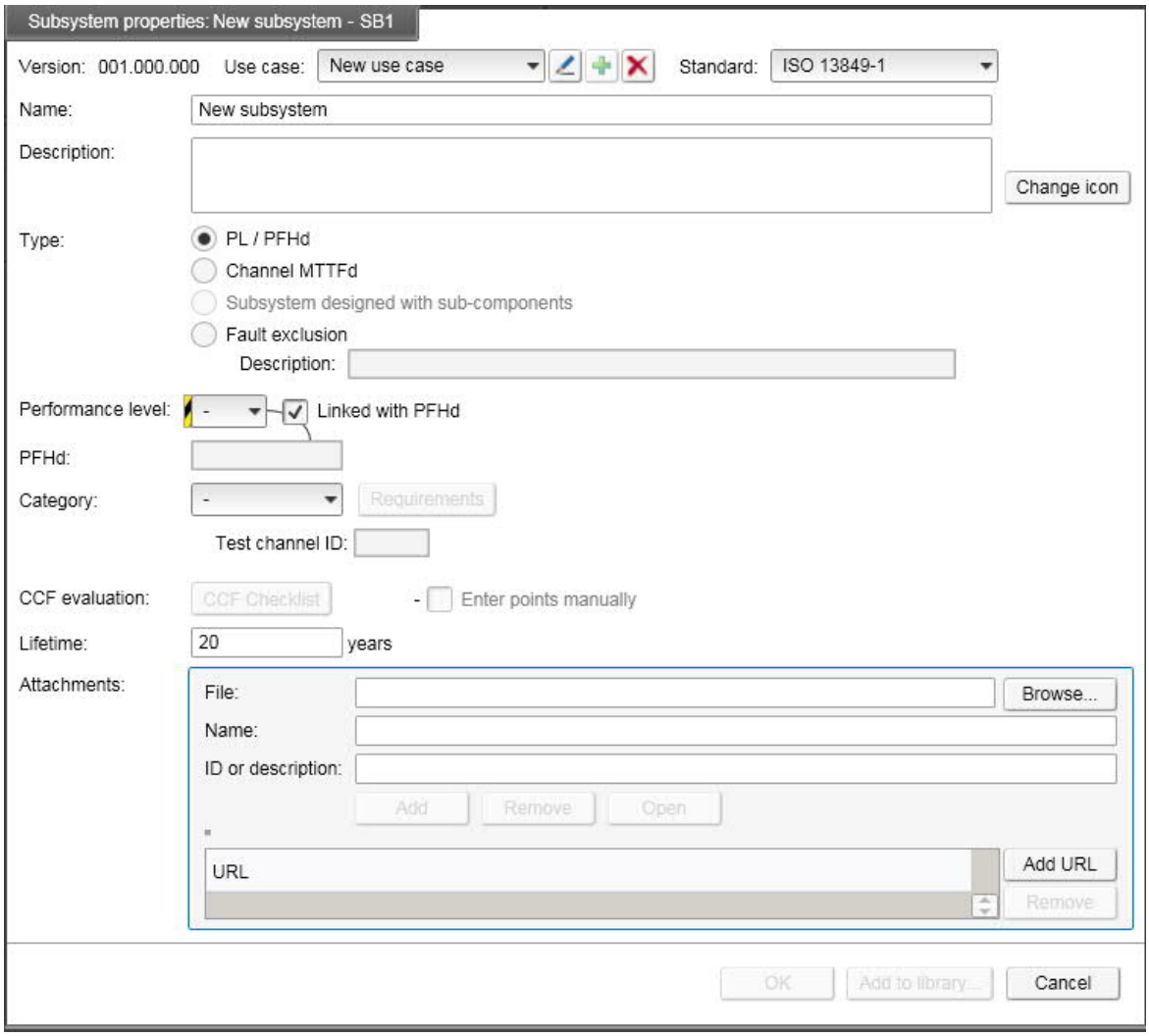



*Figure 56. A subsystem configuration window in library management*

### The dependencies, rules and restrictions on use case definition

Each use case may be defined quite independently. There are, however, the following dependencies and rules:

- One device may contain only either subsystem or subsystem element use cases.

- Subsystem use cases of type *Subsystem designed with elements* cannot be mixed with other types and the selection cannot be changed afterwards. If the user selects this type for the first use case, the other types are disabled from the new use cases and vice versa: if some other type is selected, the *Designed with elements* type cannot be selected for other use cases.
- Subsystem use cases of type *Subsystem designed with elements* must all share the same channel structure. That is: all use cases must have the same number of channels and the channels shall contain same subsystem elements.

  **Note:** all additions and deletions of elements affect all the use cases of the device.
- Subsystems may have values for both or either one of the standards.
- Elements have always values for both standards: the tool calculates the values for the other standard based on the values defined on the other standard.

# Library management workflows

There are several ways to work with the libraries to add data, information and objects to different levels of the hierarchy and edit the data. These are described in this chapter.

## Creating a new library

This chapter describes the steps needed to create a simple library with one device.

1. Create a new library by clicking **New** above the **Libraries** list and add at least all mandatory library data.
2. Select the created library and create a new manufacturer by clicking **New** above the **Manufacturers** list and add at least all mandatory library data.
3. Select the created manufacturer and create a new category by clicking **New** above the **Categories** list and add at least all mandatory category data.
4. Select the created category and create a new group by clicking **New** above the **Groups** list and add at least all mandatory group data.
5. Select the created group and create a new device by clicking **New** above the **Devices** list and add at least all mandatory device data. Click either the **Add subsystem use case** or the **Add element use case** button to proceed to use case definition.
6. In the opened subsystem/element properties window, press the **Create a new use case** button and fill in at least all mandatory use case data.
7. Fill in at least all mandatory subsystem/element data for one standard.

## Adding use cases

If you want to add a use case to a device there are two choices: select the desired device and either use the **New** button above the **Use cases** list or use the **Edit** button and then the **Create a new use** case button in the opened subsystem/element properties window.

To add a use case to an element in a subsystem designed with elements, select the desired element and press the **Edit** above the **Devices** list. Press the **Edit subsystem**

**element** button in the opened device properties window and then the **Create a new use** case button in the opened element properties window.

## Editing data

In order to change the data of any of the objects on any hierarchy level, select the object to be edited and use the **Edit** button over the appropriate list to open the appropriate property window.

To edit the use case properties the user must in addition use the **Edit the selected use case** button to open the use case properties window. The use case to be edited can be selected from the Use cases list in the library management main view or it can be selected in the subsystem/element properties window with the **Use case** selection box. One use case can be edited at a time. If the user has modified data of a use case and the use case is changed – or a new one created – the modifications are discarded. The tool gives a message about this and the user has the option to return and save the modifications.

To edit the elements of a subsystem designed with elements, select the desired element under the subsystem device and click the **Edit** button. The device properties window for the element is opened. If the device data is what was to be edited, perform the changes and press **OK**. In order to edit either the use cases of the element or the element properties, press the **Edit subsystem element** button. The element properties window is opened. Use the **Use case** selection box to select the use case and edit the element properties of the use cases or press the **Edit use case** button to open the use case properties window to edit the use case properties.

## Adding an element for a subsystem designed with elements

In order to add an element to a subsystem designed with element, select the desired subsystem and the desired channel of the subsystem and press the **Add new element** button above the **Devices** list.

## New versions

Most of the library objects exist only with one version at a time but libraries and devices can exist in several versions at the same time. Here it is described how to define the new versions.

### Creating a new version of a library

A new library version is created by selecting the desired library from the **Libraries** list and clicking **New version.** This opens the Library properties dialog, where you can edit the library data except the library name. For the new version of the library, a new library file will be created on the PC’s disk. The content from the previous library version is copied to the new file and the file of the old version remains. The user can also select to overwrite the old version. In this case the old library file will be replaced with the file of the new library version.

### Creating a new version of a Device

Create new Device version: If the user selects this option, the user can add a new version of the same device. The new device will be located in the same database (file). The device information from previous device version is copied but the use cases and application data are deleted and must be added in addition to the new device version. The user can also in this case select to overwrite old versions.

## Deleting objects

To delete an object from a library from the tool, use the **Delete** button over the appropriate list. The object, as well as all objects under it in the hierarchy, is permanently deleted from the library.

Deleting a library differs from deleting other objects. With libraries the functionality is different depending on the origins of the library. If you have imported the library, removing it from the tool does not delete the original library file(s), which still remain after the library has been removed from the tool. But if you have just created the library in the tool but have not exported it, then also all library files are deleted when removing the library from the tool.

# Library version handling

A library is uniquely identified with the Library name and version. By definition, two libraries with the same name and version are identical (identical content). To maintain this property of libraries two approaches can be applied:

1. Manual version handling
2. Automatic version handling. The user is not allowed to edit and set versions. The versions are automatically handled by the tool.

The two settings are available as options in the tool. If a library is created with automatic version handling, it is possible to adjust the versions if the tool is set to manual versioning mode.

The suggested version number format (which is followed by the tool in the automatic mode) is **#.M.C**, where

- # = Major version number. Change in this means a significant change, e.g. there is incompatibility, projects cannot be updated across the change or safety related data has changed for the worse. # is element in the set of Natural numbers.
- **M** = For supplements. If a new device is added (Device that exist in several version, or libraries that exist in several versions). M is an element in the set of Natural Numbers.
- **C** = Failure corrections or data edits. C is an element in the set of Natural numbers.

## Manual version handling

In this mode the library versioning is handled manually by tool user. The user can freely edit and use all versions in the data hierarchy for editable (non-locked) libraries. The responsibility to maintain consistency between libraries is left completely to the tool user. The tool, however, helps the user if, e.g. there exists a device with version 1.1.0 and the

user selects to create a new version, the tool suggests the new version 1.2.0. The tool also imposes some restrictions to ensure that general versioning rules are obeyed.

In this mode it is possible to create new library versions and new device versions. For other versions (e.g. manufacturer version, use case version) creation of a new version is not allowed. Editing these versions will simply overwrite the previous version.

The tool imposes the following restrictions for the versions:

1. A new device version must always have a unique combination of the two first versioning numbers # and M. A device may exist, e.g. with versions 1.1.0 and 1.2.0, or 1.1.1 and 1.2.1. Thus:

   If a device exists in version 1.1.0, it is not possible to create that device with version 1.1.1.

   If a device exists in version 1.1.0 and the user edits the device and manually increments the version to 1.1.1, the device version 1.1.0 will be overwritten and replaced with device version 1.1.1 (content of the device and all use cases remains).

2. A new library version must always have a unique combination of the two first versioning numbers # and M. A library may exist e.g. with versions 1.1.0 and 1.2.0, or 1.1.1 and 1.2.1. Thus:

   If a library exist in version 1.1.0, it is not possible to create that library with version 1.1.1.

   If a library exist in version 1.1.0 and the user edits the library data and manually increments the version to 1.1.1, the library 1.1.0 will be overwritten and replaced with library version 1.1.1.

Note: It is also not possible to first create a new version with the correct version number and then afterwards change it to a conflicting one.

### Automatic version handling

In this operational mode, the versions are handled automatically by the tool to ensure that the version handling is done consistently through the lifetime of the library. If data in the library is edited, the versions from the edited data hierarchy level on and upwards are automatically incremented. The lower levels will remain unmodified.

## Updating the libraries

Libraries are files on the PC hard disk. When new versions of the libraries become available, you can download or otherwise obtain the new library files to your PC and then use the **Import** functionality in the **Manage libraries** to get the library into use in the tool.

The libraries of ABB components can be downloaded from the tool's web site.

## Importing libraries

The import functionality can be used to get data into use by the tool. Click **Import,** browse for the correct library file and click OK. Library data can be imported from two different formats:

1. The ABB proprietary format
2. The universal data format (*VDMA 66413*)

To import a library, press the Import button in the library management main view. In the opened dialog select the correct file type and the desired library file.

If during import the tool encounters situations, where it has to do some adjustments to the imported data in order to be able to import it, it logs these occasions to a log file. If this happens, the tool prompts the user to check the log file after the import.

**Note:** Importing a VDMA library may take several minutes.

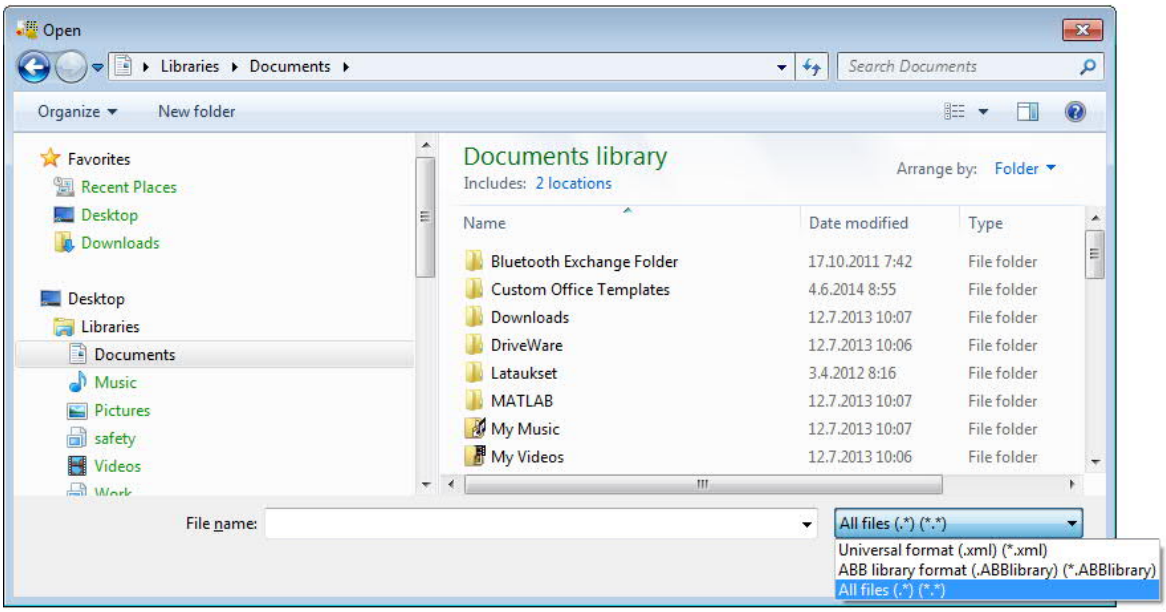



*Figure 57. The library import dialog*

## Conventions used when importing universal format libraries

When importing a universal library there are some modifications to the data representation:

- As the universal library does not explicitly contain library name and version, the Functional safety design tool uses the manufacturer data for respective library values.
- As the universal library does not contain device categories, the Functional safety design tool places the devices in *Input*, *Logic* and *Output* categories based on the Function. If there are devices, which have multiple functions selected, a *Mixed category* is created for those.
- Devices, which in universal data format libraries contain use cases from both, subsystem and element data types, will be split into two devices while imported. One device containing use cases with element data types and one device containing use cases with subsystem data types. Import Log file will give more specific information regarding the action taken.
- Universal library may contain texts in several languages. During the import the tool prompts the user to choose which language should be active after import.

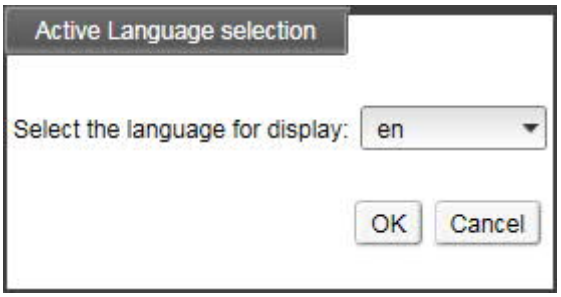



*Figure 58. The active language selection in library import*

## Exporting libraries

The export functionality is particularly useful if you want to distribute your libraries. To export a library, select the library from the **Libraries** and click **Export**. The data can be exported in the ABB proprietary format.

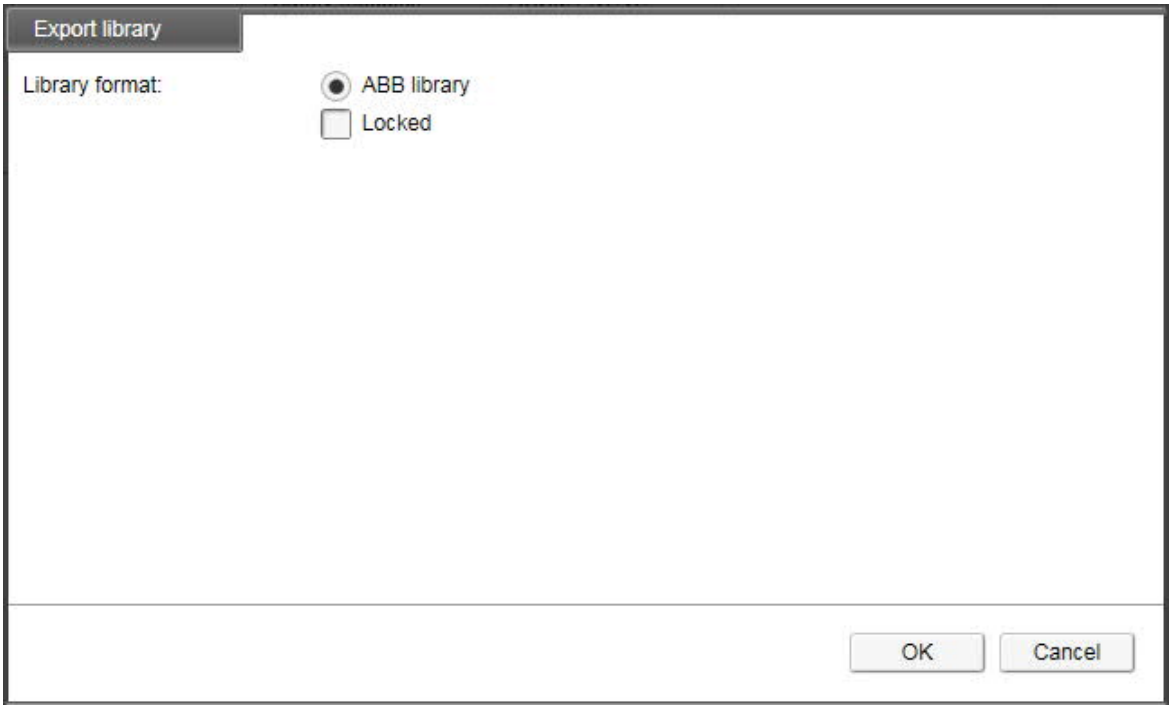



*Figure 59. The Export library dialog*

The **Locked** option makes the exported library a locked one. I.e. the exported library will be non-editable. The editable library remains also.

If during export the tool encounters situations, where it has to do some adjustments to the exported data in order to be able to export it, it logs these occasions to a log file. If this happens, the tool prompts the user to check the log file after the export.

# Locking the libraries

The tool offers the possibility to lock the ABB proprietary libraries so that they cannot be edited any more. This functionality is particularly important when verified libraries are created and distributed to tool customers. The following procedures to do this are applied:

1. When a library is created in the tool, it is saved as an editable library. From the tool GUI it is be possible to lock the library by using the **Locked** checkbox in the library properties. In this case the locked library is saved as a new file. The editable source file will also be still available. Unlocking the locked copy of the library is not possible.
2. When exporting an unlocked library it is possible to specify storage location and whether the exported library shall be editable or not.

# Updating projects with new library data

When a library component is used in a project, the safety values of the component are saved with the project so that when the project is opened again, the values are retrieved from the project file. This is done in order to keep the project as it was designed. Components' reliability/safety data can, however, change due to new knowledge about the components or improvements in the component. The component manufacturers may thus release new versions of their libraries so the update of existing projects with new and updated libraries is an important feature in the Functional safety design tool.

To launch this function open the **Help** menu and select **Update project**. This opens the screen that represents those components of the currently active project, for which the tool has found at least one newer version. The tool searches the project's components from the libraries, which are currently in use in the tool (either created in the tool or imported to the tool). If there are several versions of a library, the newest one is used. In order to successfully update the project, make sure that you have the latest libraries in the tool.

In the Update project screen the following parts can be found:

- **Update** checkboxes are for selecting the components, which are to be updated. Leave the checkbox unchecked, if you want to keep the original version. If you want to update all components, for which there is a newer version available, you can use the **Update all components** checkbox in the lower part of the screen to check all components.
- **Component** column defines where the component is used in the project. It contains the component's ID in the project and its name in the project.
- **Current version** shows which version of the component is currently used in the project.
- **Library details** tells from which library the component is from and gives the device and use case names.
- **New version(s)** shows all available newer versions of the component. You can select the version to which to update the component.

  **Note:** You can use the **Show all versions** option to see also the same or older versions of the device. With this option you can see all devices, which are found in libraries. This can be useful, e.g. when working with universal format libraries, as they don't have specific device version.
- **Use case(s)** shows the available use cases and the use case can be selected here.

**Note** All updated devices are updated with the library's currently active language. It is possible that a project contains devices from one library with different languages. If the project is updated in such a way, the previous languages are not retained.

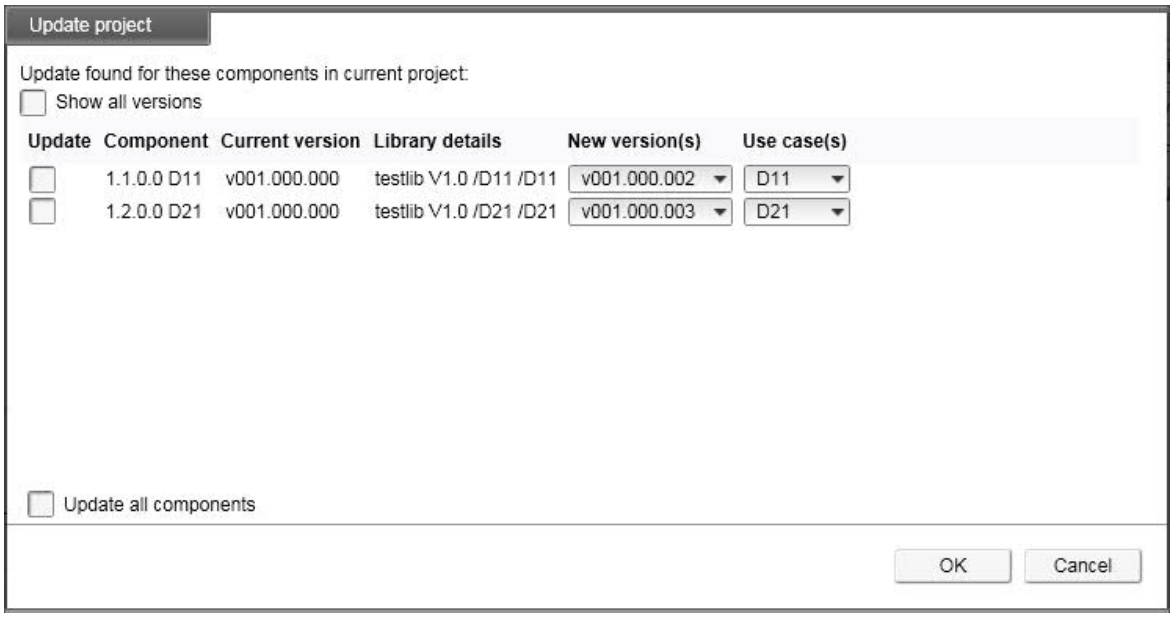



*Figure 60. Updating project with new library data*

# Further information

## Product and service inquiries

Address any inquiries about the product to your local ABB representative, quoting the type designation and serial number of the unit in question. A listing of ABB sales, support and service contacts can be found by navigating to www.abb.com/searchchannels.

## Product training

For information on ABB product training, navigate to www.abb.com/drives and select *Training courses.*

## Providing feedback on ABB Drives manuals

Your comments on our manuals are welcome. Go to www.abb.com/drives and select *Document Library – Manuals feedback form (LV AC drives).*

## Document library on the Internet

You can find manuals and other product documents in PDF format on the Internet. Go to www.abb.com/drives and select *Document Library*. You can browse the library or enter selection criteria, for example a document code, in the search field.

# Contact us

**www.abb.com/drives**
**www.abb.com/drivespartners**

3AXD10000102417 Rev J (EN) 2019-01-04