exSILentia® v4

exSILentia™

INTEGRATED SAFETY LIFECYCLE TOOL

User Guide

RELEASED 2019.07.22

Copyright © 2019 exida.com LLC. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without prior written permission of exida.com LLC.

exida.com LLC
80 North Main Street
Sellersville, PA, 18960
USA
+1 215 453 1720
http://support.exida.com

Contents

Chapter 1 Introduction **13**

Chapter 2 Installation **15**

2.1 Installation Process 15
2.2 Minimum System Requirements 17
2.3 Licensing 17
2.4 Disclaimer 19

Chapter 3 Getting Started **21**

3.1 Where Do I Begin? 21
3.1.1 Training 21
3.1.2 Website Resources 22
3.1.3 Introduction Videos 22
3.1.4 exSILentia Support 22
3.2 Launching the Program 23
3.2.1 Create a New Project 23
3.2.2 Open a Project 24
3.2.3 Save a Project 25
3.2.4 Auto-Save 25

Chapter 4 Tool Overview **27**

4.1 Dashboard 27
4.2 Process Hazard Analysis (PHA) 27
4.3 Layer of Protection Analysis (LOPA) 28
4.4 SIL Target Selection (SILect) 28
4.5 Safety Requirements Specification (SRS) 28
4.6 SIL Verification (SILver™) 29
4.7 Design SRS 29
4.8 SIS Logic 29
4.9 Proof Test Generator 30
4.10 Lifecycle Cost Estimator 31
4.11 Alarm Rationalization (SILAlarm™) 31
4.12 Life Event Recording (SILStat™) 31
4.13 exSILentia® Cyber 31

Chapter 5 Project Information **33**

5.1 Cyber Security Checklist 33

5.2 IEC 61511 Checklist 34

Chapter 6 Project Configuration **35**

6.1 Plant Types 35

6.2 Node Types 38

6.3 Safeguard Categories 44

6.4 Recommendation Categories 46

6.5 Reference Types 47

6.6 Team Roles 49

6.7 Custom Data 50

6.8 Project Abbreviations 55

6.9 Project Definitions 56

6.10 SILver Project Parameters 57

6.11 Lifecycle Cost Estimator Settings 57

6.12 Project Configuration Export and Import 58

Chapter 7 Project Libraries **61**

7.1 Causes Library 61

7.2 Safeguards Library 62

7.3 Recommendations Library 63

7.4 References Library 65

7.5 Hazard Scenarios Library 66

7.6 Enabling Conditions Library 67

7.7 Conditional Modifiers Library 68

7.8 Sensor Groups and Legs 69

7.9 Logic Solver Models 69

7.10 Logic Solvers 70

7.11 Devices 70

7.12 Device Models 70

7.13 Final Element Groups and Legs 70

7.14 Tags 71

7.15 Proven In Use Justification 71

Chapter 8 Project Risk Configuration **73**

8.1 Consequence Categories and Severity Levels 73
8.2 Severity Matrix 74
8.3 Likelihood Categories and Levels 74
8.4 Likelihood Matrix 75
8.5 Risk Matrix 76
8.6 SIL Selection 77
8.6.1 SIL Threshold 78
8.6.2 RRF Rounding Operand 78
8.7 Risk Configuration Reuse 79
Chapter 9 Report Generation 81
Chapter 10 Data Import 83
10.1 Library Import 83
Chapter 11 Data Export 85
11.1 Direct Export 85
11.2 Library Export 86
Chapter 12 Embedded Databases 87
12.1 LOPA Database 87
12.1.1 exida LOPA Database 88
12.1.2 Generic LOPA Database 88
12.1.3 User Defined Data LOPA Database 88
12.1.4 Managing LOPA Database Items 89
12.2 SERH Database 89
Chapter 13 Upgrading from exSILentia® v3 93
13.1 General Project Information 93
13.2 Process Hazard Analysis (PHA) 93
13.2.1 PHAx™ v2 94
13.2.2 exSILentia® v3 PHA Tab 94
13.3 SIF Identification 94
13.4 SIL Target Selection (SILect™) 94
13.4.1 Multiple Tolerable Risk Calibration 94
13.4.2 Risk Graph 94
13.4.3 Hazard Matrix 95
13.4.4 Frequency Based Targets/LOPA Tolerable Risk Calibration 95

13.4.5 Frequency Based Targets/LOPA Target SIL Selections 96
13.5 Safety Requirements Specification 96
13.5.1 SIF SRS 96
13.5.2 Process SRS (SRSC&E) 97
13.5.3 Design SRS 100
13.6 SIL Verification (SILver™) 100
13.7 Lifecycle Cost Estimator 102
Abbreviations 103
Terms and Definitions 105
Appendix A Dashboard 109
A.1 Project Information 109
A.2 Project Configuration 109
A.3 Risk Configuration 110
A.4 Members 110
A.5 Sessions 111
A.6 Action Items 112
A.7 Parking Lot Items 113
A.8 Library 114
A.9 Generate Report 115
A.10 Import Data 115
A.11 Export Data 115
A.12 Tool Tabs 115
A.13 Dashboard Widgets 115
Appendix B Menu Items and Short Cuts 119
B.1 Menu Toolbar 119
B.1.1 File 119
B.1.2 View 119
B.1.3 Export 120
B.1.4 Tools 120
B.1.5 Help 120
B.2 Shortcuts 121
Appendix C PHAx™ 123
C.1 Introduction 123

C.2 Hierarchy 123
C.2.1 Units 123
C.2.2 Nodes 124
C.2.3 Deviations 125
C.3 HAZOP Worksheet 126
C.3.1 Cause 127
C.3.2 Consequence 128
C.3.3 Safeguards 129
C.3.4 Safeguard Labels 130
C.3.5 Likelihood with Safeguards 131
C.3.6 Risk with Safeguards 131
C.3.7 Recommendations 131
C.3.8 LOPA 132
C.3.9 Comments 132
C.4 Navigation Tree 133
C.4.1 Tree Hierarchy / Navigation 133
C.4.2 Drag & Drop 134
C.4.3 Right Click Context Menu 135
C.5 User Interface / Usability 135
C.5.1 HAZOP Worksheet Column Widths 135
C.5.2 HAZOP Worksheet Column Visibility 136
C.5.3 Continuous Editing 136
C.5.4 Worksheet Search, Back, Forward and Bookmarks 137
C.6 PHAx™ Reports 137
C.6.1 Sections 138
C.6.2 Appendices 140
C.6.3 Columns 141
C.7 PHAx Data Import 142
C.7.1 Import Template 142
C.7.2 PHA Import 144
C.8 PHAx™ Data Export 146
Appendix D LOPAx™ 147
D.1 Introduction 147
D.2 LOPA Worksheet 148

D.2.1 Creating Hazard Scenarios 148
D.2.2 Specifying Target Frequencies 149
D.2.3 Initiating Events (IE) 150
D.2.4 Enabling Condition (EC) 152
D.2.5 Independent Protection Layers (IPL) 153
D.2.6 Conditional Modifiers (CM) 156
D.2.7 Calculating Required Risk Reduction Factors (RRF) 157
D.2.8 Comments 159
D.3 User Interface / Usability 159
D.3.1 LOPA Worksheet Column Widths 159
D.3.2 LOPA Worksheet Header Row Height 159
D.3.3 Severity Category Visibility 159
D.4 Hazard Scenario Data Transfer from PHAx™ 161
D.5 LOPAx™ Reports 162
Appendix E SILect™ 165
E.1 Introduction 165
E.2 SILect Worksheet 165
E.2.1 Creating Hazard Scenarios 166
E.2.2 Instrumented Protection Function (IPF) 167
E.2.3 Calculating the Safety Integrity Level (SIL) Target 168
E.2.4 Risk Graph 168
E.2.5 Risk Matrix 168
E.3 SILect Data Transfer 169
E.4 SILect Reports 169
Appendix F Safety Requirements Specification 171
F.1 Introduction 171
F.2 SRS Worksheet 172
F.2.1 Creating Safety Instrumented Functions 172
F.2.2 General SIS Requirements 173
F.2.3 General SIF Requirements 176
F.2.4 SIF Specific Requirements 177
F.3 Safeguard to SRS Data Transfer 179
F.4 SRS Reports 179
Appendix G SILver™ 181

G.1 Introduction 181
G.2 SILver Worksheet 184
G.2.1 Creating Safety Instrumented Functions 184
G.3 SILver Worksheet - SIF Level 185
G.3.1 General SIF Information 185
G.3.2 Architectural Constraints 186
G.3.3 Systematic Capability 187
G.3.4 Mission Time 187
G.3.5 Startup Time 187
G.3.6 SIF Demand Mode 188
G.3.7 I/O Channels on Separate Modules 188
G.3.8 Site Safety Index 188
G.4 SILver Worksheet - Sensor Part 189
G.5 SILver Worksheet - Sensor Group 191
G.5.1 Group Options 191
G.5.2 Proof Testing 192
G.5.3 Application Level Diagnostic Test 193
G.5.4 Legs 193
G.5.5 Leg Options 193
G.5.6 Devices 195
G.6 SILver Worksheet - Final Element Part 196
G.7 SILver Worksheet - Final Element Group 197
G.7.1 Group Options 197
G.7.2 Proof Testing 198
G.7.3 Partial Valve Stroke Test/Application Level Diagnostic Test 199
G.7.4 Legs 200
G.7.5 Leg Options 200
G.7.6 Devices 200
G.8 SILver Worksheet - Logic Solver Part 202
G.9 SILver Worksheet - Results 204
G.10 SILver Worksheet - Features 205
G.10.1 Beta Estimator 205
G.10.2 Proof Test Coverage Calculator 206
G.10.3 Proven In Use Justification 207
G.11 SILver Worksheet - Tags 209

G.12 SILver Data Transfer 210
G.13 SILver™ Reports 210
G.14 SILver™ Data Export 211

Appendix H Design SRS 213

H.1 Introduction 213
H.2 Design SRS Worksheet 213
H.2.1 Creating Safety Instrumented Functions 213
H.2.2 General SIF Requirements 214
H.2.3 SIF Specific Requirements 214
H.2.4 Sensor Legs, Auxiliary Input Legs, and Auxiliary Input Parameters Legs 215
H.2.5 Final Element Legs, Auxiliary Output Legs, and Auxiliary Output Parameters 215
H.3 Design SRS Data Transfer 215
H.4 Design SRS Reports 215

Appendix I Proof Test Generator 217

I.1 Introduction 217
I.2 Proof Test Generator Worksheet 217
I.2.1 Proof Test Suggestions 219
I.2.2 Proof Test Procedure 219
I.2.3 Starting PTG with an Existing Project File 222
I.3 Proof Test Generator Reports 223

Appendix J Lifecycle Cost Estimator 225

J.1 Introduction 225
J.2 Lifecycle Cost Estimator Worksheet 226
J.2.1 Estimator worksheet 226
J.2.2 Cost Benefit Analysis worksheet 228
J.3 Lifecycle Cost Estimator Reports 229

Appendix K exSILentia® Cyber 231

K.1 CyberPHAx™ 231
K.1.1 Introduction 231
K.1.2 Hierarchy 231
K.1.3 CyberPHA Worksheet 234
K.1.4 CyberPHAx Reports 237
K.2 CyberSL™ 237

K.2.1 Creating Cyber Event Scenarios 238
K.2.2 Specifying Target Likelihood 238
K.2.3 Cyber Threats (T) 238
K.2.4 Target Attractiveness 239
K.2.5 Countermeasures 240
K.2.6 Conditional Modifiers (CM) 241
K.2.7 Kill Chain Relevance 242
K.2.8 Calculating Remaining Cyber Risk 243
K.2.9 Comments 243

Disclaimer and Assumptions 245

Software License Agreement – exida exSILentia® 247

Open Source Disclosure 254

Index 257

Chapter 1 Introduction

exSILentia® v4 is a significant extension of the exSILentia® platform. exSILentia® v4 allows a suite of software tools, designed to support the Process Safety work process and Safety Instrumented System Functional Safety Lifecycle, to work seamlessly together. exSILentia® v4 reduces the effort needed to maintain information and improves overall consistency of Process Safety / Functional Safety tasks and their deliverables. exSILentia® v4 is available in several options:

PHA	Process Hazards Analysis tool
LOPA	Layer of Protection Analysis tool
PHA + LOPA	Combined Process Hazards Analysis and Layer of Protection Analysis tool
Alarm[1]	Alarm Rationalization tool
SILstat	Life Event Recording tool
Standard	Base functionality for all users requiring Functional Safety standard compliance
Analysis	Additional functionality for the Process Hazards Analysis phases of the Process Safety work process and Safety Lifecycle
Operation	Additional functionality for the Operation phases of the Safety Lifecycle
Ultimate	Complete exSILentia® functionality
Enterprise	Complete exSILentia® Safety Lifecycle tool functionality including Life Event Recording

In addition to these base options, the following functionality is available:

exSILentia® Cyber	Cyber Risk Assessments and Security Level verification to evaluate vulnerability to Cyber attacks.
DeltaV™ SIS Configurator[2]	Automatically create the logic configuration for a DeltaV™ SIS safety PLC based on the conceptual design documented in SILver™ and the Design SRS.

[1]Currently supplied as separate standalone application

[2]Requires an exSILentia® Ultimate license

exSILentia® VERSION 4

Safety Lifecycle Phase / Activity	exSILentia ®	Module Functionality	PHA	LOPA	PHA + LOPA ALARM	SILstat	STANDARD	ANALYSIS	OPERATION	ULTIMATE	ENTERPRISE
Functional Safety Management, Auditing and Assessment	IEC 61511 Compliance Documentation	Checklist for Documenting Compliance with IEC 61511 Standard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hazard & Risk Assessment (Process Hazard Analysis)	PHAx™	Record results of Process Hazard Analysis (PHA) / Hazard and Operability Study (HAZOP)	✓		✓			✓		✓	✓
Allocation of Safety Functions to Protection Layers (SIL Target Selection)	LOPAx™	Likelihood Analysis		✓	✓		✓	✓	✓	✓	✓
	SILect	Safety Integrity Level (SIL) Selection (Risk Graph, Risk Matrix, Frequency Based Targets)					✓	✓	✓	✓	✓
	SILAlarm™	Alarm Rationalization per ISA 18.2, EEMUA 191				✓				✓	✓
Safety Requirements Specification (SRS)	Process SRS	Process level Safety Requirements Specification					✓	✓	✓	✓	✓
Design and Engineering of SIS (incl SIL verification)	SILver™	Safety Integrity Level Verification, IEC 61508 compliant calculation engine					✓	✓	✓	✓	✓
	SERH Viewer	Viewer for exida Safety Equipment Reliability Handbook database (over 2000 devices)					✓	✓	✓	✓	✓
	Lifecycle Cost Estimator	Evaluate Lifecycle cost of proposed SIF designs							✓	✓	✓
	Design SRS	Detailed Design level Safety Requirements Specification								✓	✓
	SRSC&E	Creation of SIF and SIS Cause $ Effect matrices								✓	✓
Operation and Maintenance	Proof Test Generator	Creates proof test procedures for each component (organized by SIF)							✓	✓	✓
Modification	SILstat™	Recording of SIF life event data (proof test results, failures, demands) for comparison of actual to expected performance				✓					✓
Verification	Bulit-in	Peer review capability based on login allows review / approval of tool output	✓	✓	✓	✓	✓	✓	✓	✓	✓

Optional Add-on Functionality

Logic Solver Configuration	DeltaV™ SIS Configurator	Automatically generate application logic for DeltaV™ SIS								○	○
Cyber Risk Assessment	CyberPHAx™ & CyberSL™	Record Cyber Risk Assessment Results and evaluate protection levels	○	○	○		○	○	○	○	○

A high level overview of each of the software tools is provided in *Chapter 4 Tool Overview*. The main body of the user guide addresses items that are applicable to the base platform. Detailed guidance for each of the tools is provided in separate addenda. If this user guide does not answer your questions you can contact the exSILentia® Support Team via http://support.exida.com.

Chapter 2 Installation

The exSILentia® v4 installation package consists of

- exSILentia® v4 CD
- exSILentia® v4 USB key
- exSILentia® v4 User Guide

2.1 Installation Process

To install exSILentia® v4 on your computer place the exSILentia® v4 CD in your CD-ROM drive. exSILentia® v4 setup will take you through the installation process.

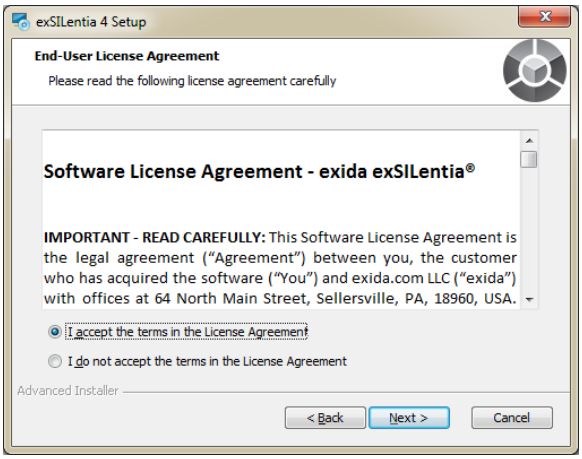
Note: Do not insert the exSILentia® v4 USB key into your computer's USB port until you have installed the exSILentia® v4 software.

If setup does not start automatically for any reason, follow these steps:

1. Insert the exSILentia® v4 CD into your CD-ROM drive.
2. Type Run in the Start Search box of the Start menu
3. Type d:\setup.exe, where d is the letter assigned to your CD-ROM drive.
4. Click OK.

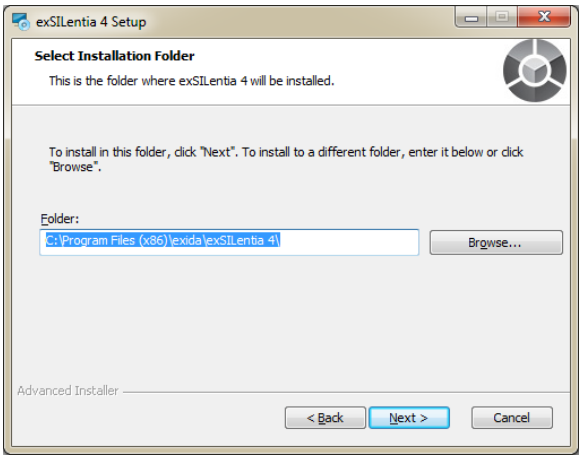
Setup starts and guides you through the installation of the exSILentia® v4 software.

To continue the installation process you will need to accept the terms and conditions of the exSILentia® v4 Software License Agreement. You can review the *license terms and conditions* by clicking on the link on the installer screen. A copy of the agreement is also included in this user guide. If you do not agree with the exSILentia® v4 Software License Agreement do not install the software on your system.

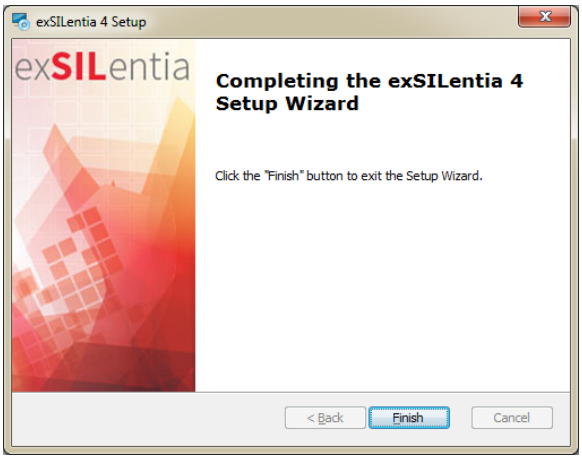


Clicking "Accept and Install" will continue the installation. The exSILentia® v4 installer will guide you through the remaining steps. The exSILentia® v4 installer will create a menu item in your programs folder and will also create an icon on your desktop.

During the installation process you will be able to indicate the location where you want the exSILentia® v4 software to be installed.



When the installation is complete, a dialog box will appear that indicates that the exSILentia® v4 Setup has been completed. Click "Finish" to conclude the installation.



In order to use exSILentia® v4 you will have to put the exSILentia® v4 USB key into a free USB port and double click the exSILentia® v4 icon or select exSILentia® v4 from your Programs menu.

2.2 Minimum System Requirements

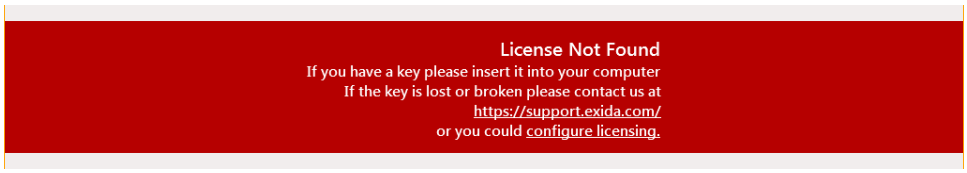
To use exSILentia® v4 your system should meet the following minimum requirements

- Microsoft® Windows 7 64-bit (all service packs installed), Windows 8 64-bit (all service packs installed), or Windows 10 64-bit (all service packs installed)
- Intel® Core™ i5 1.8 GHz or better processor
- 4 GB of RAM (8 GB recommended)
- 200 to 500 MB of free hard disk space (1 GB recommended)
- CD-ROM drive (for installation disk)
- Free USB port (for license key)
- Minimum screen resolution 1366 x 768 (1920 x 1080 recommended)

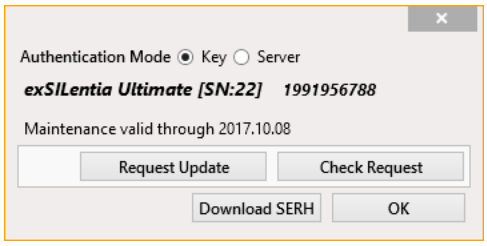
2.3 Licensing

exSILentia® v4 uses the SafeNet HASP software to enforce its licensing. Your Microsoft Windows operating system will automatically install the required SafeNet HASP Drivers when you plug the exSILentia® v4 USB key into you machine for the first time.

In order to use exSILentia® v4 you need the exSILentia® v4 USB key inserted in a USB port of your system. The exSILentia® v4 program will not work without this USB key; if the USB key cannot be detected an error message will appear. If this message appears when you do have the USB key inserted in a USB port, please try using a different USB port. If that doesn't resolve the issue, please contact exida for additional support.



In some cases you may need to configure your exSILentia® v4 USB key, if your time limited license key expired or you decide to upgrade your exSILentia® v4 license from, for example, the *PHA* option to the *PHA + LOPA* option. At the bottom of the error message above you can click on the configure licensing link. Alternatively, if your exSILentia® v4 USB key still allows launching of the tool, you can select the ***Tools - License Configuration*** menu option. Using the ***Authentication Mode*** on the License Configuration window you can select the applicable license option, either key or server. If you select key, exSILentia® will detect your current exSILentia® v4 license key and display the associated license key option. Next you can click the ***Request Update*** button, this will send your key information to exida. Upon receipt of your request, the exSILentia® v4 license processing team will validate your request and if valid generate an update file for your license key. Once you receive confirmation that this update file is available you can click the ***Check Request*** button to automatically update your exSILentia® v4 USB key.



The exSILentia® v4 licensing allows you to install the software on multiple machines, e.g. a desktop station in the office and a laptop used while traveling. However the software can only be used on the system where the USB key is inserted.

Note: exSILentia® 1.x, 2.x, 3.x USB license keys will not work with exSILentia® v4. If you have an older version of exSILentia® your old USB license key will still work for that version of the software. Multiple versions of the software can be installed on the same computer. Contact the exSILentia® team at http://support.exida.com or your local exida representative for upgrade options and pricing.

2.4 Disclaimer

The user of the exSILentia® v4 software is responsible for verification of all results obtained and their applicability to any particular situation. Calculations are performed per guidelines in applicable international standards and common methods described in subject matter literature. *exida.com LLC* accepts no responsibility for the correctness of the regulations, standards, or literature on which the tool is based. In particular, *exida.com LLC* accepts no liability for decisions based on the results of this software. The *exida.com LLC* guarantee is restricted to the correction of errors or deficiencies within reasonable period when such errors or deficiencies are brought to the attention of *exida.com LLC* in writing. *exida.com LLC* accepts no responsibility for user adjustments made to any reports automatically generated by the exSILentia® v4 software.

Chapter 3 Getting Started

3.1 Where Do I Begin?

Starting with exSILentia® v4 can be a bit overwhelming. exida has created several resources that can help you getting started.

3.1.1 Training

FSE 242: Process Hazard Analysis with exSILentia®

Process Hazard Analysis with exSILentia®, FSE 242, details how the exSILentia PHAx™ module can be used to conduct HAZOP methodology based Process Hazard Analysis. This course is targeted towards students that are experienced in process hazard analysis who want to learn how to leverage the advanced features of PHAx™. It will cover how to configure a project, define risk criteria, and use the advanced libraries to store valuable project specific information. The students will learn how to define units, nodes, and how to benefit from the PHAx™ smart deviations. It also addresses how hazard scenarios are to be defined for use in subsequent lifecycle phases.

FSE 243: Layer of Protection Analysis with exSILentia®

Layer of Protection Analysis with exSILentia®, FSE 243, explains how the exSILentia LOPAx™ module is used to conduct a Layer of Protection Analysis and how SIF requirements can be documented using the exSILentia SRS module. This course is targeted towards students that have a general understanding of layer of protection analysis and safety requirements specifications who want to learn how to leverage the advanced features of LOPAx™ and SRS. It will cover how to analyze hazard scenarios considering the frequency of initiating events and the probability of failure for each independent protection layer (IPL) as well as enabling conditions and conditional modifiers. This course will show how to calculate the required Risk Reduction Factor of an IPL and identify Safety Instrumented Functions (SIF). Users will learn how to record mandatory functional and integrity requirements for each SIF. It will teach users how to transfer data from PHAx™ to LOPAx™ as well as from LOPAx™ to SRS.

FSE 244: SIL verification with exSILentia®

SIL verification with exSILentia®, FSE 244, explains how the exSILentia SILver™ module is used to perform a SIL verification for Safety Instrumented Functions. Students will learn to leverage the tool to model different SIF architectures ranging from simple 1oo1 configuration to more complex examples. This course also covers review of the key parameters that determine the probability of failure of a SIF as well as minimum hardware fault tolerance and systematic capability aspects. It will show the impact of these parameters on the detailed design, implementation, and operation of the SIF. Furthermore, students will learn how to transfer data from the SILver™ module to the Design SRS module and subsequently complete the Design SRS requirements. Finally, the course covers the impact of proof testing and specification of proof test procedures using the Proof Test Generator module.

3.1.2 Website Resources

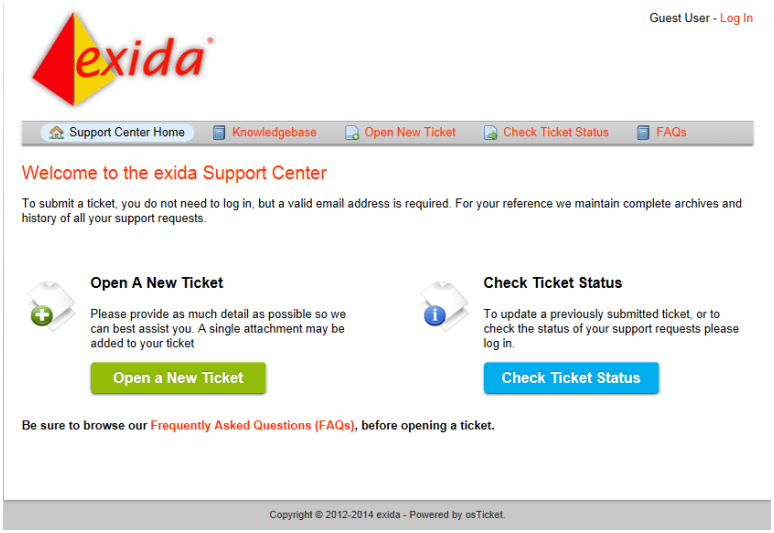
exida has launched the exSILentia® website www.exSILentia.com , where you can find general information about exSILentia®, downloads, and training information. The exida software development team has created a support website (http://support.exida.com) which includes a FAQ section. Frequently Asked Questions are addressed here. The exida website provides additional resources like white papers and an active blog addressing process & functional safety topics as well as exSILentia® specific topics. exida also conducts regular webinars, which can be attended free of charge. Make sure you are subscribed to the exida newsletter to keep up to date on the latest webinar offerings.

3.1.3 Introduction Videos

Several instructional videos were created to familiarize users with the basic functionality of exSILentia® v4. For a list of videos, see the exSILentia website at www.exSILentia.com.

3.1.4 exSILentia Support

This user guide is your first line of support when using the exSILentia® Safety Lifecycle tool. The user guide gives an overview of all options part of exSILentia® and using various examples it explains how to use the tool and its software tools. For additional support, use the support website through which you can submit your queries on the exida software products. In the exida Support Center (http://support.exida.com) you can open a new support ticket for any questions or issues you may have. You can also check on the status of any open tickets.



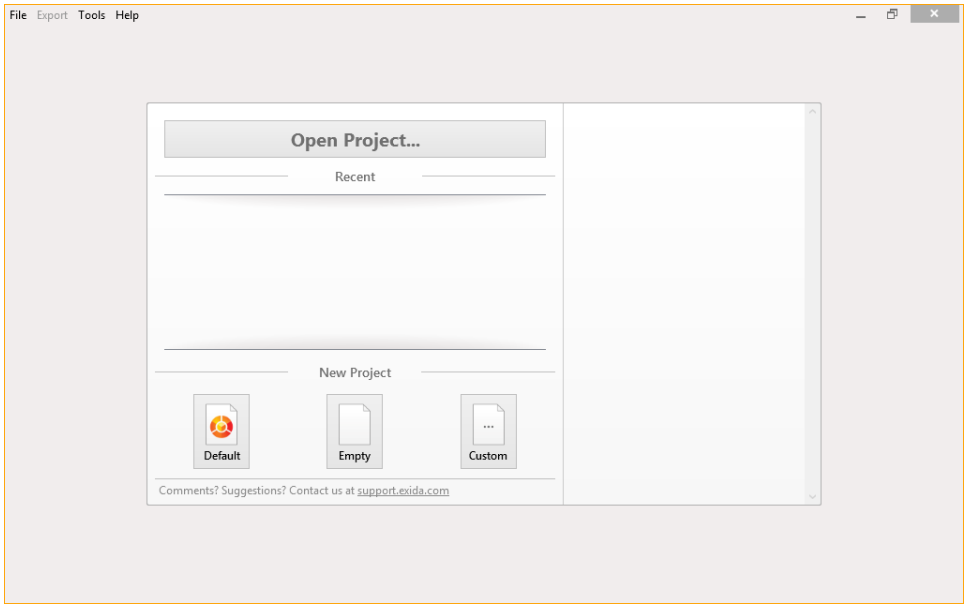
Note: We cannot answer any detailed safety lifecycle engineering questions as that would go beyond general tool support.

3.2 Launching the Program

To launch exSILentia® v4 simply double-click the exSILentia® v4 icon ( ) on your desktop or select the exSILentia® v4 program from your programs/exida folder in your Start menu.

When the exSILentia® v4 program is launched, it will automatically launch the ***Welcome Screen***. The welcome screen shows the latest release notes and news items. On the welcome screen you can:

- Open a previous project ***(Open)***.
- Create a new Default exida project ***(Default exida)***
- Create a new Empty project ***(Empty)***
- Create a new Custom project ***(Custom)***

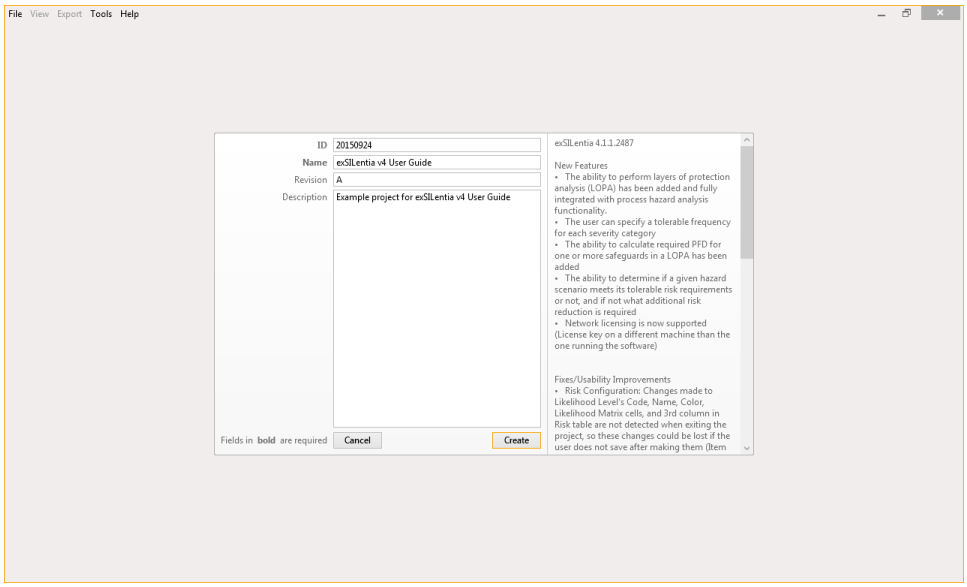


3.2.1 Create a New Project

You can define a new exSILentia® v4 project by selecting one of the three ***Create*** options.

- Default Project – Creates a new empty project with exida default project and risk configurations
- Empty Project – Creates a new empty project without any default configurations
- Custom Project – Creates a new empty project with default configurations based upon user default settings. This requires a previous file to be saved with user defaults. When this option is selected the user must navigate to a file containing the user default configurations which can be done using the navigation feature provided along the *Based on* below selection. The best way to create a user default configurations file is to initially start with an exida default configurations file which is subsequently edited and saved.

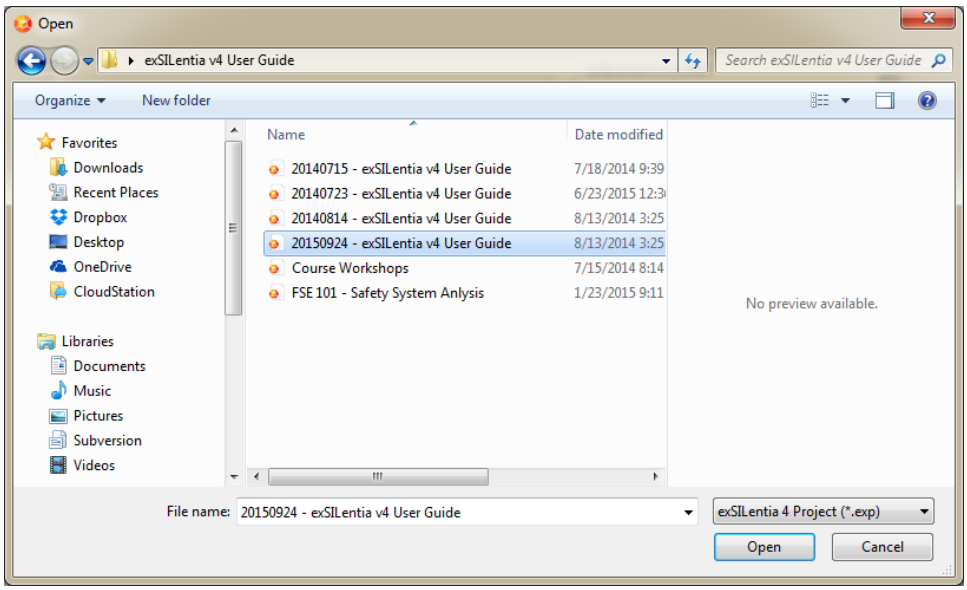
After selecting one of these three options, you can specify specific project information such as ***Project ID***, ***Project Name***, and ***Project Description***. With the basic project definition completed, exida recommends that you save the project at this time.



If you want to create a new exSILentia® v4 project once a project is already open, you can select the ***File - New*** menu option. This will create a Default Project, as described above, allowing you to immediately specify specific project information such as ***Project ID***, ***Project Name***, and ***Project Description***. If you would like to create an Empty or Custom new project you can select ***Cancel***, this will revert you to the ***Welcome Screen*** where you can choose these options.

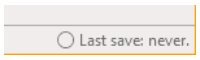
3.2.2 Open a Project

When you select ***Open*** a project, a file menu dialog box will appear allowing you to navigate to a previously saved project file. Select the file and click *Open* or double click on the filename.



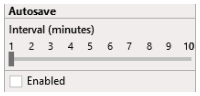
3.2.3 Save a Project

Saving a project is trivial in exSILentia®, simply select the *File* menu and click *Save* or *Save As*. In the lower right hand corner of the exSILentia® window you can see when the file was saved last.



3.2.4 Auto-Save

exSILentia® has an auto-save feature. You can enable the auto-save by clicking on the circle in front of the *Last save* information. You can enable the auto-save feature as well as specify the time interval for the auto-save ranging from every minute to every 10 minutes.



Note: When enabling auto-save, exSILentia® will overwrite your file every time the auto-save is executed. Undoing changes by simply not saving is not an option in this case.

In the unlikely event that exSILentia® abruptly stops working, or in the event that an error occurred at the time of saving, your exSILentia® project file will likely be corrupted. Since the file is encrypted, data may become unrecoverable for that file. In an event like this you can find a recovery file stored in a temporary file location (C:\Users\User Name\AppData\Local\Temp\exida\exSILentia 4\backup). The recovery files are only available for a limited period of time before being overwritten with new recovery files. exSILentia® Cloud users should contact the exida support team for assistance with file recovery.

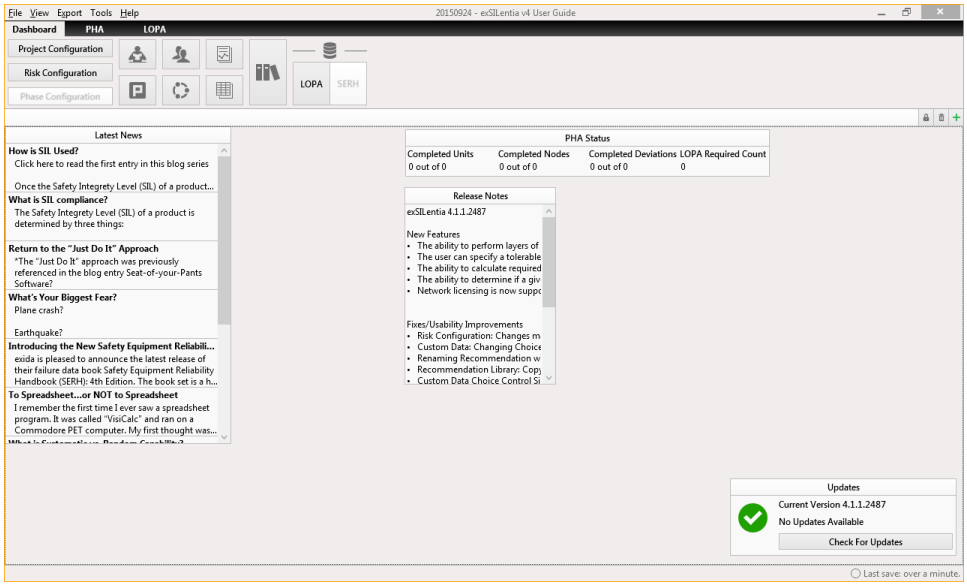
Chapter 4 Tool Overview

This chapter provides an overview of different components of the exSILentia® v4 software. The availability of some of the tools described in this chapter depends on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options).

4.1 Dashboard

The exSILentia® v4 Dashboard is the first window you will see when you open a project or after creating a new project. The dashboard is exSILentia® v4's central hub through which all lifecycle activities are initiated. It is shared by all exSILentia® v4 tools. In addition to providing the main navigation of the tool, the dashboard also provides you with the ability to evaluate the status of a project through summary information as well as graphical representation of results.

A detailed description of the various aspects of the dashboard as well as instructions on how to customize your dashboard are provided in *Appendix A Dashboard*.



4.2 Process Hazard Analysis (PHA)

The PHA tab navigates to the exSILentia® v4 process hazard analysis tool PHAx™. Availability of the PHA tab, and therefore the PHAx™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The PHAx™ tool allows process hazard analysis to be performed using the Hazard and Operability (HAZOP) methodology. For a detailed description of the PHAx™ tool refer to *Appendix C PHAx™*.

4.3 Layer of Protection Analysis (LOPA)

The LOPA tab navigates to the exSILentia® v4 layer of protection analysis tool LOPAx™. Availability of the LOPA tab, and therefore the LOPAx™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The LOPAx™ tool allows detailed layer of protection analysis to be performed for each hazard scenario, considering multiple initiating events, multiple enabling conditions, conditional modifiers, and Independent Protection Layers with different levels of effectiveness for different risk receptors as well as different initiating events. The hazard scenarios, causes, and safeguards identified during the process hazard analysis will automatically pre-populate the LOPA worksheet provided that you have used the PHAx™ tool for your process hazard analysis. For a detailed description of the LOPAx™ tool refer to *Appendix D LOPAx™*.

4.4 SIL Target Selection (SILect)

The SILect tab navigates to the exSILentia® v4 Safety Integrity Level (SIL) selection tool SILect™. Availability of the SILect tab, and therefore the SILect™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SILect™ tool supports determination of the target SIL for each Safety Instrumented Function identified in the LOPA worksheet that is required to provide risk reduction. The SILect™ tool will convert a target Risk Reduction Factor (RRF) into a target SIL. For a hazard scenario that has a remaining RRF, the SILect™ tool supports the identification of a SIF. The SILect™ tool worksheet is automatically pre-polulated with information obtained form the LOPAx™ tool. The SILect™ tool also supports SIL selection based on the Risk Graph and Risk Matrix methodologies. For a detailed description of the SILect™ tool refer to *Appendix E SILect™*.

4.5 Safety Requirements Specification (SRS)

The SRS tab navigates to the exSILentia® v4 safety requirements specification tool SRS. Availability of the SRS tab, and therefore the SRS tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SRS tool allows detailed specification of functional and integrity requirements for the Safety Instrumented System (SIS) as a whole, generic for all Safety Instrumented Functions (SIF), and specific for each SIF. The SRS constitutes the basis upon which the Safety Instrumented System and its Safety Instrumented Functions are designed. Several of the requirements will be automatically pre-polulated based on information specified in the PHA, LOPA, and SIL selection lifecycle phases. On the other hand, some requirements specified here, will automatically pre-populate fields in the SIL verification tool SILver™. For a detailed description of the SRS tool refer to *Appendix F Safety Requirements Specification*.

4.6 SIL Verification (SILver™)

The SILver tab navigates to the exSILentia® v4 Safety Integrity Level (SIL) verification tool SILver™. Availability of the SILver tab, and therefore the SILver™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SILver™ tool allows comprehensive modeling of each Safety Instrumented Function's (SIF) conceptual design within an exSILentia® v4 project. The objective during SIL verification is to determine if the conceptual design of the SIF meets the requirements specified in the Safety Requirements Specification (SRS). The SILver™ tool allows users to account for many real-life configuration options within a Safety Instrumented System (SIS), including but not limited to proof test coverage, transmitter fault direction, partial stroke testing, etc. Several of the conceptual design configuration selections will be made automatically based on information specified in the SRS phase (users can overwrite these selections if necessary). In turn some of the selections specified as part of the conceptual design verification will automatically pre-populate field in the Design SRS, Proof Test Generator, and Lifecycle Cost Estimator. The result of the SIL verification will be an Achieved Safety Integrity Level for the specific SIF's conceptual design. For a detailed description of the SILver™ tool refer to *Appendix G SILver™*.

4.7 Design SRS

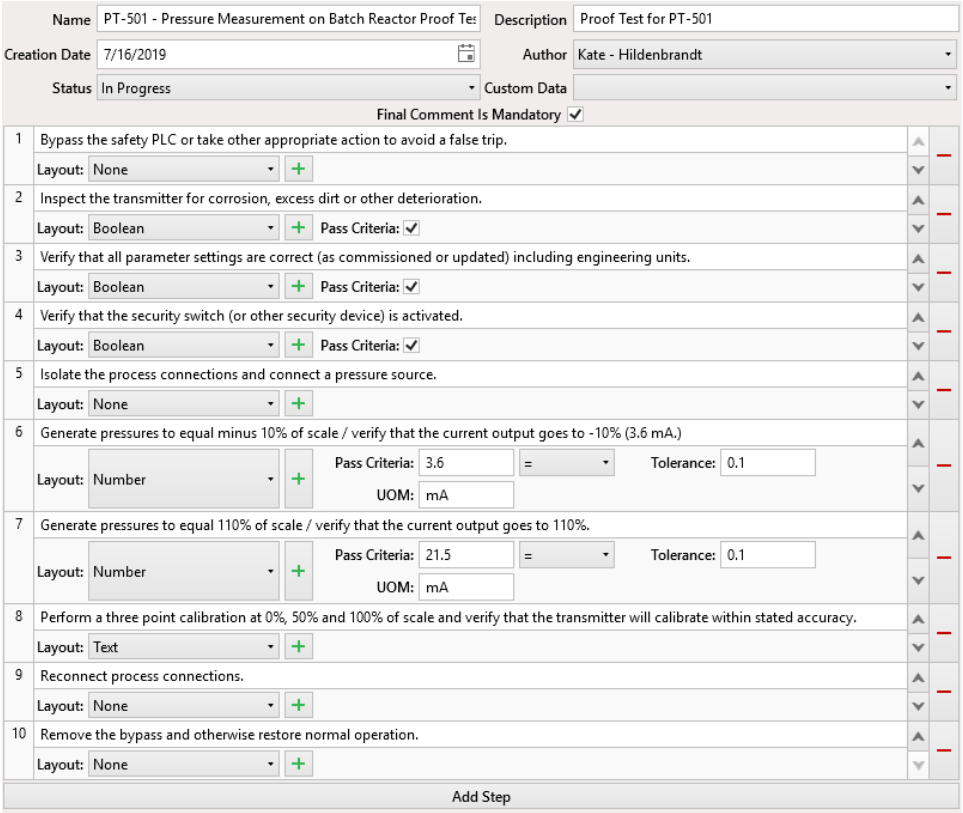
The Design SRS (DSRS) tab navigates to the exSILentia® v4 detailed design Safety Requirements Specification tool Design SRS. Availability of the Design SRS tab, and therefore the Design SRS tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The Design SRS tool allows detailed design specification of functional requirements for each Safety Instrumented Function (SIF) identified in the exSILentia® project. The detailed design requirements are a result of the conceptual design evaluation performed using the SILver™ tool. Most of the detailed design requirements will be automatically pre-polulated based on information specified in the SIL verification phase. For a detailed description of the Design SRS tool refer to *Appendix H Design SRS*.

4.8 SIS Logic

The SIS Logic tab navigates to the exSILentia® v4 Safety Instrumented System (SIS) application logic generation tool SIS Logic. Availability of the SIS Logic tab, and therefore the SIS Logic tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SIS Logic tool assists in automatically generating the application program/logic configuration for a specific target Safety PLC based on your SILver™ and Design SRS modeling. The SIS Logic tool substantially reduces the amount of time needed to generate the application program/logic configuration while eliminating the potential for interpretation and transcription errors. For a detailed description of the SIL Logic tool refer to the designated user guide for each of the target Safety PLC platforms.

4.9 Proof Test Generator

The Proof Test Generator provides proof test steps for all SIF devices selected for the SERH and allows the user to create application specific proof test procedures. Availability of the Proof Test Generator tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The Proof Test Generator tool allows detailed specification of proof tests to be performed for each equipment item specified during your Conceptual Design Engineering work. Default, product specific, proof tests with associated proof test coverage factors are provided from the exida Safety Equipment Reliability Handbook (SERH) database. The Proof Test Generator tool allows you to customize these proof test for use in your specific application. For a detailed description of the Proof Test Generator tool refer to *Appendix I Proof Test Generator*.



4.10 Lifecycle Cost Estimator

The Cost tab navigates to the exSILentia® v4 Lifecycle Cost Estimator tool. Availability of the Cost tab, and therefore the Lifecycle Cost Estimator tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The Lifecycle Cost Estimator tool supports the evaluation of a Safety Instrumented Function's conceptual design on the basis of expected overall lifecycle cost, accounting for aspects such proof test cost and proof test frequency. The Lifecycle Cost Estimator tool can assist in making an economical justification why a particular conceptual design may be better than an alternate conceptual design where both meet the same functional and integrity requirements. The Lifecycle Cost Estimator tool relies on completion of the conceptual design specification in the SIL verification phase. Most conceptual design performance variables will be automatically pre-polulated based on information specified in the SIL verification phase. For a detailed description of the Lifecycle Cost Estimator tool refer to *Appendix J Lifecycle Cost Estimator*.

4.11 Alarm Rationalization (SILAlarm™)

SILAlarm™ is currently available as a standalone tool. Please refer to the SILAlarm™ User Guide for guidance on using the SILAlarm™ tool.

4.12 Life Event Recording (SILStat™)

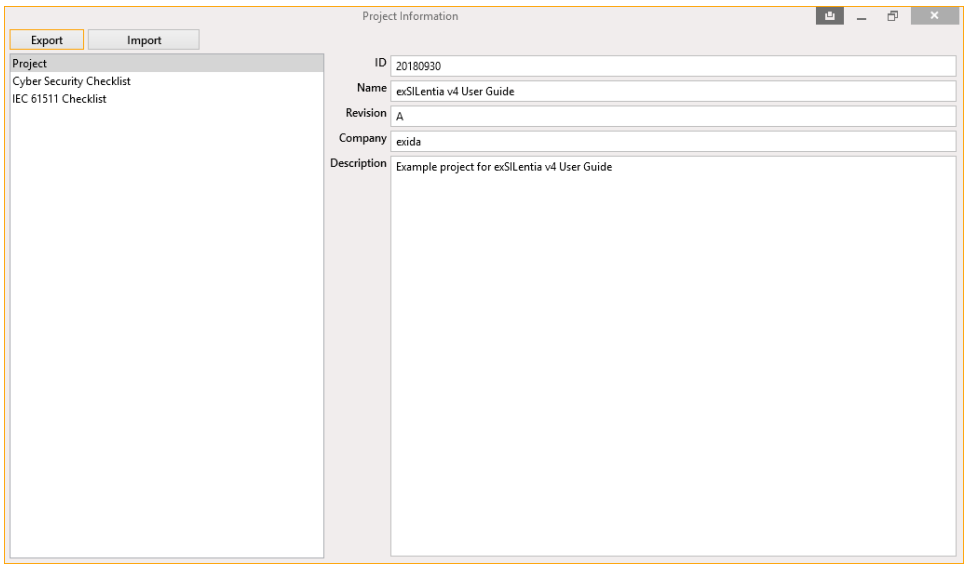
The exSILentia® SILStat™ module is tightly linked to exSILentia® v4 but is used as a standalone entity. Please refer to the SILStat™ User Guide for guidance on using the SILStat™ tool.

4.13 exSILentia® Cyber

The CyberPHA tab navigates to the exSILentia® v4 cyber process hazard analysis tool CyberPHAx™ whereas the CyberSL™ tab navigates to the exSILentia® v4 cyber security level tool CyberSL™. Availability of the CyberPHA and CyberSL tabs, and therefore the exSILentia® Cyber tools CyberPHAx™ and CyberSL™, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The CyberPHAx™ tool allows cyber risk assessment to be performed based on the process industry Hazard and Operability (HAZOP) methodology. The CyberSL™ tool allows for a security level evaluation to be performed on the various countermeasures identified for a particular threat. For a detailed description of the CyberPHAx™ and CyberSL™ tools refer to *Appendix K exSILentia® Cyber*.

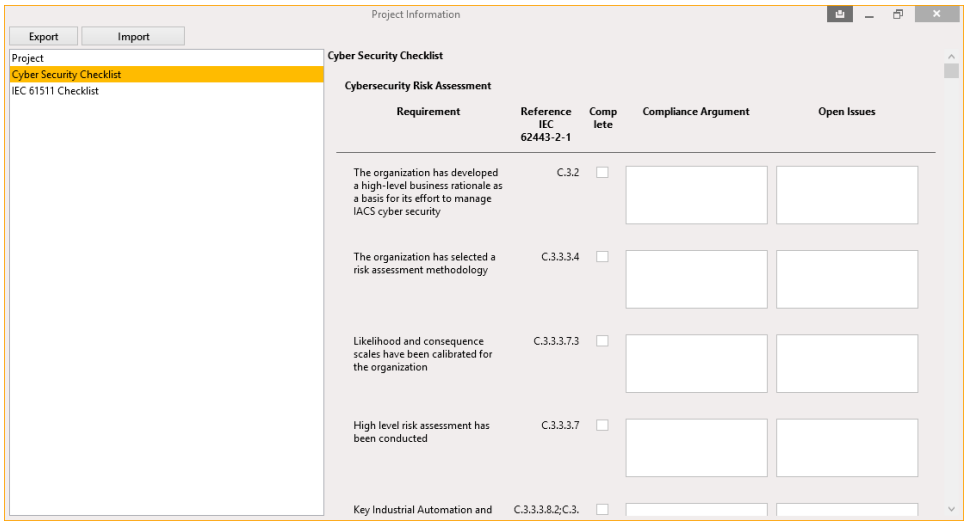
Chapter 5 Project Information

In exSILentia® v4 when you create a project, a ***Project ID*** and ***Project Name*** are required to be specified. In addition you can specify a ***Revision*** and a ***Project Description***. This information can be reviewed and modified in the Project Information window. To access the Project Information data, click on ***Project Information*** on the exSILentia® v4 Dashboard and select the Project Tab. Alternatively you can select the ***View - Project Information*** menu option.



5.1 Cyber Security Checklist

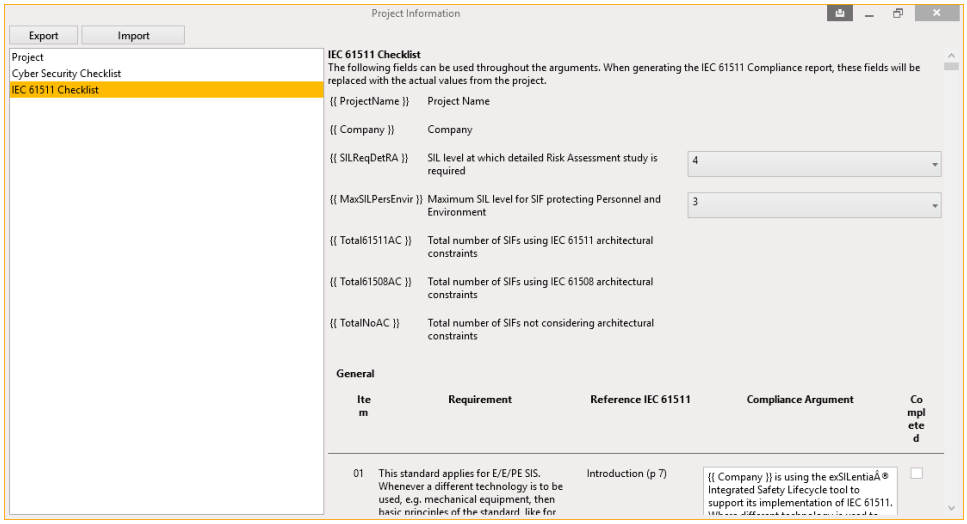
The Cyber Security Checklist feature in the Project Information allows you to review requirements from IEC 62443-2-1 and document how you are compliant with these requirements. This allows you to address cyber security concerns regarding your Safety Instrumented System.



5.2 IEC 61511 Checklist

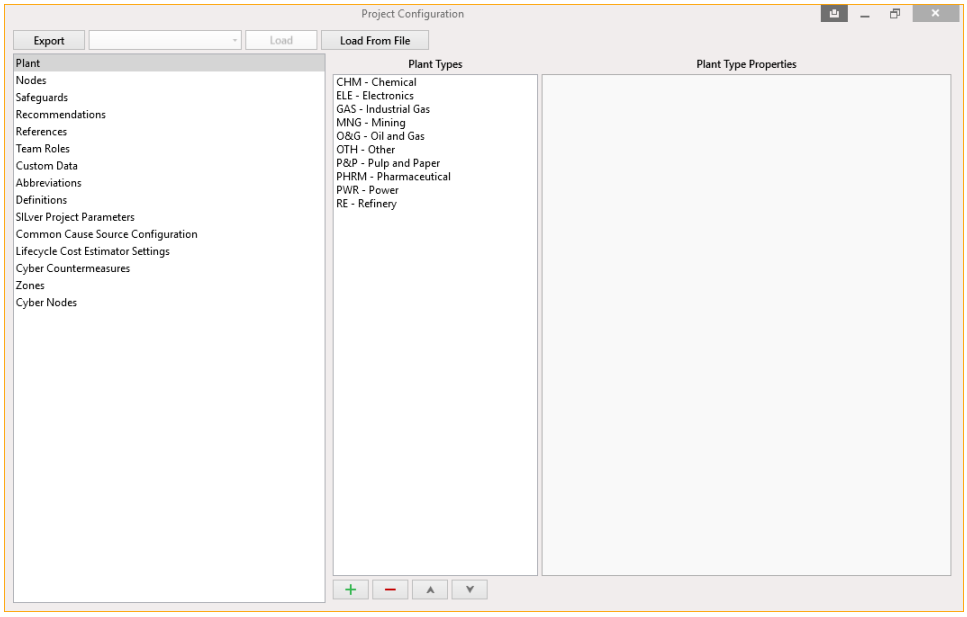
The IEC 61511 Checklist feature in the Project Information allows you to review requirements from IEC 61511 second edition and document how you are compliant with these requirements. This allows you to prepare a safety case for your entire project.

Within the IEC 61511 Checklist you can define text fields that you can use throughout your argument. The {{ ProjectName }} field for example will be using the Project Name for this project as you have defined it within the Project Information.



Chapter 6 Project Configuration

exSILentia® v4 provides detailed project configuration options to dramatically increase the efficiency and consistency of the various work activities to be performed. The various configuration options are explained in detail in the subsequent sections. exSILentia® v4 comes with a comprehensive set of exida default configuration settings. You can add, modify, or delete the values associated with the exida defaults which will be retained within the exSILentia® v4 project file. exida defaults can always be accessed by creating a new project or by importing them as explained in section *6.12 Project Configuration Export and Import*. You can also export your modified configurations for use in other projects.



6.1 Plant Types

The exSILentia® v4 Plant project configuration defines a relationship between various plant types and process types that are typical for that plant type. You can document the plant/process type being reviewed using the Plant configuration. The default exSILentia® v4 plant types are:

- Refinery
- Chemical
- Oil & Gas
- Power
- Industrial Gas
- Pharmaceutical
- Pulp & Paper
- Electronics
- Mining
- Other

The following default process types are identified for the various plant types:

Refinery	Chemical
Continuous Catalytic Regeneration (CCR) Reformer Crude Distillation Delayed Coker Fixed Bed Reformer Fluid Catalytic Cracking Fluid Coker Hydrocracker Sulfur Recovery Unit Tank Farm / Blending Utilities Waste Water Treatment Water Plant Ultra Low Sulfur Diesel (ULSD) Unit	Nitriles Polymers Monomers Ammonia Plant Acrylates Chlorine Plant Nitric Acid Plant Batch Hydrogenation Products Ethylene Plant Sulfuric Acid Plant Fine Chemicals Hazardous Waste Treatment

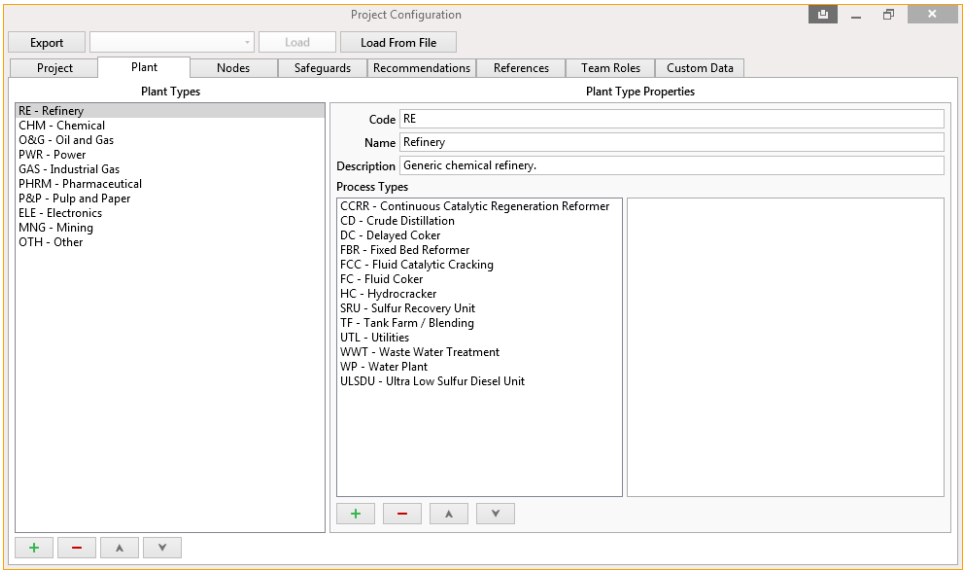
Oil & Gas	Power
Offshore Oil Platform Pipelines Steam Assisted Gravity Drainage (SAGD) Liquified Natural Gas (LNG) Gas Odorization Fuel Storage Facility Biodiesel	Cogeneration Fuel Oil / Gas Boilers Hydroelectric Nuclear Pulverized Fuel Boilers Wind Turbine Photovoltaic Municipal Incinerator

Industrial Gas	Pharmaceutical
Cryogenic Air Distillation Hydrogen Carbon Monoxide Plant Membrane Helium Plant Pipelines	Bulk API (Active Pharmaceutical Ingredient) Production High Containment Facility Biotech Production Facility

Pulp & Paper	Electronics

Mining	Other
	Sewage Treatment Plant Passenger Transport Project Risk Management

To review the plant types that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Plant Type Tab.



You can easily make changes to the default Plant Types and associated Process Types in the Project Configuration.

To add a Plant Type to the Project Configuration:

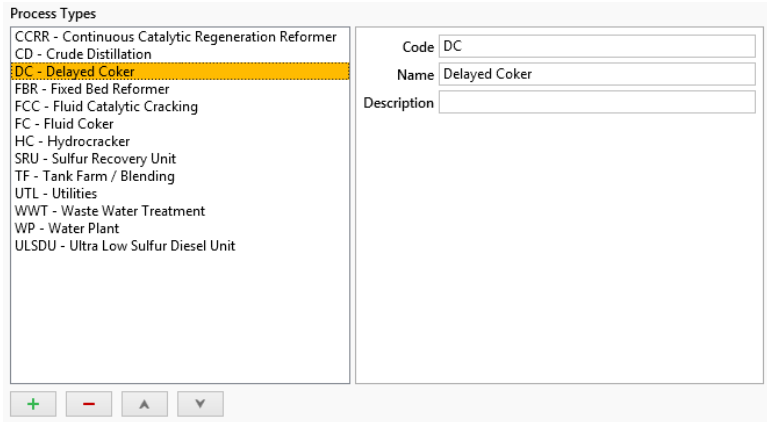
- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Plant Type Properties, i.e. *Code*, *Name*, and *Description*

To modify a Plant Type in the Project Configuration:

- Highlight the Plant Type
- Edit the Plant Type Properties, i.e. *Code*, *Name*, and *Description*
- Click on Save

To delete a Plant Type from the Project Configuration:

- Highlight the Plant Type
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Plant Type and its Plant Type Properties



To add a Process Type to a Plant Type:

- Click on the green plus (**+**) symbol in the lower left hand portion of the Process Types window
- Edit the Process Type Properties, i.e. *Code*, *Name*, and *Description*

To modify a Process Type for a given Process Type:

- Highlight the Process Type
- Edit the Process Type Properties, i.e. *Code*, *Name*, and *Description*
- Click on Save

To delete a Process Type from a given Plant Type:

- Highlight the Process Type
- Click on the red minus (**-**) symbol in the lower left hand portion of the Process Type window
- This will remove that Process Type and its Process Type Properties

6.2 Node Types

exSILentia® v4 has been designed to support smart deviations. Process Hazard Analysis deviations will be assigned based on the Node Type you assign to your node. The deviations are based upon process parameters and guidewords applicable to specific process node types. You must verify that the available options and settings are applicable and sufficient for your specific plant application and environment. exSILentia® v4 comes with a set of default Node Types and associated deviations. You can add to, modify, or delete the default node types and deviations based on your project needs. The default node types and associated deviations are:

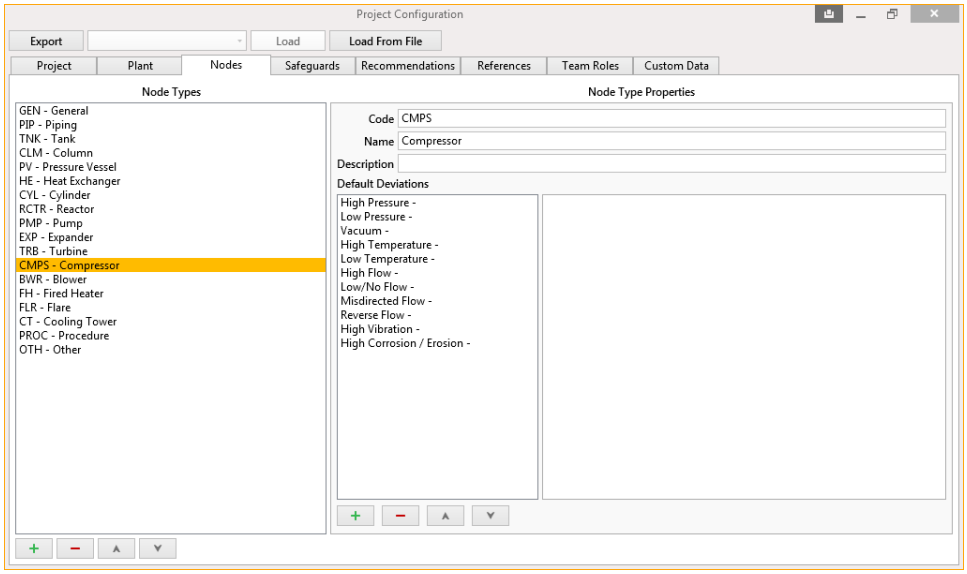
Parameter	Guide word	Deviation	Node Type																									
			Agitator	Blower	Centrifuge	Column	Compressor	Condenser	Cooling Tower	Cylinder	Expander	Filter	Fired Heater	Flare	General	Generator	Global	Heat Exchanger	Mixer	Piping	Pressure Vessel	Procedure	Pump	Reactor	Separator	Tank	Turbine	Other
Pressure	More	High Pressure		x	x	x	x	x		x	x	x	x	x				x	x	x	x		x	x	x	x	x	x
	Less	Low Pressure		x	x	x	x	x		x	x	x	x	x				x	x	x	x		x	x	x	x	x	x
	No	Vacuum		x	x	x	x	x		x	x	x	x	x				x	x	x	x		x	x	x	x	x	x
Temperature	More	High Temperature	x	x	x	x	x	x	x	x	x	x	x	x		x		x	x	x	x		x	x	x	x	x	x
	Less	Low Temperature	x	x	x	x	x	x		x	x	x	x	x		x		x	x	x	x		x	x	x	x	x	x
Flow	More	High Flow		x	x		x	x			x	x	x	x				x	x	x			x		x		x	x
	Less/No	Low/No Flow		x	x		x	x	x		x	x	x	x				x	x	x			x		x		x	x
	As well as	Misdirected Flow		x	x		x	x	x		x	x	x	x				x	x	x			x		x		x	x
	Reverse	Reverse Flow		x	x		x	x			x	x	x	x				x	x	x			x		x		x	x
Level	More	High Level				x		x	x										x		x			x	x	x		x
	Less/No	Low Level				x		x	x										x		x			x	x	x		x
Phase	No	Loss of Phase				x		x													x			x	x	x		x
	As well as	Additional Phase				x		x													x			x	x	x		x
	Other than	Wrong Phase				x		x													x			x	x	x		x

Parameter	Guide word	Deviation	Node Type																									
			Agitator	Blower	Centrifuge	Column	Compressor	Condenser	Cooling Tower	Cylinder	Expander	Filter	Fired Heater	Flare	General	Generator	Global	Heat Exchanger	Mixer	Piping	Pressure Vessel	Procedure	Pump	Reactor	Separator	Tank	Turbine	Other
Composition	More	High Concentration			x	x		x	x			x	x	x					x	x	x			x	x	x		x
	Less	Low Concentration			x	x		x	x				x	x					x	x	x			x	x	x		x
	As well as	Contaminants			x	x		x	x			x	x	x				x	x	x	x			x	x	x		x
	Part of	Missing Component			x	x		x					x	x					x	x	x			x	x	x		x
	Other than	Wrong Material			x	x		x					x	x				x	x	x	x			x	x	x		x
Mixing	More	Excessive Mixing	x		x														x					x		x		x
	Less/No	Less/No Mixing	x		x														x					x		x		x
	As well as	Foaming	x		x	x		x											x		x			x	x	x		x
	Reverse	Phase Separation	x			x		x													x			x	x	x		x
Reaction	More	High Reaction				x				x			x								x			x		x		x
	Less/No	Less/No Reaction											x											x				x
	As well as	Side Reaction				x				x			x								x			x		x		x
	Part of	Incomplete Reaction																						x				x
	Reverse	Reverse Reaction																										x
	Other than	Wrong Reaction																										x
Weight	More	High Weight																						x				x
	Less	Low Weight																	x					x				x

Parameter	Guide word	Deviation	Node Type																										
			Agitator	Blower	Centrifuge	Column	Compressor	Condenser	Cooling Tower	Cylinder	Expander	Filter	Fired Heater	Flare	General	Generator	Global	Heat Exchanger	Mixer	Piping	Pressure Vessel	Procedure	Pump	Reactor	Separator	Tank	Turbine	Other
Vibration	More	High Vibration	x	x	x		x		x		x					x			x				x				x	x
	Less	Low Vibration																	x									x
Utilities	More	Utility Surge	x																									x
	Less	Reduced Utility	x																									x
	No	Loss of Utility																										x
	As well as	Contaminated Utility																										x
Corrosion/Erosion	More	High Corrosion/Erosion	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x		x	x	x	x	x	x
Start-up	Part of	Incomplete Start-up													x	x												x
	Other than	Improper Start-up													x	x												x
Shutdown	Part of	Incomplete Shutdown													x	x												x
	Other than	Improper Shutdown													x	x												x
Maintenance	Less	Inadequate Maintenance													x													x
	No	Inability to Maintain													x													x
	As well as	Added Effort to Maintain													x													x
	Other than	Improper Maintenance													x	x												x

Parameter	Guide word	Deviation	Node Type																									
			Agitator	Blower	Centrifuge	Column	Compressor	Condenser	Cooling Tower	Cylinder	Expander	Filter	Fired Heater	Flare	General	Generator	Global	Heat Exchanger	Mixer	Piping	Pressure Vessel	Procedure	Pump	Reactor	Separator	Tank	Turbine	Other
Procedure	More	Error of Commission																				x						x
	No	Error of Omission																				x						x
	Reverse	Opposite Action Taken																				x						x
	Other than	Wrong Action Taken																				x						x

To review the node types and associated deviations that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Node Type Tab.



To add a Node Type:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Node Type
- Edit the Node Type Properties, i.e. *Code*, *Name*, and *Description*

To modify a Node Type:

- Highlight the Node Type
- Edit the Node Type Properties, i.e. *Code*, *Name*, and *Description*

To delete a Node Type:

- Highlight the Node Type
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Node Type and its Node Type Properties

To add a Deviation to a Node Type:

- Highlight the Node Type
- Click on the green plus (**+**) symbol in the right hand portion of the Node Type properties window
- Highlight the new Deviation
- Edit the *Deviation Name*

To modify a specific Deviation:

- Highlight the Node Type
- Highlight the Deviation
- Edit the *Deviation Name*

To delete a Deviation from a Node Type:

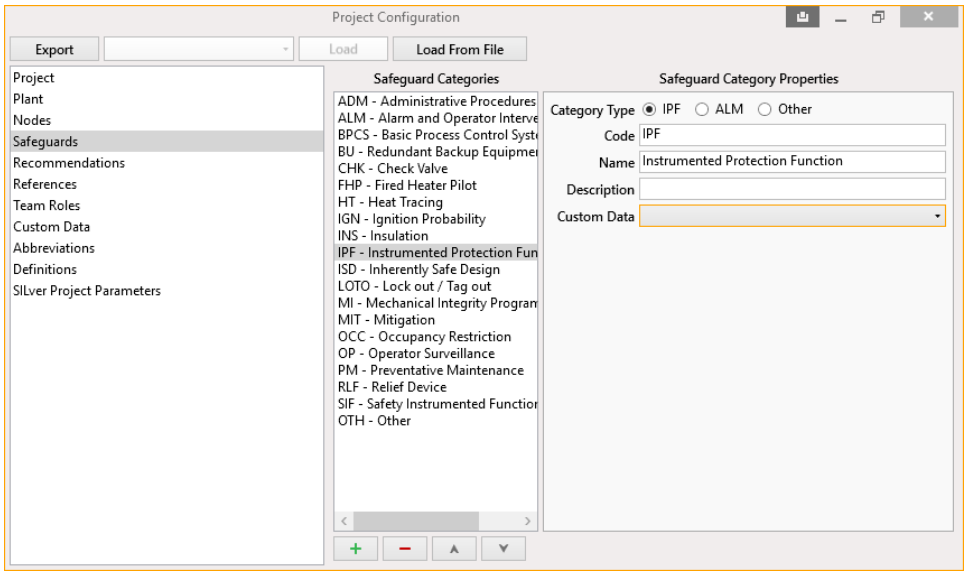
- Highlight the Node Type
- Highlight the Deviation
- Click on the red minus (-) symbol in the right hand portion of the Node Type properties window
- This will remove that Deviation from the Node Type selected

6.3 Safeguard Categories

exSILentia® v4 comes with a set of default Safeguard Categories. You can add categories, modify, or delete the default categories based on your project needs. The default safeguard categories are:

Abbreviation	Name
ADM	Administrative Procedures
ALM	Alarm and Operator Intervention
BPCS	Basic Process Control System
BPD	Buckling Pin Device
BU	Redundant Backup Equipment / System
CHK	Check Valve
CNV	Conservation Vent
DEL	Deluge System
DIKE	Dike or Bund
EVP	Explosion Vent Panel
FA	Flame Arrestor
FHP	Fired Heater Pilot
HT	Heat Tracing
IGN	Ignition Probability
INS	Insulation
IPF	Instrumented Protection Function
ISD	Inherently Safe Design
LOTO	Lock out / Tag out
MI	Mechanical Integrity Program
MIT	Mitigation
OCC	Occupancy Restriction
OP	Operator Surveillance
PM	Preventative Maintenance
RD	Rupture Disk
RLF	Relief Device
OTH	Other

To review the safeguard categories that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Safeguards Tab.



To add a Safeguard Category:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Safeguard Category
- Select the Safeguard Category Type, i.e. IPF, ALM, Other
- Edit the Safeguard Category Properties, i.e. *Code*, *Name*, and *Description*
- Click on Save

Note: The **Safeguard Category Type** allow you to define if a safeguard category is of type IPF, ALM, or Other. Based on these selections certain additional fields will be available as part of a safeguard. For example any safeguard category of type IPF will have additional Interlock fields available as well as a **Is SIF** checkbox. The latter is the unique identifier for exSILentia® v4 to indicate that a safeguard should be considered in subsequent Safety Instrumented Function related lifecycle phases.

To modify a Safeguard Category:

- Highlight the Safeguard Category
- Modify the Safeguard Category Type, i.e. SIF, IPL, Other
- Edit the Safeguard Category Properties, i.e. *Code*, *Name*, and *Description*
- Click on Save

To delete a Safeguard Category:

- Highlight the Safeguard Category
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Safeguard Category and its Safeguard Category Properties

To link Custom Data (see section *6.7 Custom Data*) to a Safeguard Category:

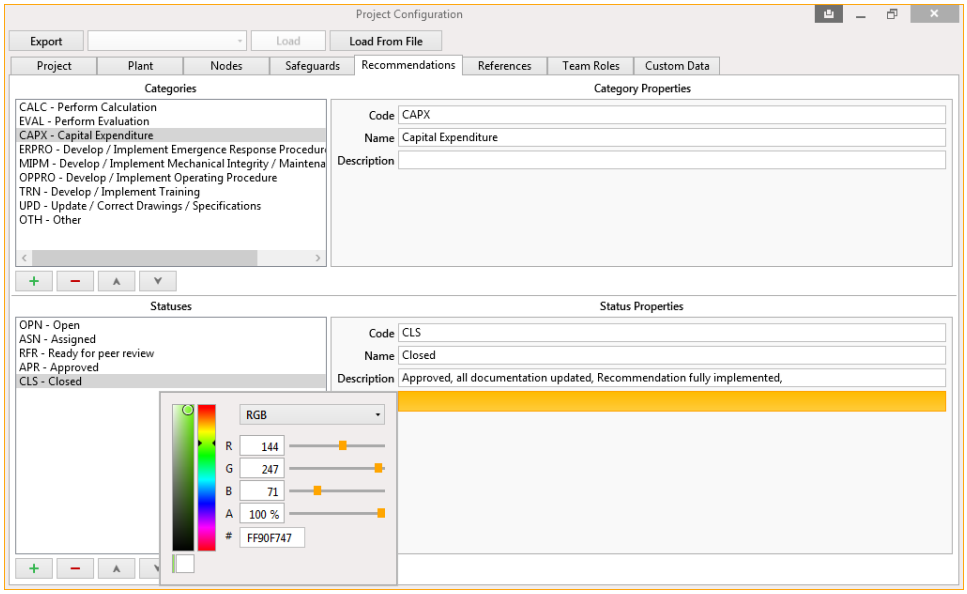
- Highlight the Safeguard Category
- Click on the Custom Data drop down
- Select the applicable Custom Data item

6.4 Recommendation Categories

exSILentia® v4 comes with a set of default Recommendation Categories. You can add categories, modify, or delete the default categories based on your project needs. The default recommendation categories are:

Abbreviation	Name
CALC	Perform Calculation
CAPX	Capital Expenditure
ERPRO	Develop / Implement Emergence Response Procedure
EVAL	Perform Evaluation
MIPM	Develop / Implement Mechanical Integrity / Maintenance Procedure
OPPRO	Develop / Implement Operating Procedure
TRN	Develop / Implement Training
UPD	Update / Correct Drawings / Specifications
OTH	Other

To review the recommendation categories that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Recommendations Tab.



To add a Recommendation Category:

- Click on the green plus (+) symbol in the lower left hand portion of the Category window
- Highlight the new Recommendation Category
- Edit the Recommendation Category Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Click on Save

To modify a Recommendation Category:

- Highlight the Recommendation Category
- Edit the Recommendation Category Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Click on Save

To delete a Recommendation Category:

- Highlight the Recommendation Category
- Click on the red minus (-) symbol in the lower left hand portion of the Category window
- This will remove that Recommendation Category and its Recommendation Category Properties

You can also make changes to the Recommendation Status options.

To add a Recommendation Status:

- Click on the green plus (+) symbol in the lower left hand portion of the Status window
- Highlight the new Recommendation Status
- Edit the Recommendation Status Properties, i.e. *Code*, *Name*, *Description*, and select a *Color*
- Click on Save

To modify a Recommendation Status:

- Highlight the Recommendation Status
- Edit the Recommendation Status Properties, i.e. *Code*, *Name*, *Description*, and select a *Color*
- Click on Save

To delete a Recommendation Status:

- Highlight the Recommendation Status
- Click on the red minus (-) symbol in the lower left hand portion of the Status window
- This will remove that Recommendation Status and its Recommendation Status Properties

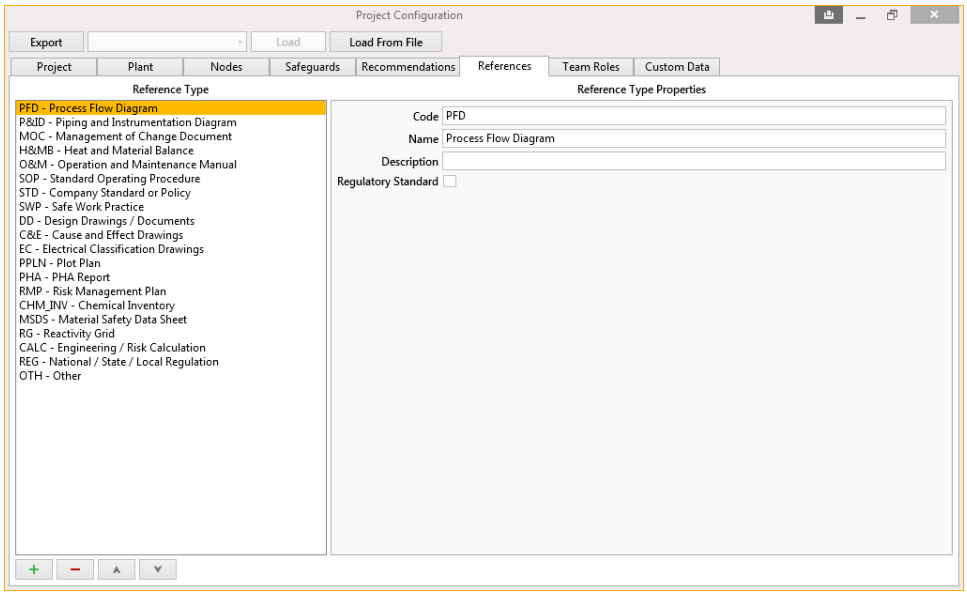
6.5 Reference Types

exSILentia® v4 comes with a set of default Reference Types. You can add categories, modify, or delete the default categories based on your project needs. The default reference types are:

Abbreviation	Name
C&E	Cause and Effect Drawing
CALC	Engineering / Risk Calculation
CHM_INV	Chemical Inventory
CSTD	Company Standard or Policy
DD	Design Drawing / Document
EC	Electrical Classification Drawing
H&MB	Heat and Material Balance
ISTD	Industry Standard

Abbreviation	Name
MOC	Management Of Change Document
MSDS	Material Safety Data Sheet
O&M	Operation and Maintenance Manual
P&ID	Piping and Instrumentation Diagram
PFD	Process Flow Diagram
PHA	PHA Report
PPLN	Plot Plan
REG	National / State / Local Regulation
RG	Reactivity Grid
RMP	Risk Management Plan
SOP	Standard Operating Procedure
SWP	Safe Work Practice
OTH	Other

To review the reference types that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the References Tab.



To add a Reference Category:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Reference Category
- Edit the Reference Category Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Indicate if this category represents a *Regulatory Standard* by clicking the checkbox
- Click on Save

Note: By indicating if a reference category is a Regulatory Standard, any documents marked with the particular reference category will be included in the regulatory standard section of the various reports.

To modify a Reference Category:

- Highlight the Reference Category
- Edit the Reference Category Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Click on Save

To delete a Recommendation Category:

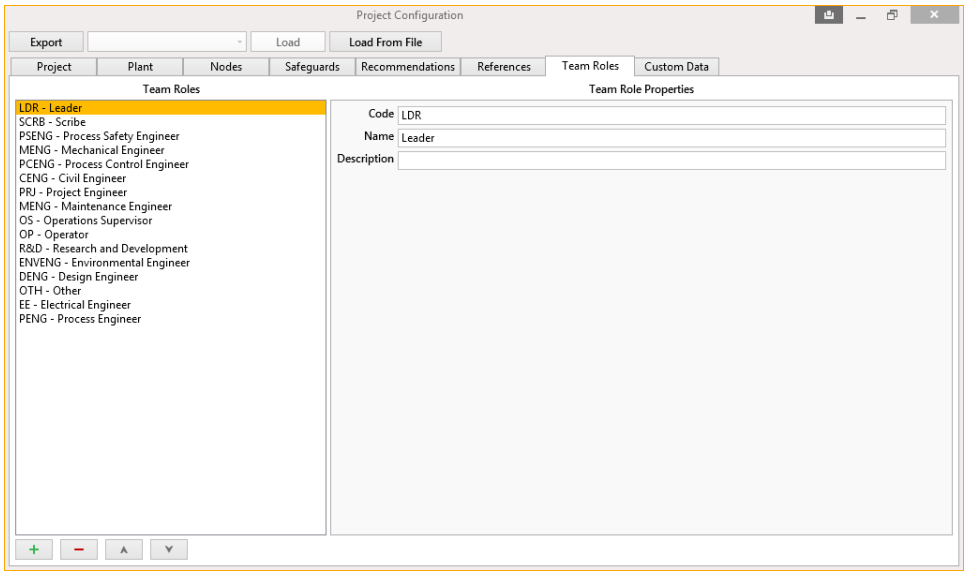
- Highlight the Reference Category
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Reference Category and its Reference Category Properties

6.6 Team Roles

exSILentia® v4 comes with a set of default Team Roles. You can add roles, modify, or delete the default roles based on your project needs. The default ream roles are:

Abbreviation	Name
CENG	Civil
DENG	Design
EE	Electrical
ENV	Environmental
IT	Information Technology
LDR	Leader
MAIN	Maintenance
MTN	Mechanical
PCENG	Process Control
PENG	Process
PRJ	Project Management
PSENG	Process Safety
OP	Operator
OS	Operations Supervisor
R&D	Research and Development
SCRB	Scribe
OTH	Other

To review the team roles that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Team Roles Tab.



To add a Team Role:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Team Role
- Edit the Team Role Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Click on Save

To modify a Team Role:

- Highlight the Team Role
- Edit the Team Role Properties, i.e. *Abbreviation*, *Name*, and *Description*
- Click on Save

To delete a Team Role:

- Highlight the Team Role
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Team Role and its Team Role Properties

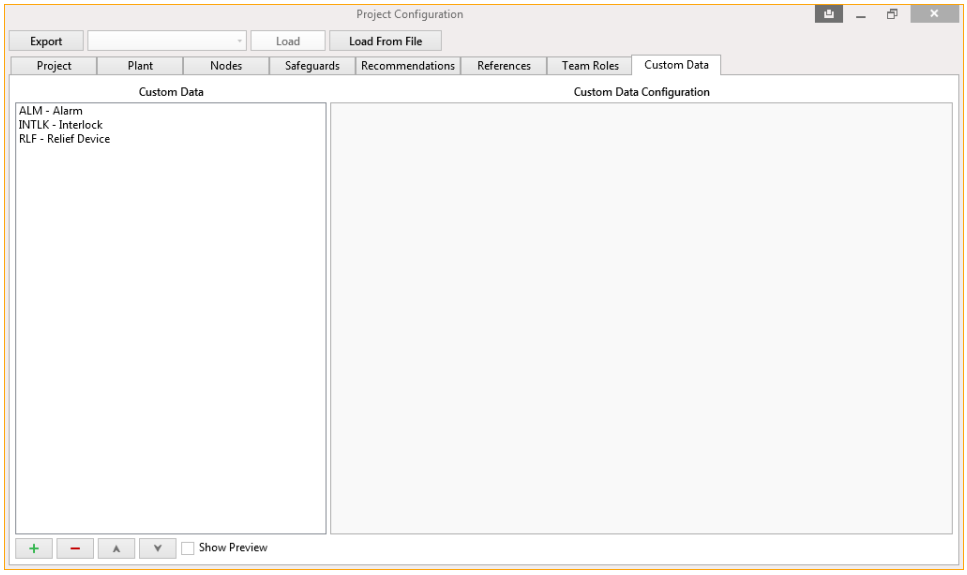
6.7 Custom Data

exSILentia® v4 provides you with the ability to define custom data. Custom data allows you to specify additional information you want to record for a specific entity within an exSILentia® v4 project. An example of where custom data may come in handy is to enable specification of previously undefined process safety information (PSI) to be used in the project. The default exida project has two custom data types available to support the process safety information. These are:

- Alarm Data
- Relief Device Data

The Custom Data functionality provides for the specification of several data fields for each data type.

To review the custom data that is defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Custom Data Tab.



To add Custom Data:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Custom Data Configuration
- Edit the Custom Data Properties, i.e. *Code* and *Name*
- Click on Save

To modify Custom Data:

- Highlight the Custom Data
- Edit the Custom Data Properties, i.e. *Code* and *Name*
- Click on Save

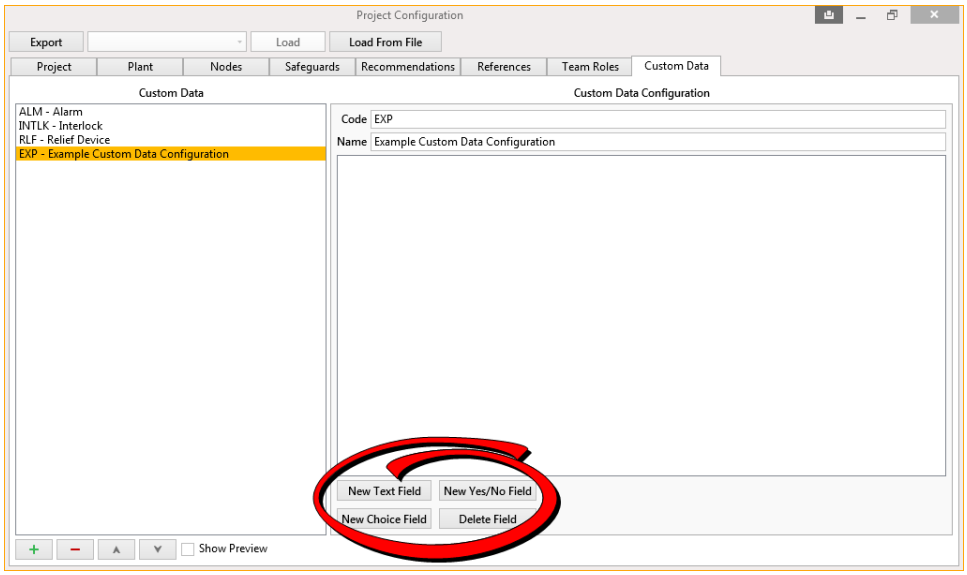
To delete Custom Data:

- Highlight the Custom Data
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Custom Data and its Custom Data Properties

Once custom data is defined in a project, you can add data fields to it. A data field can be of type Text, Yes/No, or Choice (which allows combo box information to be specified).

To add a Custom Data Field:

- Determine what type of field you want to add
- Select the *New Text Field*, *New Yes/No Field*, or *New Choice Field* button in the lower left hand portion of the Custom Data Configuration window
- Highlight the new Custom Data Field
- Edit the Custom Data Field Properties, i.e. *Name*, *Unit*, *Description*, and *Default Text* as applicable.
- Use the Up and Down arrow buttons to move the new Custom Data Field in the right order.
- Click on Save



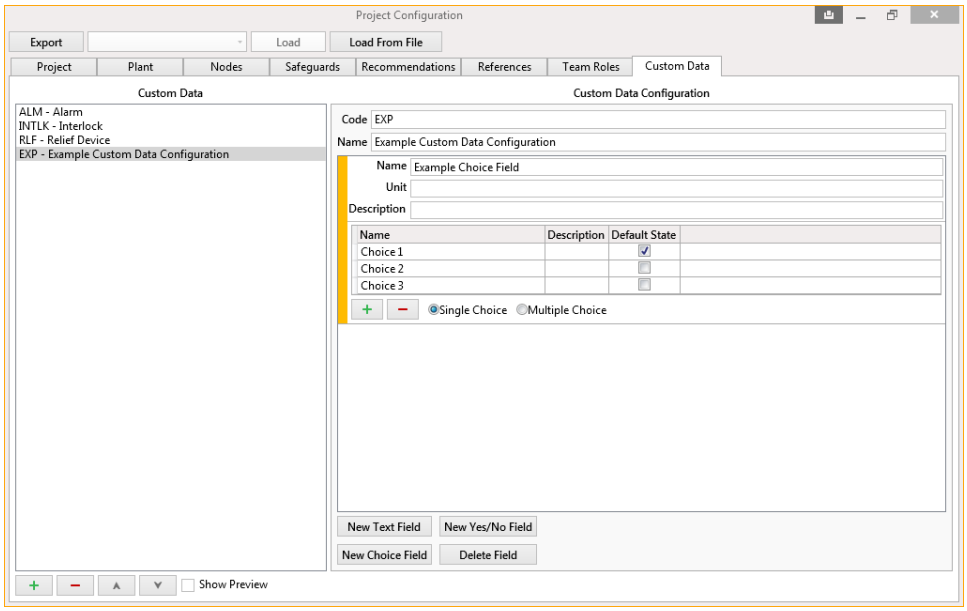
To modify a Custom Data Field:

- Highlight the Custom Data Field
- Edit the Custom Data Properties, i.e. *Name*, *Unit*, *Description*, and *Default Text* as applicable.
- Use the Up ▲ and Down ▼ arrow buttons to adjust the Custom Data Field sequence, if necessary.
- Click on Save

To delete a Custom Data Field:

- Highlight the Custom Data Field
- Click on the *Delete Field* button in the lower left hand portion of the Custom Data Configuration window
- This will remove that Custom Data Field and its Custom Data Field Properties

If you select ***Choice*** as the type for the custom data field, you will have the option to define entries for the combo box associated wit the data field. The data field can be setup to accept single selections only or multiple selections.



To add selection items for a Choice Custom Data Field Type:

- Click on the green plus (**+**) symbol in the lower left hand portion within the Custom Data Field window
- Highlight the new Choice Selection
- Edit the Choice Selection Properties, i.e. *Name* and *Description*
- Repeat this process until all Choice selections have been specified

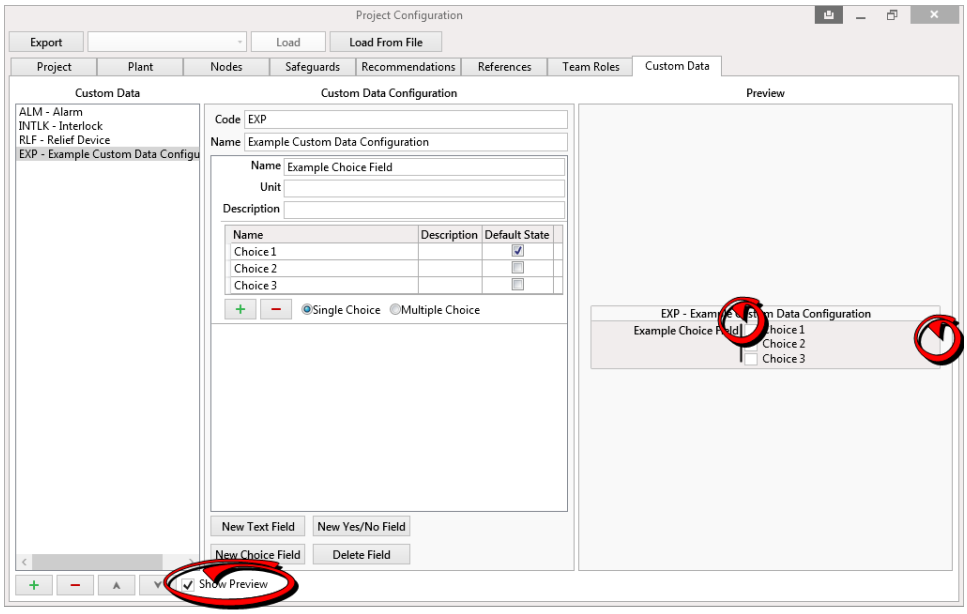
To modify a Choice Selection:

- Highlight the Choice Selection
- Edit the Choice Selection Properties, i.e. *Name* and *Description*
- Click on Save

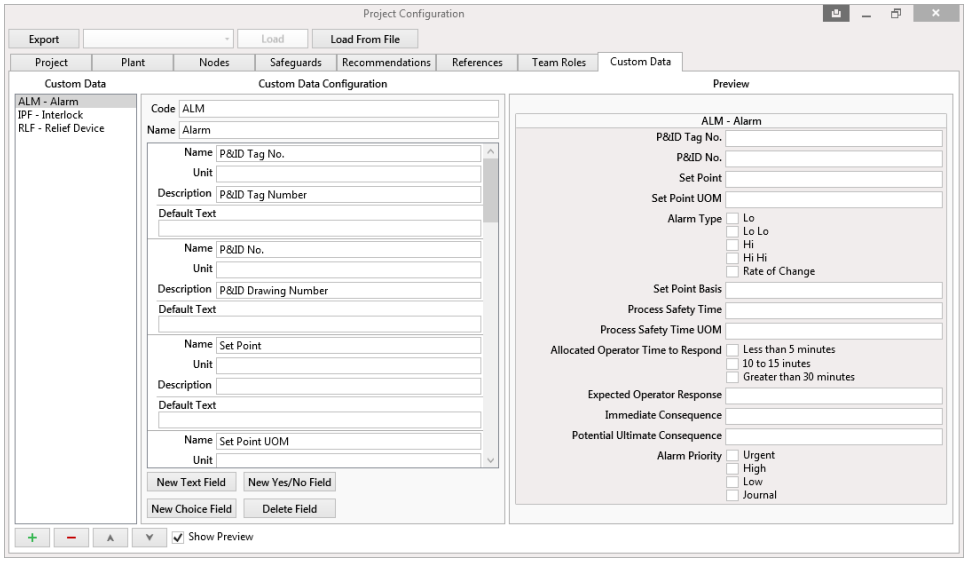
To delete a Choice Selection:

- Highlight the Choice Selection
- Click on the red minus (**-**) symbol in the lower left hand portion within the Custom Data Field window
- This will remove that Choice Selection and its Choice Selection Properties

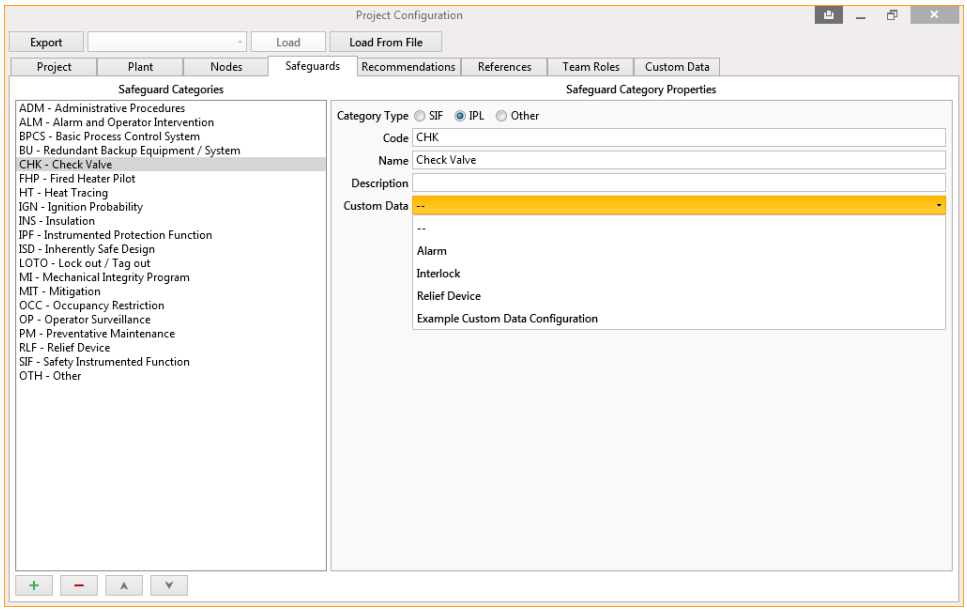
To see how the Custom Data will be displayed in the exSILentia® tool, check the ***Show Preview*** check box. You can re-size the form in this Preview window. Simply drag the right hand side of the custom data form in the Preview to adjust its width. You can also drag the (invisible) divider line between the custom field name column and the custom data field data entry field column to adjust the width distribution between the two columns. To accommodate the custom data form in the Preview you may need to increase the Preview section size. You can do this by adjusting the size of the complete Project Configuration window and/or dragging the divider line between the Custom Data Configuration section and the Preview section of the Custom Data Tab.



The figure below provides a partial example using the ALM – Alarm Process Safety Information exida default data and shows two text fields and a choice field.



To assign Custom Data to, for example, a Safeguard Category in exSILentia® v4, select the Safeguards Tab in the Project Configuration window, select the Safeguard Category to which the Custom Data must be assigned, and use the drop down list on the Safeguard Category Properties portion of the Safeguards window to select the applicable Custom Data option.

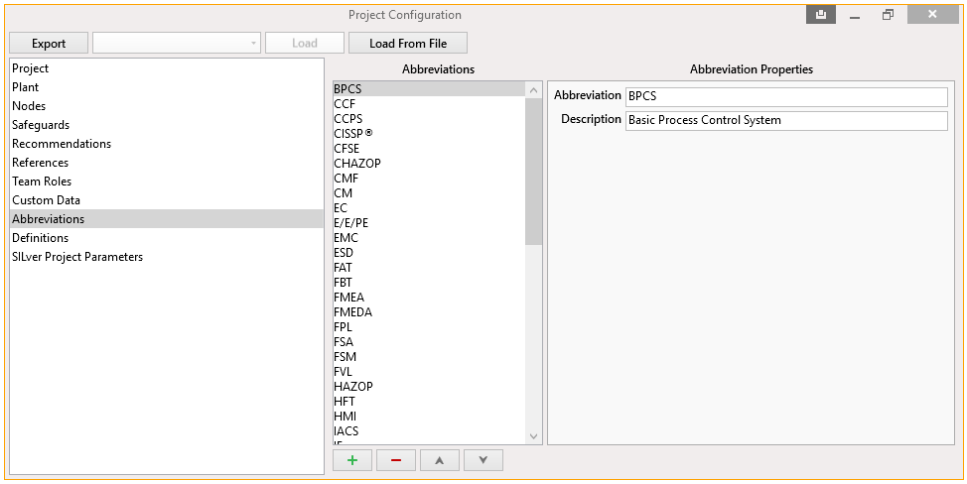


Note: Custom Data may be used for more than one custom data type, i.e. "ALM - Alarm Process Safety Information" can be linked to an Alarm safeguard category and could at the same time be used for an "OCC - Occupancy Restriction" safeguard category if those two categories require identical Custom Data.

6.8 Project Abbreviations

exSILentia® v4 comes with a set of default Abbreviations. You can add, modify, or delete the default abbreviations based on your project needs.

To review the abbreviations that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Abbreviations Tab.



To add an Abbreviation:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Abbreviation
- Edit the Abbreviation Properties, i.e. *Abbreviation* and *Description*
- You can reorder the Abbreviation using the **Up** and **Down** arrows
- Click on Save

To modify an Abbreviation:

- Highlight the Abbreviation
- Edit the Abbreviation Properties, i.e. *Abbreviation* and *Description*
- Click on Save

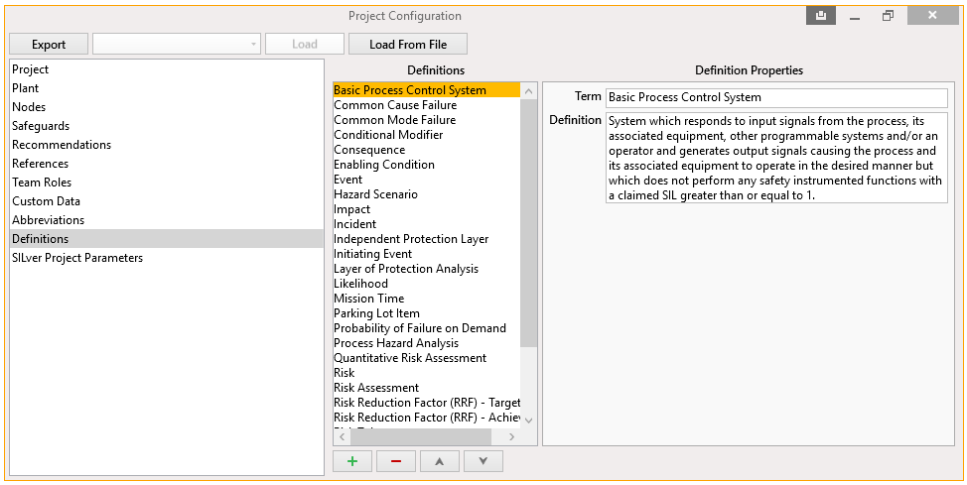
To delete an Abbreviation:

- Highlight the Abbreviation
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Abbreviation and its Abbreviation Properties

6.9 Project Definitions

exSILentia® v4 comes with a set of default Definitions. You can add, modify, or delete the default definitions based on your project needs.

To review the definitions that are defined in your project click on ***Project Configuration*** on the exSILentia® v4 Dashboard and select the Definitions Tab.



To add a Definition:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Definition
- Edit the Definition Properties, i.e. *Term* and *Definition*
- You can reorder the Definition using the **Up** and **Down** arrows
- Click on Save

To modify a Definition:

- Highlight the Definition
- Edit the Definition Properties, i.e. *Term* and *Definition*
- Click on Save

To delete a Definition:

- Highlight the Definition
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Definition and its Definition Properties

6.10 SILver Project Parameters

The SILver project parameters allow you to select defaults and project settings for the entire SIL verification project. These can be modified per SIF in the SILver module.

The SILver project parameters begin with the General SIF Information defaults. This includes:

- Architectural Constraints
- Systematic Capability
- Mission Time
- Startup Time
- Demand Rate Mode

These SIF Parameters are explained in further detail in the SILver Worksheet - SIF Level in Appendix G. You can also choose if you would like IO channels on separate modules throughout the project.

For Sensors and Final Elements you can choose defaults for:

- Site Safety Index
- Beta Factor
- Mean Repair Time
- Proof Testing
- Leg Options

These Sensor and Final Element Group options are explained in further detail in Appendix G.

For Logic Solvers you can choose defaults for:

- Site Safety Index
- Beta Factor
- Mean Repair Time

These Logic Solver options are explained in further detail in Appendix G.

6.11 Lifecycle Cost Estimator Settings

The Lifecycle Cost Estimator Settings allow you to specify lifecycle cost parameters that apply to the entire exSILentia® project. These parameters are:

- Discount Rate in percentages
- Plant Life in years
- Monetary Symbol, e.g. $, €

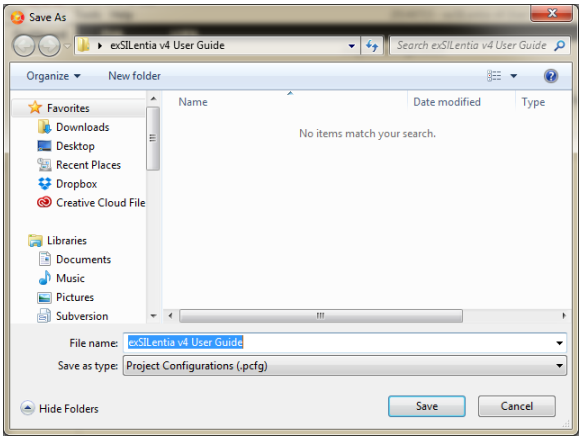
These parameters impact the overall lifecycle cost as calculated in the Lifecycle Cost Estimator tool.

6.12 Project Configuration Export and Import

The Project Configuration settings can be exported and saved as a .pcfg file external to the exSILentia® v4 project. Once a Project Configuration settings .pcfg file is available external to the the exSILentia® v4 project it can be imported.

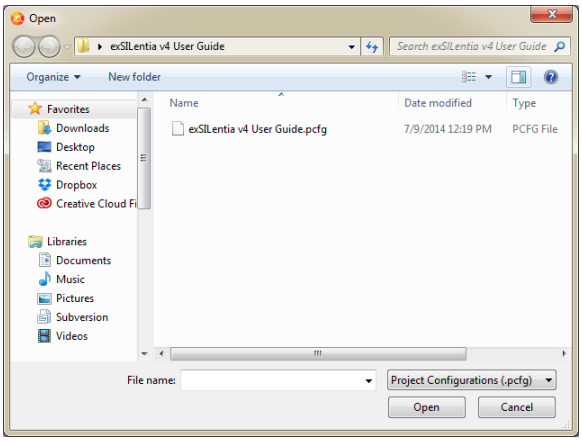
To export Project Configuration settings:

- On the exSILentia® v4 Dashboard, click on ***Project Configuration***
- Click on ***Export*** in the upper left hand corner of the project configuration window
- Browse to the location where you want to save the .pcfg file
- Specify a file name
- Click on Save



To load previously saved Project Configuration settings:

- On the exSILentia® v4 Dashboard, click on ***Project Configuration***
- Click on the ***Load From File*** button at the top of the project configuration window
- Browse to the location where the .pcfg file is located
- Select the file
- Click on Open (alternatively double click on the file)



If there is more than one possible set of default values within a project, the appropriate set would be first selected from the drop down box which would trigger the loading of the default values to use.

Note: As exSILentia® v4 project schema can be expanded with every release, some older project configurations, e.g. based on v4.0 or v4.1, may not set specific parameters like Safeguard Category type, as this parameter was introduced after those releases. You should verify your project configuration if the source file is older than the current released version of the software.

Chapter 7 Project Libraries

exSILentia® v4 provides build in libraries for identical items that can be (re-)used in multiple locations. A library item is a unique entity that can be referenced in multiple locations. A change to the library item will automatically be applied to all locations the library item is referenced. Using libraries will dramatically increase the efficiency and consistency of the various work activities to be performed. Libraries are defined for the following items:

- Causes
- Safeguards
- Recommendations
- References
- Hazard Scenarios
- Enabling Conditions
- Conditional Modifiers
- Sensor Groups and Legs
- Logic Solver Models
- Logic Solver
- Devices
- Device Models
- Final Element Groups and Legs
- Tags
- Proven In Use Justification

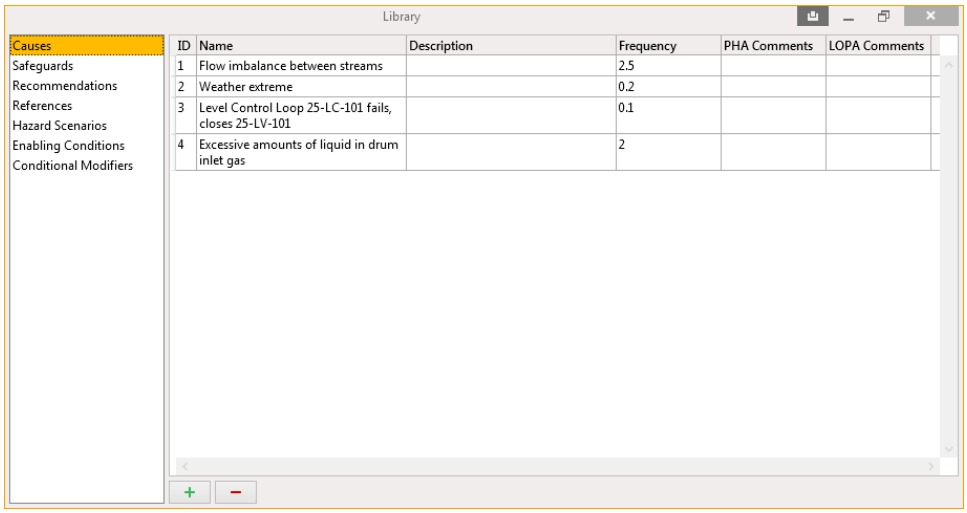
Library items can be defined while you are using the various exSILentia® v4 tools or prior to your use of the tool. When you open a library you will be able to see where the library item is used. If you predefine library items they will show up in italic font, indicating they are not assigned to anything, and the location used will be blank.

7.1 Causes Library

Causes that are defined in the Causes Library are available for use in various parts of exSILentia® v4 such as the PHAx™ HAZOP worksheet and the LOPAx™ worksheet. Causes can be added from within the Causes Library overview or as part of performing various Process Hazard Analysis or Layer of Protection Analysis tasks.

Note: Causes are referred to as Initiating Events in Layer of Protection Analysis terminology.

To review causes defined in the Causes Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Causes Library item.



To add a Cause to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Cause Properties, i.e. *Name*, *Description*, and *Frequency* (if known at this point)
    - The PHA Comments and LOPA Comments are typically only specified when the respective analysis is conducted

To modify a Cause in the library:

- Highlight the Cause
- Edit the Cause Properties, i.e. *Name*, *Description*, and *Frequency*
- Click on Save

To delete a Cause from the library:

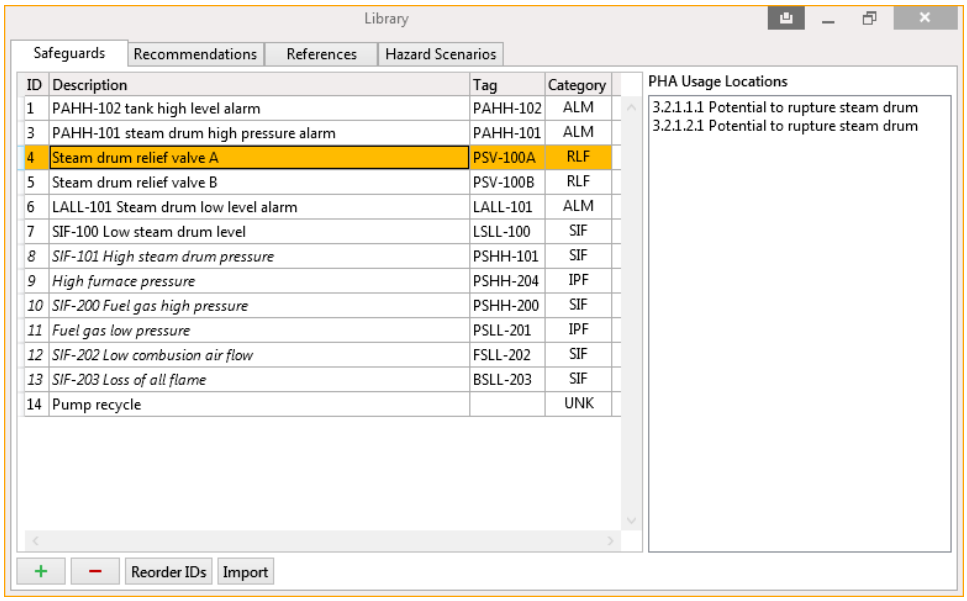
- Highlight the Cause
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Cause and its Cause Properties

CAUTION: Deleting a cause from the library deletes every instance of that cause on every worksheet where it has previously been used.

7.2 Safeguards Library

Safeguards that are defined in the Safeguards Library are available for use in various parts of exSILentia® v4 such as the PHAx™ HAZOP worksheet. Safeguards can be added from within the Safeguards Library overview or as part of performing various Process Hazard Analysis tasks.

To review safeguards defined in the Safeguards Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Safeguards Library item.



To add a Safeguard to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Safeguard Properties, i.e. *Name*,*Description*, *Tag* (if available), *PFD* (if known at this point), and select the *Category* from the drop down box
    - See section*6.3* for more information on Safeguard Categories

To modify a Safeguard in the library:

- Highlight the Safeguard
- Edit the Safeguard Properties, i.e. *Name*, *Description*, *Tag* (if available), *PFD*, and select the *Category* from the drop down box
- Click on Save

To delete a Safeguard from the library:

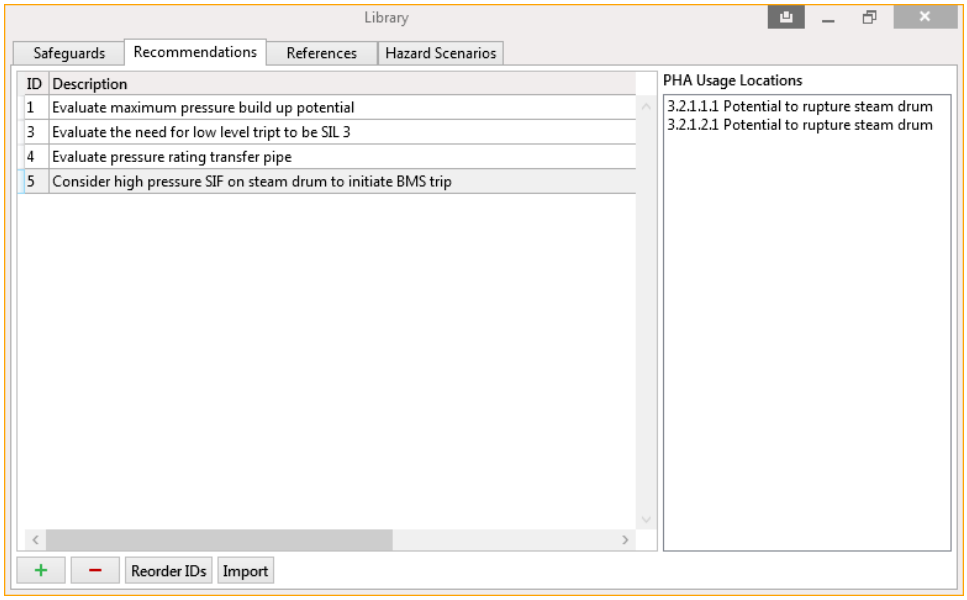
- Highlight the Safeguard
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Safeguard and its Safeguard Properties

CAUTION: Deleting a safeguard from the library deletes every instance of that safeguard on every worksheet where it has previously been used.

7.3 Recommendations Library

Recommendations that are defined in the Recommendations Library are available for use in various parts of exSILentia® v4 such as the PHAx™ HAZOP worksheet. Recommendations can be added from within the Recommendations Library overview or as part of performing various Process Hazard Analysis tasks. Recommendations, however, are generally entered as part of a review utilizing the various worksheets or software tools.

To review recommendation defined in the Recommendations Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Recommendations Library item.



To add a Recommendation to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Recommendation Properties, i.e. *Name*, *Description*, select the *Category* from the drop down box, select the *Assigned to* from the drop down box, specify the *Due Date*, and select the *Status* from the drop down box.
    - See section *6.4* for more information on Recommendation Categories
    - See section *A.4* for more information on Team Members

To modify a Recommendation in the library:

- Highlight the Recommendation
- Edit the Recommendation Properties, i.e. *Name*, *Description*, select the *Category* from the drop down box, select the *Assigned to* from the drop down box, specify the *Due Date*, and select the *Status* from the drop down box.
- Click on Save

CAUTION: Modifying a recommendation in the library will impact all instances where the recommendation is used.

To delete a Recommendation from the library:

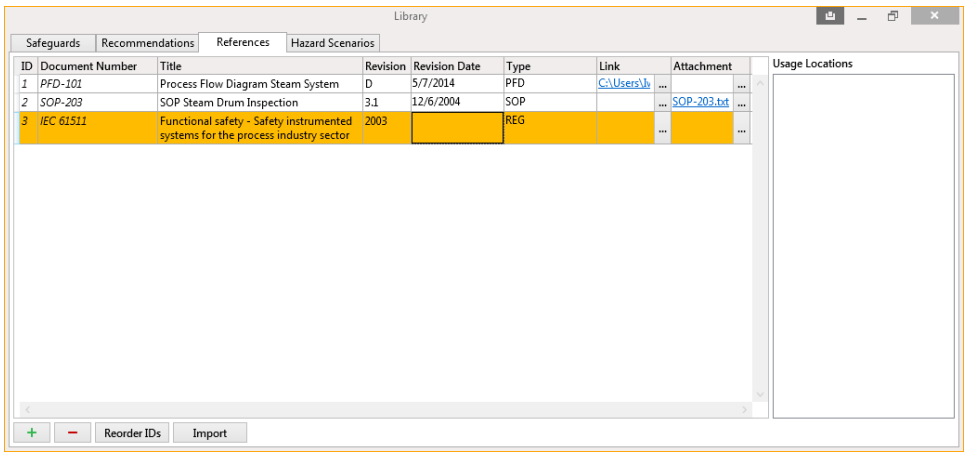
- Highlight the Recommendation
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Recommendation and its Recommendation Properties

CAUTION: Deleting a recommendation from the library deletes every instance of that recommendation on every worksheet where it has previously been used.

7.4 References Library

References that are defined in the References Library are available for use in various parts of exSILentia® v4 as well as for reporting purposes. References can be added from within the Reference Library overview or as part of performing various lifecycle tasks. It is useful to enter standard References in the References library prior to their use as this will increase overall efficiency.

To review references defined in the Reference Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the References Library item.



To add a Reference to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Reference Properties, i.e. *Document Number*, *Title*, *Description*, *Revision*, *Revision Date*, and select the *Reference Type* from the drop down box.
    - See section *6.5* for more information on Reference Types
- You can create a hyperlink (*Link*) to the reference or embed (*Attachment*) the actual reference in the project

To modify a Reference in the library:

- Highlight the Reference
- Edit the Reference Properties, i.e. *Document Number*, *Title*, *Description*, *Revision*, *Revision Date*, and select the *Reference Type* from the drop down box.
- You can delete the reference *Link* or *Attachment* by clicking on the red ***X*** icon next to the link or attachment. You can then specify an alternate file to hyperlink or embed.
- Click on Save

CAUTION: Modifying a reference in the library will impact all instances where the reference is used.

To delete a Reference from the library:

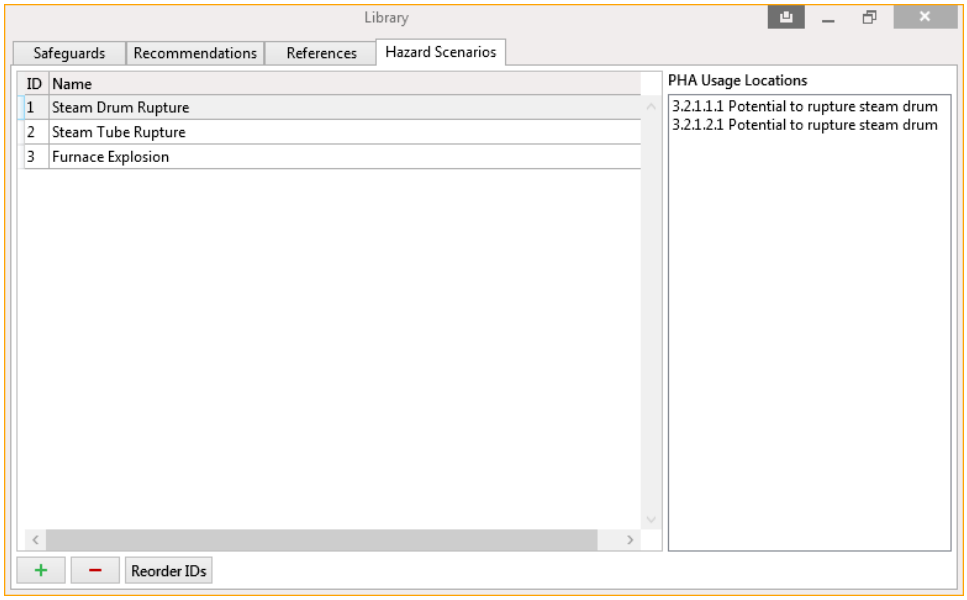
- Highlight the Reference
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Reference and its Reference Properties

CAUTION: Deleting a reference from the library deletes every instance of that reference where it has previously been used.

7.5 Hazard Scenarios Library

Hazard Scenarios that are defined in the Hazard Scenarios Library are available for use in various parts of exSILentia® v4 such as the PHAx™ HAZOP worksheet and the LOPAx™ worksheet. Hazard Scenarios can be added from within the Hazard Scenarios Library overview or as part of performing various lifecycle tasks.

To review hazard scenarios defined in the Hazard Scenarios Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Hazard Scenarios Library item.



To add a Hazard Scenario to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Hazard Scenario Properties, i.e. *Name*

To modify a Hazard Scenario in the library:

- Highlight the Hazard Scenario
- Edit the Hazard Scenario Properties, i.e. *Name*
- Click on Save

CAUTION: Modifying a hazard scenario in the library will impact all instances where the hazard scenario is used.

To delete a Hazard Scenario from the library:

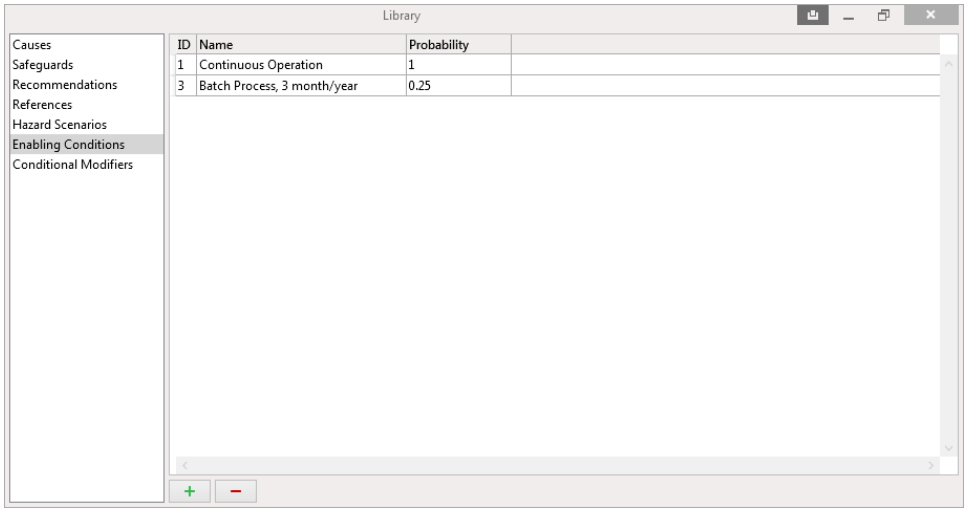
- Highlight the Hazard Scenario
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Hazard Scenario and its Hazard Scenario Properties

CAUTION: Deleting a hazard scenario from the library deletes every instance of that hazard scenario on every worksheet where it has previously been used.

7.6 Enabling Conditions Library

Enabling Conditions that are defined in the Enabling Conditions Library are available for use in various parts of exSILentia® v4 such as the LOPAx™ worksheet. Enabling Conditions can be added from within the Enabling Conditions Library overview or as part of performing various Layer of Protection Analysis tasks.

To review enabling conditions defined in the Enabling Conditions Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Enabling Conditions Library item.



To add a Enabling Condition to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Enabling Condition Properties, i.e. *Name* and *Probability* (if known)

To modify a Enabling Condition in the library:

- Highlight the Enabling Condition
- Edit the Enabling Condition Properties, i.e. *Name*, *Probability* (if known)
- Click on Save

To delete a Enabling Condition from the library:

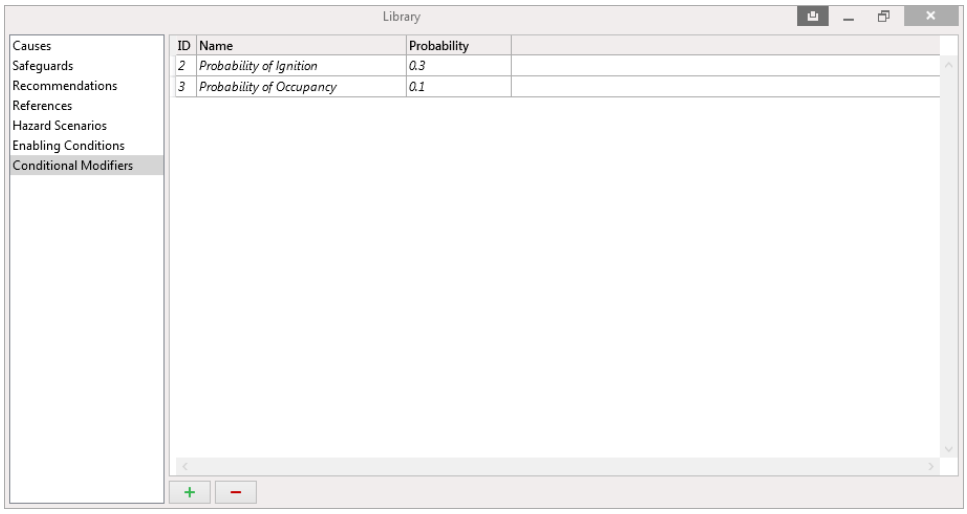
- Highlight the Enabling Condition
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Enabling Condition and its Enabling Condition Properties

CAUTION: Deleting a enabling condition from the library deletes every instance of that enabling condition on every worksheet where it has previously been used.

7.7 Conditional Modifiers Library

Conditional Modifiers that are defined in the Conditional Modifiers Library are available for use in various parts of exSILentia® v4 such as the LOPAx™ worksheet. Conditional Modifiers can be added from within the Conditional Modifiers Library overview or as part of performing various Layer of Protection Analysis tasks.

To review conditional modifiers defined in the Conditional Modifiers Library click on ***Library*** icon on the exSILentia® v4 Dashboard, or select the ***View - Library*** menu option, and select the Conditional Modifiers Library item.



To add a Conditional Modifier to the library:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Conditional Modifier Properties, i.e. *Name* and *Probability* (if known)

To modify a Conditional Modifier in the library:

- Highlight the Conditional Modifier
- Edit the Conditional Modifier Properties, i.e. *Name* and *Probability* (if known)
- Click on Save

To delete a Conditional Modifier from the library:

- Highlight the Conditional Modifier
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Conditional Modifier and its Conditional Modifier Properties

CAUTION: Deleting a conditional modifier from the library deletes every instance of that conditional modifier on every worksheet where it has previously been used.

7.8 Sensor Groups and Legs

The library stores each sensor group defined in SIL Verification in the SILver module. The group information stored in the library includes:

- Group Name
- Description
- Application Test Parameters
- Voting
- Beta Factor
- Mean Repair Time
- Proof Test Parameters
- Places Used

Likewise, the library stores each sensor leg defined in SIL Verification in the SILver module. The leg information stored in the library includes:

- Leg Name
- Description
- Places Used

These parameters can be modified in the library if you prefer, and will be updated accordingly in the SILver module. For details on each of these parameters see section *G.5 SILver Worksheet - Sensor Group*.

7.9 Logic Solver Models

The library stores each Logic Solver Model used during SIL Verification in the SILver module. One Logic Solver Model can be used for various Logic Solvers and can be selected from exida's Safety Equipment Reliability Handbook database or entered as a User Defined Logic Solver Model. You can also add Logic Solver Models directly into the library if you have, for example, many logic solvers of the same model from the same vendor in a process.

To add a Logic Solver Model directly into the library, select the + button, and select a Logic Solver Model from exida's SERH.

7.10 Logic Solvers

The library stores each individual Logic Solver defined during SIL Verification in the SILver module. Each Logic Solver specified during the design of your safety instrumented system is given a unique entry in the library, making it possible to re-use the Logic Solver in different SIFs. For more information on Logic Solvers see section *G.8 SILver Worksheet - Logic Solver Part*.

7.11 Devices

The library stores each individual device defined during SIL Verification in the SILver module. Each sensor or final element specified during the design of your safety instrumented system is given a unique entry in the library, making it possible to re-use the device in different SIFs. For more information on Sensor Devices see section *G.5 SILver Worksheet - Sensor Group*. For more information on Final Element Devices, see section *G.7 SILver Worksheet - Final Element Group*.

7.12 Device Models

The library stores each Device Model used during SIL Verification in the SILver module. One Device Model can be used for various devices and can be selected from exida's Safety Equipment Reliability Handbook database or entered as a User Defined device model. You can also add Device Models directly into the library if you have, for example, many sensors or final elements of the same model from the same vendor in a process.

To add a Device Model directly into the library, select the + button, and select a device model from exida's SERH.

7.13 Final Element Groups and Legs

The library stores each final element group defined in SIL Verification in the SILver module. The group information stored in the library includes:

- Group Name
- Description
- Application Test Parameters
- Voting
- Beta Factor
- Mean Repair Time
- Proof Test Parameters
- Places Used

Likewise, the library stores each final element leg defined in SIL Verification in the SILver module. The leg information stored in the library includes:

- Leg Name
- Description
- Places Used

These parameters can be modified in the library if you prefer, and will be updated accordingly in the SILver module. For details on each of these parameters see section *G.7 SILver Worksheet - Final Element Group*.

7.14 Tags

The library stores tag information input in the SILver module during SIL Verification. The tags can also be input directly into the library and linked to a Sensor Leg or Final Element Leg. For more details on tags, see section *G.11 SILver Worksheet - Tags*.

7.15 Proven In Use Justification

The library stores each Proven In Use Justification completed during SIL Verification in the SILver module. For more details on Proven In Use Justification, see section *G.10 SILver Worksheet - Features*.

Chapter 8 Project Risk Configuration

To define your tolerable risk levels, you can either select the exida default risk matrix or configure a risk matrix to match the risk criteria that are applied to the project. Once a risk matrix is configured, it may be exported and saved for import to future projects. An exSILentia® v4 project can contain multiple risk matrices, you will need to specify which matrix needs to be considered for the current project.

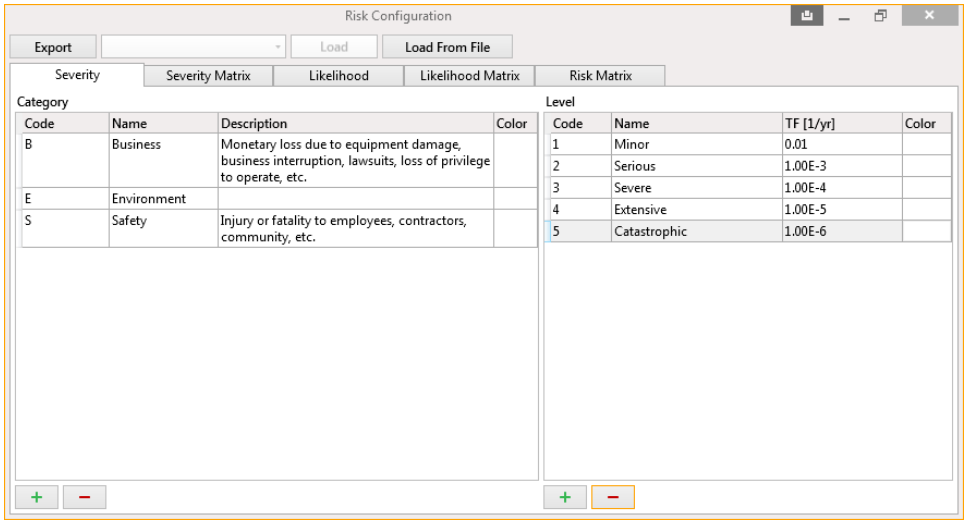
Risk is the product of consequence and likelihood. exSILentia® v4 allows detailed configuration of both consequence and likelihood categories and levels which provide complete customization options of the risk matrix used in the project.

To access the Project Risk Configuration information, click on ***Risk Configuration*** on the exSILentia® v4 Dashboard. Alternatively you can select the ***View - Risk Configuration*** menu option.

8.1 Consequence Categories and Severity Levels

The first task in specifying the project risk matrix is to define the applicable consequence categories and severity levels. To do so use the following steps:

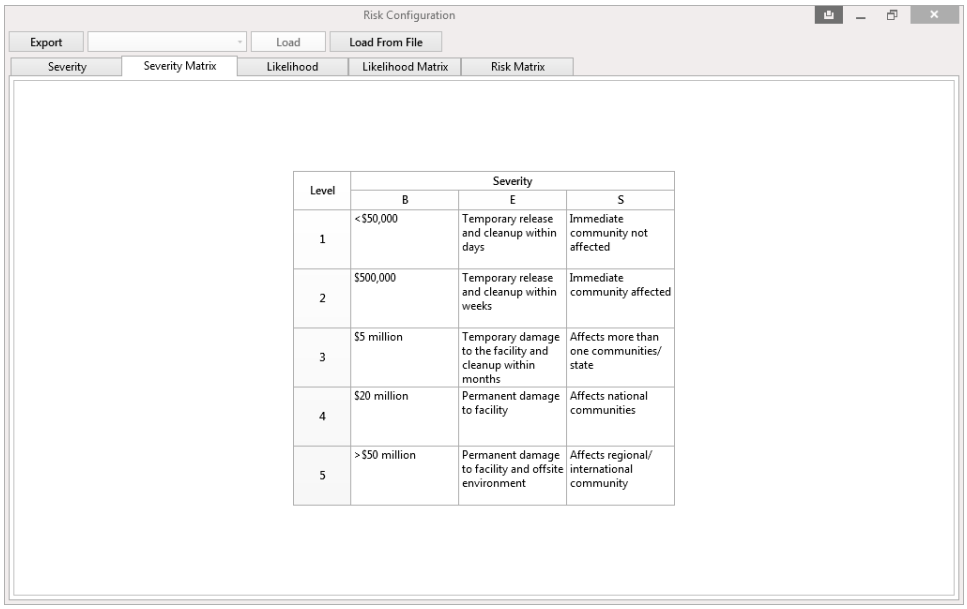
1. In the ***Risk Configuration*** window select the ***Severity*** Tab
2. The information initially shown is the exida default risk matrix (unless you selected the *create an empty project* option when starting this project in which case all entries will be blank).
3. Severity categories can be added or deleted by using the plus (**+**) or minus (**-**) symbols in the lower left corner of the left window pane.
4. You can edit the default information for severity category *Code*, *Name*, and *Description* or enter the relevant information for severity categories you may have added.
5. Severity levels can be added or deleted by using the plus (**+**) or minus (**-**) symbols in the lower left corner of the right window pane.
6. You can edit the default information for severity level *Code*, *Name*, and *Tolerable Frequency* or enter the relevant information for severity levels you may have added.



8.2 Severity Matrix

The second task in specifying the project risk matrix is to define the applicable consequence/severity matrix. To do so use the following steps:

1. Ensure you specified all relevant information on the Severity Tab (see section *8.1 Consequence Categories and Severity Levels*)
2. In the ***Risk Configuration*** window select the ***Severity Matrix*** Tab
3. The information initially shown is part of the exida default risk matrix (unless you selected the *create an empty project* option when starting this project in which case the severity matrix will be blank).
4. The Severity Matrix matches severity levels to severity categories. The matrix is prepopulated based on the on the information you specified on the severity tab.
5. You can edit the information in the matrix cells or enter the relevant information as applicable.

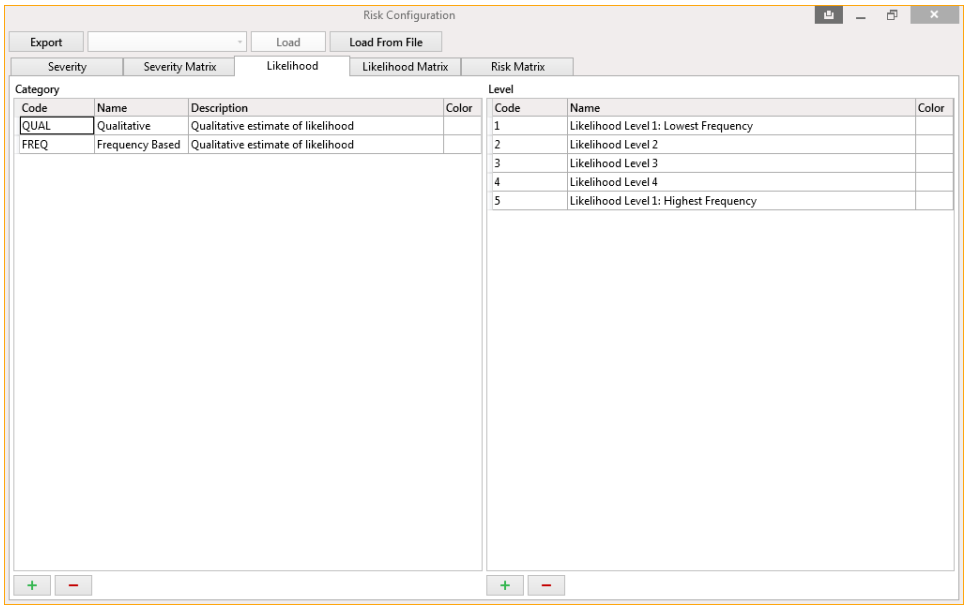


Level	Severity		
	B	E	S
1	<$50,000	Temporary release and cleanup within days	Immediate community not affected
2	$500,000	Temporary release and cleanup within weeks	Immediate community affected
3	$5 million	Temporary damage to the facility and cleanup within months	Affects more than one communities/ state
4	$20 million	Permanent damage to facility	Affects national communities
5	>$50 million	Permanent damage to facility and offsite environment	Affects regional/ international community

8.3 Likelihood Categories and Levels

The third task in specifying the project risk matrix is to define the applicable likelihood categories and levels. To do so use the following steps:

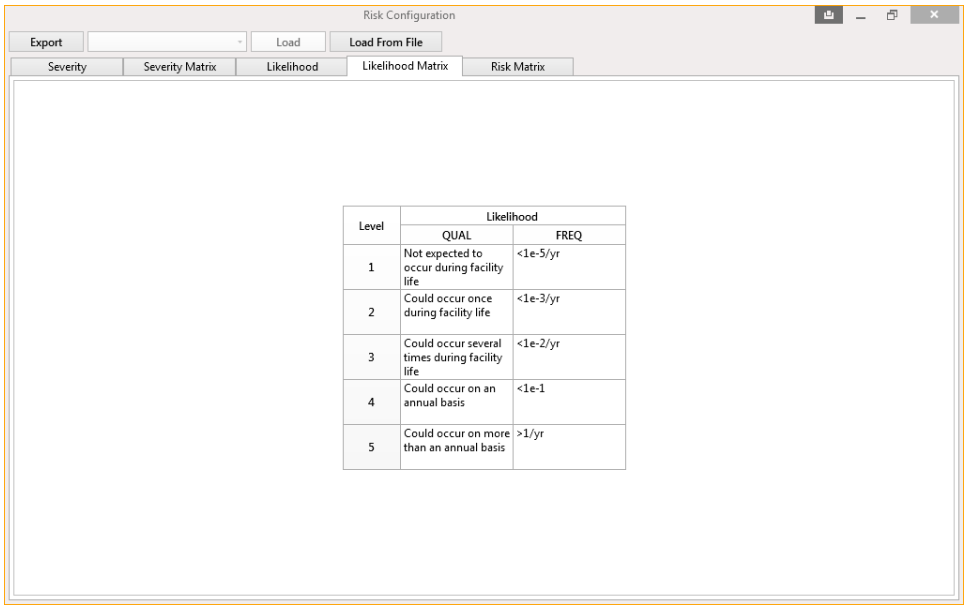
1. In the ***Risk Configuration*** window select the ***Likelihood*** Tab
2. The information initially shown is the exida default risk matrix (unless you selected the *create an empty project* option when starting this project in which case all entries will be blank).
3. Likelihood categories can be added or deleted by using the plus (**+**) or minus (**-**) symbols in the lower left corner of the left window pane.
4. You can edit the default information for likelihood category *Code*, *Name*, and *Description* or enter the relevant information for likelihood categories you may have added.
5. Likelihood levels can be added or deleted by using the plus (**+**) or minus (**-**) symbols in the lower left corner of the right window pane.
6. You can edit the default information for likelihood level *Code* and *Name* or enter the relevant information for likelihood levels you may have added.



8.4 Likelihood Matrix

The fourth task in specifying the project risk matrix is to define the applicable likelihood matrix. To do so use the following steps:

1. Ensure you specified all relevant information on the Likelihood Tab (see section *8.3 Likelihood Categories and Levels*)
2. In the ***Risk Configuration*** window select the ***Likelihood Matrix*** Tab
3. The information initially shown is part of the exida default risk matrix (unless you selected the *create an empty project* option when starting this project in which case the likelihood matrix will be blank).
4. The Likelihood Matrix matches likelihood levels to likelihood categories. The matrix is prepopulated based on the on the information you specified on the likelihood tab.
5. You can edit the information in the matrix cells or enter the relevant information as applicable.

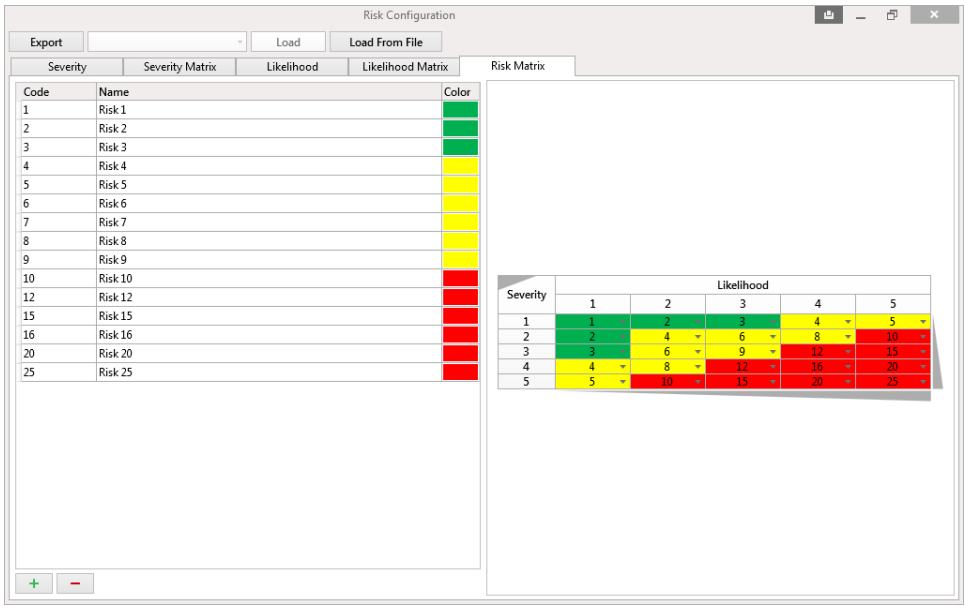


Level	Likelihood	
	QUAL	FREQ
1	Not expected to occur during facility life	<1e-5/yr
2	Could occur once during facility life	<1e-3/yr
3	Could occur several times during facility life	<1e-2/yr
4	Could occur on an annual basis	<1e-1
5	Could occur on more than an annual basis	>1/yr

8.5 Risk Matrix

The final task in specifying the project risk matrix is to combine the consequence/severity and likelihood matrices. To do so use the following steps:

1. Ensure you specified all relevant information for the Severity and Likelihood Matrices (see section *8.2* and *8.4*)
2. In the ***Risk Configuration*** window select the ***Risk Matrix*** Tab
3. The information initially shown is part of the exida default risk matrix (unless you selected the *create an empty project* option when starting this project in which case the severity matrix will be blank).
4. The Risk Matrix is prepopulated based on the on the information you specified for the severity and likelihood levels.
5. Risk levels can be added or deleted by using the plus (**+**) or minus (**-**) symbols in the lower left corner of the window.
6. You can edit the default information for risk *Code* and *Name*or enter the relevant information for risk level you may have added. Next you can specify a *Color* that represents the risk level by double clicking the color box and making the appropriate selection.
7. Within the Risk Matrix shown in the right window pane, each cell is a drop down box. You can select the appropriate Risk Level for each matrix cell based on the risk levels defined in the left window pane.
8. The severity and likelihood axis of the risk matrix can independently be set in an ascending or descending order by clicking on the gray triangle at the right side and/or bottom of the risk matrix respectively.
9. The severity and likelihood axis can be swapped by clicking on the gray triangle in the upper left hand portion of the Risk Matrix.

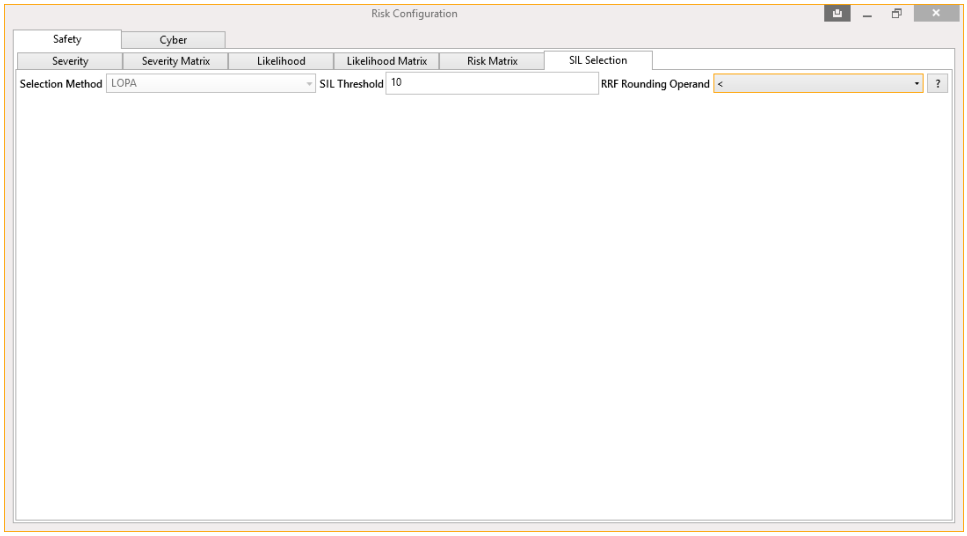


8.6 SIL Selection

For users who will eventually perform Safety Integrity Level target selection, the selection method and its associated parameters must be specified as part of the risk configuration. To do this click on the SIL Selection tab.

For the Layer Of Protection Analysis (LOPA) based SIL target selection method there are two parameters that can be specified:

- SIL Threshold
- RRF Rounding Operand



Both parameters are descried below and relate to the range of risk reduction factors associated with each SIL as shown in the following figure.

SIL	Target PFD_{AVG}	Target RRF
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10,000 to ≤ 100,000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1,000 to ≤ 10,000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤ 1,000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤ 100

8.6.1 SIL Threshold

The SIL Threshold parameter determines how the required risk reduction is translated into a Target SIL given the range of Risk Reduction that is presented by each SIL level.

In an advanced quantitative LOPA, where initiating event frequencies and IPL probability of failures are not quantified in whole orders of magnitude, a resulting required risk reduction factor could be any value within the SIL range. For example, a calculated required risk reduction of 45 lies within the SIL 1 range. One could conclude that therefore the target SIL is 1. However a conceptual design engineer seeing a target SIL of 1, could develop a Safety Instrumented Function that meets the requirements of SIL 1, but only achieves a risk reduction of 20. This solution would not provide enough risk reduction.. Therefore, the correct way to communicate the actual requirement is to tell the conceptual design engineer that the target SIL of 1 includes a minimum risk reduction of 45, i.e. SIL 1 + RRF > 45. For users who do not want to communicate the additional RRF requirement, the target SIL could also be communicated as SIL 2.

The SIL Threshold allows you to specify at what point you want to include the RRF requirement and at what point you want to specify the next higher SIL level. The default SIL Threshold of 10, will not increase the target SIL and always include the required risk reduction factor. A SIL threshold at the lower boundary of 1, would always specify the next higher SIL level. Within exSILentia® users can choose any integer value between 1 and 10 for their SIL threshold setting.

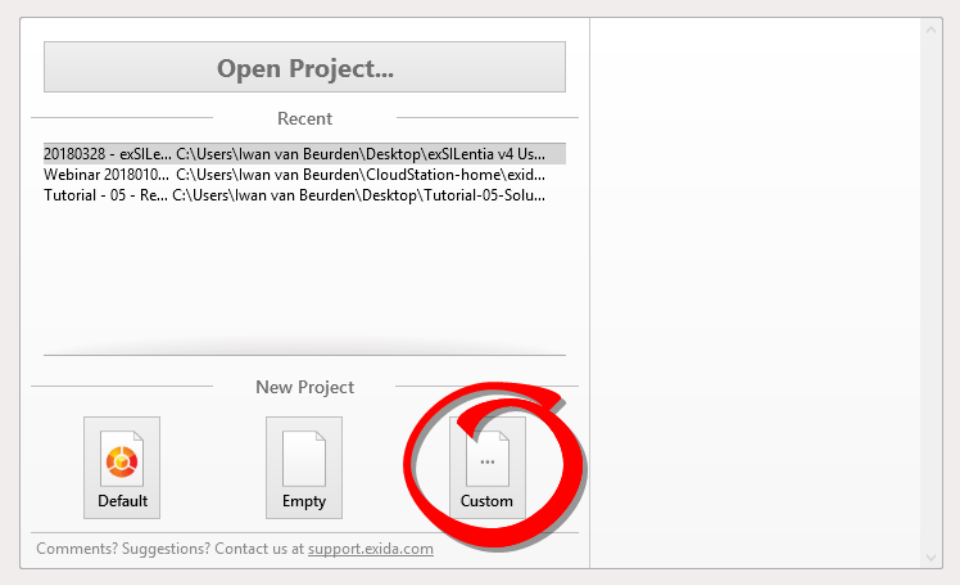
8.6.2 RRF Rounding Operand

The RRF Rounding Operand parameter determines how the required risk reduction is translated into a Target SIL given the upper limit of the Risk Reduction range presented by each SIL level.

Looking at the ranges of risk reduction to the SIL level, one would notice that as the RRF is the reciprocal value of PFD_{AVG}, a Risk Reduction Factor of 100 is still considered within the SIL 1 range. However, within the process industry, a RRF of 100 is typically equated to the lower limit of SIL 2. Within the exSILentia® risk configuration, users can choose if a required risk reduction of 100 should be considered as a target SIL 1 or a target SIL 2 by choosing the RRF Rounding Operand as "≤"or "<"respectively. The default RRF Rounding Operand is "<".

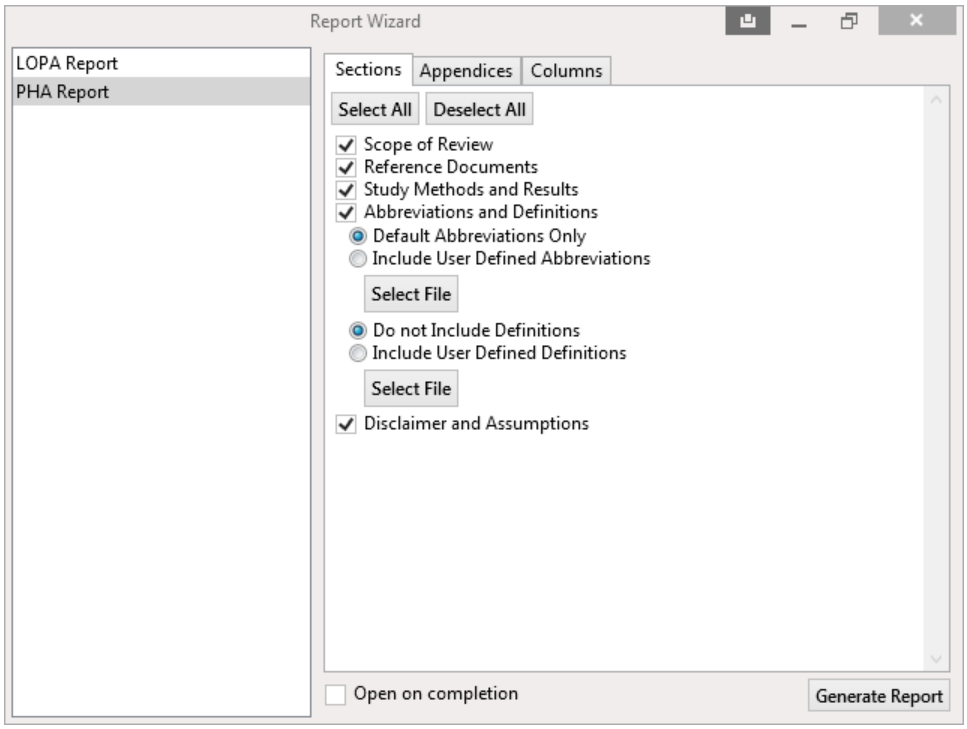
8.7 Risk Configuration Reuse

Being able to reuse a project Risk Configuration can save a significant amount of time when defining a new project. At the same time changing a risk configuration in the middle of a project can have a dramatic impact. When using exSILentia® v4 there is an easy way to prepare the risk configuration for a new project based on the risk configuration of an existing project. When creating a new project, simply select the ***Custom*** option for the new project. This will allow you to select an existing project that both the project configuration and risk configuration will be based on. None of the project details will be copied only the project and risk configuration information will be transferred to the new project.

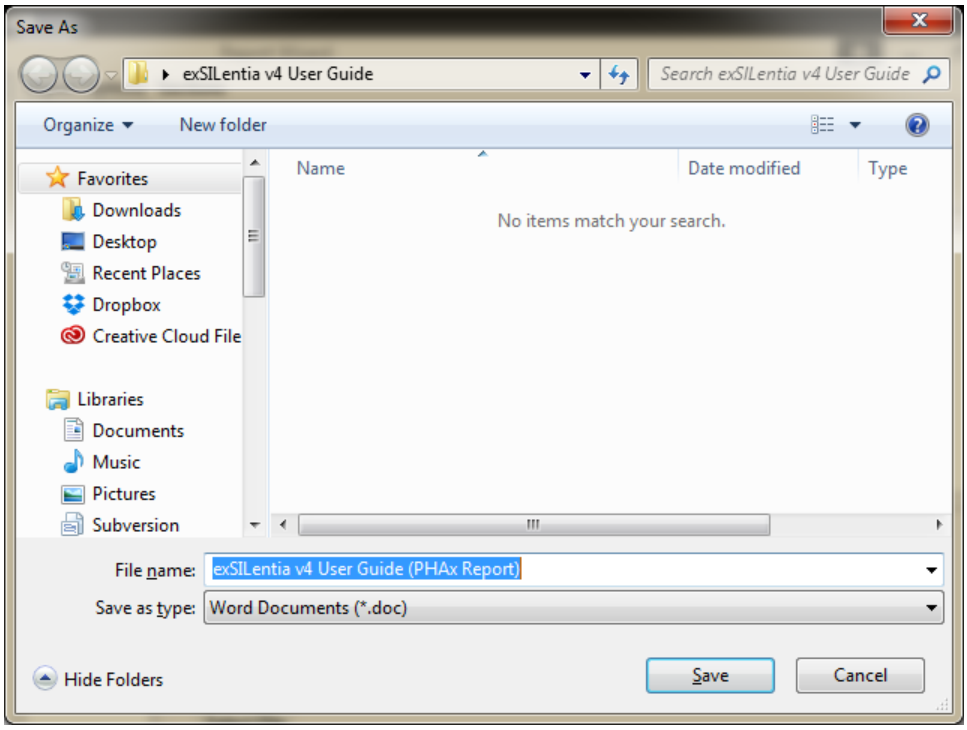


Chapter 9 Report Generation

To generate a report output for your project you can click on the ***Generate Report*** button on the exSILentia® v4 dashboard or you can select Generate Report from the ***Export*** menu. This will launch the Report Wizard.



The Report Wizard will allow you to select the report you want to generate. In addition through the Report Options selections you can control what sections are included within the report. Once you completed making all appropriate report option selections you can click the ***Generate Report*** button in the lower right hand portion of the Report Wizard window. This will open the Save As dialog and prompt you with a default name which is based on the project file name.



If the ***Launch Associated Viewer*** checkbox (to the left of the *Generate Report* button) was checked it will automatically open the generated report.

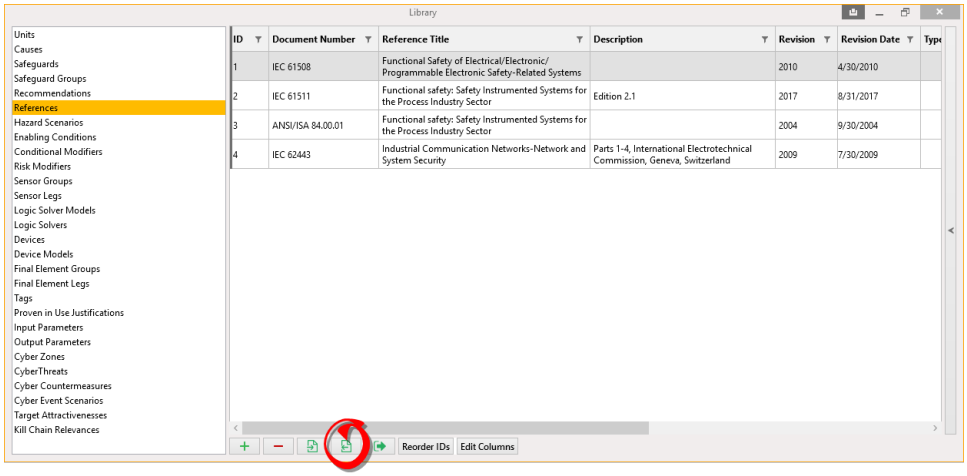
Specific exSILentia® v4 tool report generation is described in each tool's detailed functionality description.

Chapter 10 Data Import

exSILentia® v4 supports data imports into the Library. An overview is provided below.

10.1 Library Import

exSILentia® v4 supports data import into the various libraries as defined in *Chapter 7 Project Libraries*. The library imports (as well as exports) use a Microsoft Excel .xlsx worksheet as the interface. The import feature will create a new item for each row that exists within the .xlsx file, regardless if the same named item already exists. The import feature is available using the highlighted button below which is available for each library. To import click the import button of the specific library and select the import file using the file browser that appears.



Note: The easiest way to ensure your import format conforms with what exSILentia® v4 is expecting, it is best to export from the desired library and use this exported file as the template to create the import file. The text of certain fields must match what is expected or the field will not import.

The following screen shot shows a Microsoft Excel worksheet, prepared as an import file for the hazard scenario library. The first row contains the column headings and the subsequent rows contain the data to be imported. Notice column D which communicates a Boolean value of Yes/No regarding the completeness of the LOPA. You must follow this format of TRUE or FALSE in this case to represent Yes/No to ensure correct import into the exSILentia® v4 hazard scenario library.

	A	B	C	D	E	F
1	ID	Name	Description	Is LOPA Complete?	LOPA Comments	
2	1	Runaway Reaction from Decomposition		FALSE		
3						
4						
5						
6						
7						
8						

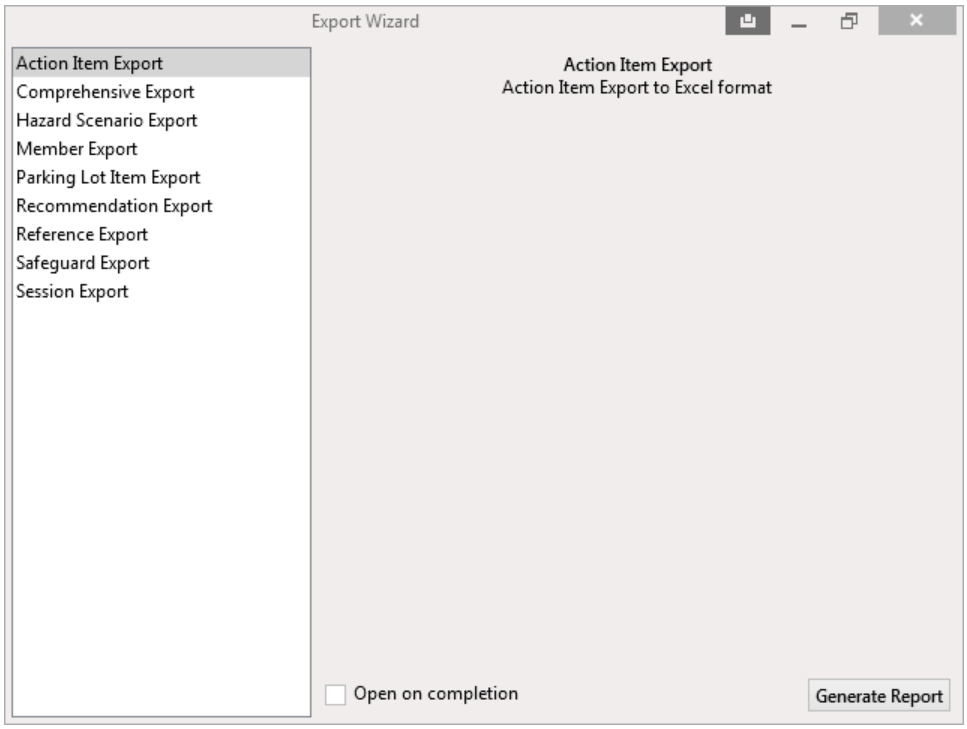
CAUTION: The headings of the Microsoft Excel .xlsx file to be imported must match what is expected for the given library. Importing into the incorrect library will yield unanticipated results.

Chapter 11 Data Export

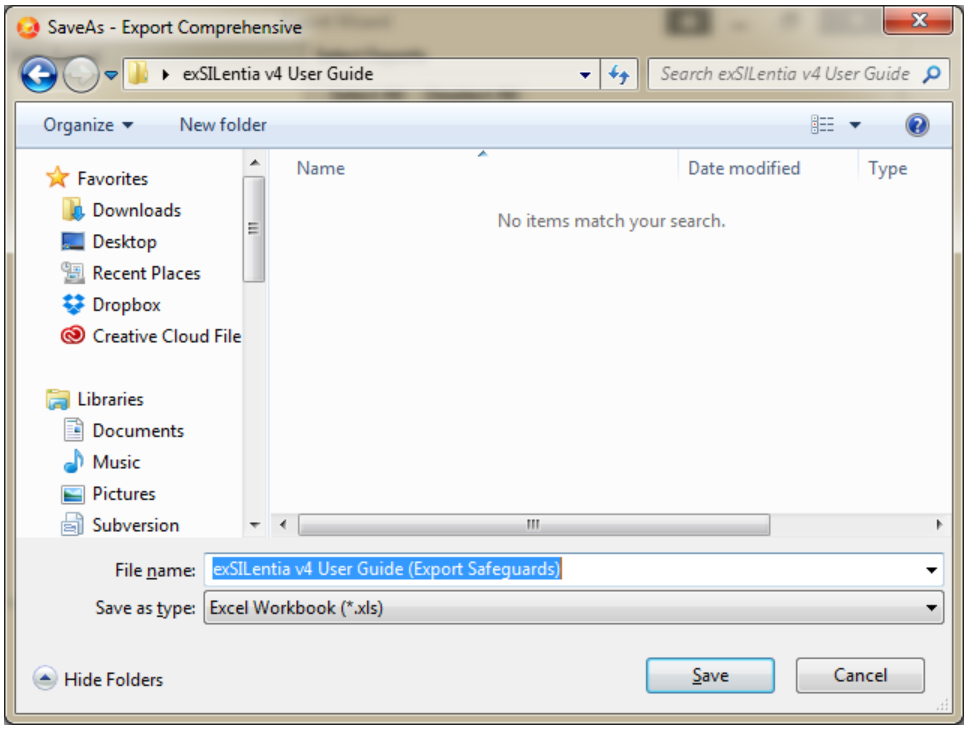
exSILentia® v4 supports two types of data export. Direct Exports which will export data from your project using predefined export templates and Library Exports. An overview of both is provided below.

11.1 Direct Export

To export data from your project using predefined export templates, you can click on the ***Data Export*** button on the exSILentia® v4 dashboard or you can select Export Data from the ***Export*** menu. This will launch the Export Wizard.



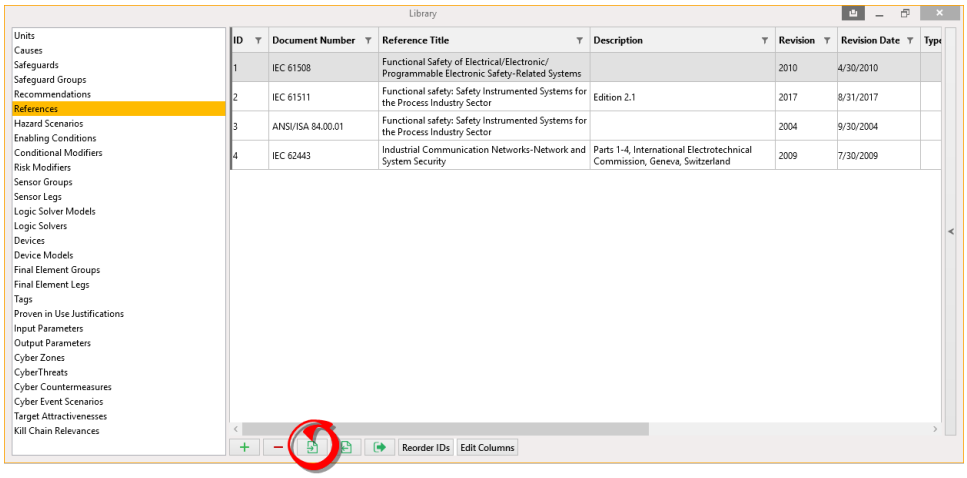
The Export Wizard will allow you to select what data you want to export. The Comprehensive Export will create a single workbook with separate worksheets for Safeguards, Recommendations, Members, Action Items, References, and Sessions. Once you make the appropriate data export selections you can click the ***Export*** button in the lower right hand portion of the Export Wizard window. This will open the Save As dialog and prompt you with a default name which is based on the project file name.



Specific exSILentia® v4 tool data export is described in each tool's detailed functionality description.

11.2 Library Export

exSILentia® v4 supports data export from the various libraries as defined in *Chapter 7 Project Libraries*. The library exports (as well as imports) use a Microsoft Excel .xlsx worksheet as the interface. The export feature exports all items within the selected library. The export feature is available using the highlighted button below which is available for each library. To export click the export button of the specific library and specify the file name on the save as dialog that appears.

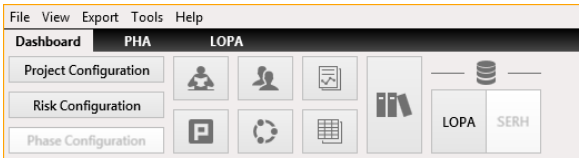


Chapter 12 Embedded Databases

Consistency and efficiency during the execution of the various Safety Lifecycle tasks revolves around the use and availability of reliability data. exSILentia® is equipped with two embedded databases. These are:

- LOPA database
- SERH database

The embedded databases are accessible through the respective tools that they are used in. In addition they can be accessed from the exSILentia® v4 Dashboard.



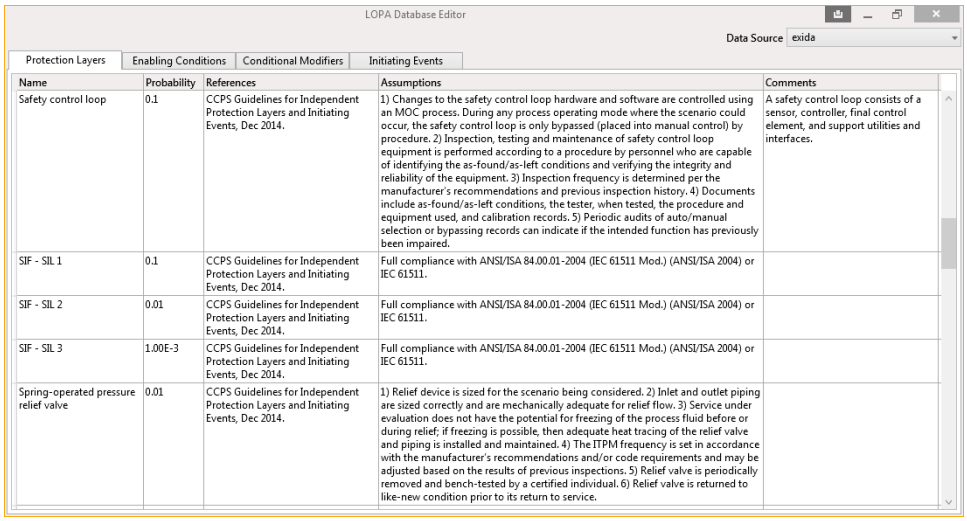
12.1 LOPA Database

exSILentia® v4 provides an embedded LOPA database. The LOPA database provides a mechanism to store properties, like assumptions, references, and data, for different Initiating Events, Enabling Conditions, Independent Protection Layers, and Conditional Modifiers. These properties can easily be (re-)used throughout the various LOPA worksheets. When a database item is referenced in the LOPA worksheet, the properties of the database item are copied to the LOPA worksheet item. Any changes to the database item will not be propagated to the LOPA worksheet. Therefore a database change will not impact previous work performed.

The LOPA database contains three sub-databases/data sources. These are:

- exida
- Generic
- User Defined Data

You can access the LOPA database by clicking on the LOPA icon on the exSILentia® v4 Dashboard. On the LOPA Database Editor dialog you can switch between the different data sources through the drop down list on the upper right hand side of the database dialog. You can also switch between the different data item types, e.g. protection layers, enabling conditions, conditional modifiers, and initiating events using the tabs on the dialog.


LOPA Database Editor

Data Source exida

Protection Layers | Enabling Conditions | Conditional Modifiers | Initiating Events

Name	Probability	References	Assumptions	Comments
Safety control loop	0.1	CCPS Guidelines for Independent Protection Layers and Initiating Events, Dec 2014.	1) Changes to the safety control loop hardware and software are controlled using an MOC process. During any process operating mode where the scenario could occur, the safety control loop is only bypassed (placed into manual control) by procedure. 2) Inspection, testing and maintenance of safety control loop equipment is performed according to a procedure by personnel who are capable of identifying the as-found/as-left conditions and verifying the integrity and reliability of the equipment. 3) Inspection frequency is determined per the manufacturer's recommendations and previous inspection history. 4) Documents include as-found/as-left conditions, the tester, when tested, the procedure and equipment used, and calibration records. 5) Periodic audits of auto/manual selection or bypassing records can indicate if the intended function has previously been impaired.	A safety control loop consists of a sensor, controller, final control element, and support utilities and interfaces.
SIF - SIL 1	0.1	CCPS Guidelines for Independent Protection Layers and Initiating Events, Dec 2014.	Full compliance with ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) (ANSI/ISA 2004) or IEC 61511.	
SIF - SIL 2	0.01	CCPS Guidelines for Independent Protection Layers and Initiating Events, Dec 2014.	Full compliance with ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) (ANSI/ISA 2004) or IEC 61511.	
SIF - SIL 3	1.00E-3	CCPS Guidelines for Independent Protection Layers and Initiating Events, Dec 2014.	Full compliance with ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) (ANSI/ISA 2004) or IEC 61511.	
Spring-operated pressure relief valve	0.01	CCPS Guidelines for Independent Protection Layers and Initiating Events, Dec 2014.	1) Relief device is sized for the scenario being considered. 2) Inlet and outlet piping are sized correctly and are mechanically adequate for relief flow. 3) Service under evaluation does not have the potential for freezing of the process fluid before or during relief; if freezing is possible, then adequate heat tracing of the relief valve and piping is installed and maintained. 4) The ITPM frequency is set in accordance with the manufacturer's recommendations and/or code requirements and may be adjusted based on the results of previous inspections. 5) Relief valve is periodically removed and bench-tested by a certified individual. 6) Relief valve is returned to like-new condition prior to its return to service.	

12.1.1 exida LOPA Database

The exida LOPA database is a read-only database with initiating event frequencies and independent protection layer probabilities of failure on demand. The data is evaluated by exida and deemed applicable for use in process industry layer of protection analysis. The exida LOPA database is automatically installed on your system with the exSILentia® v4 installation. Updates to this database will be included in exSILentia® v4 updates. Note that there is no data specified for enabling conditions and conditional modifiers in the exida LOPA database as these are application specific.

12.1.2 Generic LOPA Database

The Generic LOPA database is one of two databases that you as a user can define. The Generic LOPA database is a database that resides on the computer that exSILentia® v4 is installed on. Any data item, initiating event, enabling condition, independent protection layer, or conditional modifier, that you define in the Generic LOPA database will be available for all exSILentia® v4 projects that you perform on the particular computer. When you open your exSILentia® v4 project on a different computer with a fresh install of exSILentia® v4, the database items properties will still be available if you referenced the database item in the LOPA Worksheet, however the database item will no longer show up as a item you can reference from the database. Your LOPA worksheet calculations will not be affected.

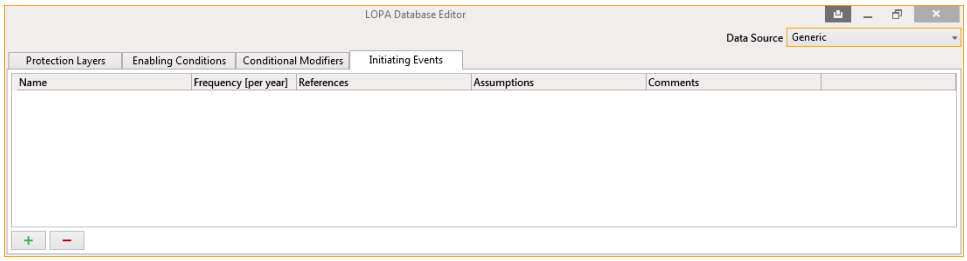
The Generic LOPA Database file is automatically stored in the ..\Documents\exida\exSILentia 4\generic.lopadb location. You can copy the generic.lopadb file to a different machine to ensure the same user defined LOPA database is available for use in that specific exSILentia® v4 installation.

12.1.3 User Defined Data LOPA Database

The User Defined Data LOPA Database is the second database that you as a user can define. In contrast to the Generic LOPA database, the User Defined Data database is embedded within the specific exSILentia® v4 project file. Therefore when you open the project file on a different computer, the same database items will be available as on the original computer the project was created on. On the other hand when you create a new project the database items from the User Defined Data LOPA database will no longer exist. This functionality is specifically intended for projects with a project specific LOPA database.

12.1.4 Managing LOPA Database Items

You can review LOPA database entries by clicking on the LOPA icon on the exSILentia® v4 Dashboard which will launch the LOPA Database Editor dialog. When you select the Generic LOPA database or User Defined Data LOPA Database Data Source you will be able to maintain the respective entries, i.e. add, modify or delete a database items. The management of a protection layer, enabling condition, conditional modifier, or initiating event database item is identical, you just need to make sure you have selected the appropriate LOPA Database tab.



To add a Database Item to the LOPA database:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Edit the Database Item Properties directly in the grid layout, i.e. *Name*,*Frequency* or *Probability*, *Reference*, *Assumptions*, and *Comments*

To modify a Database Item in the library:

- Highlight the Database Item
- Edit the Database Item Properties directly in the grid layout, i.e. *Name*,*Frequency* or *Probability*, *Reference*, *Assumptions*, and *Comments*

To delete a Database Item from the library:

- Highlight the Database Item
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Database Item and its Properties

12.2 SERH Database

exSILentia® v4 provides an embedded safety equipment failure rate database for use in SIL verification. The exida Safety Equipment Reliability Handbook (SERH) provides a collection of failure rate data that is applicable for use in Safety Instrumented System (SIS) conceptual design verification in the process industry. The Safety Equipment Reliability Handbook is the ultimate reference source for any safety engineer involved in Conceptual Design and Safety Integrity Level verification. The set comes in three different volumes

Volume 01: Sensors

This includes Fire and Gas, Flame Monitoring, Flow, Level, Pressure, Proximity, and Temperature measurements

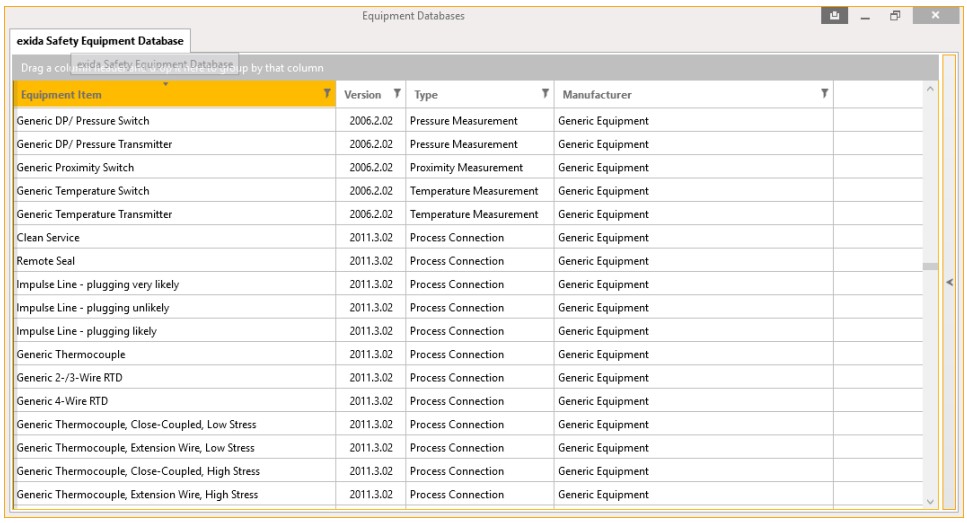
Volume 02: Logic Solvers and Interface Modules

This includes Barriers, Surge protection devices, Relays, logic solvers, Fire and Gas Systems, and solenoid drivers

Volume 03: Final Elements

This includes Final Element interfaces such as solenoids and digital valve positioners, Pneumatic interfaces such as Quick Exhaust valves, Actuators, Valves such as ball, butterfly, gate, etc. valves, and Gas Pressure Regulating Valves.

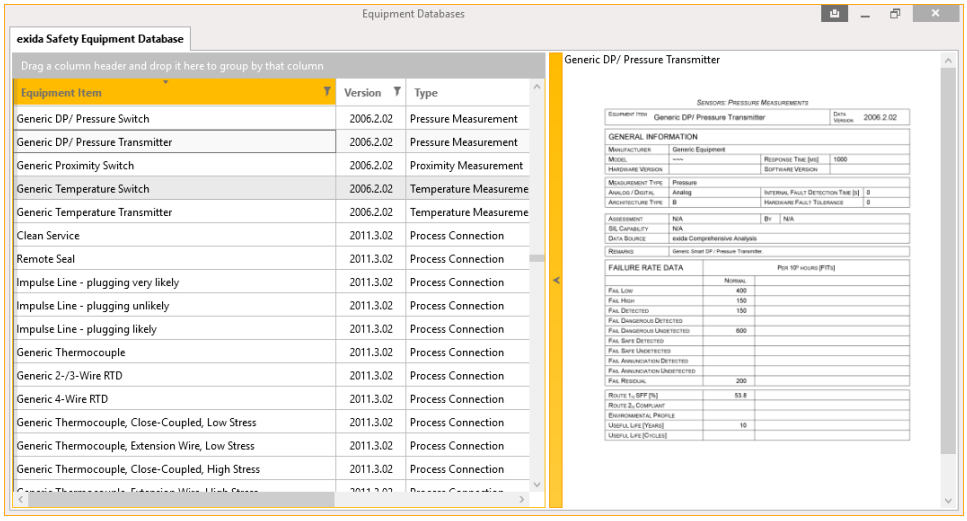
You can access the SERH database by clicking on the SERH icon on the exSILentia® v4 Dashboard. This will launch the SERH database window. Within the window you can search, sort, filter etc. to view the equipment items in the database.


Equipment Databases

exida Safety Equipment Database

Equipment Item	Version	Type	Manufacturer
Generic DP/ Pressure Switch	2006.2.02	Pressure Measurement	Generic Equipment
Generic DP/ Pressure Transmitter	2006.2.02	Pressure Measurement	Generic Equipment
Generic Proximity Switch	2006.2.02	Proximity Measurement	Generic Equipment
Generic Temperature Switch	2006.2.02	Temperature Measurement	Generic Equipment
Generic Temperature Transmitter	2006.2.02	Temperature Measurement	Generic Equipment
Clean Service	2011.3.02	Process Connection	Generic Equipment
Remote Seal	2011.3.02	Process Connection	Generic Equipment
Impulse Line - plugging very likely	2011.3.02	Process Connection	Generic Equipment
Impulse Line - plugging unlikely	2011.3.02	Process Connection	Generic Equipment
Impulse Line - plugging likely	2011.3.02	Process Connection	Generic Equipment
Generic Thermocouple	2011.3.02	Process Connection	Generic Equipment
Generic 2-/3-Wire RTD	2011.3.02	Process Connection	Generic Equipment
Generic 4-Wire RTD	2011.3.02	Process Connection	Generic Equipment
Generic Thermocouple, Close-Coupled, Low Stress	2011.3.02	Process Connection	Generic Equipment
Generic Thermocouple, Extension Wire, Low Stress	2011.3.02	Process Connection	Generic Equipment
Generic Thermocouple, Close-Coupled, High Stress	2011.3.02	Process Connection	Generic Equipment
Generic Thermocouple, Extension Wire, High Stress	2011.3.02	Process Connection	Generic Equipment

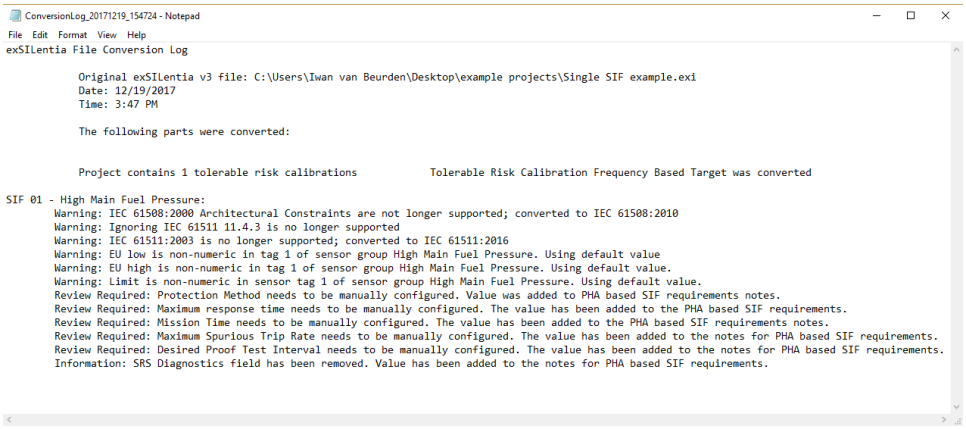
By expending the right hand side bar, you will be able to view the SERH data page for the equipment item that you selected.



Chapter 13 Upgrading from exSILentia® v3

This chapter provides an overview of differences between the exSILentia® v3 and exSILentia® v4 software. exSILentia® v4 can open exSILentia® v3 format project files, but will at that point convert the project information to the new exSILentia® v4 format. In most cases the conversion is one-to-one between the two versions of the software, however in some cases the structure of the two versions differ which require a specific conversion algorithm to be implemented. For each of the exSILentia® v3 tools an overview is provided on how information is converted for which there is no direct one-to-one relationship with an exSILentia® v4 data item.

When you upgrade your exSILentia® v3 project to the exSILentia® v4 format, a log will be created of all conversion actions taken. The log will be embedded as a reference in the exSILentia® v4 project. In addition the original exSILentia® v3 project file will be embedded as a reference as well.


ConversionLog_20171219_154724 - Notepad

File Edit Format View Help

```
exSILentia File Conversion Log

            Original exSILentia v3 file: C:\Users\Iwan van Beurden\Desktop\example projects\Single SIF example.exi
            Date: 12/19/2017
            Time: 3:47 PM

            The following parts were converted:


            Project contains 1 tolerable risk calibrations           Tolerable Risk Calibration Frequency Based Target was converted

SIF 01 - High Main Fuel Pressure:
        Warning: IEC 61508:2000 Architectural Constraints are not longer supported; converted to IEC 61508:2010
        Warning: Ignoring IEC 61511 11.4.3 is no longer supported
        Warning: IEC 61511:2003 is no longer supported; converted to IEC 61511:2016
        Warning: EU low is non-numeric in tag 1 of sensor group High Main Fuel Pressure. Using default value
        Warning: EU high is non-numeric in tag 1 of sensor group High Main Fuel Pressure. Using default value.
        Warning: Limit is non-numeric in sensor tag 1 of sensor group High Main Fuel Pressure. Using default value.
        Review Required: Protection Method needs to be manually configured. Value was added to PHA based SIF requirements notes.
        Review Required: Maximum response time needs to be manually configured. The value has been added to the PHA based SIF requirements.
        Review Required: Mission Time needs to be manually configured. The value has been added to the PHA based SIF requirements notes.
        Review Required: Maximum Spurious Trip Rate needs to be manually configured. The value has been added to the notes for PHA based SIF requirements.
        Review Required: Desired Proof Test Interval needs to be manually configured. The value has been added to the notes for PHA based SIF requirements.
        Information: SRS Diagnostics field has been removed. Value has been added to the notes for PHA based SIF requirements.
```

13.1 General Project Information

The following table lists exSILentia® v3 general project information fields that are no longer supported in exSILentia® v4. The table also documents the conversion action applied on these fields.

exSILentia® v3 Field	Conversion Action
Company	The company name is added to the Project Description.
Project Leader	A Team Member is created. The leader flag is set for the team member. The first space in the Project Leader text field is interpreted as the separator between first name and last name.
Project Initiated	The project start date is added to the Project Description.

13.2 Process Hazard Analysis (PHA)

There are two aspects to conversion of PHA information from exSILentia® v3. The conversion of the standalone tool information and conversion of PHA information available within exSILentia® v3.

13.2.1 PHAx™ v2

The PHAx™ component of exSILentia® v3 was available as a standalone product. This standalone product was PHAx™ v2. To convert a PHAx™ v2 project to the exSILentia® v4 PHAx module, simply open a PHAx™ v2 project file. On the project open dialog, see section *3.2 Launching the Program*, select the *PHAx 2 Project (.pxi)* file type and then select the appropriate project file.

The PHAx™ v2 project information is completely converted to exSILentia® v4.

13.2.2 exSILentia® v3 PHA Tab

The information on the exSILentia® v3 PHA tab is a result of importing PHA data from for example PHAx™ v2. As this information is not directly linked to a PHA, none of the information is imported in to exSILentia® v4.

13.3 SIF Identification

In exSILentia® v4, Safety Instrumented Functions are *Safeguards* of type *Independent Protection Function* (IPF) that are marked as SIF. For each SIF identified in the exSILentia® v3 project, a safeguard is created of type IPF with the **Is SIF** checkbox checked. During the conversion process, the exSILentia® v3 SIF Identification information is transferred to the relevant Safeguard.

13.4 SIL Target Selection (SILect™)

The SILect™ tool has seen the most dramatic change going from exSILentia® v3 to exSILentia® v4. The main changes in v4 include:

- In v4 there is one tolerable risk specification per Risk Category (Safety, Environmental, Business, etc) option for the Layer of Protection Analysis method.
- In v4 there is one SIL Target Selection method hazard scenario, i.e. Risk Matrix, Risk Graph, or Frequency Based Targets.
- In v4 the Layer of Protection Analysis functionality extracted into standalone LOPA tool, with the SIL Selection step finalized in SILect.

The changes to the SILect™ tool structure and their impact if any are described in the following sections.

13.4.1 Multiple Tolerable Risk Calibration

For exSILentia® v3 projects that have multiple tolerable risk calibrations defined, the exSILentia® v3 to exSILentia® v4 conversion will determine which tolerable risk calibration method was used most. This will be set as the method according to which the conversion will be executed. SILect™ selections for SIFs that were made using a different method within the exSILentia® v3 project will not be transferred to exSILentia® v4. The affected SIFs will be identified in the conversion log for further evaluation.

13.4.2 Risk Graph

exSILentia® v4 supports the Risk Graph SIL Target Selection method. When converting an exSILentia® v3 project that uses the Risk Graph SIL Target Selection method, the Risk Graph tolerable risk calibration and individual SIF selections will be placed in a temporary container, embedded in the project file.

13.4.3 Hazard Matrix

The exSILentia® v3 Hazard Matrix tolerable risk calibration is directly copied into the exSILentia® v4 Risk Configuration Risk Matrix. The Hazard Matrix method is renamed to Risk Matrix. To review the exSILentia® v4 Risk Configuration click on the Risk Configuration button on the Dashboard, see *Chapter 8 Project Risk Configuration*.

The exSILentia® v4 SILect™ module supports the Risk Matrix SIL Target Selection method. When converting an exSILentia® v3 project that uses this SIL Target Selection method, the individual SIF selections will be placed in a temporary container, embedded in the project file. Upon release of the SILect™ module the data conversion will be completed.

13.4.4 Frequency Based Targets/LOPA Tolerable Risk Calibration

The exSILentia® v3 Frequency Based Targets/LOPA SIL Target Selection methods are all converted to the exSILentia® v4 Risk Configuration as described in section *8.1 Consequence Categories and Severity Levels*. Each of the six methods available in exSILentia® v3 specify a tolerable frequency based on a severity level selection. As such when converting the Frequency Based Target (FBT) tolerable risk calibration, only the Severity Categories, Severity Levels, and Severity Matrix will be specified. The resulting exSILentia® v4 Risk Configuration will have no Likelihood settings. For each of the risk receptors defined in exSILentia® v3 that are included in the tolerable risk calibration a Severity Category is created.

The SIL Threshold parameter specified with each FBT tolerable risk calibration is converted to a SILect™ phase parameter, outside of the exSILentia® v4 Risk Configuration.

Linear Tolerable Risk

The *Health and Safety Executive*, *IEC 61511-3, Annex D, E*, and *Single Tolerable Risk Quantitative* FBT tolerable risk calibration options are all covered by the Linear Tolerable Risk conversion. These tolerable risk calibrations are not a direct fit for the exSILentia® v4 Risk Configuration as they only specify a single target frequency. The actual severity levels are defined through a combination of individual event consequence and a risk tolerance set per year for each risk receptor. For the conversion of these tolerable risk calibrations all Severity Levels are determined for each risk receptor while determining the associated tolerable frequency. For each unique tolerable frequency a Severity Level is defined in the exSILentia® v4 Risk Configuration. Though the conversion results in an exact match, it is recommended that you review your SIL Target Selection results upon completion of the conversion.

Single Tolerable Risk Qualitative

The Qualitative option of the Single Tolerable Risk calibration option is a close fit for the exSILentia® v4 Risk Configuration. In the conversion a fixed set of 7 Severity Levels is created. The weight factors specified for the personnel category are used to calculate the tolerable frequency for each severity level. Generic descriptions are used of the severity level names. If weight factors differ for the different risk receptors, you should review your SIL Target Selection results upon completion of the conversion.

Tolerable Risk Categories (Qualitative)

The Qualitative option of the Tolerable Risk Categories is a direct fit for the exSILentia® v4 Risk Configuration. Tolerable risk calibration level descriptions are directly copied into the exSILentia® v4 project.

Tolerable Risk Categories (Quantitative)

The Quantitative option of the Tolerable Risk Categories is a close fit for the exSILentia® v4 Risk Configuration. The Personnel Fatalities and Personnel Injuries risk receptors are combined into 1 Severity Category. Tolerable risk calibration level descriptions are directly copied into the exSILentia® v4 project.

13.4.5 Frequency Based Targets/LOPA Target SIL Selections

The exSILentia® v3 Frequency Based Targets/LOPA SIL Target Selections match directly to the exSILentia® v4 LOPAx™ worksheet, see section *D.2 LOPA Worksheet*. The main difference between the exSILentia® v3 Frequency Based Targets/LOPA SIL Target Selections and the exSILentia® v4 LOPAx™ worksheet from a conversion perspective is how the Independent Protection Layer (IPL) effectiveness for different Severity Categories is identified. In exSILentia® v3 one can set different Probability of Failure on Demand (PFD), or Risk Reduction Factor (RRF), for each of the different risk receptors (Severity Categories), In exSILentia® v4 there is only one probability of failure, or risk reduction factor, per IPL. The IPL is then either flagged as effective of ineffective for a specific Severity Category.

During the conversion if the PFD of an IPL is set to 1, it is assumed that the IPL is not effective for that specific Severity Category. If the PFD is less than 1, it is set as effective for that specific Severity Category and the value of the PFD specified for the Personnel Risk Receptor is used to define the IPL probability of failure. If you used different probability of failure smaller than 1 for an IPL, you should review your SIL Target Selection results upon completion of the conversion.

Since exSILentia® v3 did not distinguish in the user interface between Independent Protection Layers and Conditional Modifiers, all IPLs are converted as if they are IPLs. You will need to manually move IPLs to the Conditional Modifier category if so desired.

13.5 Safety Requirements Specification

The exSILentia® v3 Safety Requirements Specification will be documented through the combination of Process SRS and Design SRS. In exSILentia® v4 the SIF SRS is replaced by the equivalent of the exSILentia® v3 Process SRS, thought the functionality of the exSILentia® v4 SRS is drastically expanded. The Design SRS has become and separate module in exSILentia® v4.

13.5.1 SIF SRS

The following table lists exSILentia® v3 SIF SRS fields that are no longer supported in exSILentia® v4 or whose type changed from exSILentia® v3 to exSILentia® v4. The table also documents the conversion action applied on these fields.

exSILentia® v3 Field	Conversion Action
SIF Test Interval	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Overall Response Time	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Protection Method	Changed from text field to toggle field with options ***de-energize to trip*** and ***energize to trip***. Selection set to ***de-energize to trip***, the v3 field text is added to the Notes.
Max. Spurious Trip Rate	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Diagnostics	The diagnostic description is added to the Notes.
Notes	Added text from fields where a type change occurred from v3 to v4.
Sensor Part Description	The sensor part description is added to the Input / Output Functional Relationship field.
Logic Solver Part Description	The logic solver part description is added to the Input / Output Functional Relationship field.
Final Element Part Description	The final element part description is added to the Input / Output Functional Relationship field.

The following table lists exSILentia® v3 SIF SRS fields that have been renamed or redefined in exSILentia® v4. The core functionality of these fields has not been affected, the name and/or functionality has been improved.

exSILentia® v3 Field	exSILentia® v4 Field
SIF Test Interval	Desired Proof Test Interval Sensor Part Desired Proof Test Interval Logic Solver Part Desired Proof Test Interval Final Element Part
Overall Response Time	Maximum Response Time SIF
Sensor Part Description Logic Solver Part Description Final Element Part Description	Input / Output Functional Relationship

13.5.2 Process SRS (SRS$^{C\&E}$)

The exSILentia® v3 Process SRS consists of three main topics, General SIS Requirements, General SIF Requirements, and SIF Specific (PHA based) Requirements.

General SIS Requirements

The following table lists exSILentia® v3 Process SRS General SIS Requirements fields that are no longer supported in exSILentia® v4 or whose type changed from exSILentia® v3 to exSILentia® v4. The table also documents the conversion action applied on these fields.

exSILentia® v3 Field	Conversion Action
Action on Logic Solver Fault Detection	Added boiler plate text to field text.

exSILentia® v3 Field	Conversion Action
Environment Conditions	The boiler plate text and environment conditions text is added to the Other Environmental Extremes field.
Interior Equipment Environment	The interior equipment environment conditions text is added to the Other Environmental Extremes field.
Exterior Equipment Environment	The exterior equipment environment conditions text is added to the Other Environmental Extremes field.

The following table lists exSILentia® v3 Process SRS General SIS Requirements fields that have been renamed or redefined in exSILentia® v4. The core functionality of these fields has not been affected, the name and/or functionality has been improved.

exSILentia® v3 Field	exSILentia® v4 Field
Environment Conditions Interior Equipment Environment Exterior Equipment Environment	Other Environmental Extremes

General SIF Requirements

The following table lists exSILentia® v3 Process SRS General SIF Requirements fields that are no longer supported in exSILentia® v4 or whose type changed from exSILentia® v3 to exSILentia® v4. The table also documents the conversion action applied on these fields.

exSILentia® v3 Field	Conversion Action
Max. Spurious Trip Rate	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Demand Mode	Changed from text field to list field. Field is left blank, the v3 field text is added to the General SIF Notes.
Mission Time	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Maximum Response Time Sensor	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Maximum Response Time Logic Solver	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Maximum Response Time Final Element	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Test Interval	Changed from text field to number field. Field is left blank, the v3 field text is added to the General SIF Notes.
Design Guidelines	Changed from text field to reference field. Field is left blank, the v3 field text is added to the General SIF Notes.
Transmitter Low Detection	The transmitter low detection description is added to the Transmitter Fail Safe State field.
Transmitter Low Detection Value	The transmitter low detection value is added to the Transmitter Fail Safe State field.
Transmitter High Detection	The transmitter high detection description is added to the Transmitter Fail Safe State field.

exSILentia® v3 Field	Conversion Action
Transmitter High Detection Value	The transmitter high detection value description is added to the Transmitter Fail Safe State field.
Diagnostics	The diagnostic description is added to the General SIF Notes.
Maintenance Override Text 1	The maintenance override text 1 field is added to the General SIF Maintenance Override field.
Maintenance Override Text 2	The maintenance override text 2 field is added to the General SIF Maintenance Override field.

The following table lists exSILentia® v3 Process SRS General SIF Requirements fields that have been renamed or redefined in exSILentia® v4. The core functionality of these fields has not been affected, the name and/or functionality has been improved.

exSILentia® v3 Field	exSILentia® v4 Field
Test Interval	Desired Proof Test Interval Sensor Part Desired Proof Test Interval Logic Solver Part Desired Proof Test Interval Final Element Part
Transmitter Low Detection Transmitter Low Detection Value Transmitter High Detection Transmitter High Detection Value	Transmitter Fail Safe State
Maintenance Override Text 1 Maintenance Override Text 2	General SIF Maintenance Override

SIF Specific (PHA based) Requirements

The following table lists exSILentia® v3 Process SRS SIF Specific Requirements fields that are no longer supported in exSILentia® v4 or whose type changed from exSILentia® v3 to exSILentia® v4. The table also documents the conversion action applied on these fields.

exSILentia® v3 Field	Conversion Action
SIF Test Interval	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Overall Response Time	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Protection Method	Changed from text field to toggle field with options ***de-energize to trip*** and ***energize to trip***. Selection set to ***de-energize to trip***, the v3 field text is added to the Notes.
Max. Spurious Trip Rate	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.
Diagnostics	The diagnostic description is added to the Notes.
Notes	Added text from fields where a type change occurred from v3 to v4.
Demand Source	Added text from Demand fields where a type change occurred from v3 to v4.
Demand Rate	Changed from text field to number field. Field is left blank, the v3 field text is added to the Demand Source.

exSILentia® v3 Field	Conversion Action
Demand Mode	Changed from text field to list field. Field is left blank, the v3 field text is added to the Demand Source.
Mission Time	Changed from text field to number field. Field is left blank, the v3 field text is added to the Notes.

The following table lists exSILentia® v3 Process SRS SIF Specific Requirements fields that have been renamed or redefined in exSILentia® v4. The core functionality of these fields has not been affected, the name and/or functionality has been improved.

exSILentia® v3 Field	exSILentia® v4 Field
SIF Test Interval	Desired Proof Test Interval Sensor Part Desired Proof Test Interval Logic Solver Part Desired Proof Test Interval Final Element Part
Overall Response Time	Maximum Response Time SIF

13.5.3 Design SRS

The exSILentia® v4 the Design SRS has become a separate module meant to document the conceptual SIS design after SIL Verification is complete. exSILentia v3 SRS data will be completely converted to the v4 format, with a change log detailing all changes upon conversion.

13.6 SIL Verification (SILver™)

When opening an exSILentia® v3 project in exSILentia® v4, all equipment items that are selected in your project will be updated per the latest version of the Safety Equipment Reliability Handbook database. If all of your project data is up to date this will have no impact. If some of your data is out of date, this could have an impact on your calculated SIF. Any user defined data is unaffected by this action.

exSILentia® v4 SILver uses an updated algorithm to account for logic solver I/O channels and modules. I/O channels are included in the sensor and final element group voting. In addition you can indicate if channels should land on different I/O modules, in which case the I/O modules are also included in the sensor and final element groups.

CAUTION: It is unrealistic to expect that SILver in exSILentia® v4 will yield the same results as SILver in exSILentia® v3 due to the change in logic solver channel and module handling as well as potential for updated failure rate data.

The following table lists exSILentia® v3 SILver™ fields or selections that are no longer supported in exSILentia® v4. The table also documents the conversion action applied on these fields and if the conversion action could impact the calculated SIL verification results of the SIF.

exSILentia® v3 Field/Selection	Conversion Action	SIFs Impacted
Architectural Constraints: Use IEC 61511 tables [ignore 11.4.3 for Type A devices]	Architectural Constraints selection is changed to ***Use IEC 61511 Tables*** per IEC 61511-1:2016.	Yes
Architectural Constraints: Use IEC 61511	Architectural Constraints selection is changed to ***Use IEC 61508 Tables*** per IEC 61511-1:2016.	Yes

exSILentia® v3 Field/Selection	Conversion Action	SIFs Impacted
Architectural Constraints: Use IEC 61508:2000	Architectural Constraints selection is changed to ***Use IEC 61508 Tables*** per IEC 61508-2:2010 in accordance with IEC 61511-1:2016 clause 11.4.3, you should review the SILver results for the affected SIFs.	Yes
Application Test Method - IEC 61508:2010	The selection is no longer supported. The modeling of all application level tests will be done using the ***IEC 61508:2010*** modeling methodology.	No
Application Test Method - IEC 61508:2000	The selection is no longer supported. The modeling of all application level tests will be done using the ***IEC 61508:2010*** modeling methodology.	Yes
Sensor Group Voting: 1oo1D	Change to ***1oo1*** voting and set ***Trip on Transmitter Fault*** to ***Yes***	No
Sensor Group Voting: 1oo2D	Change to ***1oo2*** voting and set ***Trip on Transmitter Fault*** to ***No***	No

The following table lists exSILentia® v3 SILver™ fields that have been renamed in exSILentia® v4. The functionality of these fields has not been affected, the name and/or description has been improved.

exSILentia® v3 Field	exSILentia® v4 Field
Maintenance Capability Index	Site Safety Index
Architectural Constraints: Use IEC 61508:2010 tables [per 61511-1 11.4.5]	IEC 61511-1 11.4.5, IEC 61508:2010 tables
Architectural Constraints: Use IEC 61511 tables	IEC 61511-1 tables 5 & 6
Sensor Group Configuration: Alarm setting	Transmitter Fault Direction
Sensor Group Configuration: Over/Under Range	Out of Range Detection
Sensor Group Configuration: Alarm Filter	Transmitter Fault Filter
Sensor Group Configuration: Alarm Voted as Trip	Trip on Transmitter Fault

The following table lists specific exSILentia® v3 to exSILentia® v4 SILver™ conversion actions including if the conversion action could impact the calculated SIL verification results of the SIF.

Conversion Action	exSILentia® v3 to v4 Conversion Step Description	SIFs Impacted
Logic Solver I/O Channel Count	The v3 to v4 converter only converts the automatically determined number of I/O channels due to a restructuring of the I/O channel handling.	Yes
Tag EU Low	The v3 to v4 converter attempts to convert the v3 string to a Decimal value in v4. If the converter is not successful the Range Low value in v4 will be left empty	No

Conversion Action	exSILentia® v3 to v4 Conversion Step Description	SIFs Impacted
Tag EU High	The v3 to v4 converter attempts to convert the v3 string to a Decimal value in v4. If the converter is not successful the Range High value in v4 will be left empty	No
Tag Trip Limit	The v3 to v4 converter attempts to convert the v3 string to a Decimal value in v4. If the converter is not successful the Limit value in v4 will be left empty	No

13.7 Lifecycle Cost Estimator

The exSILentia® v4 Lifecycle Cost Estimator module functionality is an extension of the Lifecycle Cost Estimator functionality in exSILentia® v3. All information is converted into the new exSILentia® v4 functionality.

Abbreviations

BMS	Burner Management System
BPCS	Basic Process Control System
C&E	Cause and Effect
CCF	Common Cause Failure
CFSE	Certified Functional Safety Expert
CFSP	Certified Functional Safety Professional
CHAZOP	Control Hazard & Operability Analysis
CISSP	Certified Information Systems Security Professional
CM	Conditional Modifier
CMF	Common Mode Failure
DTT	De-energize To Trip
E/E/PE	Electrical/Electronic/Programmable Electronic
EC	Enabling Condition
EMC	Electro-Magnetic Compatibility
ESD	Emergency Shutdown
ETT	Energize To Trip
FAT	Factory Acceptance Testing
FBT	Frequency Based Targets
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Modes Effects and Diagnostic Analysis
FPL	Fixed Program Language
FSA	Functional Safety Assessment
FSM	Functional Safety Management
FVL	Full Variability Language
HAZOP	Hazard and Operability study
HFT	Hardware Fault Tolerance
HMI	Human Machine Interface
IACS	Industrial Automated Control System
IE	Initiating Event
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
ISA	Instrumentation, Systems and Automation Society
L	Likelihood
LOPA	Layer of Protection Analysis
LVL	Limited Variability Language
MOC	Management Of Change
MTTFS	Mean Time To Fail Spurious
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand

PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of a Dangerous Failure per Hour
PHA	Process Hazard Analysis
PIU	Proven In Use / Prior Use
PLC	Programmable Logic Controller
PSI	Process Safety Information
PTC	Proof Test Coverage
PTI	Proof Test Interval
QRA	Quantitative Risk Assessment
R	Risk
RRF	Risk Reduction Factor
S	Severity of Consequence
SAT	Site Acceptance Testing
SCAI	Safety Controls, Alarms and Interlocks
SERH	Safety Equipment Reliability Handbook
SFF	Safe Failure Fraction
SG	Safeguard
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SILac	Achieved Safety Integrity Level based on Architectural Constraints
SILcap	Achieved Safety Integrity Level based on Equipment Systematic Capability
SILpfd	Achieved Safety Integrity Level based on Safety Instrumented Function probability of failure
SIS	Safety Instrumented System
SLC	Safety Lifecycle
SOP	Standard Operating Procedure
SRS	Safety Requirements Specification
SSI	Site Safety Index
β-factor	Beta factor, indicating common cause susceptibility
DD	Dangerous Detected
DU	Dangerous Undetected
SD	Safe Detected
SU	Safe Undetected
AD	Annunciation Detected
AU	Annunciation Undetected
No Effect	Failure of a component that is part of the safety critical circuit that has no impact on the successful execution of the safety function

Terms and Definitions

Basic Process Control System	System that responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but that does not perform any safety instrumented functions with a claimed SIL greater than or equal to 1.
Common Cause Failure	Failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.
Common Mode Failure	Failure of two or more channels in the same way, causing the same erroneous result.
Conditional Modifier	One of several possible probabilities included in scenario risk calculations when risk criteria endpoints are expressed in impact terms (e.g., fatalities) instead of in primary loss event terms (e.g., release, vessel rupture). Conditional modifiers include, but are not necessarily limited to: • Probability of a hazardous atmosphere • Probability of ignition or initiation • Probability of explosion • Probability of personnel presence • Probability of injury or fatality • Probability of equipment damage or other financial impact
Consequence	The undesirable result of an incident, usually measured in health and safety effects, environmental impacts, loss of property, and business interruption costs.
Enabling Condition	A condition that makes possible the initiating event or initiating cause of a scenario. An enabling condition is neither a failure nor a protection layer. It consists of an operation or condition that does not directly cause the scenario, but that must be present or active in order for the scenario to proceed to a loss event. Note that mitigating factors, such as the probability of personnel presence or of emergency evacuation, are conditional modifiers and not enabling conditions. The term enabling event is sometimes used for enabling condition. The term enabling condition is preferred, since enabling conditions are not generally events but rather conditional states.
Event	An occurrence involving a process that is caused by equipment performance or human action or by an occurrence external to the process. Events include initiating events, loss events and success or failure of safeguards.
Failure Modes Effects and Diagnostic Analysis	A systematic procedure during which each failure mode of each component is examined to determine the effect of that failure on the system and whether that failure is detected by any automatic diagnostic function

Hardware Fault Tolerance	The number of dangerous random failures tolerated by a system while still maintaining the ability to successfully perform the safety function
Hazard Scenario	Scenario that consists of one or more sequence of events that results in a final consequence of concern. Each hazard scenario consists of at least one cause - consequence pair.
Impact	A measure of the ultimate loss and harm of a loss event. Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss, and recovery costs.
Incident	An event or sequence of events that either resulted in or had the potential to result in adverse impacts.
Independent Protection Layer	A device, system, or action that is capable of preventing a scenario from proceeding to the undesired consequence regardless of the initiating event or the action of any other protection layer associated with the scenario.
Initiating Event	The event that initiates the scenario leading to the undesired consequence.
Layer of Protection Analysis	An approach that analyzes incident scenario(s) (cause-consequence pair(s)) using values for the initiating event frequencies, enabling conditions, independent protection layer failure probabilities, and conditional modifiers as applicable in order to compare a hazard scenario risk estimate to risk criteria to determine if additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario based hazard evaluation procedure such as a HAZOP Study.
Likelihood	A measure of the expected frequency with which an event occurs. This may be expressed as a frequency (e.g. events per year), a probability of occurrence during a time interval (e.g. annual probability), or a conditional probability (e.g. probability of occurrence, given that a precursor event has occurred).
Mean Time To Repair	The expected time to repair equipment items in case of a failure detected by automatic equipment item diagnostics
Mission Time	The time period that a SIF is expected to be operational. Typically this period corresponds to the interval when all devices are either replaced or refurbished to “as new condition”. It should not be confused with the proof test interval.
Probability of Failure on Demand	The probability that a system or other protective measure will fail to perform a specified function on demand. PFD is expressed as a dimensionless number ranging from zero to one.
Process Hazard Analysis	A hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

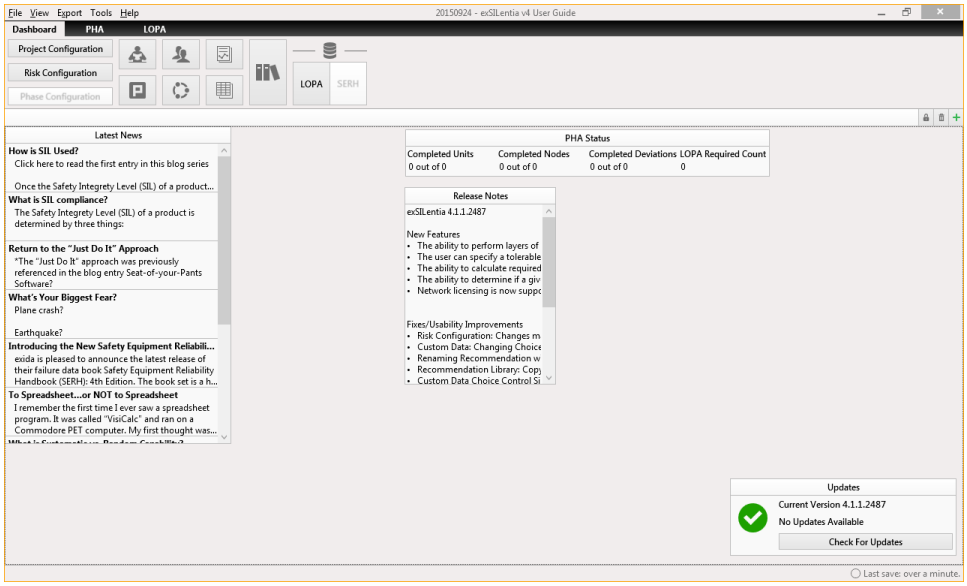
Proven In Use / Prior Use	A Proven In Use assessment is a study of product operational hours, revision history, fault reporting system, and field failures to determine if there is evidence of systematic design faults in a product. The IEC 61508 standard provides levels of operational history required for each SIL level.
Quantitative Risk Assessment	The systematic development of numerical estimates of the expected frequency and consequence of potential incidents associated with a facility or operation based on engineering evaluation and mathematical techniques.
Risk	A measure of human injury, environmental damage, economic loss, loss of intellectual property or loss of privacy in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified version of this relationship expresses risk as the product of the likelihood and the consequences (i.e. Risk = Consequence x Likelihood) of an incident.
Risk Assessment	The process by which the results of a risk analysis (i.e. risk estimates) are used to make decisions, either through relative risk ranking of risk reduction strategies or through comparison with tolerable risk levels.
Risk Mitigation	A reduction of risk due to a reduction of the likelihood or impact associated with a loss event.
Risk Receptor	Something which could come to harm, including human health, environment, or financial well-being.
Risk Reduction Factor (RRF) - Achieved	The measure of the degree of risk reduction achieved by a safeguard, countermeasure, or protection strategy. Achieved RRF can be expressed as the ratio of unmitigated risk divided by mitigated risk resulting from that safeguard, countermeasure, or protection strategy. For an independent low demand safety function, this can be expressed as the reciprocal of the average probability of failure on demand.
Risk Reduction Factor (RRF) - Target/Required	The measure of the degree of risk reduction needed to achieve tolerable risk. RRF can be expressed as the ratio of unmitigated risk divided by tolerable risk. Within exSILentia® a distinction is made between *Target* and *Required* RRF. *Target RRF* is used to identify the risk reduction needed to achieve tolerable risk resulting from the LOPA/SIL selection. *Required RRF* is used to identify the risk reduction specified in the SRS which the SIF as designed should meet. The required RRF is typically equal to or greater than the target RRF (if the user decides to round the target RRF).
Risk Tolerance	1. Willingness by authority having jurisdiction to live with a risk so as to secure certain benefits in the confidence that the risk is one that is worth taking and that it is being properly controlled. However, it does not imply that everyone would agree without reservation to take that risk or have it imposed on them. 2. Risk the organization is willing to accept.

Risk Tolerance Criteria	A predetermined measure of risk used to aid decisions about whether further efforts to reduce risk are warranted.
Safety	Freedom from unacceptable risk.
Safety Integrity Level	Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the electronic / programmable electronic safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest [IEC 61508-4]
Safety Integrity Level - Target/Required	Within exSILentia® a distinction is made between *Target* and *Required* SIL. *Target SIL* is used to identify the SIL needed to achieve tolerable risk resulting from the LOPA/SIL selection. *Required SIL* is used to identify the SIL specified in the SRS which the SIF as designed should meet. The required SIL is typically equal to the target SIL but would allow different target SILs to result from the different SIL selection methods.
Severity	A measure of the degree of impact of a particular consequence.
SIL Threshold	Parameter to specify the boundary between target Safety Integrity Levels Assume a calculated Required Risk Reduction Factor of 29, which would fall in the 10 - 100 Risk Reduction range. With a SIL Threshold Ratio of 1, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 2. The calculated Risk Reduction Factor is in this case greater than the SIL determination threshold which lies at 10 (10 * 1). With a SIL Threshold Ratio of 3, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 1. The calculated Risk Reduction Factor is in this case less than the SIL determination threshold which lies at 30 (10 * 3).
Startup Time	The time it takes to re-start the process after a shutdown
Systematic Capability	Indication of systematic failure protection for an equipment item. Per IEC 61511 users of existing hardware either need to select hardware that is developed and assessed per IEC 61508 or justify the use of that hardware. The objective of the assessment or justification is to identify that there are “no” systematic problems with the equipment item under consideration. Systematic failure protection is part of IEC 61508 compliant development processes, alternatively sufficient recorded experience can also be used to identify that there is no known systematic problem.
Useful Life	That portion of life when the failure rate can be described by the exponential distribution, i.e. constant failure rate. The useful life follows infant mortality or burn-in and precedes the wear-out portions of the overall life. For functional safety applications, devices are expected to be replaced at the end of their useful life.

Appendix A Dashboard

The exSILentia® v4 Dashboard is the first window you will see when you open a project or after creating a new project. The dashboard is exSILentia® v4's central hub through which all lifecycle activities are initiated. It is shared by all exSILentia® v4 tools. In addition to providing the main navigation of the tool, the dashboard also provides you with the ability to evaluate the status of a project through summary information as well as graphical representation of results.

The configuration of your dashboard will depend on your exSILentia® v4 license. Some of the dashboard functions are applicable to all software tools within the exSILentia® v4 framework, other options are tightly linked to one of the software tools. The various features of the dashboard are described in the subsequent sections.



A.1 Project Information

The projection information of your exSILentia® v4 project is described in detail in *Chapter 1 Project Information*. Project Information allows you to change your Project Identifier, Name, and Description, among others.

A.2 Project Configuration

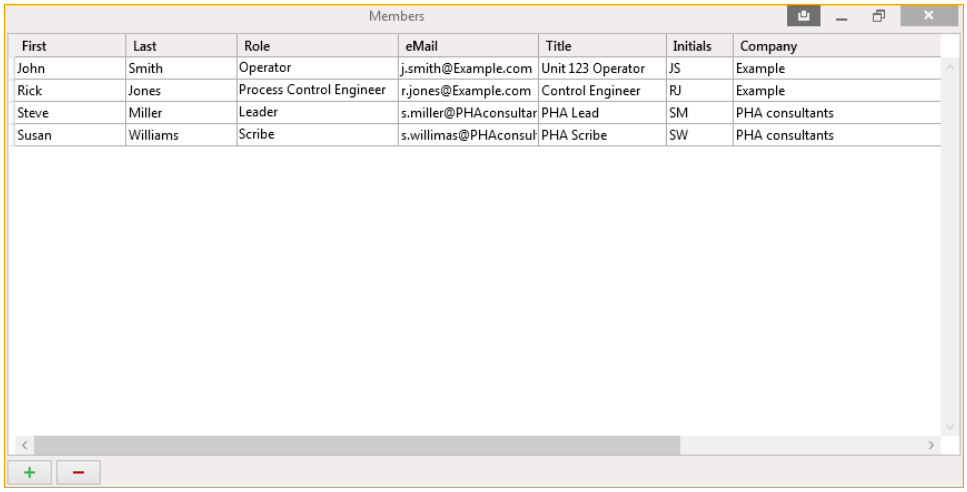
The configuration of your exSILentia® v4 project is described in detail in *Chapter 6 Project Configuration*. Project Configuration allows you to change many of the project default options and values.

A.3 Risk Configuration

The risk configuration that applies to your exSILentia® v4 project is described in detail in *Chapter 8 Project Risk Configuration*. In the Risk Configuration you can define your tolerable risk levels and you can either select the exida default risk matrix or configure a risk matrix to match the risk criteria that are applicable to your project.

A.4 Members

exSILentia® v4 provides the ability to define various team members and document their roles. Once team members are defined, they can be associated with various work sessions. To access an overview of all team members defined for the current project click on the ***Members*** button on the dashboard. Alternatively you can select the ***View - Members*** menu option.



To add a Team Member:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Team Member
- Edit the Team Member Properties, i.e. *First Name*, *Last Name*, *Initials*, *Title*, *e-mail*, and *Notes*
    - Note that the initials are used when assigning recommendations
- Specify a role by selecting an option from the drop down list (the Team Roles can be modified from within the project configuration)
- Click on Save

To modify a Team Member:

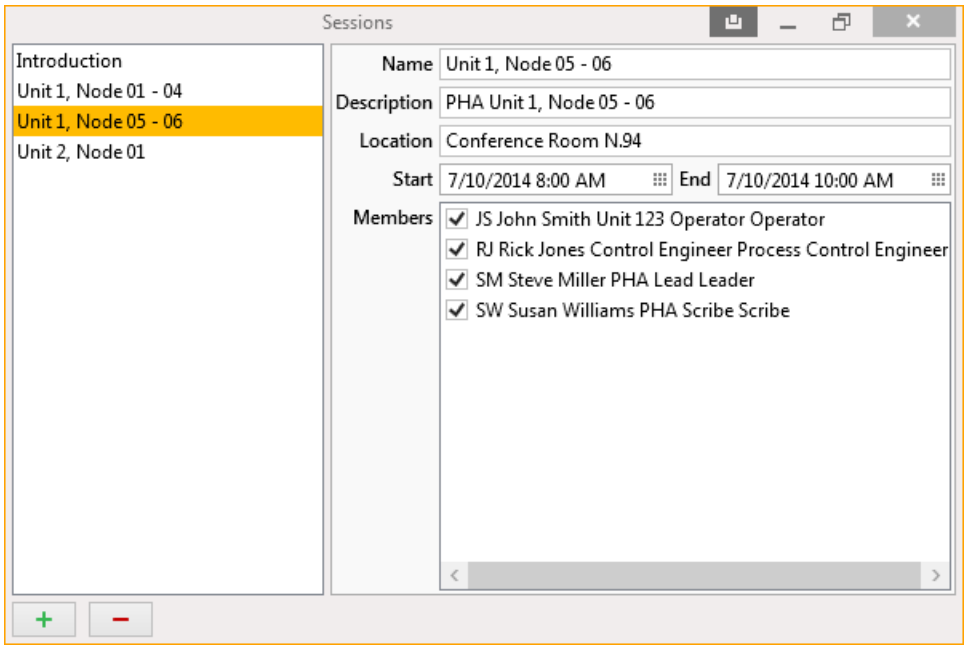
- Highlight the Team Member
- Edit Team Member Properties, i.e. *First Name*, *Last Name*, *Initials*, *Title*, *e-mail*, and *Notes*
- Click on Save

To delete a Team Member:

- Highlight the Team Member
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Team Member and its Team Member Properties

A.5 Sessions

exSILentia® v4 provides the ability to define (work) sessions and document dates and associated participants. To access an overview of all defined sessions for the current project click on the ***Sessions*** button on the dashboard. Alternatively you can select the ***View - Sessions*** menu option.



To add a Session:

- Click on the green plus (+) symbol in the lower left hand portion of the window
- Highlight the new Session
- Edit the Session Properties, i.e. *Name*, *Description*, and *Location*
- Select the Session Start Date using the calendar function
- Select the Session End Date using the calendar function
- Check the relevant check boxes to indicate which Team Members are part of the Session
- Click on Save

To modify a Session:

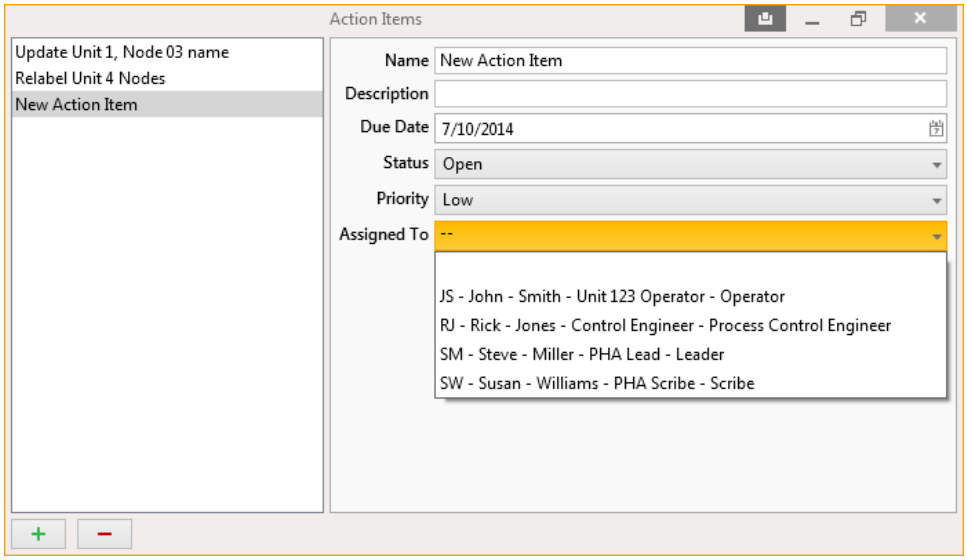
- Highlight the Session
- Edit Session Properties, i.e. *Name*, *Description*, and *Location*
- Modify the Session Start Date using the calendar function
- Modify or select the Session End Date using the calendar function
- Check or uncheck the relevant check boxes to indicate which Team Members are part of the Session
- Click on Save

To delete a Session:

- Highlight the Session
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Session and its Session Properties

A.6 Action Items

exSILentia® v4 provides the ability to define action items. Action items are intended for tasks to be performed that will extend beyond the duration of a single session. To access an overview of all defined action items for the current project click on the ***Action Items*** button on the dashboard. Alternatively you can select the ***View - Action Items*** menu option.



To add an Action Item:

- Click on the green plus (**+**) symbol in the lower left hand portion of the window
- Highlight the new Action Item
- Edit the Action Item Properties, i.e. *Name*and *Description*
- Select the Action Item Due Date using the calendar function
- Select the Action Item Status using the drop down selections; Open (default value), Closed, or Review
- Select the Action Item Priority using the drop down selections; Low, Medium, or High
- Select the Action Item Responsible Person using the drop down selection based on the defined team members
- Click on Save

To modify an Action Item:

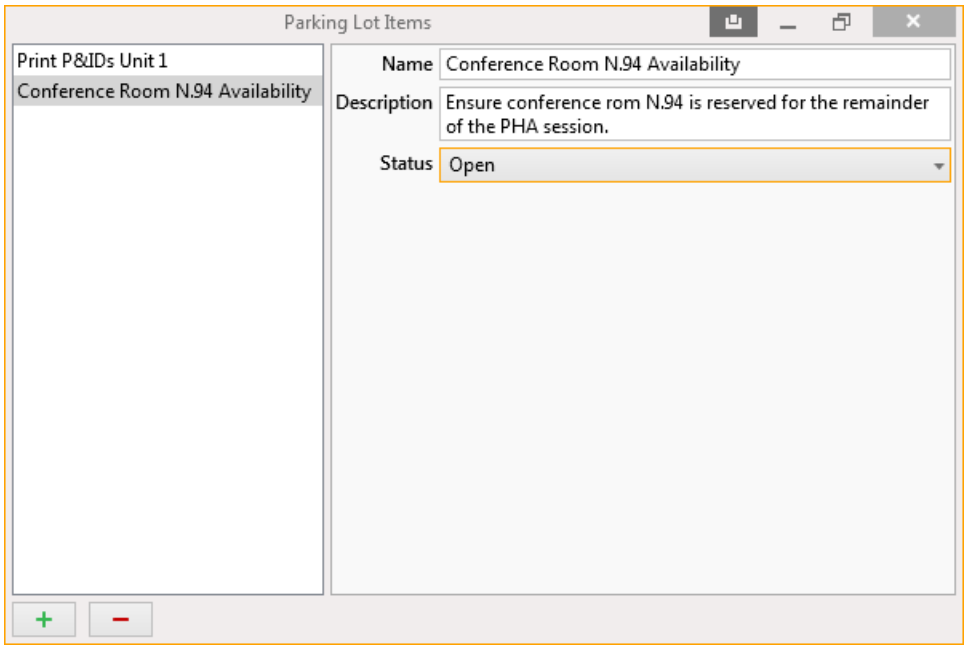
- Highlight the Action Item
- Edit Action Item Properties, i.e. *Name* and *Description*
- Modify the Action Item Due Date using the calendar function
- Modify or select the Action Item *Status* and /or *Priority*
- Modify the Action Item *Responsible Person*
- Click on Save

To delete an Action Item:

- Highlight the Action Item
- Click on the red minus (**-**) symbol in the lower left hand portion of the window
- This will remove that Action Item and its Action Item Properties

A.7 Parking Lot Items

exSILentia® v4 provides the ability to define parking lot items. Parking lot items are intended for short term tasks to be performed such as obtaining information overnight for the next session, i.e. a focused short term task. To access an overview of all defined parking lot items for the current project click on the ***Parking Lot Items*** button on the dashboard. Alternatively you can select the ***View - Parking Lot Items*** menu option.



To add a Parking Lot Item:

- Click on the green plus (+) symbol in the lower left hand portion of the window
- Highlight the new Parking Lot Item
- Edit the Parking Lot Item Properties, i.e. *Name*and *Description*
- Select the Parking Lot Item Status using the drop down selections; Open (default value), Closed, or Review
- Click on Save

To modify a Parking Lot Item:

- Highlight the Parking Lot Item
- Edit Parking Lot Item Properties, i.e. *Name* and *Description*
- Modify or select the Parking Lot Item *Status*
- Click on Save

To delete a Parking Lot Item:

- Highlight the Parking Lot Item
- Click on the red minus (-) symbol in the lower left hand portion of the window
- This will remove that Parking Lot Item and its Parking Lot Item Properties

A.8 Library

The library capability, build into exSILentia® v4, for identical items that can be (re-)used in multiple locations, can dramatically increase the efficiency and consistency of the various work activities performed. A detailed description of the Library functionality as well as an overview of the items for which libraries are defined is provided in *Chapter 7 Project Libraries*.

A.9 Generate Report

The generate report option allows you to auto generate reports for the various exSILentia® v4 tools. Depending on the tool selected additional, more detailed, options may be available. The report generation is described in detail in *Chapter 9 Report Generation* and for each individual exSILentia® v4 tool in their respective Appendix.

A.10 Import Data

The import data option allows you to import data from other software tools and MS Excel worksheets/workbooks if properly formatted into exSILentia® v4. The data import is described in detail in *Chapter 10 Data Import*.

A.11 Export Data

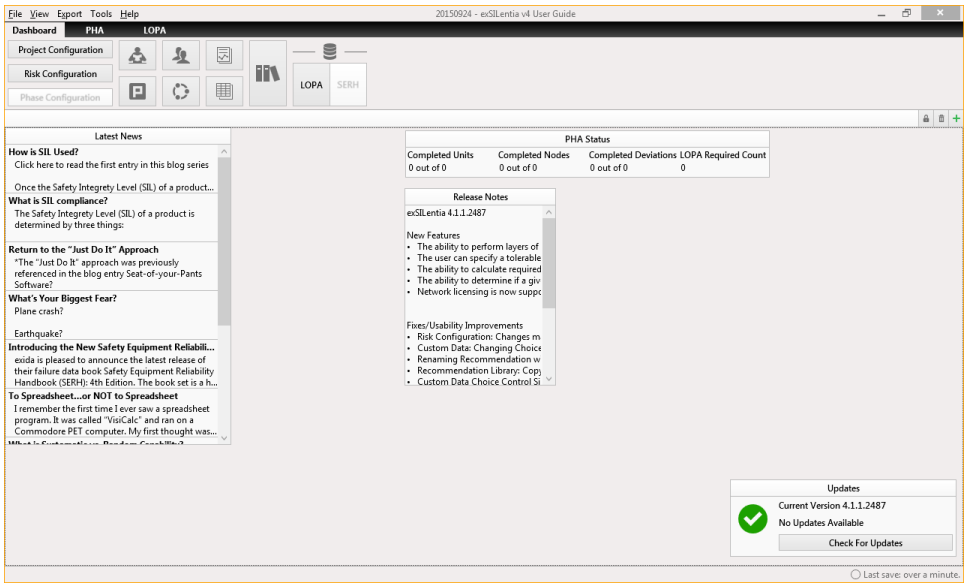
The export data option allows you to export data out of the various exSILentia® v4 tools to a MS Excel worksheet/workbook. Depending on the tool selected additional, more detailed, options may be available. The data export is described in detail in *Chapter 11 Data Export* and for each individual exSILentia® v4 tool in their respective Appendix.

A.12 Tool Tabs

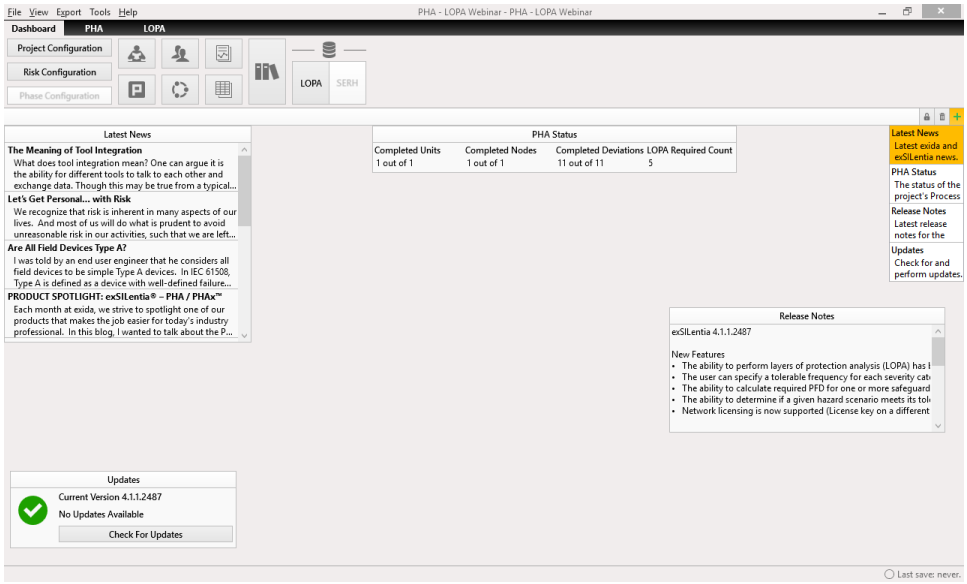
The tool tabs on the exSILentia® v4 dashboard allow you to navigate between the different lifecycle activities. The exSILentia® v4 main window will change based on your tool selection to allow for optimal layout of the different lifecycle tasks.

A.13 Dashboard Widgets

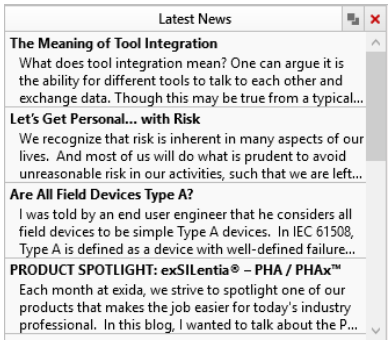
The exSILentia® v4 dashboard allows you to display widgets with useful information. The type of information ranges from status of work perform to news items and release notes.

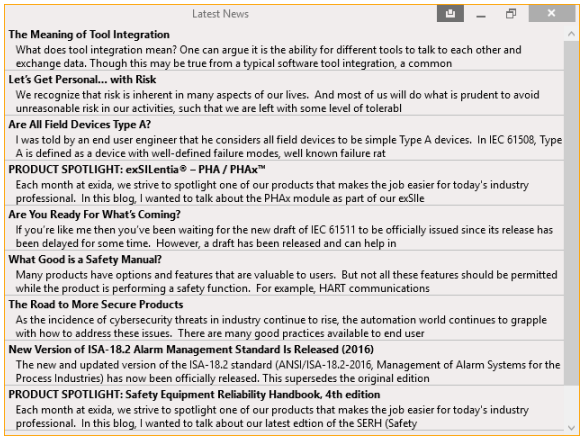


You can move widgets on the desktop through dragging . You can add widgets by clicking on the green "**+**" in the upper right hand corner of the widget area. This will show you the available widgets.



If you want to know more about the information displayed in a widget you can however over the title bar of the widget and click on the "expand" button. This will make the widget pop out. If you want to remove a widget from your dashboard, simply however over the title bar of the widget and click the red "***x***".





To remove all widgets from you desktop click on the delete icon in the upper right hand corner of the widget area.

To lock all widgets in place click on the lock icon in the upper right hand corner of the widget area.

Appendix B Menu Items and Short Cuts

exSILentia® v4 has an interactive menu toolbar. The menu toolbar will make certain menu items available based on the software tool that you are using. In addition to these dynamic menu items, a wide range of short cuts have been implemented to make the tool use more efficient. An overview of the exSILentia® v4 menu items as well as available short cuts is provided in this appendix.

B.1 Menu Toolbar

The Menu toolbar consists of the following main menus:

- File
- View
- Export
- Tools
- Help

Menu items available for each of these main menus are identified in the following sections.

B.1.1 File

Menu Item	Keyboard Shortcut	Function Description
New	Ctrl+N	Launches a new project
Open	Ctrl+O	Allows you to browse to a project file to be opened
Recent		Shows recent projects that may then be opened
Save	Ctrl+S	Saves the project file
Save As	Ctrl+Shift+S	Allows you to save a project with a different file name
Close	Ctrl+E	Closes current project while keeping application open
Exit	Alt+F4	Closes the application

B.1.2 View

Menu Item	Keyboard Shortcut	Function Description
Project Configuration		Launches the Project Configuration window
Risk Configuration		Launches the Risk Configuration window
Library		Has four sub- items to launch the Safeguards, Recommendations, References, and Hazard Scenarios Library window respectively
Members		Launches the Members window
Sessions		Launches the Sessions window
Action Items		Launches the Action Items window
Parking Lot Items		Launches the Parking Lot Items window

B.1.3 Export

Menu Item	Keyboard Shortcut	Function Description
Generate Report		Allows you to auto generate reports for the various exSILentia® v4 tools. Depending on the tool selected additional, more detailed, options may be available. • PHA Report • LOPA Report • Process SRS • SIL verification • Design SRS • Proof Test Generation
Export Data		Allows you to export data out of the various exSILentia® v4 tools to a MS Excel worksheet/workbook. Depending on the tool selected additional, more detailed, options may be available.

B.1.4 Tools

Menu Item	Keyboard Shortcut	Function Description
License Configuration		Allows you to request an update to your license key and subsequently check for an available update (requires exida license key processing)
Plugins		Provides a list of user created exSILentia® v4 plug-in modules (once interfaces are made public)
Modules		Provides a list of all licensed exSILentia® v4 software modules and their individual versions

B.1.5 Help

Menu Item	Keyboard Shortcut	Function Description
View Help		Launches the help window
User Guide		Allows you to access all User Guide material
Check for Updates		Allows you to check if a more recent version of the exSILentia® v4 program is available and install that newer version if applicable
Contact exida		Will launch a web browser and directs you to the exSILentia® online support ticket system. Here you will be able to launch a support request.
Release Notes		Allows you to see the history of feature upgrades

Menu Item	Keyboard Shortcut	Function Description
About		Shows the current exSILentia® v4 version number and license information

B.2 Shortcuts

For a Microsoft Windows based application you would expect a certain set of standard shortcuts, these are also available in exSILentia® v4 in a wide variety of locations. The following is a limited overview of some of the shortcuts implemented.

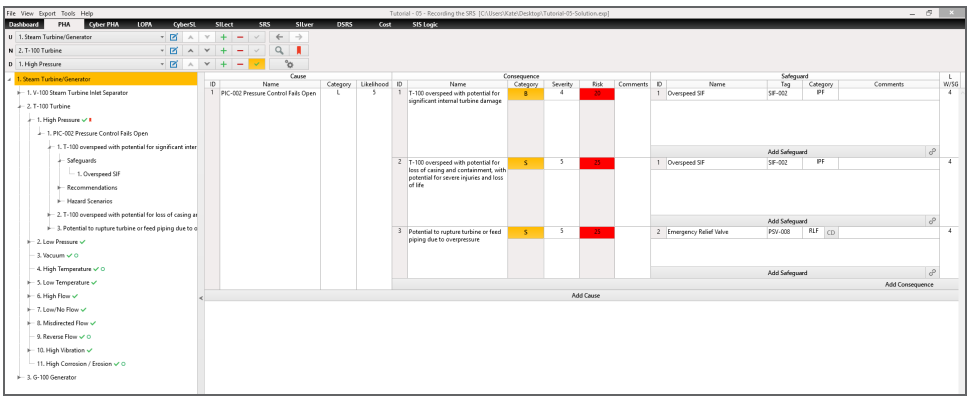
Keyboard Shortcut	Function Description
Ctrl+C	Copy
Ctrl+V	Paste
Ctrl+X	Cut
Delete (Del)	Deletes the currently selected item(s)
Enter	Create a new item
Shift+Enter	Create a new child item
Shift+Enter	In HAZOP Worksheet when consequence or associated Safeguard or Recommendation selected: Create a new Safeguard
Ctrl+Shift+Enter	In HAZOP Worksheet when consequence or associated Safeguard or Recommendation selected: Create a new Recommendation
Tab	In worksheet changes focus to next field from left to right, top to bottom
Shift+Tab	In worksheet changes focus to previous field from right to left, bottom to top
Up/Down/Left/Right	In worksheet changes focus to relevant surrounding field

Appendix C PHAx™

The PHA tab navigates to the exSILentia® v4 process hazard analysis tool PHAx™. Availability of the PHA tab, and therefore the PHAx™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The PHAx™ tool allows process hazard analysis to be performed using the Hazard and Operability (HAZOP) methodology.

C.1 Introduction

The HAZOP functionality in the PHAx™ tool uses a spreadsheet type interface with defined columns for the various HAZOP items.



In the subsequent sections the PHAx™ tool hierarchy, the worksheet, and its reporting capability will be explained.

C.2 Hierarchy

The hierarchical top level for an exSILentia® v4 project is a plant. Within the plant level several units can be defined and within the unit level nodes can be defined. Deviations which are the cornerstone of the HAZOP methodology are defined for each node.

- **Plant (exSILentia® v4 project)**
  - **Units**
    - **Nodes**
      - **Deviations**

C.2.1 Units

A unit allows division of an exSILentia® v4 project plant.

To add a Unit:

- Click on the green plus (**+**) symbol in the Unit row
- Edit the Unit Properties, i.e. *Name*, select the *Plant Type* from the drop down box (optional), and select the *Process Type* from the drop down box (optional)
    - See section *6.1* for more information on Plant and Process Types

Note: The default value for Plant Type is *Unknown*. The Process Type field will remain blank without drop down box selections until a Plant Type has been defined.

Upon completion of all study items associated with a particular unit, the *Complete* check box can be checked. The box to the far right of the unit will turn orange and show a green bold check mark.

To navigate between units you can use the navigation tree in the left hand side bar, click the Unit drop down box and select the desired Unit, or click on the up or down icons until the applicable Unit is selected.

To modify a Unit:

- Highlight the Unit
- Click the icon
- Edit the Unit Properties, i.e. *Name*, select the *Plant Type* from the drop down box (optional), and select the *Process Type* from the drop down box (optional)

To delete a Unit:

- Highlight the Unit
- Click on the red minus (**-**) symbol in the Unit row
- Click *Yes* to confirm you want to delete the Unit
- This will remove that Unit, its Unit Properties, and all associated data

C.2.2 Nodes

A HAZOP Node represents a specific section of the plant unit system in which (the deviations of) the design/process intent are evaluated.

To add a Node:

- Select the Unit where the node will be added
- Click on the green plus (**+**) symbol in the Node row
- Edit the Node Properties, i.e. *Name*, *Node Intention*, and *Comments* (optional)
- To take advantage of Smart Deviations:
    - Check the Smart Deviation check box
    - Within the Node Window, select the node type from the drop down box that aligns with the actual process node

Upon completion of all study items associated with a particular node, the *Complete* check box can be checked. The box to the far right of the node will turn orange and show a green bold check mark.

To navigate between nodes you can use the navigation tree in the left hand side bar, click the Node drop down box and select the desired Node within a Unit, or click on the up or down icons until the applicable Node is selected for the selected Unit.

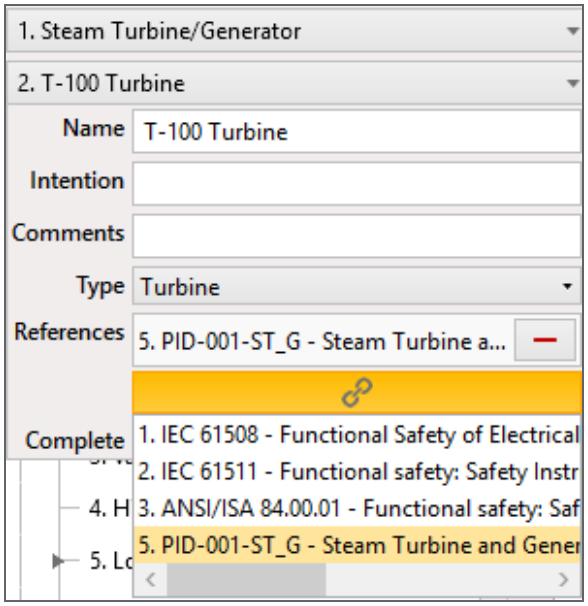
To modify a Node:

- Highlight the Node
- Click the icon
- Edit the Node Properties, i.e. *Name*, *Node Intention*, and *Comments* (optional)

To delete a Node:

- Highlight the Node
- Click on the red minus (-) symbol in the Node row
- Click *Yes* to confirm you want to delete the Node
- This will remove that Node, its Node Properties, and all associated data

You can link references from the reference library (see section *7.4* for more information on the Reference Library) to a Node by clicking on the link Icon and selecting a reference from the list of available references. Once a reference is linked, you can click on the red minus (-) symbol to remove the link.



C.2.3 Deviations

A HAZOP Node Deviation is a way in which the process conditions may depart from its design/process intent. It is created by combining guide words with process parameters resulting in a possible deviation from design intent.

If you selected the Smart Deviations check box when defining the Node the deviations associated with the specific Node Type will be automatically defined for the Node. The following steps can be used if you did not use Smart Deviations or want to add or modify the Smart Deviations. You will also be able to delete a smart deviation if it is not applicable to the Node, however to document that you considered the specific deviation it is better to leave it in the project and mark it as not applicable.

To add a Deviation:

- Select the Node where the deviation will be added
- Click on the green plus (+) symbol in the Deviation row
- Edit the Deviation Properties, i.e. *Name* and *Design Intent*

Upon completion of all study items associated with a particular deviation, the *Complete* check box can be checked. The box to the far right of the deviation will turn orange and show a green bold check mark.

If for a deviation no causes or consequences of no significance are found, then the "No Issues" check box can be checked. This will document "No Issues Found " on the worksheet.

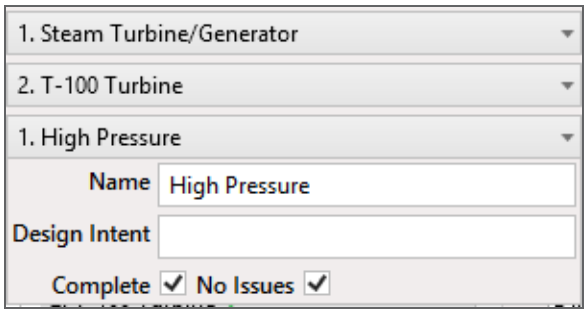
To navigate between deviations you can use the navigation tree in the left hand side bar, click the Deviation drop down box and select the desired Deviation within a Node, or click on the up or down icons until the applicable Deviation is selected for the selected Node.

To modify a Deviation:

- Highlight the Deviation
- Click the icon
- Edit the Deviation Properties, i.e. *Name* and *Design Intent*

To delete a Deviation:

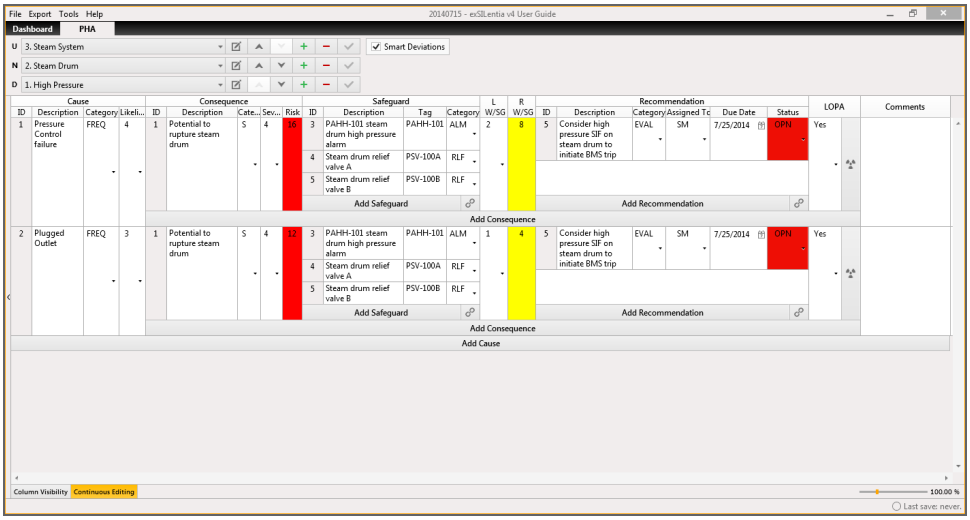
- Highlight the Deviation
- Click on the red minus (-) symbol in the Deviation row
- Click *Yes* to confirm you want to delete the Deviation
- This will remove that Deviation, its Deviation Properties, and all associated data



C.3 HAZOP Worksheet

The PHAx™ tool HAZOP worksheet uses columns for the selected Deviation in a spreadsheet type interface. This allows the Cause data to be viewed quickly so one Cause-Consequence pair can be compared to another Cause-Consequence pair within the same Deviation. Within the worksheet columns buttons exist for adding Causes, Consequences, Safeguards, and Recommendations. For Cause and Consequences content can be edited directly from within the worksheet. Content for the Safeguards and Recommendations can also be directly edited from within the worksheet, however as they are part of the Project Libraries (see *Chapter 7 Project Libraries*) additional functionality is available. Within the worksheet you will be able to add a new Safeguard or Recommendation. When you begin typing a new name for a Safeguard or Recommendation the auto-complete feature will display a list of Safeguards or Recommendations which match the entered text. You can double click on an item in the list to create a link between the relevant Safeguard or Recommendation and the current Cause-Consequence pair.

An example of the PHAx™ tool HAZOP worksheet is shown in the figure below.



C.3.1 Cause

PHAx™ causes are comprised of four related data fields, i.e. ID, Description, Cause Category, and Cause Likelihood. The Cause ID is automatically generated and assigned to ensure relational data integrity. If more than one Likelihood Category was defined in the Risk Matrix, a drop down list will allow you to select the applicable Cause Category. The Cause Likelihood is intended to be the likelihood with NO Safeguards or the scenario where all safeguards have failed. When combining the Cause Likelihood with the Consequence Severity a Risk Without Safeguards is obtained from the Risk Matrix. The Cause Likelihood is selected from a drop down list of likelihoods configured within the Risk Matrix. The list that appears is based on the associated Cause Category.

To add a Cause:

- Click on the ***Add Cause*** button at the bottom of the HAZOP worksheet
- Edit the Cause Properties, i.e. *Description*, *Cause Category*, and *Cause Likelihood*
- Once a Cause Description has been entered you can click the ***Enter*** key on your keyboard to add a new Cause

To delete a Cause:

- Highlight the Cause ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Cause is really to be deleted

CAUTION: Deleting a Cause will delete all consequences, safeguards, and recommendations that are related to it.

C.3.2 Consequence

PHAx™ consequences are comprised of five related data fields, i.e. ID, Description, Consequence Category, Severity, and Risk. The Consequence ID is automatically generated and assigned to ensure relational data integrity. If more than one Consequence Category was defined in the Risk Matrix, a drop down list will allow you to select the applicable Category. The Consequence Severity is selected from a drop down list that is based on the Consequence Category selected. The Risk, representing the risk without safeguards, is automatically determined based on the Risk Matrix given the Cause Likelihood and Consequence Severity selected.

To add a Consequence:

- Click on the ***Add Consequence*** button that is in line with the Cause that you want to add the Consequence to.
- Enter Consequence *Description*, and choose the Severity Categories that apply. Multiple severity categories can be attributed to one consequence. For each applicable category, choose the severity from the drop down and the tool will show the applicable Risk from the Risk Configuration.
    - If you often analyze all severity categories, select the 'Severity Categories Start as Applicable' check box. In this case all severity categories will be automatically selected (buttons will be orange), and you can indicate if any are not applicable (button will appear gray). If you would like to hide categories that do not apply select the 'Hide Non Applicable Severity Categories' check box.
    - If you often analyze one severity category at a time, leave the 'Severity Categories Start as Applicable' check box unchecked. In this case the categories are not applicable by default (buttons will be gray), and you can indicate which are applicable (button will appear orange).
    - If you prefer, you can select 'Ask for Severity Categories', and the tool will allow you to select applicable categories from a window upon adding each new consequence.
- Once a Consequence Description has been entered you can click the ***Enter*** key on your keyboard to add a new Consequence

To delete a Consequence:

- Highlight the Consequence ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Consequence is really to be deleted

CAUTION: Deleting a Consequence will delete all safeguards and recommendations that are related to it.

C.3.3 Safeguards

PHAx™ safeguards are comprised of four related data fields, i.e. ID, Description, Safeguard Tag, and Safeguard Category. The Safeguard ID is automatically generated and assigned to ensure relational data integrity. The Safeguard Tag can be used to uniquely identify a specific Safeguard within a process plant. The Safeguard Tag also enables links to the Safeguard from other applications. The Safeguard Category is selected from a drop down list. Categorizing Safeguards allows for enhanced safeguard reporting. Furthermore Safeguard Category specific process safety information can be specified by clicking on the Category Icon. In addition to the four data fields identified above, Custom Data/process safety information data fields can be configured in the Custom Data section within the Project Configuration (see section *6.7*).

To add a New Safeguard:

- Click on the ***Add Safeguard*** button that is in line with the Consequence that you want to add the Safeguard to
- Edit the Safeguard Properties, i.e. *Description*, *Safeguard Tag*, and *Safeguard Category*
- Once a Safeguard Description has been entered you can click the ***Enter*** key on your keyboard to add a new Safeguard

To add a Safeguard directly from the Safeguard Library:

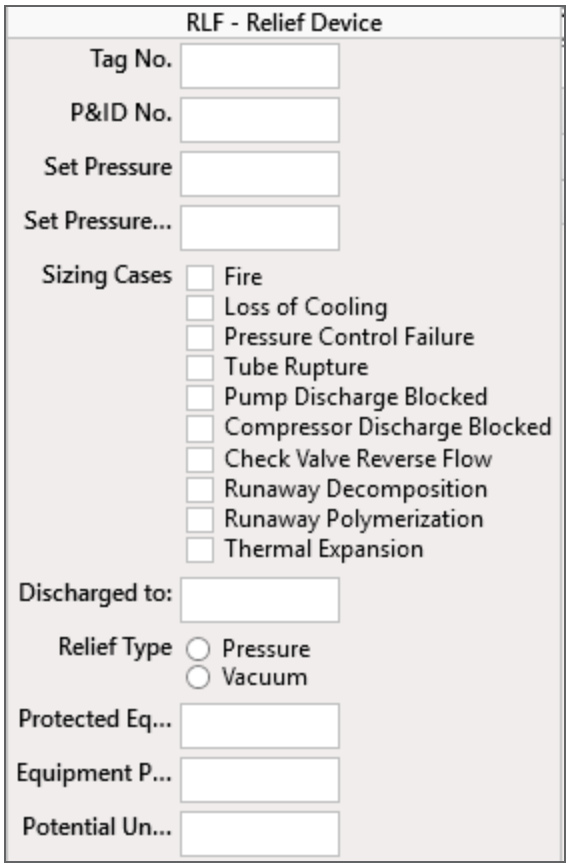
- Click on the Link Safeguard Icon
- For ease, search the safeguard library using the search bar at the bottom of the link window. This will search all attributes of the safeguard including name, tag, and type as well as any labels applied to the safeguard.
- Highlight the Safeguard to add
- Click on ***Add***

To delete a Safeguard:

- Highlight the Safeguard ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Safeguard is really to be deleted

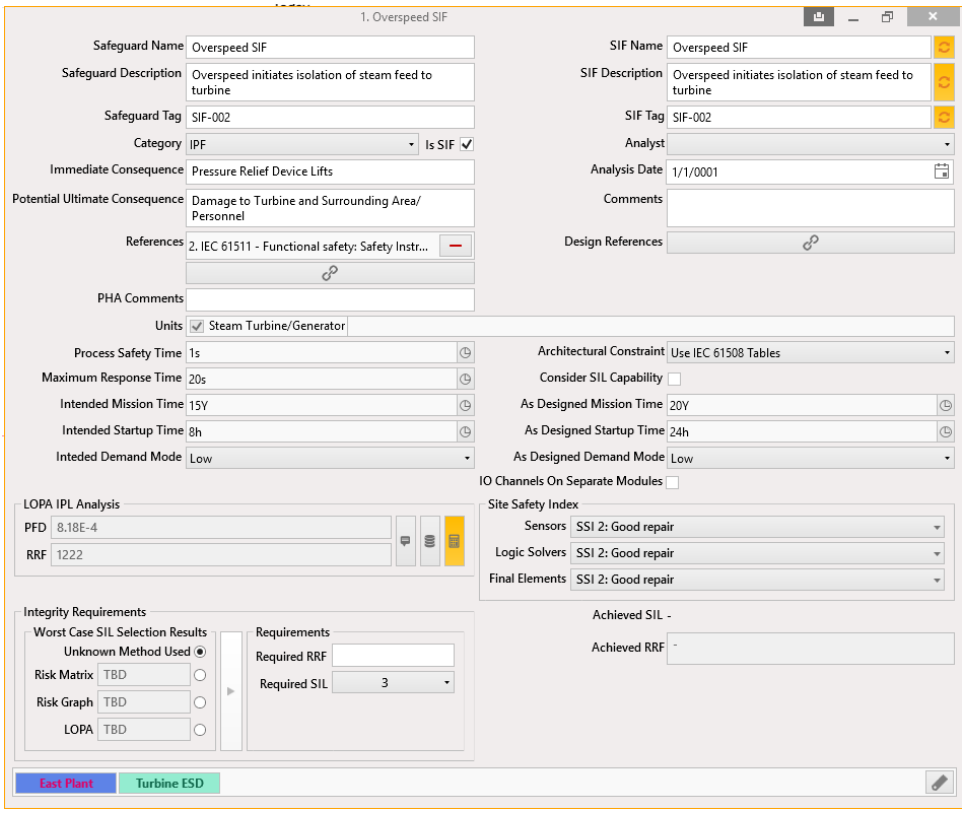
Note: When a Safeguard is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Safeguard from the Library. Click **Yes** or **No** as applicable.

To edit the Custom Data/process safety information for a safeguard, click on the icon. The applicable Custom Data entry form will appear.



C.3.4 Safeguard Labels

User defined labels can be defined in the library under the labels entry. The label name, description and label color can be configured there. To apply labels to a safeguard, navigate to the safeguard library, and view the safeguard. At the bottom of the safeguard view, select the label button and apply the appropriate labels from the list. There is no limit to the number of labels applied to a safeguard.



C.3.5 Likelihood with Safeguards

The Likelihood with Safeguards is intended to reflect the Cause Likelihood assuming ALL Safeguards are successful. The Likelihood is selected from a drop down list of likelihoods configured within the Risk Matrix. The list that appears is based on the associated Cause Category.

C.3.6 Risk with Safeguards

The Risk with Safeguards is automatically determined based on the Risk Matrix given the Likelihood with Safeguards and Consequence Severity selected.

C.3.7 Recommendations

PHAx™ recommendations are comprised of six related data fields, i.e. ID, Description, Category, Assigned to, Due Date, and Status. The Recommendation ID is automatically generated and assigned to ensure relational data integrity. The Recommendation Category is selected from a drop down list. Categorizing Recommendation allows for easy recommendation sorting and reporting. The Assigned to is selected from a drop down list. The list is populated with Member names that can be configured from the Dashboard (see section *A.4*). The Due Data is selected from the pop-up calendar. The Status is selected from a drop down list where *Open* is the default value.

To add a New Recommendation:

- Click on the ***Add Recommendation*** button that is in line with the Consequence that you want to add the Recommendation to
- Edit the Recommendation Properties, i.e. *Description*, *Category*, *Assigned to*, *Due Date*, and *Status*
- Once a Recommendation Description has been entered you can click the ***Enter*** key on your keyboard to add a new Recommendation

To add a Recommendation directly from the Recommendation Library:

- Click on the Link Recommendation Icon
- Highlight the Recommendation to add
- Click on ***Add***

To delete a Recommendation:

- Highlight the Recommendation ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Recommendation is really to be deleted

C.3.8 LOPA

The LOPA column allows the PHA team to record if a detailed Layer of Protection Analysis (LOPA) is required for a specific Cause-Consequence pair scenario. The drop down list allows a *Yes*, *No*, or *N/A* (default) selection. When a Cause-Consequence pair scenario is to be further evaluated it can be assigned to a Hazard Scenario. To add, edit, or remove a Hazard Scenario click on the Hazard Scenario icon .

Note: The Cause-Consequence pair will only be available for further evaluation in the LOPAx™ worksheet if the LOPA drop down box selection is ***Yes***, even when the Cause-Consequence pair is assigned to a Hazard Scenario.

To create a new Hazard Scenario for a Cause-Consequence pair:

- Click on the green **+** symbol
- Edit the Hazard Scenario Properties, i.e. *Name* (the Hazard Scenario ID is automatically generated and assigned to ensure relational data integrity)
- Once a Consequence Description has been entered you can click the ***Enter*** key on your keyboard to add a new Consequence

To add a Hazard Scenario to a Cause-Consequence pair:

- Highlight the applicable Hazard Scenario
- Click on the ***Left*** arrow

To remove a Hazard Scenario from a Cause-Consequence pair:

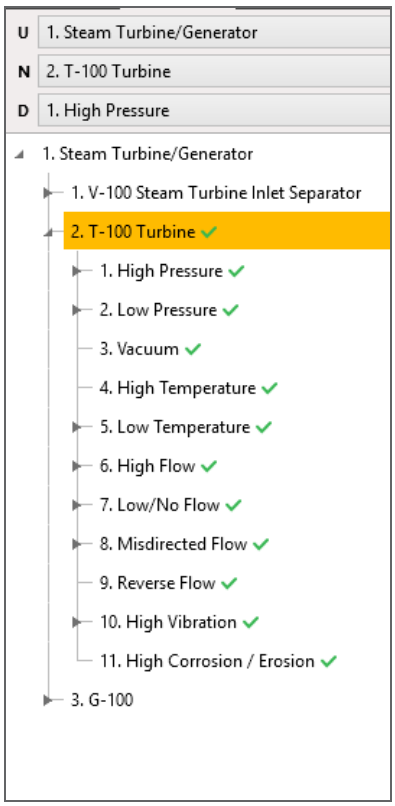
- Highlight the assigned Hazard Scenario
- Click on the ***Right*** arrow

C.3.9 Comments

Comments can be edited directly in the Comments text box. A Comment is associated with a single Cause. To delete a comment, highlight the text and click on the ***Delete*** key on your keyboard.

C.4 Navigation Tree

The exSILentia® v4 PHAx™ tool uses a Navigation Tree to allow for easy moving between the different HAZOP worksheets. In addition the navigation tree provides you with an outline of the project worksheets hierarchy. It allows you to quickly identify items that are completed and items that are not through the presence or absence of the completion mark next to the item.



C.4.1 Tree Hierarchy / Navigation

The PHAx™ Navigation Tree allows a quick glance at the project hierarchy from the Unit all the way down to the Safeguards, Recommendations, and Hazard Scenarios. In addition it allows rapid navigation throughout the project by double clicking on any entry. The Navigation Tree also has Expand and Contract buttons to allow a portion of the hierarchy to be expanded or collapsed. This allows for quick reference to make changes without having to navigate back and forth repeatedly. This also ensures that you can compare entries rather quickly by switching the selection back and forth.

C.4.2 Drag & Drop

The PHAx™ Navigation Tree is enabled with drag and drop actions. This allows you to move a particular Unit, Node, Deviation, Cause, Consequence, Safeguard, Recommendation, and/or Hazard Scenario. For instance, you can drag a Node from one Unit to a different Unit or you can drag that Node onto a different Node within the same Unit to reorder them. The table below provides a complete overview of the drag and drop operations.

As you are dragging you can hover over the potential destination which may be collapsed and it will automatically expand. As you drag down or up within the Navigation Tree, the tree will scroll in the direction you are dragging the item.

Note: If you are in the middle of a drag and drop operation and you wish to abort you can press the escape (**ESC**) key on your keyboard to abort the operation.

Drag	Drop On	Operation
Unit	Unit	Moves Unit directly above the Unit that it was dropped on.
Node	Unit	Moves Node to end of the Unit that it was dropped on.
Node	Node	Moves Node directly below the Node that it was dropped on, either within the same Unit or a different Unit.
Deviation	Node	Moves Deviation to end of the Node that it was dropped on.
Deviation	Deviation	Moves Deviation directly below the Deviation that it was dropped on, either within the same Node or a different Node.
Cause	Deviation	Moves Cause to end of the Deviation that it was dropped on.
Cause	Cause	Moves Cause directly below the Cause that it was dropped on, either within the same Deviation or a different Deviation.
Consequence	Cause	Moves Consequence to end of the Cause that it was dropped on.
Consequence	Consequence	Moves Consequence directly below the Consequence that it was dropped on, either within the same Cause or a different Cause.
Safeguard	Consequence	Moves Safeguard to the end of the Safeguard list within the Consequence. Since a Safeguard is a Library item, the link to the old Consequence will be replaced with a link to the new Consequence.
Safeguard	Safeguard	Moves Safeguard to the location it is dropped, allowing user to reorder the safeguards.
Recommendation	Consequence	Moves Recommendation to the end of the Recommendation list within the Consequence. Since a Recommendation is a Library item, the link to the old Consequence will be replaced with a link to the new Consequence.
Recommendation	Recommendation	Not permitted. The order of the Recommendations within a Consequence is chronological, this list is not sorted and cannot be reordered.

Drag	Drop On	Operation
Hazard Scenario	Consequence	Moves Hazard Scenario to the end of the Hazard Scenario list within the Consequence. Since a Hazard Scenario is a Library item, the link to the old Consequence with be replaced with a link to the new Consequence.
Hazard Scenario	Hazard Scenario	Not permitted. The order of the Hazard Scenarios within a Consequence is chronological, this list is not sorted and cannot be reordered.

C.4.3 Right Click Context Menu

The PHAx™ Navigation Tree is equipped with a right click context menu. The following options are available in the context menu:

- View
- Cut
- Copy
- Paste
- Delete
- Bookmark

When right clicking on a Deviation an additional menu item is available:

- Open PHA Worksheet

This menu option will open the PHAx™ Worksheet associated with the particular deviation in a separate window. This will allow you to review the particular deviation's information while working on documenting the process hazard analysis information for another deviation.

Within the Navigation Tree you can right click on any item except Safeguards and Recommendations to Copy the selected item or Copy all of the items contained therein and Paste them to the same location or a different location depending upon the available hierarchy.

C.5 User Interface / Usability

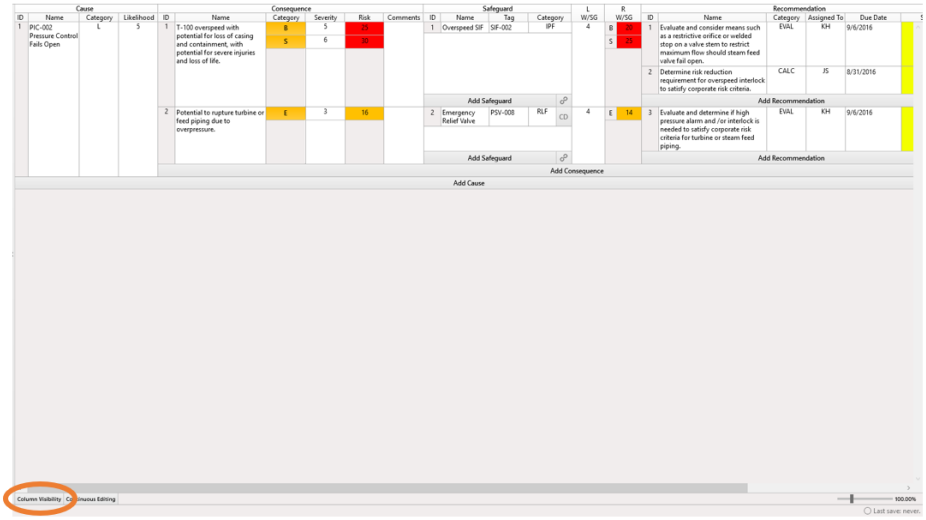
The PHAx™ tool allows several User Interface customizations to allow you to setup the tool to the best of your liking and improve your overall efficiency.

C.5.1 HAZOP Worksheet Column Widths

When using the PHAx™ tool HAZOP worksheet, the number of columns in the worksheet and the width of your screen can result in not all columns being displayed on your screen. Scrolling left and right to be able to view the respective columns can be inconvenient during a PHA session. PHAx™ allows you to adjust the width of each column on the HAZOP worksheet by placing the cursor over a vertical line between column headings and drag left or right until the column is the desired width.

C.5.2 HAZOP Worksheet Column Visibility

In addition to adjusting the width of the columns in the PHAx™ tool HAZOP worksheet, you can also decide that certain columns are not relevant for your PHA session. You can hide these columns on the worksheet. To do so, click on the *Column Visibility* button at the lower left hand side of the HAZOP worksheet. This will bring up a list of all column headings on the worksheet. The list shows a check mark in front of each heading. The check mark indicates that the column is visible on the worksheet. My clicking on a specific column heading, the column will be hidden on the worksheet and the check mark in front of the column heading will be removed. By default all columns are visible, so a check mark will appear in front of each column heading.

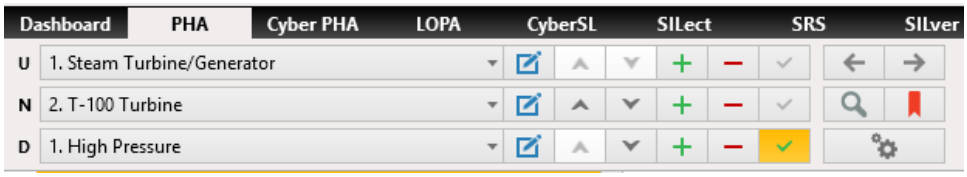


C.5.3 Continuous Editing

The PHAx™ tool HAZOP worksheet is developed such that the user can document the PHA results using the keyboard only, minimizing the need to switch back and forth from keyboard to mouse. For users who prefer to be using both keyboard and mouse, the continuous editing option has been implemented in the worksheet. This option is comparable to older style HAZOP worksheet implementations such as PHAx™ v2.x.

C.5.4 Worksheet Search, Back, Forward and Bookmarks

The PHA worksheet allows the user to search the entire PHA using the Search Button in the header, next to the Nodes. To find a particular item in the worksheet, the user can select the Search button and enter the name, description, or tag they are looking for. This will show the all places the item is found and allow the user to select an entry and navigate to it.



The PHA worksheet allows the user to move back and forward to the previous deviations analyzed. It also allows the user to set bookmarks at any unit, node, deviation, cause, consequence, safeguard or recommendation. This makes it possible to navigate easily to specific places in the worksheet. To set a bookmark, the user can select a location, right click and select bookmark from the menu. To find a bookmark select the Bookmark button in the header, next to the search button. This will show all bookmarks, allowing the user to choose a location by double clicking the specific bookmark.

C.6 PHAx™ Reports

In order to generate a PHAx™ report select the *PHA Report* option from the Report Wizard. The Report Wizard will show applicable Report Options, i.e. *Sections*, *Appendices*, *Columns*, and *User Data*.

C.6.1 Sections

The Sections Report Option allows you to define the sections that you want to include in your PHA report. You can include/exclude sections by simply checking or un-checking the check boxes in front of the respective sections. A select all and deselect all option are available to quickly include or exclude all sections.

The optional report sections are:

- Scope of Review
  - Documents general project information, defined process description, PHA participants, PHA sessions, and overview of all Units and Nodes considered in the PHA.
- Reference Documents
  - Documents all reference documents used in the PHA including regulatory documents.
- Study Methods and Results
  - Documents overall PHA objectives, PHA methods utilized, Risk Ranking used, major hazards identified, and Recommendations.
- Abbreviations and Definitions
  - Documents exida default abbreviations and optionally user defined abbreviations and definitions.
- Disclaimer and Assumptions
  - Documents the PHAx™ module specific disclaimer and relevant assumptions in the software.

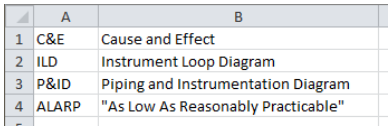
Note that members/PHA participants that are defined with the role "Leader" will be identified within the PHA participants overview as Project Leader.

Reference Documents

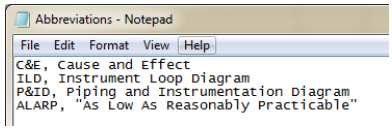
The PHA Report will provide two separate sections with reference documents, one section with Regulatory documents named *Applicable Standards*and one section with all other documents. Regulatory documents should have the Reference type Reg, see section *6.5 Reference Types* which describes the definition of reference types within the Project Configuration.

Abbreviations and Definitions

The PHA Report has a set of default abbreviations. You can include a set of additional user defined abbreviations by selecting the *Include User Defined Abbreviations* radio button. After pressing the ***Select File*** button the open file dialog will appear and you will be able to navigate to a separate file containing your list of abbreviations. Four file types are supported .xlsx, .xls, .txt, and .csv. You will need to specify the file type in the open file dialog. Examples of user defined abbreviation files are shown below.

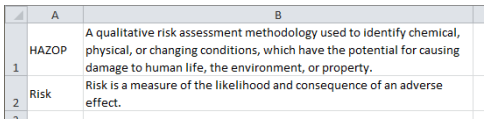


	A	B
1	C&E	Cause and Effect
2	ILD	Instrument Loop Diagram
3	P&ID	Piping and Instrumentation Diagram
4	ALARP	"As Low As Reasonably Practicable"

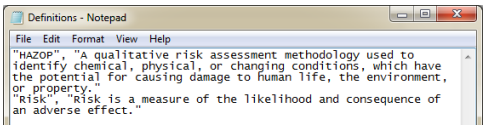


Note: The user defined abbreviations file must not contain a header row. For .xlsx and .xls files the abbreviation must appear in column A and the associated description must appear in the adjacent cell in column B. For .txt and .csv files the abbreviation must appear in line with the description and separated by a comma. The description may contain a comma, but if it does, the description must be surrounded with quotes. Quote symbols in any of the file types will be removed during the report generation.

You can also add definitions to your PHA Report by selecting the *Include User Defined Definitions* radio button. After pressing the ***Select File*** button the open file dialog will appear and you will be able to navigate to a separate file containing your list of definitions. Four file types are supported .xlsx, .xls, .txt, and .csv. You will need to specify the file type in the open file dialog. Examples of user defined definition files are shown below.



	A	B
1	HAZOP	A qualitative risk assessment methodology used to identify chemical, physical, or changing conditions, which have the potential for causing damage to human life, the environment, or property.
2	Risk	Risk is a measure of the likelihood and consequence of an adverse effect.



Note: The user defined definition file must not contain a header row. For .xlsx and .xls files the term must appear in column A and the associated definition must appear in the adjacent cell in column B. For .txt and .csv files the term must appear in line with the definition and separated by a comma. The description may contain a comma, but if it does, the description must be surrounded with quotes. Quote symbols in any of the file types will be removed during the report generation.

C.6.2 Appendices

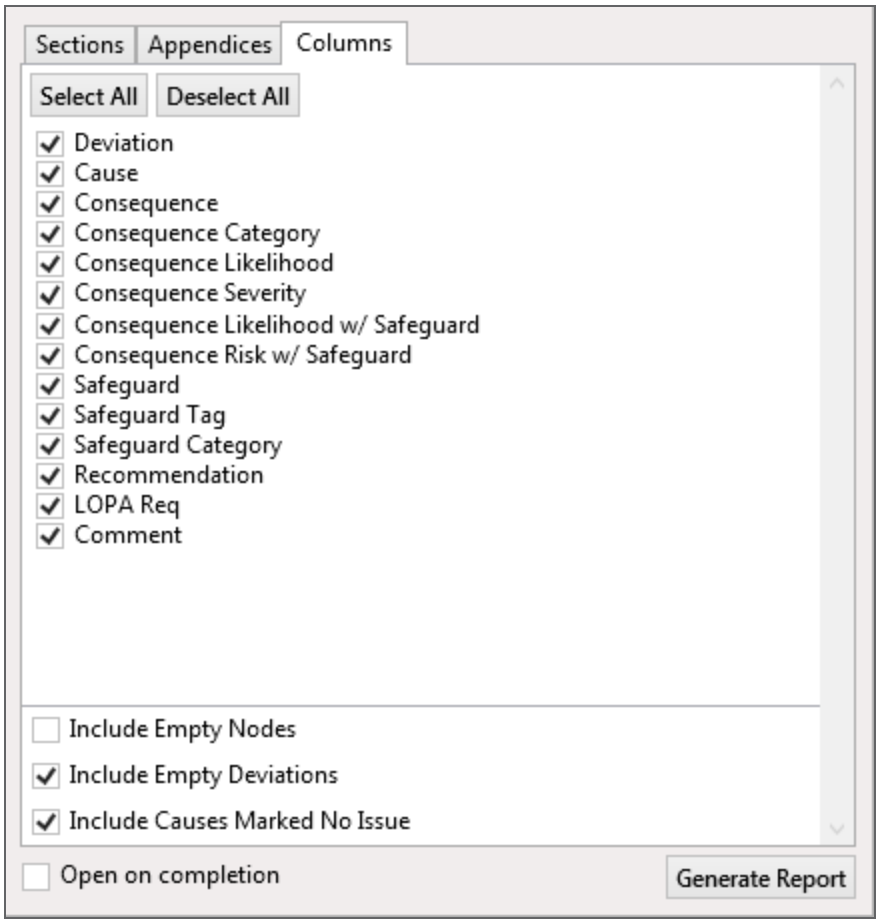
The Appendices Report Option allows you to define the appendices that you want to include in your PHA report. The appendices will document the detailed HAZOP worksheets, Facility Siting Checklists etc. You can include/exclude appendices by simply checking or un-checking the check boxes in front of the respective appendices. A select all and deselect all option are available to quickly include or exclude all appendices.

HAZOP Recommendations

When you include the HAZOP Recommendation appendix in your PHA report you have the option to determine the order in which you want the recommendations to be documented. You can sort based on *Risk*, Recommendation *Category*, or *Recommendation*.

C.6.3 Columns

The Columns Report Option allows you to define which columns will be included in the *HAZOP Worksheets* portion of the PHA report, provided that you included the HAZOP worksheets Appendix. You can include/exclude columns by simply checking or un-checking the check boxes in front of the respective columns. A select all and deselect all option are available to quickly include or exclude all columns.



Each of the check boxes in the Columns Report Option window corresponds to a column within the HAZOP Worksheet.

If you check the *Include Empty Deviations* check box, any deviation that does not have a Cause associated with it will be included in the PHA report. If you check the *Include Causes Marked No Issue* check box, any causes which are marked ***No Issue*** will be included in the report.

C.7 PHAx Data Import

C.7.1 Import Template

The following fields are supported for import into PHA. The fields appear in the 2nd row and must have the following name as specified in the Field Name column. The data must appear within the 3rd row and beyond. If the file is a .CSV the field names must appear within the first row and the data following in the 2nd row and beyond.

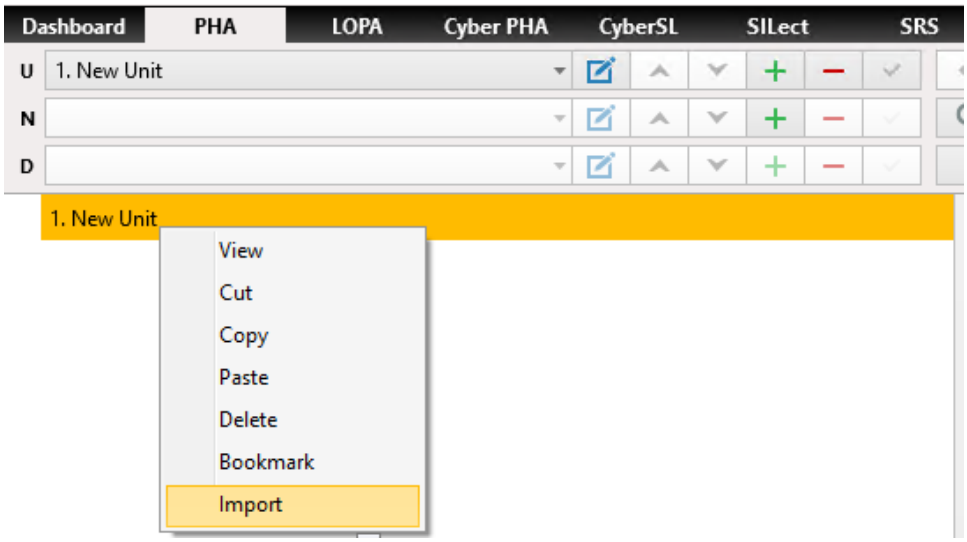
Category	Field Name	Data Type	Valid Values	Required
Unit	Unit Name	String		

Category	Field Name	Data Type	Valid Values	Required
Node Information	Node Name	String		X
	Intention	String		
	Node Reference	String	List of one or more references delimited by a semicolon ';'	
Deviation	Deviation Name	String		X
	Design Intent	String		
	Complete	String	"TRUE", "T", "YES", "FALSE", "F", "NO" Blank or not specified is unchecked	
	No Issues	String	"TRUE", "T", "YES", "FALSE", "F", "NO" Blank or not specified is unchecked	
Cause	Cause Name	String		X
	Cause Category	String	Matches Code field in Likelihood Categories	
	Likelihood	String	Matches Code field in Likelihood Levels	
	Frequency	Decimal		
Consequence	Consequence Name	String		X
	Severity Category	String	Matches Code field in Severity Category	
	Severity	String	Matches Code field in Severity Levels	
	Consequence Comments	String		
	Likelihood w/ Safeguards	String	Matches Code field in Likelihood Levels	
	LOPA	String	"TRUE", "T", "YES", "FALSE", "F", "NO", "N/A"	
	Hazard Scenario	String		
Safeguards	Safeguard Name	String		X
	Safeguard Description	String		
	Safeguard Tag	String		
	Safeguard Category	String	Matches Code property in Safeguard Category within the Project Configuration	
	Safeguard is SIF	String	"TRUE", "T", "YES", "FALSE", "F", "NO" Note: Requires Safeguard Category to be selected that has its Category Type set to IPF	
	Safeguard Reference	String	List of one or more references delimited by a semicolon ';'	
	Safeguard Comments	String		

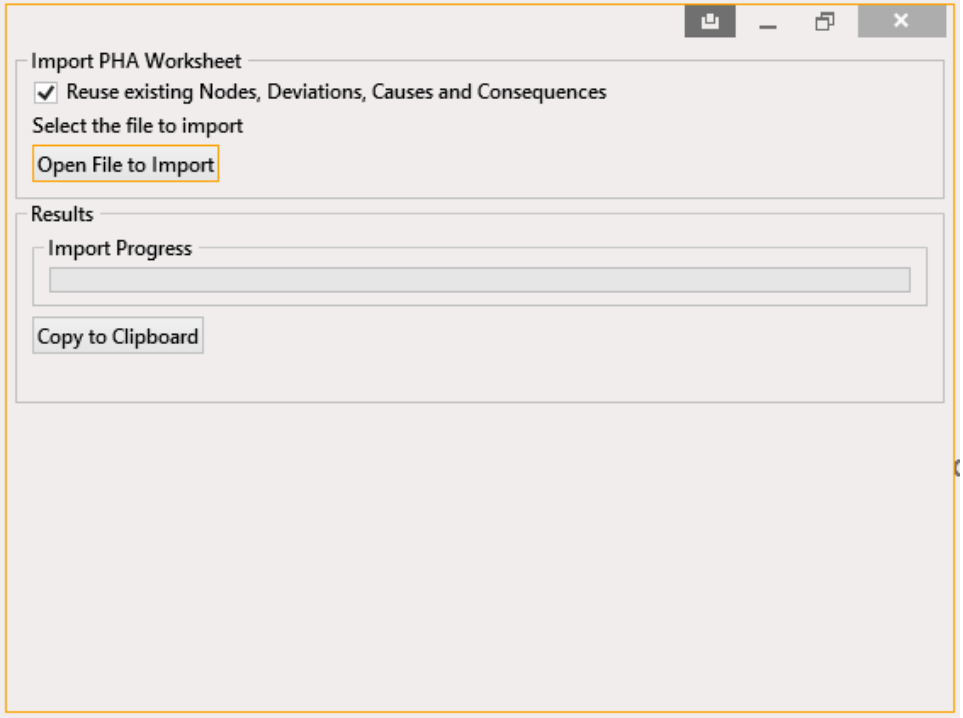
Category	Field Name	Data Type	Valid Values	Required
Recommendations	Recommendation Name	String		X
	Recommendation Description	String		
	Recom. Category	String	Matches Code property in Recommendation Category within the Project Configuration	
	Recom. Assigned To	String	"Firstname Lastname"	
	Recom. Due Date	Date		
	Recom. Status	String	Matches Code property in Recommendation Status within the Project Configuration	
	Recommendation Comments	String		

C.7.2 PHA Import

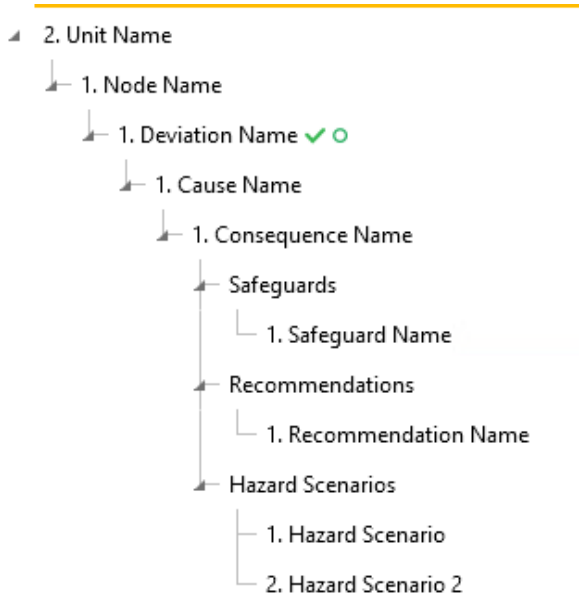
Open PHA and select a target unit to import into or create a new unit and select it. Right click on the unit and choose Import from the context menu.



A dialog will appear. Click on the button Open File to Import. The file types that you can select include .xls, .xlsx, .xlsm and .csv. You may select more than one file to import. See the next section on the template. If you want to reuse existing Nodes, Deviations, Causes and Consequences check that box prior to importing. This setting will always default to unchecked.



After the import completes you should see the tree view populated with your imported items as shown below in this example import.

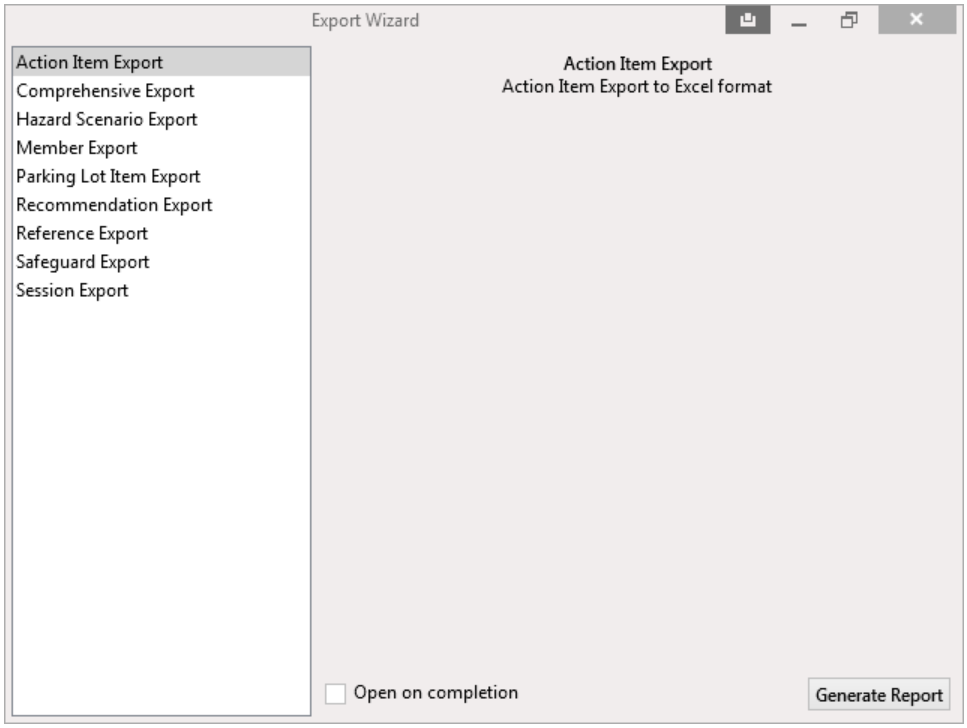


C.8 PHAx™ Data Export

In order to export PHAx™ data select the *Export Data* button from the Dashboard, this will launch the Export Wizard. The Export Wizard will show applicable Export Selections, i.e. *Action Item*, *Comprehensive*, *Hazard Scenario*, *Member*, *Parking Lot Item*, *Recommendation*, *Reference*, *Safeguard*, and *Session*.

When you select any of the PHAx™ export selections, except the *Comprehensive* option, and click on **Export Selected**, the relevant data will be exported to a MS Excel Worksheet creating a single Workbook for each selected export item. If you select the *Comprehensive* export selection a single Workbook will be generated with worksheets for each of the individual selection options except for the Parking Lot Items.

In some cases when you use the export data function, you may be asking for a particular export selection to be generated while no data is available for that option. exSILentia® v4 will in that case not create a Workbook or Worksheet for that item.

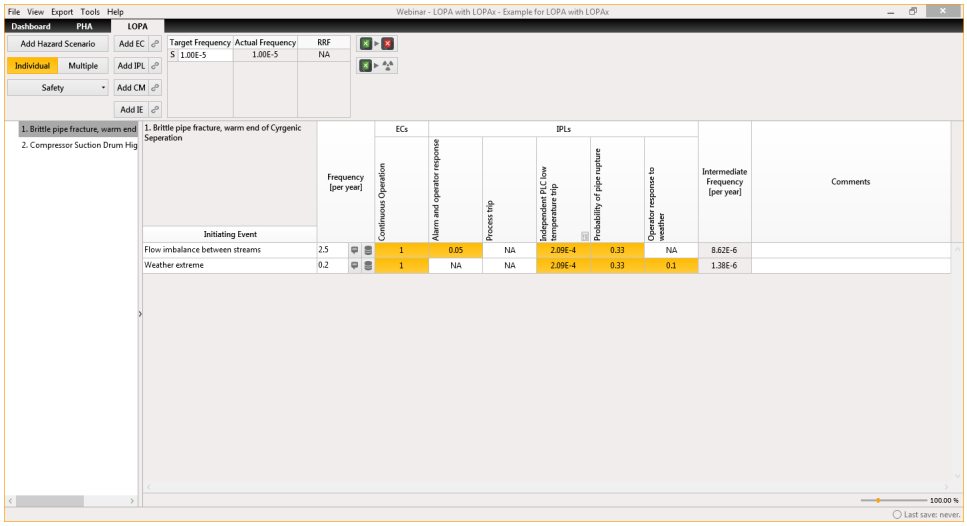


Appendix D LOPAx™

The LOPA tab navigates to the exSILentia® v4 layer of protection analysis tool LOPAx™. Availability of the LOPA tab, and therefore the LOPAx™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The LOPAx™ tool allows layer of protection analysis to be performed using a Hazard Scenario basis with multiple initiating events and variable effectiveness of protection layers for each initiating event and each Severity Category.

D.1 Introduction

The layer of protection analysis functionality in the LOPAx™ tool uses a spreadsheet type interface that enables the specification of multiple Initiating Events (IE) and their associated Enabling Conditions (EC), Independent Protection Layers (IPL), and Conditional Modifiers (CM).

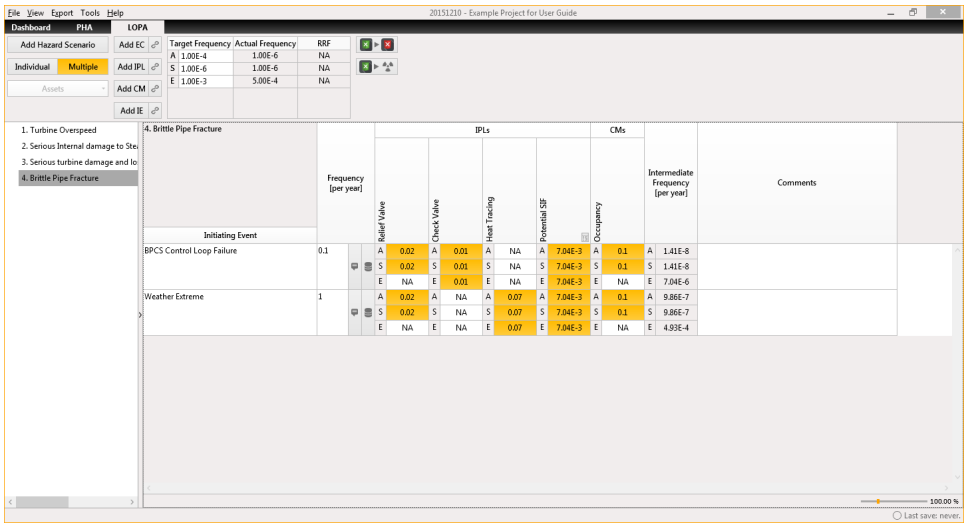


In the subsequent sections the LOPAx™ worksheet, its embedded risk reduction calculations functionality, and its reporting capability will be explained. The available interfaces with the PHAx™ tool will also be addressed.

D.2 LOPA Worksheet

The LOPAx™ tool layer of protection analysis worksheet uses a spreadsheet type interface for the evaluation of each Hazard Scenario. This provides a clear overview of the applicable initiating events and protection layers for the respective Severity Categories. Within the worksheet interface buttons exist for adding Initiating Events (IE), Enabling Conditions (EC), Independent Protection Layers (IPL), and Conditional Modifiers (CM) to the LOPA Worksheet for a specific Hazard Scenario. Applicability of a EC, IPL, and/or CM can be edited directly in the worksheet. As the Initiating Events, Enabling Conditions, Independent Protection Layers, and Conditional Modifiers are part of the Project Libraries (see *Chapter 7 Project Libraries*) they can be linked to existing items. The LOPA worksheet consists of three main areas: the toolbar, the Hazard Scenario list, and the workspace.

An example of the LOPAx™ tool layer of protection analysis worksheet is shown in the figure below.



D.2.1 Creating Hazard Scenarios

LOPAx™ Hazard Scenarios are comprised of two related data fields, i.e. ID and Name. The Hazard Scenario ID is automatically generated and assigned to ensure relational data integrity. Hazard Scenarios can be defined manually within the LOPAx™ tool or obtained from the work previously done using the PHAx™ tool. The transferring of data from PHA to LOPA is described in section *D.4 Hazard Scenario Data Transfer from PHAx™*.

To add a Hazard Scenario:

- Click on the ***Add Hazard Scenario*** button in the upper left hand corner of the toolbar
- This will immediately add the Hazard Scenario to the Hazard Scenario list

To edit the Hazard Scenario Name:

- Right click on the Hazard Scenario in the Hazard Scenario list and select edit, or
- Double click the Hazard Scenario name in the upper left hand corner of the worksheet

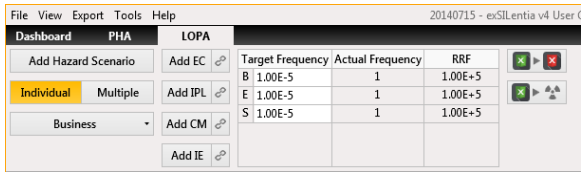
To delete a Hazard Scenario:

- Select the Hazard Scenario in the Hazard Scenario list
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Hazard Scenario is really to be deleted

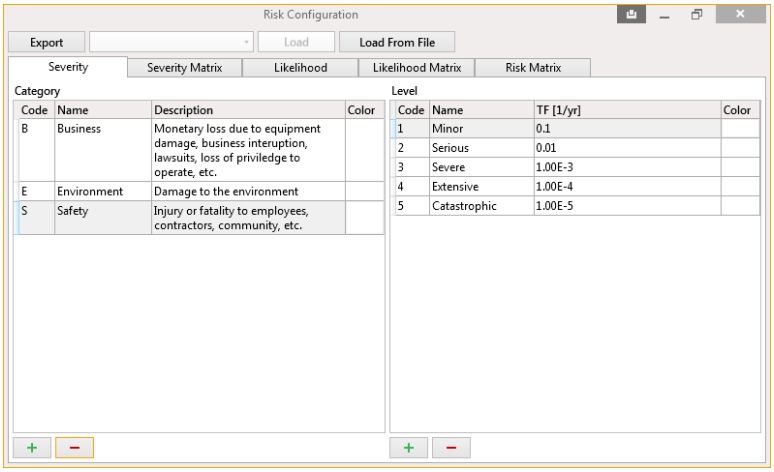
CAUTION: Deleting a Hazard Scenario will delete all instances where the Hazard Scenario was used. This will include any linking done in the PHAx™ tool.

D.2.2 Specifying Target Frequencies

LOPAx™ uses Target Frequencies to help determine if the accident frequency is tolerable. In case the accident frequency is higher than the target frequency a required risk reduction will be determined that must be implemented to bring the frequency to a tolerable level. For Hazard Scenarios that are manually defined within the LOPA worksheet, LOPAx™ will define a target frequency of 1.00E-5 events per year. You can update these target frequency by directly editing in the LOPAx™ worksheet toolbar. The target frequency should be defined on a per year basis. Note that the target frequencies do not need the same for all Severity Categories.



When transferring data from PHA to LOPA, see section *D.4 Hazard Scenario Data Transfer from PHAx™*, the target frequencies will be automatically defined based on the severity level selections related to the Hazard Scenario. The target frequencies that are used in this case were defined earlier in the Risk Configuration, see section *8.1 Consequence Categories and Severity Levels*.



D.2.3 Initiating Events (IE)

An initiating event represents the start of a hazard scenario sequence. During the process hazard analysis, Initiating Events are referred to as Causes. Though the label is different, in PHAx™and LOPAx™ the cause and initiating event entities are the same.

To add a new Initiating Event:

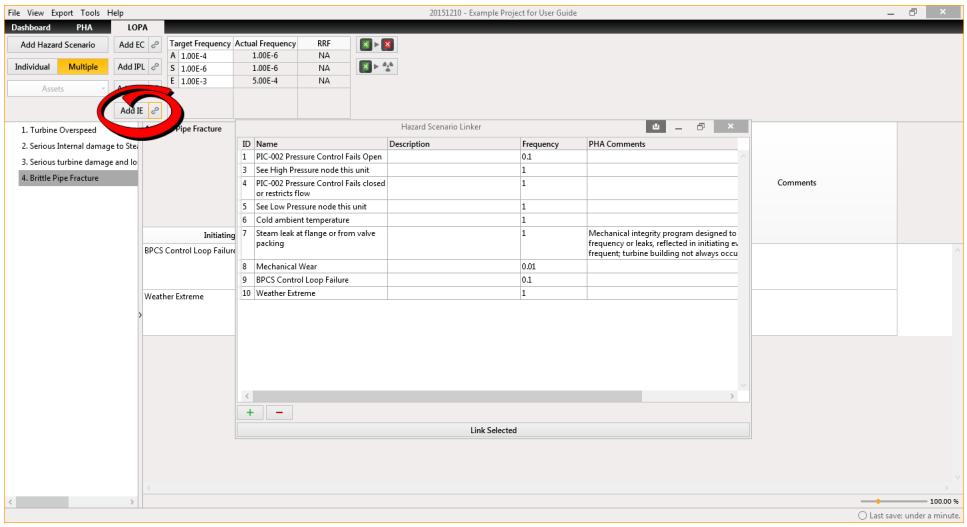
- Click on the ***Add IE*** button at the upper left hand corner of the toolbar
- This will immediately add the Initiating Event to the LOPAx™ Worksheet
- This will also add the Initiating Event to the Causes (Initiating Events) library

To edit the Initiating Event Name:

- Double click the initiating event name in the worksheet, or
- Right click on the initiating event in the worksheet and select edit

To add an Initiating Event directly from the Causes (Initiating Events) Library:

- Click on the Link Initiating Event Icon
- Highlight the Initiating Event(s) to add
- Click on ***Link Selected***



To delete an Initiating Event:

- Highlight the Initiating Event
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Initiating Event is really to be deleted

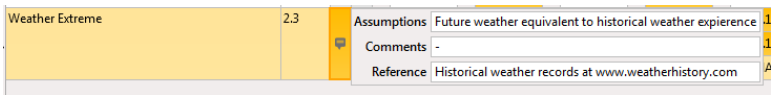
Note: When an Initiating Event is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Initiating Event from the Library. Click **Yes** or **No** as applicable.

When you add an initiating event a default initiating event frequency of 1 per year is associated with the initiating event. This value can of course be update as needed. There are two ways to update the associated initiating event frequency, you can

- Directly edit the frequency within the workspace, or
- Reference one of the LOPA databases, see section *12.1 LOPA Database* regarding the source or population of these databases

To directly edit the frequency within the workspace:

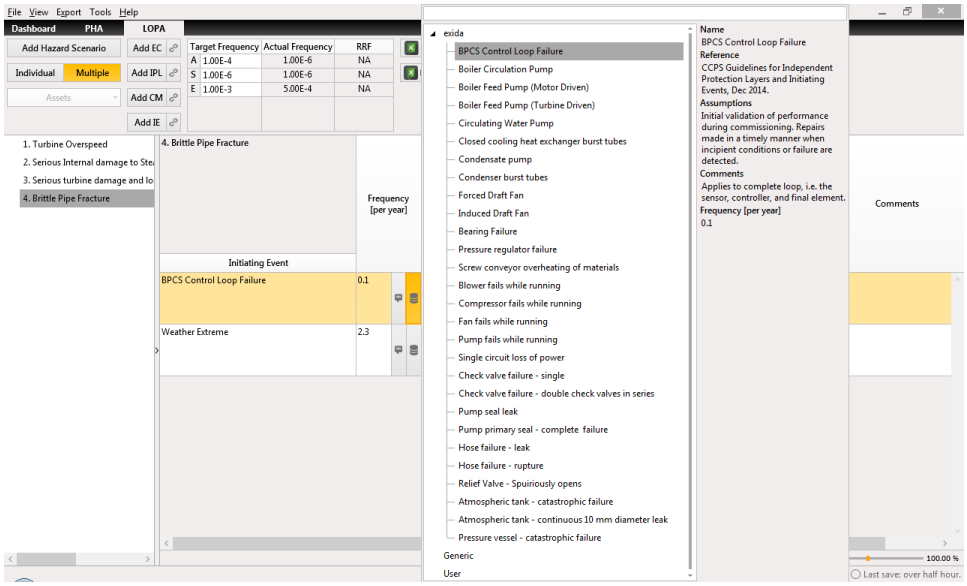
- Highlight the Initiating Event frequency value
- Type in the applicable value (frequency must be per year)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon



To obtain data from one of the LOPA databases:

- Click on the database icon
- Select the applicable initiating event from the database
- Click on ***Apply Data***
- A warning message will appear asking for confirmation to overwrite any existing data
- Upon confirmation, the applicable initiating event frequency, assumptions, comments, and reference will be copied to the selected Initiating Event

Note: When an Initiating Event is used in multiple locations, changing its properties (including the initiating event frequency) will impact all locations where that initiating event is used.



D.2.4 Enabling Condition (EC)

An enabling condition is a situation that must occur at the same time as a given initiating event to allow that specific initiating event to propagate to a consequence of interest. A typical enabling condition is time at use; this would allow to account for batch process operation where initiating event frequencies may be based on an assumption of continuous operation.

To add a new Enabling Condition:

- Click on the ***Add EC*** button at the upper left hand corner of the toolbar
- This will immediately add the Enabling Condition to the LOPAx™ Worksheet
- This will also add the Enabling Condition to the Enabling Conditions library

To edit the Enabling Condition Name:

- Double click the Enabling Condition name in the worksheet, or
- Click on the Edit icon when hovering over the Enabling Condition, or
- Right click on the Enabling Condition in the worksheet and select edit

To add an Enabling Condition directly from the Enabling Condition Library:

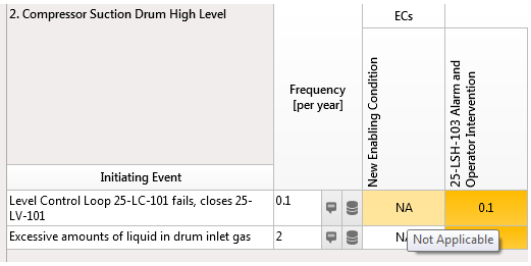
- Click on the Link Enabling Condition Icon
- Highlight the Enabling Condition(s) to add
- Click on ***Link Selected***

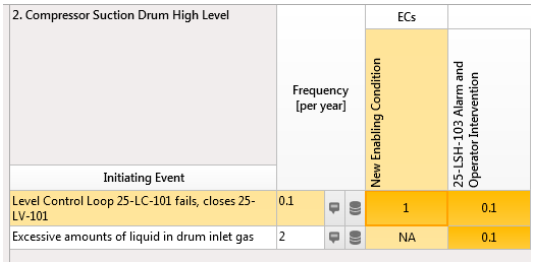
To delete an Enabling Condition:

- Highlight the Enabling Condition
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Enabling Condition is really to be deleted

Note: When an Enabling Condition is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Enabling Condition from the Library. Click **Yes** or **No** as applicable.

When you add an Enabling Condition a default probability of the situation occurring of 1 is associated with the Enabling Condition. In addition the Enabling Condition is set to be Not Applicable (NA) to all Initiating Events in the LOPAx™ Worksheet. Applicability and probability of the situation occurring can be update as needed. To change the applicability of an enabling condition to a specific initiating event, simply double click the intersection of enabling condition and initiating event. The NA will then change to the probability associated with the enabling condition.



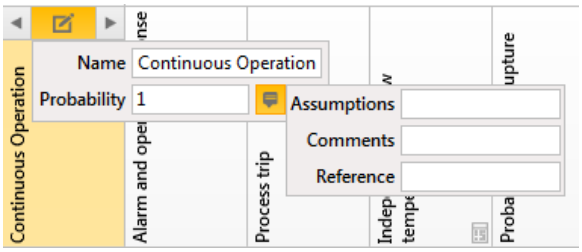


There are two ways to update the Enabling Condition probability, you can

- Manually edit the probability, or
- Reference one of the LOPA databases, see section *12.1 LOPA Database* regarding the source or population of these databases

To manually edit the probability:

- Click on the Edit icon when hovering over the Enabling Condition or right click on the Enabling Condition in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon



To obtain data from one of the LOPA databases:

- Click on the database icon
- Select the applicable Enabling Condition from the database
- Click on ***Apply Data***
- A warning message will appear asking for confirmation to overwrite any existing data
- Upon confirmation, the applicable Enabling Condition probability, assumptions, comments, and reference will be copied to the selected Enabling Condition

Note: When an Enabling Condition is used in multiple locations, changing its properties (including the enabling condition probability) will impact all locations where that enabling condition is used.

D.2.5 Independent Protection Layers (IPL)

An independent protection layer (IPL) is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. Typical independent protection layers are BPCS interlock, operator responding to alarm, check valve, relief valve, etc. During the process hazard analysis, Independent Protection Layers are referred to as Safeguards. Though the label is different, in PHAx™and LOPAx™ the safeguard and independent protection layers are the same.

To add a new Independent Protection Layer:

- Click on the ***Add IPL*** button at the upper left hand corner of the toolbar
- This will immediately add the Independent Protection Layer to the LOPAx™ Worksheet
- This will also add the Independent Protection Layer to the Safeguards library

To edit the Independent Protection Layer Name:

- Double click the Independent Protection Layer name in the worksheet, or
- Click on the Edit icon when hovering over the Independent Protection Layer, or
- Right click on the Independent Protection Layer in the worksheet and select edit

To add an Independent Protection Layer directly from the Independent Protection Layer Library:

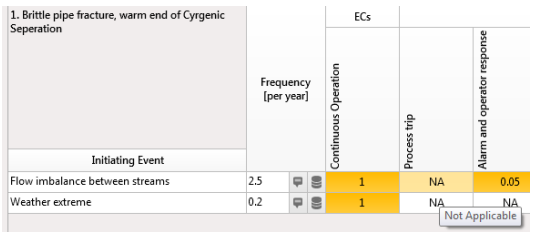
- Click on the Link Independent Protection Layer Icon
- Highlight the Independent Protection Layer(s) to add
- Click on ***Link Selected***

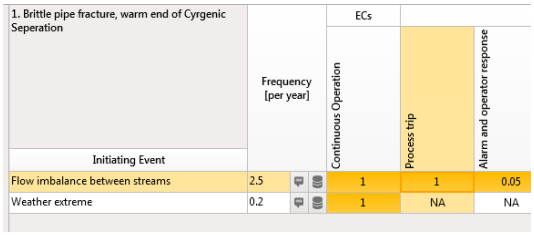
To delete an Independent Protection Layer:

- Highlight the Independent Protection Layer
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Independent Protection Layer is really to be deleted

Note: When an Independent Protection Layer is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Independent Protection Layer from the Library. Click **Yes** or **No** as applicable.

When you add an Independent Protection Layer a default probability of failure of 1 is associated with the Independent Protection Layer. In addition the Independent Protection Layer is set to be Not Applicable (NA) to all Initiating Events in the LOPAx™ Worksheet. Applicability and probability of failure can be update as needed. To change the applicability of an independent protection layer to a specific initiating event, simply double click the intersection of independent protection layer and initiating event. The NA will then change to the probability associated with the enabling condition.



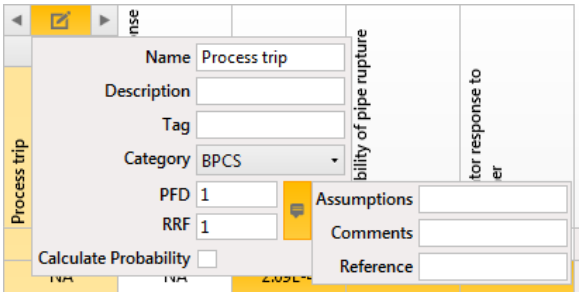


There are two ways to update the Independent Protection Layer probability, you can

- Manually edit the probability, or
- Reference one of the LOPA databases, see section *12.1 LOPA Database* regarding the source or population of these databases

To manually edit the probability:

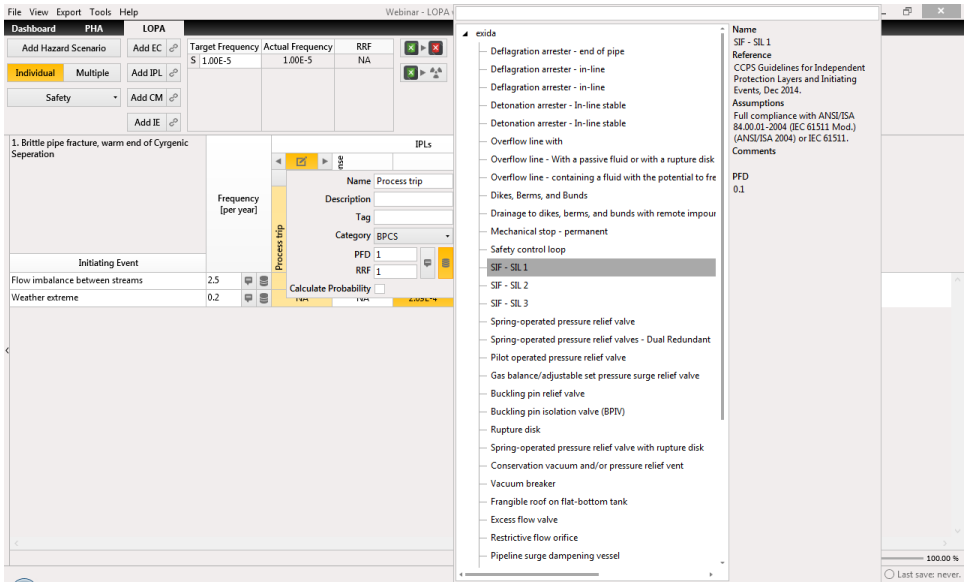
- Click on the Edit icon when hovering over the Independent Protection Layer or right click on the Independent Protection Layer in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon



To obtain data from one of the LOPA databases:

- Click on the database icon
- Select the applicable Independent Protection Layer from the database
- Click on ***Apply Data***
- A warning message will appear asking for confirmation to overwrite any existing data
- Upon confirmation, the applicable Independent Protection Layer probability, assumptions, comments, and reference will be copied to the selected Independent Protection Layer

Note: When an Independent Protection Layer is used in multiple locations, changing its properties (including the independent protection layer probability) will impact all locations where that enabling condition is used.



D.2.6 Conditional Modifiers (CM)

A conditional modifier is typically defined as one of the three independent factors of probability of ignition, probability of occupancy, and probability of injury, i.e. probabilities generally associated with the post incident part of an incident sequence.

To add a new Conditional Modifier:

- Click on the ***Add CM*** button at the upper left hand corner of the toolbar
- This will immediately add the Conditional Modifier to the LOPAx™ Worksheet
- This will also add the Conditional Modifier to the Conditional Modifiers library

To edit the Conditional Modifier Name:

- Double click the Conditional Modifier name in the worksheet, or
- Click on the Edit icon when hovering over the Conditional Modifier, or
- Right click on the Conditional Modifier in the worksheet and select edit

To add a Conditional Modifier directly from the Conditional Modifier Library:

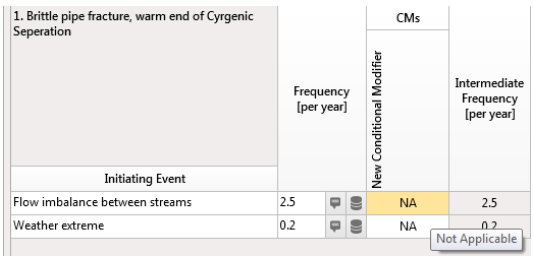
- Click on the Link Conditional Modifier Icon
- Highlight the Conditional Modifier(s) to add
- Click on ***Link Selected***

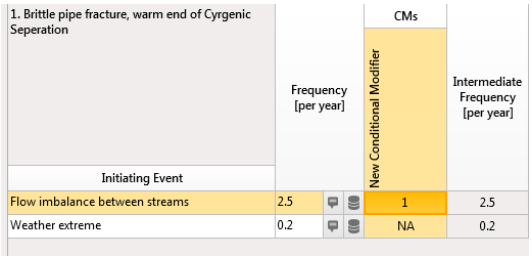
To delete a Conditional Modifier:

- Highlight the Conditional Modifier
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Conditional Modifier is really to be deleted

Note: When a Conditional Modifier is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Conditional Modifier from the Library. Click **Yes** or **No** as applicable.

When you add a Conditional Modifier a default probability of 1 is associated with the Conditional Modifier. In addition the Conditional Modifier is set to be Not Applicable (NA) to all Initiating Events in the LOPAx™ Worksheet. Applicability and probability can be update as needed. To change the applicability of an conditional modifier to a specific initiating event, simply double click the intersection of conditional modifier and initiating event. The NA will then change to the probability associated with the conditional modifier.



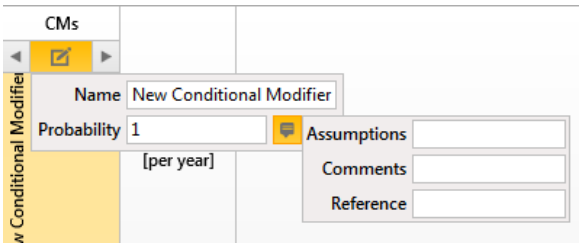


There are two ways to update the Conditional Modifier probability, you can

- Manually edit the probability, or
- Reference one of the LOPA databases, see section *12.1 LOPA Database* regarding the source or population of these databases

To manually edit the probability:

- Click on the Edit icon when hovering over the Conditional Modifier or right click on the Conditional Modifier in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon



To obtain data from one of the LOPA databases:

- Click on the database icon
- Select the applicable Conditional Modifier from the database
- Click on ***Apply Data***
- A warning message will appear asking for confirmation to overwrite any existing data
- Upon confirmation, the applicable Conditional Modifier probability, assumptions, comments, and reference will be copied to the selected Conditional Modifier

Note: When a Conditional Modifier is used in multiple locations, changing its properties (including the conditional modifier probability) will impact all locations where that conditional modifier is used.

D.2.7 Calculating Required Risk Reduction Factors (RRF)

The LOPAx™ Worksheet determines an Intermediate Frequency for each initiating event in a hazard scenario. This Intermediate frequency is calculated by multiplying the initiating event frequency with the probabilities associated with the applicable Enabling Conditions, Independent Protection Layers, and Conditional Modifiers. The calculated Intermediate Frequency is displayed on the right hand side of the worksheet for each initiating event.

The actual hazard scenario frequency is calculated by adding each initiating event's intermediate frequency. This hazard scenario actual frequency is displayed in the menu bar of the worksheet for each severity Category.

Hazard Scenario Risk Reduction Factor

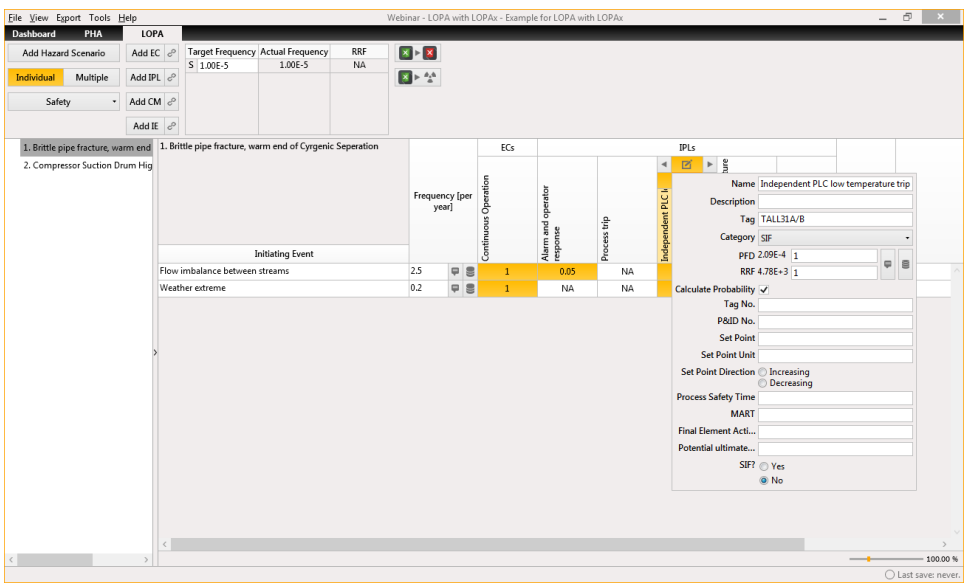
Given the target frequency specified and the actual frequency calculated a target Risk Reduction Factor (RRF) for the hazard scenario is calculated. If the actual frequency is less than or equal to the target frequency, the Risk Reduction Factor will state a NA for not applicable, indicating no further risk reduction is required. The calculated Risk Reduction Factor is input to the SIL Target Selection performed in the SILect™ tool where a Safety Instrumented Function is to be defined that protects against the initiating events identified for the hazard scenario.

Specific IPL Risk Reduction Factor

If the hazard scenario risk reduction factor indicates that additional risk reduction is needed, LOPAx™ can also determine the required risk reduction for one of more specific Independent Protection Layers. This is useful for a scenario where one of the independent protection layers identified is a potential Safety Instrumented Function, rather than assuming a specific target SIL the tool will allow the calculation of the exact risk reduction required for.

To enable the automatic required risk reduction calculation for a specific independent protection layer:

- Click on the Edit icon when hovering over the Independent Protection Layer, or right click on the Independent Protection Layer in the worksheet and select edit, and select the ***Calculate Probability*** check box, or
- Click on the Calculator icon when hovering over the Independent Protection Layer



The calculation algorithm will look at the severity category with the worst case difference between actual and target frequency and use that as the basis for the Risk Reduction Factor calculation.

If you indicate that you want to “calculate probability for multiple independent protection layers, LOPAx™ will perform a similar calculation assuming that each IPL must provide adequate risk reduction weighed to the initiating event, or initiating events, they are protecting against.

If the target frequency cannot be met due to the limited applicability of the independent protection layer, the calculated required risk reduction will be 1, i.e. the probability of failure on demand of the independent protection layers is assumed to be 1. In this case a target risk reduction will be indicated for the hazard scenario.

An Independent Protection Layer that is marked of type SIF, where risk reduction is required, is automatically flagged for subsequent activities in the Safety Lifecycle. In this case the calculated Risk Reduction Factor is simply to be converted into a target SIL during the SIL Target Selection performed in the SILect™ tool.

D.2.8 Comments

Comments can be edited directly in the Comments text box. A Comment is associated with a single Initiating Event. To delete a comment, highlight the text and click on the ***Delete*** key on your keyboard. Note that LOPAx Comments are independent of the PHAx Comments.

D.3 User Interface / Usability

The LOPAx™ tool allows several User Interface customizations to allow you to setup the tool to the best of your liking and improve your overall efficiency.

D.3.1 LOPA Worksheet Column Widths

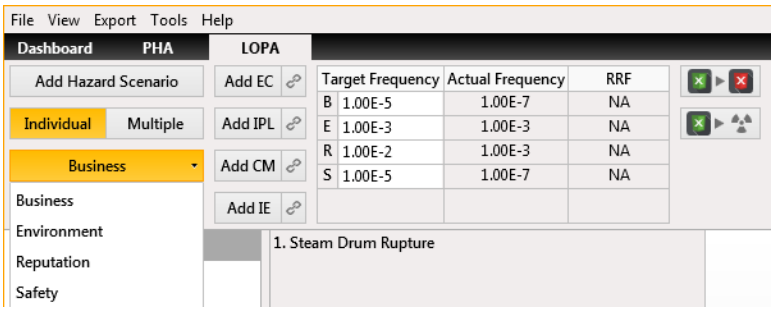
When using the LOPAx™ worksheet, the number of columns in the worksheet and the width of your screen can result in not all columns being displayed on your screen. Scrolling left and right to be able to view the respective columns can be inconvenient during a LOPA session. LOPAx™ allows you to adjust the width of each column on the LOPA worksheet by placing the cursor over a vertical line between column headings and drag left or right until the column is the desired width. LOPAx™ also allows you to change the width of the navigation list by placing the cursor over the vertical line between the navigation list and the worksheet area. You can hide or unhide the navigation list by clicking on the line between the navigation list and the worksheet area.

D.3.2 LOPA Worksheet Header Row Height

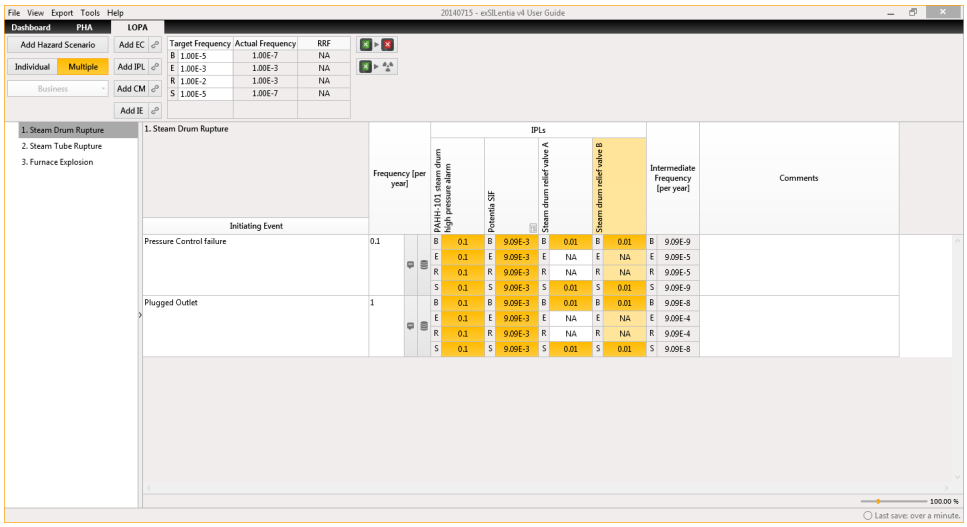
In addition to adjusting the width of the columns in the LOPAx™ worksheet, you can also adjust the height of the Column Header Row by placing the cursor over the horizontal line right under the Initiating Event header line and dragging up or down until the header row has the desired height.

D.3.3 Severity Category Visibility

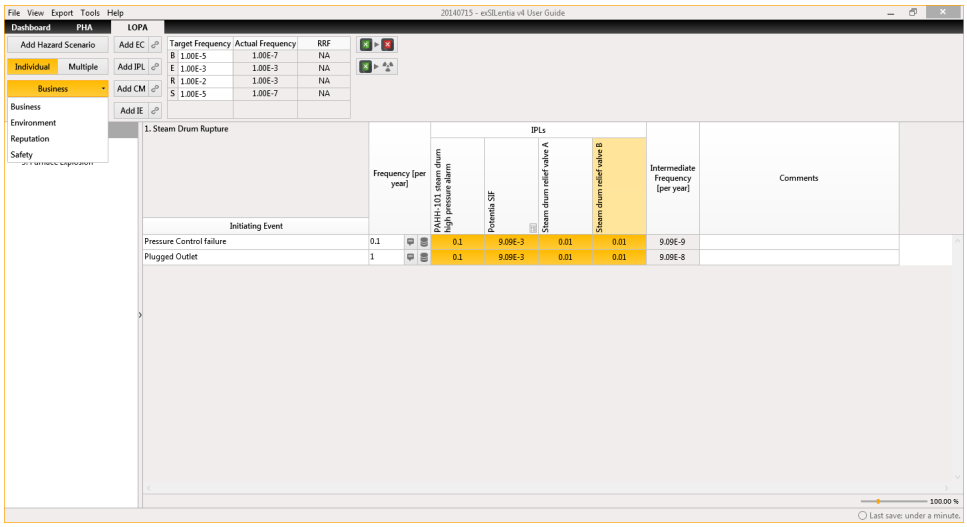
The LOPAx™ worksheet is designed such that you can perform a LOPA analysis for each Severity Category individually or for all Severity Categories at the same time. The number of separate Severity Category options depend on your risk configuration, see section *8.1 Consequence Categories and Severity Levels*. To switch between single severity category and all severity categories visibility modes click on the ***Individual*** and ***Multiple*** buttons in the upper left hand corner of the LOPAx™ worksheet. The dropdown box underneath these two buttons allows you to select the different severity categories in case you have opted to look at each LOPA analysis seperately.



When opting to review the LOPA analysis for multiple severity categories at the same time the LOPAx™ worksheet can be easily used to determine for which severity categories a protection layer is considered effective.



When opting to review the LOPA analysis for a single severity category at a time, the LOPAx™ worksheet limits the visibility to only those selections that are applicable.



D.4 Hazard Scenario Data Transfer from PHAx™

The exSILentia® v4 integration of Process Safety / Functional Safety software tools allows for seamless data exchange between the different phases of the Lifecycle. If the Process Hazard Analysis was performed using PHAx™, Hazard Scenarios were created, and the associated Cause-Consequence pair was flagged for LOPA evaluation, information from the PHA can be automatically transferred to LOPAx™. The PHA data is transfer to the LOPA Worksheet as indicated in the table below.

PHA	LOPA	Comments
Cause	Initiating Event	
Safeguard	Independent Protection Layer	Upon transfer the IPL is set to be Not Applicable (NA) to its associated Initiating Events
Consequence Severity Level	Target Frequency	If the hazard scenario is linked to multiple cause-consequence pairs with different severity levels, the worst case severity level will be used to determine the target frequency. The target frequency is defined for each Severity Category separately.

The automatic transferring of data from the PHA to the LOPA worksheet ensures that all relevant information is transferred. As a user you will still need to determine if PHA identified safeguards are indeed IPLs and assign the relevant probability of failures. In addition you will need to assign the applicable frequency to each Initiating Event and review any potential Enabling Condition and/or Conditional Modifiers.

There are two ways to transfer data from the PHA to the LOPA worksheet, you can transfer data

- for all hazard scenarios at once
- for one hazard scenario at a time

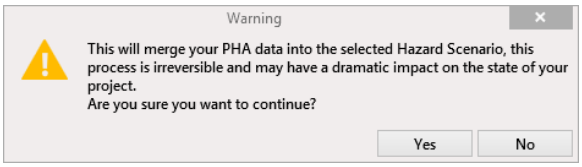
To transfer data for all hazard scenarios at once:

- Select the LOPA tab in exSILentia®
- Click on the ***Load data from PHA for all hazard scenarios*** button

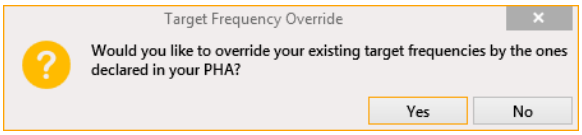
To transfer data for one hazard scenario at a time:

- Select the LOPA tab in exSILentia®
- Select the desired Hazard Scenario in the Navigation List
- Click on the ***Load data from PHA for current Hazard scenario*** button

When transferring data there are two warning messages that you will need to answer affirmatively. The first warning advises you that the PHA information will be merged into the existing Hazard Scenario LOPA information which could delete information that you specified previously.



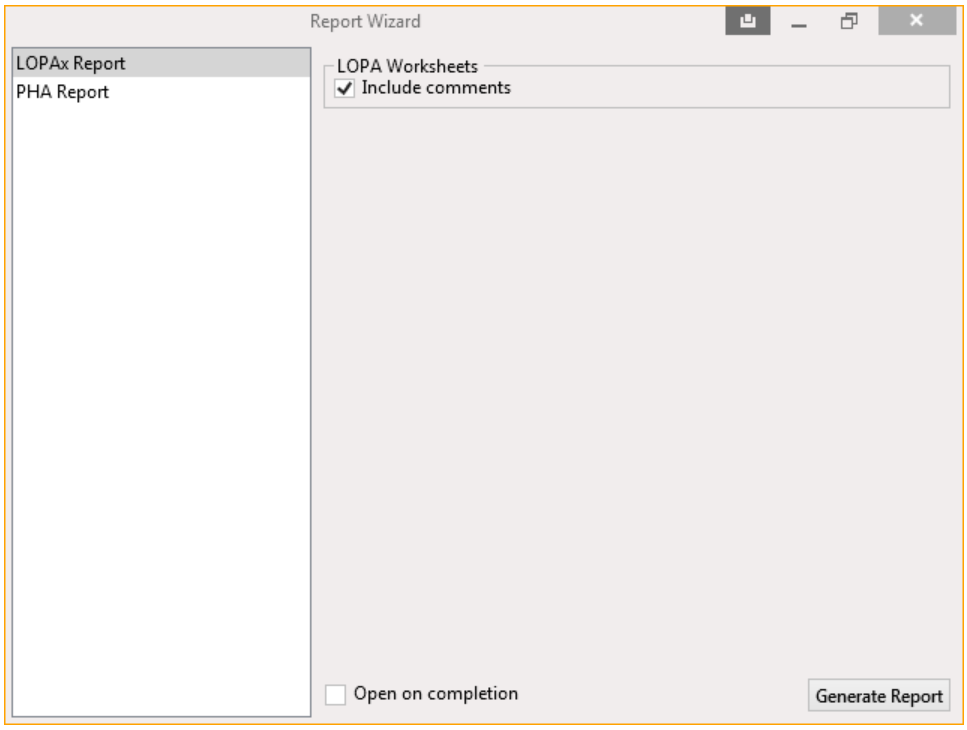
The second warning advises you that the currently specified target frequency for the hazard scenario will be overwritten.



D.5 LOPAx™ Reports

In order to generate a LOPAx™ report select the *LOPA Report* option from the Report Wizard. The Report Wizard will show applicable Report Options.

The Report Option allows you to include or exclude LOPA worksheet comments in your LOPA report.

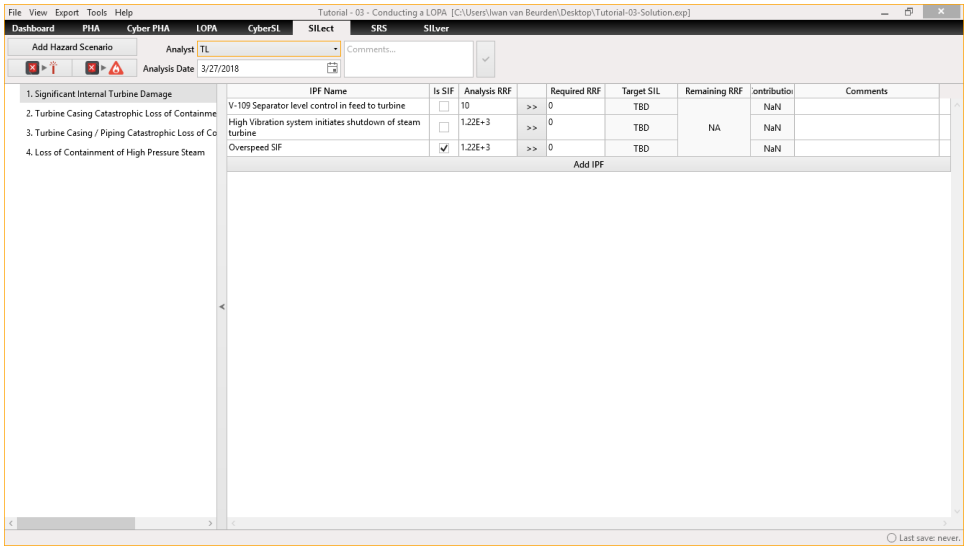

Report Wizard
LOPAx Report
PHA Report
LOPA Worksheets
Include comments
Open on completion
Generate Report

Appendix E SILect™

The SILect tab navigates to the exSILentia® v4 Safety Integrity Level (SIL) selection tool SILect™. Availability of the SILect tab, and therefore the SILect™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SILect™ tool supports determination of the target SIL for each Safety Instrumented Function identified in the LOPA worksheet that is required to provide risk reduction. The SILect™ tool also supports SIL selection based on the Risk Graph and Risk Matrix methodologies.

E.1 Introduction

The Safety Integrity Level selection process in the SILect™ tool is rather straight forward. The interface depends on the type of SIL selection method used, e.g. LOPA, Risk Graph, or Risk Matrix.

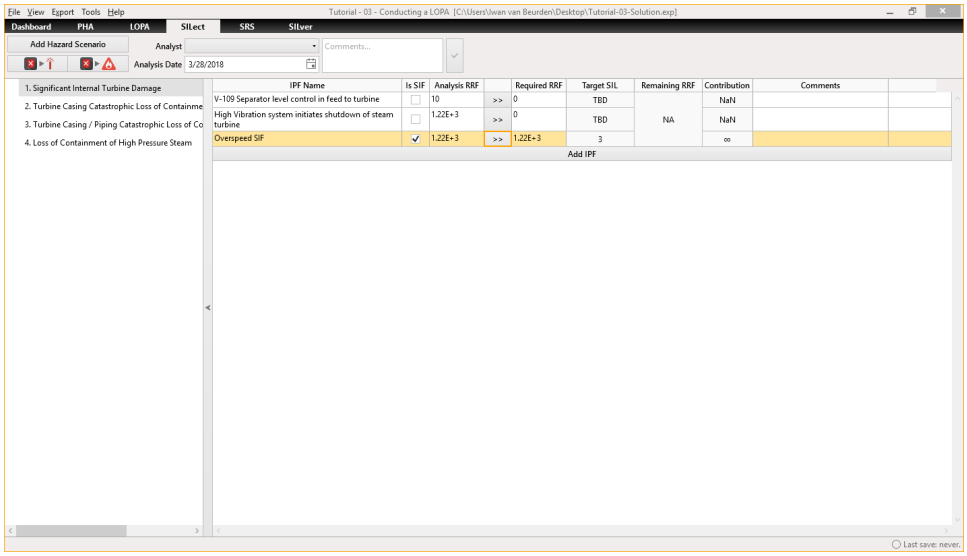


In the subsequent sections the SILect™ worksheet, the embedded relationship between hazard scenarios and Safety Instrumented Functions, and its reporting capability will be explained. The available interfaces with the LOPAx™ tool will also be addressed.

E.2 SILect Worksheet

The SILect™ tool safety integrity level target selection worksheet interface depends on the type of SIL selection method used, e.g. LOPA, Risk Graph, or Risk Matrix. The SIL target selection is performed for each Hazard Scenario individually as tolerable risk is defined on a per hazard scenario basis. Within the LOPA based SIL selection worksheet interface buttons exist for adding hazard scenarios as well as Instrumented Protection Functions (IPF). The Hazard Scenarios and Instrumented Protection Functions are part of the Project Libraries (see *Chapter 7 Project Libraries*). The SILect™ worksheet consists of three main areas: the toolbar, the Hazard Scenario list, and the workspace.

An example of the SILect™ tool LOPA based SIL target selection worksheet is shown in the figure below.



E.2.1 Creating Hazard Scenarios

SILect™ Hazard Scenarios are comprised of two related data fields, i.e. ID and Name. The Hazard Scenario ID is automatically generated and assigned to ensure relational data integrity. Hazard Scenarios can be defined manually within the SILect™ tool or obtained from the work previously done using the PHAx™ and LOPAx™ tools. The transferring of data from PHA and/or LOPA to SILect is described in section *E.3 SILect Data Transfer*.

To add a Hazard Scenario:

- Click on the ***Add Hazard Scenario*** button in the upper left hand corner of the toolbar
- This will immediately add the Hazard Scenario to the Hazard Scenario list

To edit the Hazard Scenario Name:

- Right click on the Hazard Scenario in the Hazard Scenario list and select view

To delete a Hazard Scenario:

- Select the Hazard Scenario in the Hazard Scenario list
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Hazard Scenario is really to be deleted

CAUTION: Deleting a Hazard Scenario will delete all instances where the Hazard Scenario was used. This will include any linking done in the PHAx™ and LOPAx™ tools.

E.2.2 Instrumented Protection Function (IPF)

An Instrumented Protection Function (IPF) is an instrumented safeguard that prevents a particular hazard scenario from proceeding to its undesired consequence. If the amount of risk reduction assigned to the IPF is greater than 10, then by definition, the IPF is a Safety Instrumented Function (SIF). During the process hazard analysis, Instrumented Protection Functions are referred to as Safeguards, while during the layer of protection analysis they are referred to as Independent Protection Layers. Though the label is different, in PHAx™, LOPAx™, and SILect™ the safeguard, independent protection layers, and instrumented protection functions entities are the same.

To add a new Instrumented Protection Function to a Hazard Scenario:

- Select the Hazard Scenario in the Hazard Scenario list
- Click on the ***Add IPF*** button at the top of the SILect™ workspace
- This will immediately add the Instrumented Protection Function to the SILect™ Worksheet
- This will also add the Instrumented Protection Function to the Safeguards library

To edit the Instrumented Protection Function Name:

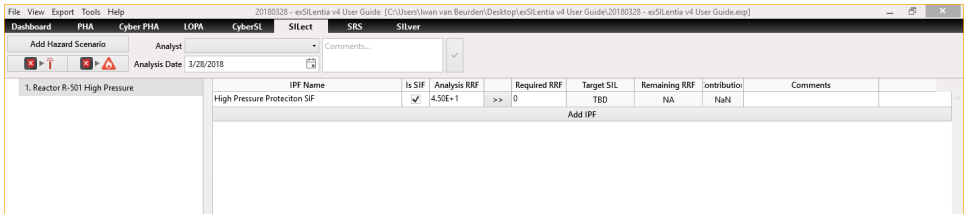
- Double click the Instrumented Protection Function name in the worksheet, or
- Right click on the Instrumented Protection Function in the worksheet and select view

To delete an Instrumented Protection Function:

- Highlight the Instrumented Protection Function
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Instrumented Protection Function is really to be deleted

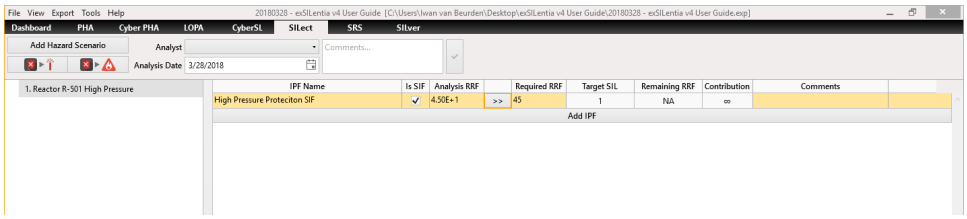
Note: When an Instrumented Protection Function is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Instrumented Protection Function from the Library. Click **Yes** or **No** as applicable.

When you add an Instrumented Protection Function a default Analysis RRF of 1 is associated with the Instrumented Protection Function. In addition the Is SIF checkbox is unchecked. To define that the instrumented protection function is a SIF, simply click the checkbox. To specify the Analysis RRF double click the default RRF of 1 and type the appropriate value.



E.2.3 Calculating the Safety Integrity Level (SIL) Target

To perform the actual SIL target selection, transfer the Analysis RRF over to the Required RRF by clicking on the RRF transfer button >>. You can also manually type in the Required RRF, for example if you want to apply rounding. The target SIL will then be automatically calculated considering the Risk Configuration SIL Selection settings as described in section *8.6 SIL Selection*. Comments can be edited directly in the Comments text box. A Comment is associated with a single Instrumented Protection Function. To delete a comment, highlight the text and click on the ***Delete*** key on your keyboard. You can also include a comment for the entire SIL selection exercise in the header, or at the end of SIL Selection for each SIF.



E.2.4 Risk Graph

To perform SIL Selection using the Risk Graph, use the drop down in the header to choose this method. Once 'Risk Graph' is selected, the view will change to show the Risk Graph from the Risk Configuration. Choose the Risk Category (Safety, Environmental, Business or Custom Risk Categories) using the drop down under the header. Then for each IPF, select the corresponding Likelihood and Consequence levels. For each Parameter defined, choose the associated A or B path. Additionally, you can add Risk Modifiers into the SIL Selection model, or example any IPL or conditional modifier that is relevant to the SIL Selection.

The tool will show the following results for each SIF under the heading Target SIL:

- Under the heading 'Category' the resulting target SIL Level for the Risk Category is shown,
- Under the heading 'Hazard Scenario' the resulting target SIL Level for the entire Hazard Scenario is shown. This is the worst case between the different Risk Categories.
- Under the heading 'Overall'; the final resulting target SIL Level is shown. This is the worst case between all Hazard Scenarios the SIF will guard against.

Additional IPL's can be added or deleted.

E.2.5 Risk Matrix

To perform SIL Selection using the Risk Matrix, use the drop down in the header to choose this method. Once 'Risk Matrix' is selected, the view will change to show the Risk Matrix from the Risk Configuration. Choose the Risk Category (Safety, Environmental, Business or Custom Risk Categories) using the drop down under the header. Then for each IPF, select the corresponding Likelihood and Consequence levels. Additionally, you can add Risk Modifiers into the SIL Selection model, or example any IPL or conditional modifier that is relevant to the SIL Selection.

The tool will show the following results for each SIF under the heading Target SIL:

- Under the heading 'Category' the resulting target SIL Level for the Risk Category is shown,
- Under the heading 'Hazard Scenario' the resulting target SIL Level for the entire Hazard Scenario is shown. This is the worst case between the different Risk Categories.
- Under the heading 'Overall'; the final resulting target SIL Level is shown. This is the worst case between all Hazard Scenarios the SIF will guard against.

Additional IPL's can be added or deleted.

E.3 SILect Data Transfer

The exSILentia® v4 integration of Process Safety / Functional Safety software tools allows for seamless data exchange between the different phases of the Lifecycle. If the Layer of Protection Analysis was performed using LOPAx™, Hazard Scenarios and Independent Protection Layers were defined. If the Independent Protection Layers are of type IPF, they could represent potential SIFs.

The automatic transferring of data from the LOPA to the SILect worksheet ensures that all relevant information is transferred. As a user there is very little left to do, other than confirming that the required risk reduction from the analysis work applies to the IPF and if the IPF is an actual SIF.

When you open the SILect™ tab in exSILentia® v4, you will notice that the hazard scenarios and Independent Protection Layers of type IPF with their associated Analysis RRF automatically populate the SILect™ workspace. You can now transfer the Analysis RRF over to the Required RRF to perform the target SIL selection.

There are two ways to transfer the Analysis RRF over to the Required RRF, you can do this

- for all hazard scenarios at once
- for one hazard scenario at a time

To transfer data for all hazard scenarios at once:

- Select the SILect tab in exSILentia®
- Click on the ***Load analysis required RRF for all hazard scenarios in the project*** button

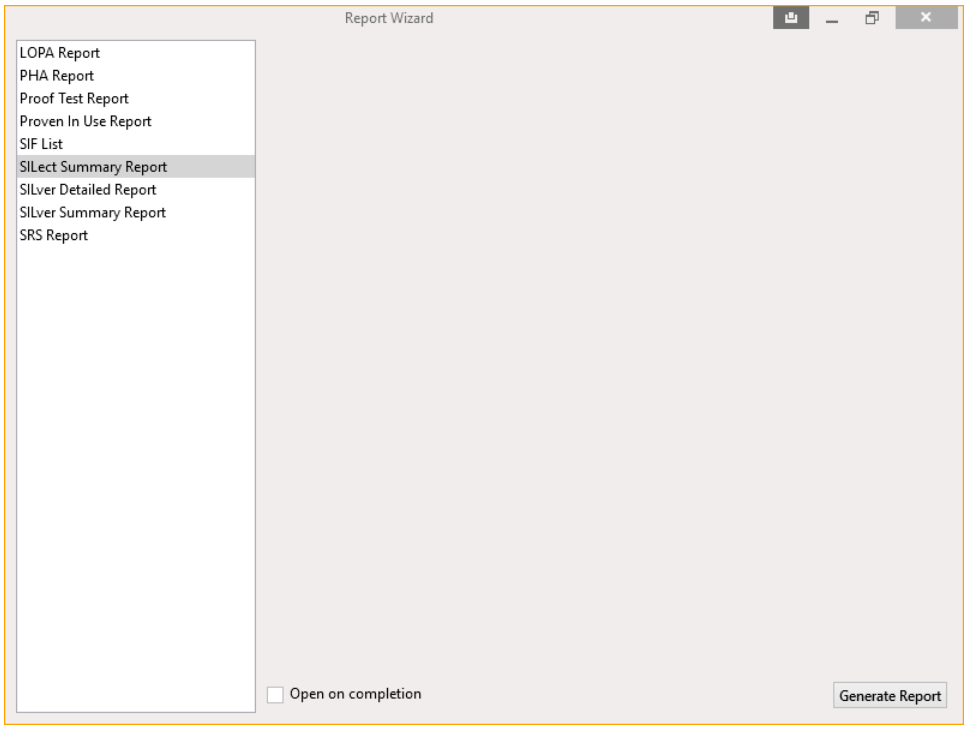
To transfer data for one hazard scenario at a time:

- Select the SILect tab in exSILentia®
- Select the desired Hazard Scenario in the Navigation List
- Click on the ***Load analysis required RRF for the current hazard scenario*** button

The target SILs will be automatically calculated for each Instrumented Protection Function considering the Risk Configuration SIL Selection settings as described in section *8.6 SIL Selection*.

E.4 SILect Reports

In order to generate a SILect™ report select the *SILect Summary Report* option from the Report Wizard. The Report Wizard will show applicable Report Options.

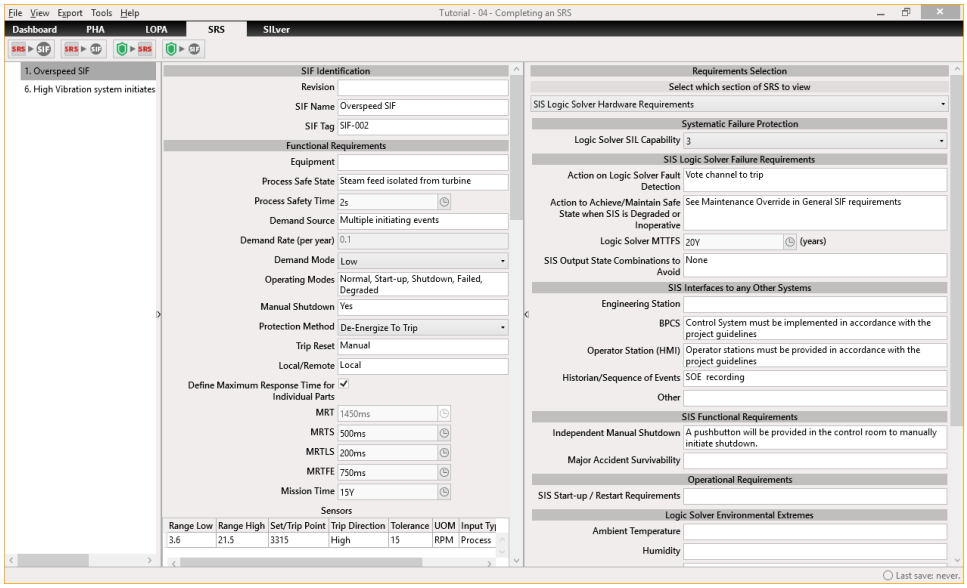

Report Wizard
LOPA Report
PHA Report
Proof Test Report
Proven In Use Report
SIF List
SILect Summary Report
SILver Detailed Report
SILver Summary Report
SRS Report
Open on completion
Generate Report

Appendix F Safety Requirements Specification

The SRS tab navigates to the exSILentia® v4 safety requirements specification tool SRS. Availability of the SRS tab, and therefore the SRS tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SRS tool allows detailed specification of functional and integrity requirements for the Safety Instrumented System (SIS) as a whole, generic for all Safety Instrumented Functions (SIF), and specific for each SIF.

F.1 Introduction

The Safety Requirements Specification functionality in the SRS tool uses a template type interface that enables the specification of general SIS, general SIF, and SIF specific requirements.

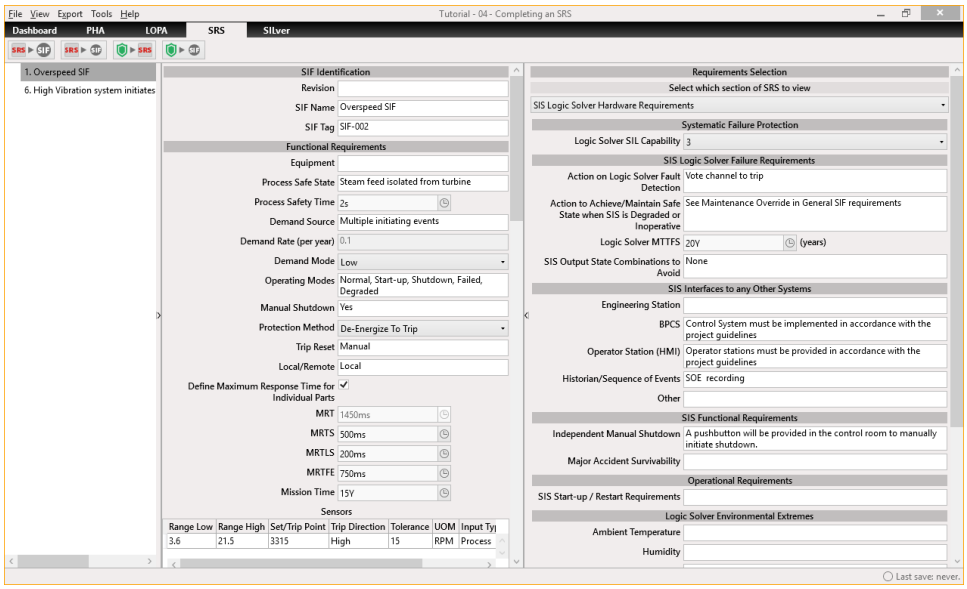


In the subsequent sections the SRS worksheet, its template structure and integrated relationship between general SIS, general SIF, and SIF specific requirements, and its reporting capability will be explained. The available interfaces with the SILect™ and SILver™ tools will also be addressed.

F.2 SRS Worksheet

The Safety Requirements Specification functionality in the SRS tool uses a template type interface that enables the specification of general SIS, general SIF, and SIF specific requirements. The output of the SRS tool is a detailed Safety Requirements Specification document. Furthermore, much of the information specified here, will serve as the basis for the SIL verification task. The interface has been set up such that specification of requirements benefits from information defined in previous phases of the Lifecycle as well as information defined as generally applying to the SIS and all SIFs. The work flow is setup such that you define general requirements first and then transfer those requirements to the individual SIF specific requirements. The SRS worksheet consists of three main areas: the toolbar, the SIF navigation list, and the workspace.

An example of the SRS tool safety requirements specification worksheet is shown in the figure below.



F.2.1 Creating Safety Instrumented Functions

Within exSILentia® v4 Safety Instrumented Functions (SIF) are Safeguards of Safeguard Category Type IPF (Instrumented Protection Function) where the *"Is SIF"* property is checked. The exSILentia® v4 SIFs therefore comprise of many related data fields inherited from Safeguards, IPFs, and SIF specific fields. Each SIF has a unique Safeguard ID which is automatically generated and assigned to ensure relational data integrity. SIFs can be defined manually within the SRS tool or obtained from the work previously done using the PHAx™, LOPAx™, and/or SILect™ tools. The transferring of data from PHA to SRS, LOPA to SRS, and/or SIL selection to SRS is described in section *F.3 Safeguard to SRS Data Transfer*.

To add a SIF:

- Click on the ***New SIF*** button in the upper left hand corner of the toolbar
- This will immediately add the SIF to the SIF navigation list

To edit the SIF properties:

- Right click on the SIF in the SIF navigation list and select view, or
- Edit the SIF Name and SIF Tag directly in the toolbar

To delete a SIF:

- Select the SIF in the SIF navigation list
- Right click on the SIF and select ***Delete***, click on the ***Delete SIF*** button, or click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the SIF is really to be deleted

CAUTION: Deleting a SIF will delete all instances where the SIF was used. This will include any linking done in the PHAx™, LOPAx™, and/or SILect™ tools.

F.2.2 General SIS Requirements

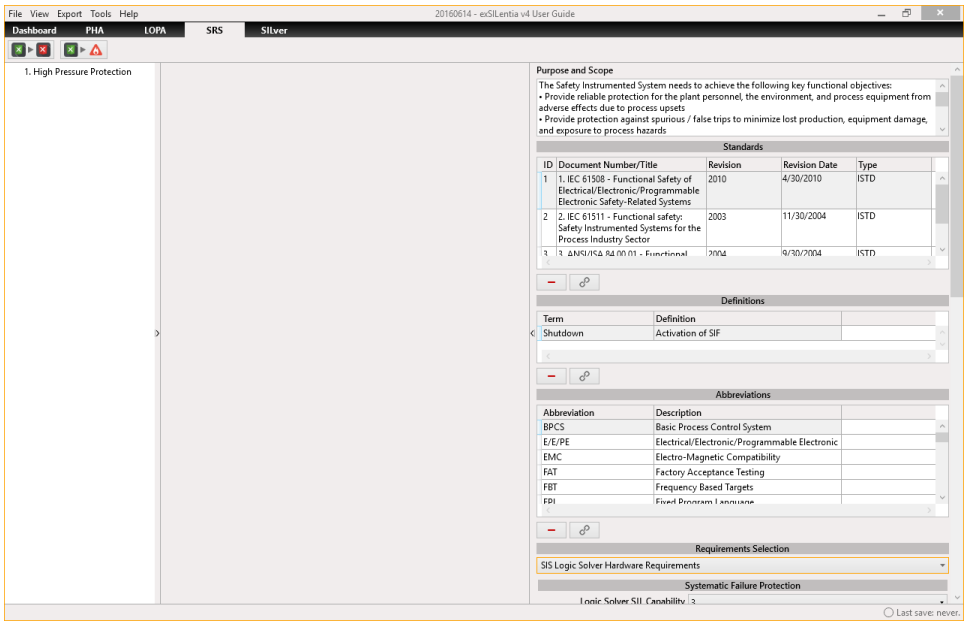
The SRS tool divides the General SIS requirements into 3 sections, i.e. General Information, SIS Logic Solver Hardware Requirements, and SIS Application Software Requirements. These 3 sections together with the General SIF Requirements (see below) can be specified in the right hand area of the SRS worksheet. Using the ***Requirements Selection*** drop down box you can navigate between requirements sections.

General Information

The General Information section of the General SIS Requirements allows you to specify an overall purpose and scope of the SIS, specify specific references, and terms and abbreviations that are applicable to the SRS document.

To edit the SRS General Information:

- Select ***General Information*** from the ***Requirements Selection*** drop down box
- Edit the relevant information on the right hand side of the worksheet



To add a reference to the list of standards/references in the General Information section:

- Click the green plus (**+**) symbol below the list of references
- From the overview of references defined in the reference library that appears select the applicable reference you want to add and click the ***Link*** button

To add a definition to the list of definitions in the General Information section:

- Click the green plus (**+**) symbol below the list of definitions
- From the overview of definitions defined in the definition library that appears select the applicable definition you want to add and click the ***Link*** button

To add an abbreviation to the list of abbreviations in the General Information section:

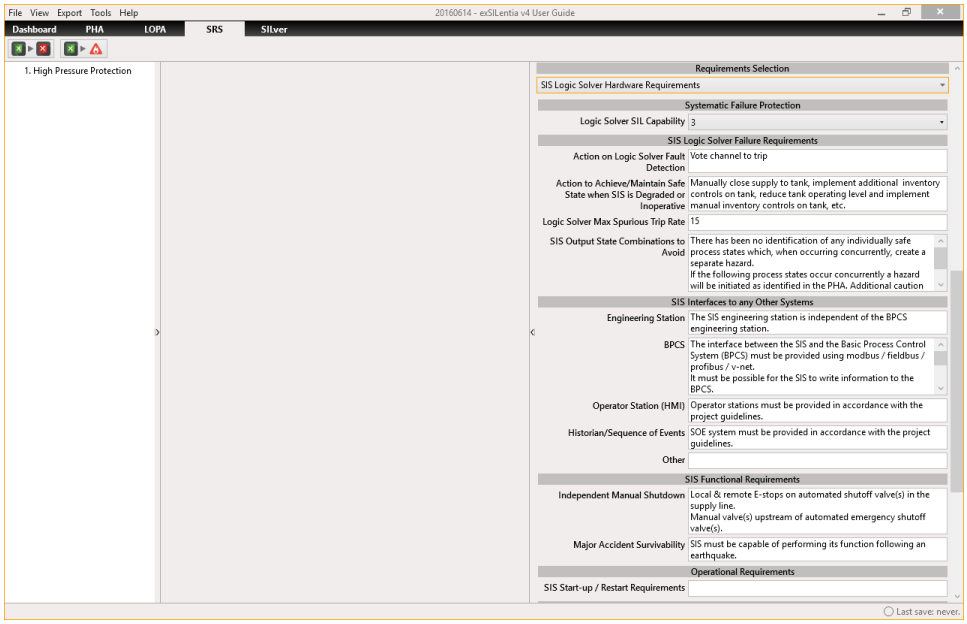
- Click the green plus (**+**) symbol below the list of abbreviations
- From the overview of abbreviations defined in the abbreviation library that appears select the applicable abbreviation you want to add and click the ***Link*** button

SIS Logic Solver Hardware Requirements

The SIS Logic Solver Hardware Requirements section of the General SIS Requirements allows you to specify general requirements with regard to the hardware of the Safety Instrumented System, focusing specifically on the logic solver. Aspects that need to be addressed revolve around the systematic capability of the logic solver, the expected response of the logic solver upon detection of a failure, etc. In addition, interfaces to an engineering station, the BPCS etc. should be specified as well as environmental extremes the logic solver must be able to withstand. All requirements are specified through text fields.

To edit the SRS SIS Logic Solver Hardware Requirements:

- Select ***SIS Logic Solver Hardware Requirements*** from the ***Requirements Selection*** drop down box
- Edit the relevant information on the right hand side of the worksheet



In addition to the exSILentia® v4 defined SRS fields for the SIS Logic Solver Hardware Requirements you can add your own requirement fields through the **Custom Data** option which is shown at the bottom of the list of SIS Logic Solver Hardware Requirements. From the dropdown box select the applicable custom data data-set. This will add the fields specified in the custom data data-set to the exSILentia® v4 defined fields.

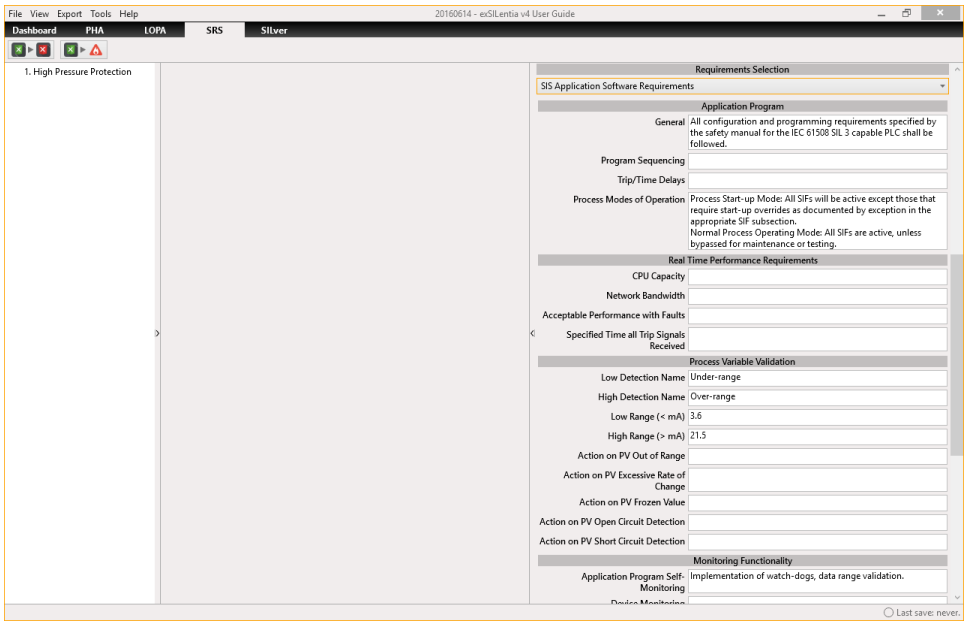
CAUTION: Deleting or changing the custom data data-set will remove all associated fields from the project. Any custom data specified information will be lost.

SIS Application Software Requirements

The SIS Application Software Requirements section of the General SIS Requirements allows you to specify general requirements with regard to the user defined application program of the Safety Instrumented System. Aspects that need to be addressed revolve around structure of the application program, validation of process variables, performance, and monitoring functionality. Furthermore ,communication interfaces must be defined as well as any requirements to support normal operation and test and maintenance activities like proof testing. All requirements are specified through text fields.

To edit the SRS SIS Application Software Requirements:

- Select ***SIS Application Software Requirements*** from the ***Requirements Selection*** drop down box
- Edit the relevant information on the right hand side of the worksheet



In addition to the exSILentia® v4 defined SRS fields for the SIS Application Software Requirements you can add your own requirement fields through the **Custom Data** option which is shown at the bottom of the list of SIS Application Software Requirements. From the dropdown box select the applicable custom data data-set. This will add the fields specified in the custom data data-set to the exSILentia® v4 defined fields.

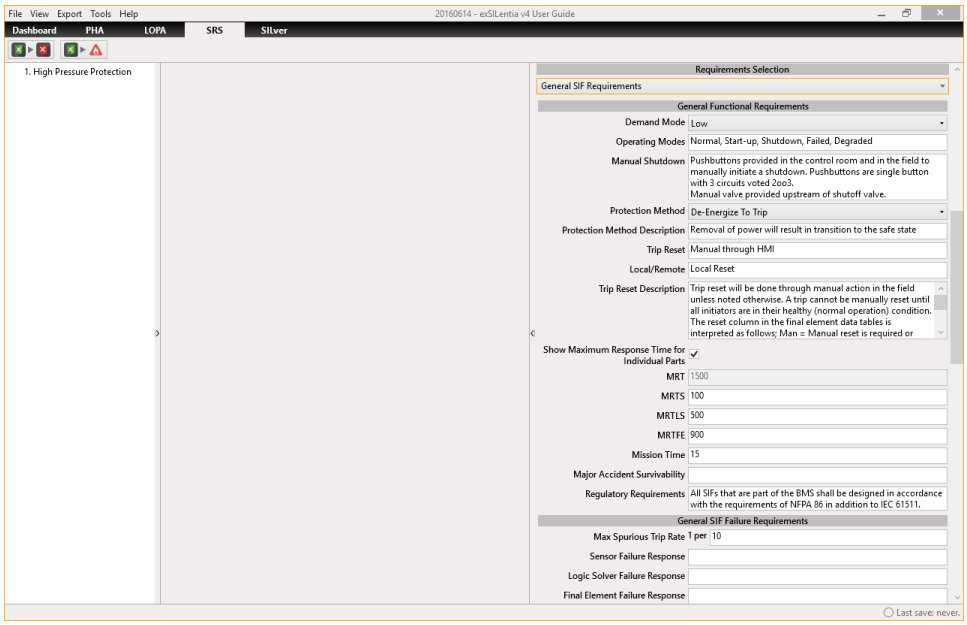
CAUTION: Deleting or changing the custom data data-set will remove all associated fields from the project. Any custom data specified information will be lost.

F.2.3 General SIF Requirements

The General SIF Requirements section allows you to specify requirements that are valid for all SIFs. You will be able to copy these general requirements to the individual SIF Specific Requirements. Aspects that need to be addressed revolve around operating modes, operator interfaces for manual shutdown and trip reset, and response time requirements. In addition, performance requirements must be addressed as well as desired proof test intervals and environmental extremes for the field equipment of the SIF. All requirements are specified through text fields.

To edit the SRS General SIF Requirements:

- Select ***General SIF Requirements*** from the ***Requirements Selection*** drop down box
- Edit the relevant information on the right hand side of the worksheet

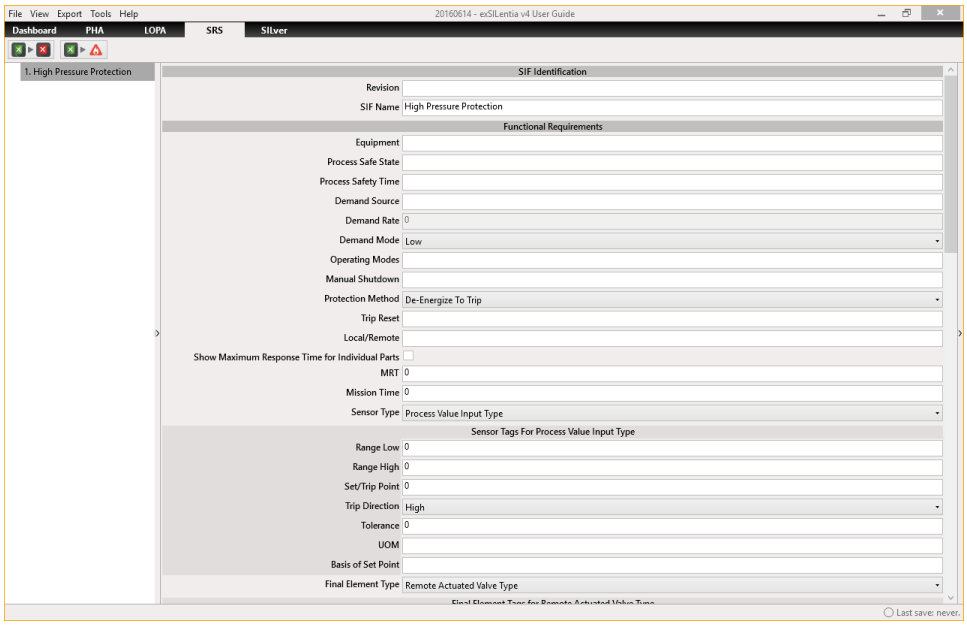


In addition to the exSILentia® v4 defined SRS fields for the General SIF Requirements you can add your own requirement fields through the **Custom Data** option which is shown at the bottom of the list of General SIF Requirements. From the dropdown box select the applicable custom data data-set. This will add the fields specified in the custom data to the exSILentia® v4 defined fields. By adding custom data to the General SIF Requirements you will automatically add the same custom data fields to the set of SIF specific requirements fields.

CAUTION: Deleting or changing the custom data data-set will remove all associated fields from the project. For General SIF Requirements custom data this also means that the fields will be removed from the SIF Specific Requirements. Any custom data specified information will be lost.

F.2.4 SIF Specific Requirements

The SIF Specific Requirements are, as their name already indicates, specified for each SIF individually. Though some requirements for different SIFs may be identical, and therefore specified in the General SIF Requirements section, it is essential that each SIF is addressed individually to ensure that the conceptual design that results will adequately protect against the specific hazard scenario identified. The SIF Specific Requirements are specified in the left hand area of the SRS worksheet. Simply select a SIF from the SIF navigation list and edit the applicable fields. Aspects that need to be addressed are those identified for the General SIF Requirements as well as SIF specific items like process variable ranges, trip point, units of measure (UOM), safety action, etc. The majority of requirements are specified through text fields.



There are two ways to copy specifications from the General SIF Requirements to SIF Specific Requirements. You can copy data from the general SIF requirements to SIF specific requirements

- for all SIFs at once
- for one SIF at a time

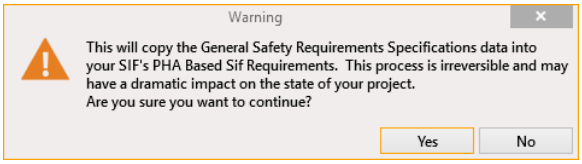
To transfer data for all SIFs at once:

- Click on the ***Load data from General SIF Requirements to SIF Specific Requirements for all SIFs*** button

To transfer data for one SIF at a time:

- Select the desired SIF in the SIF Navigation List
- Click on the ***Load data from General SIF Requirements to SIF Specific Requirements for current SIF*** button

When transferring data, you will receive a warning that advises you that the General SIF Requirements data will be merged into the existing SIF(s) Specific Requirements which could delete information that you specified previously.



F.3 Safeguard to SRS Data Transfer

The exSILentia® v4 integration of Process Safety / Functional Safety software tools allows for seamless data exchange between the different phases of the Lifecycle. If the Process Hazard Analysis was performed using PHAx™ and Safeguards where defined of Safeguard Category Type IPF additional data fields where added to the safeguard. One of these data fields allowed you to check the *"Is SIF"* property which ensured that the specific SIF showed up in the SIF navigation list in the SRS tool. Similarly, if the Layer of Protection Analysis was performed using LOPAx™ or the SIL selection was done using SILect™ and Safeguards/IPLs defined of Safeguard Category Type IPF the same additional data fields were added to the safeguard. Any data specified in the safeguards data fields can be automatically transferred to the SRS tool.

There are two ways to transfer safeguard data to the Safety Requirements Specification. You can copy safeguard data to a SIF's SRS data

- for all SIFs at once
- for one SIF at a time

To transfer data for all SIFs at once:

- Click on the ***Copy safeguard data to SRS for all SIFs*** button

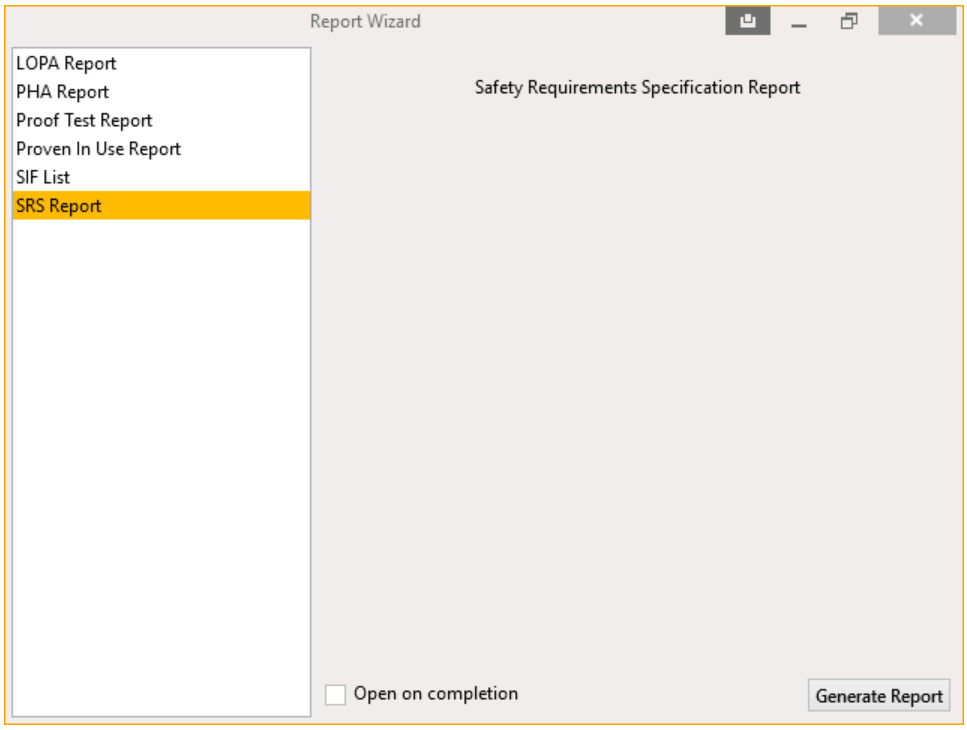
To transfer data for one SIF at a time:

- Select the desired SIF in the SIF Navigation List
- Click on the ***Copy safeguard data to SRS for selected SIF*** button

When transferring data, you will receive a warning that advises you that the safeguard data will be copied into the SIF(s) Specific Requirements which could overwrite information that you specified previously.

F.4 SRS Reports

In order to generate a SRS report select the *SRS Report* option from the Report Wizard. There are no Report Options for the SRS report.


Report Wizard
LOPA Report
PHA Report
Proof Test Report
Proven In Use Report
SIF List
SRS Report
Safety Requirements Specification Report
Open on completion
Generate Report

Appendix G SILver™

The SILver tab navigates to the exSILentia® v4 Safety Integrity Level (SIL) verification tool SILver™. Availability of the SILver tab, and therefore the SILver™ tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The SILver™ tool allows comprehensive modeling of each Safety Instrumented Function's (SIF) conceptual design within an exSILentia® v4 project to determine if that conceptual design meets the requirements specified in the Safety Requirements Specification (SRS). The result of the SIL verification will be an Achieved Safety Integrity Level for the specific SIF's conceptual design.

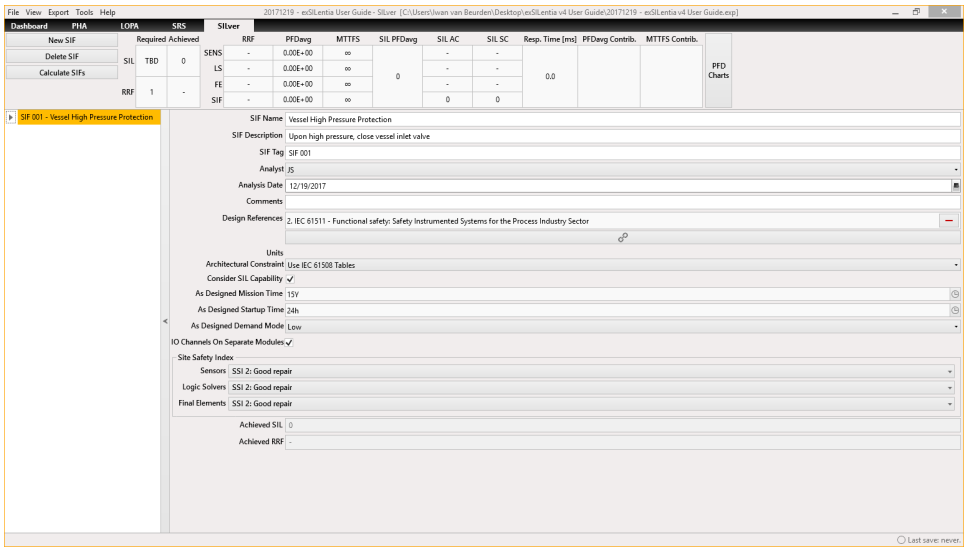
G.1 Introduction

The SILver™ tool uses a discrete Markov model calculation technique during all analyses. For equipment selections, it features the exida Safety Equipment Reliability Handbook database. This allows you to perform a reliability analysis of your favorite equipment without the hassle of manually filling in all reliability data, while ensuring accurate calculation results. The exSILentia® development process, and specifically the SILver™ calculation engine development, meets IEC 61508 software development process requirements. The user of the SILver™ tool should review and understand all assumptions that are the basis of SILver™ calculations. The user is also responsible for reviewing all selections made during the analysis.

Note: SIL verification using the exSILentia® SILver™ tool can be performed for all conceptual designs up to SIL 4. For any safety functions that need to achieve SIL 4, independent verification of the results should be performed by the user as required by IEC 61508 / IEC 61511.

When modeling a SIF conceptual design in SILver™, it is essential to understand the structure of the SILver™ tool. Similar to the functional safety standards IEC 61508 and IEC 61511, SILver™ distinguishes three unique parts in a SIF:

- Sensor Part
- Logic Solver Part
- Final Element Part

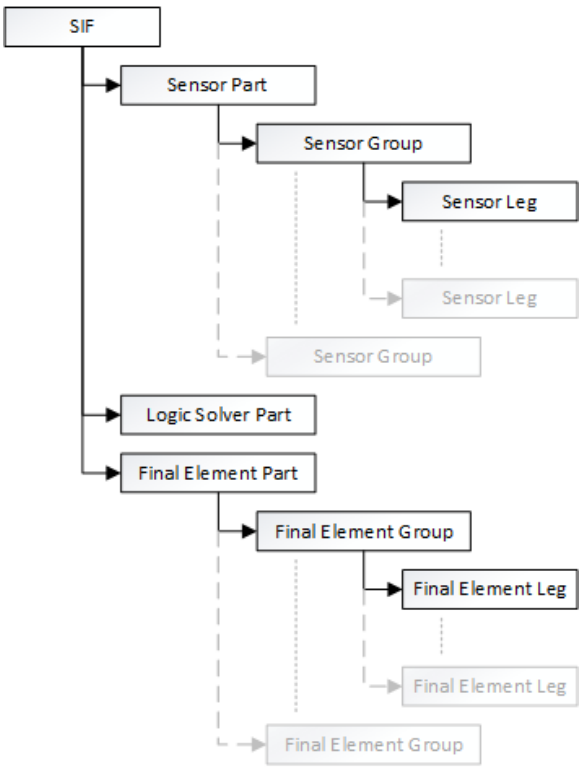


More detailed modeling of a SIF's conceptual design is supported through the ability to divide the Sensor Part and the Final Element Part into groups. A maximum of 4 groups is supported for both the Sensor Part and the Final Element Part. These groups allows you to model voting arrangements between groups of equipment items, e.g. a main fuel valve in series with 4 individual burners valves.

SILver™ supports the following voting options for voting between groups (in words with X being the number of groups):

- 1ooX: one group needs to trip for the safety function to trip.
- XooX: all groups need to trip for the safety function to trip.
- 2oo3: two out of three groups need to trip for the safety function to trip; available only in case 3 groups are used in the conceptual design.

SILver™ supports further definition of the Sensor and Final Element groups through the use of legs. These legs can be either identical or diverse. The maximum number of legs within a group depends on the voting arrangements available for the particular group.



SILver™ provides the following voting options for Sensor groups:

- 1oo1
- 1oo2, 2oo2
- 1oo3, 2oo3, 3oo3
- 1oo4, 2oo4, 3oo4, 4oo4
- 1oo5, 2oo5, 3oo5, 4oo5, 5oo5 (Identical legs only)
- MooN (Identical legs only)

SILver™ provides the following voting options for Final Element groups:

- 1oo1
- 1oo2, 2oo2
- 1oo3, 2oo3, 3oo3
- 1oo4, 4oo4
- 2oo4 [2oo(1oo2)] (Identical legs only)
- 1oo5, 5oo5 (Identical legs only)
- 6oo6 (Identical legs only)
- 7oo7 (Identical legs only)
- 8oo8 (Identical legs only)
- 9oo9 (Identical legs only)
- MooN (Identical legs only)

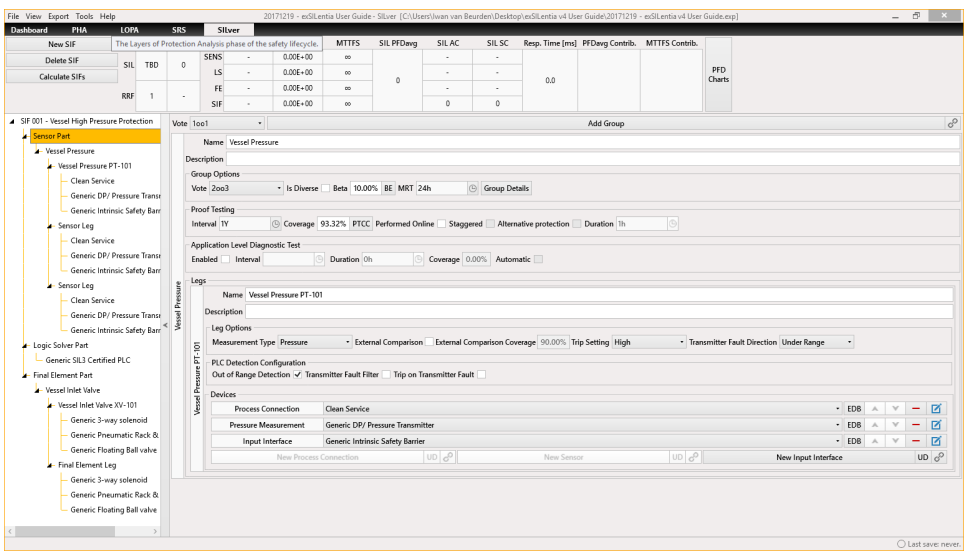
Note: Given the flexibility of the voting arrangements within the Sensor and Final Element groups, SIFs are typically modeled using a single group only.

In the subsequent sections the SILver™ worksheet, its modeling options for sensors, logic solvers, and final elements, and its reporting capability will be explained. In addition the concept of devices and device models will be addressed. The available interfaces with the SRS tool will also be addressed.

G.2 SILver Worksheet

The SILver™ tool conceptual design verification worksheet uses an interactive interface to effectively guide you through the steps of modeling a SIF's conceptual design. This allows you to focus on the, for that task, relevant portion of the SIF, e.g. from SIF level to leg level. Within the interface buttons exist for adding and deleting SIFs, as well as specification of detailed parameters like PLC detection behavior for analog sensor signals. The SILver™ tool interface also allows you to easily interact with the Safety Equipment Reliability Handbook database (see section *12.2 SERH Database*). In addition sensor groups and legs as well as final element groups and legs are part of the Project Libraries (see *Chapter 7 Project Libraries*). This elevates the ability to re-use conceptual design components to the next level. In addition SILver™ introduces the concept of devices and device models, the latter will allow you to easily find your project preferred equipment when you are modeling your conceptual design. The SILver™ worksheet consists of four main areas: the toolbar, the SIF list, the SIF diagram, and the workspace.

An example of the SILver™ tool conceptual design verification worksheet is shown in the figure below.



G.2.1 Creating Safety Instrumented Functions

Within exSILentia® v4 Safety Instrumented Functions (SIF) are Safeguards of Safeguard Category Type IPF (Instrumented Protection Function) where the *"Is SIF"* property is checked. The exSILentia® v4 SIFs therefore comprise of many related data fields inherited from Safeguards, IPFs, and SIF specific fields. Each SIF has a unique Safeguard ID which is automatically generated and assigned to ensure relational data integrity. SIFs can be defined manually within the SILver™ tool or obtained from the work previously done using the PHAx™, LOPAx™, SILect™, and/or SRS tools. The transferring of data from PHA, LOPA, and SIL selection to SIL verification and SRS to SIL verification is described in section *G.12 SILver Data Transfer*.

To add a SIF:

- Click on the ***New SIF*** button in the upper left hand corner of the toolbar
- This will immediately add the SIF to the SIF navigation list

To edit the SIF properties:

- Right click on the SIF in the SIF navigation list and select view, or
- Edit the SIF Name and SIF Tag directly in the SIF worksheet (see below)

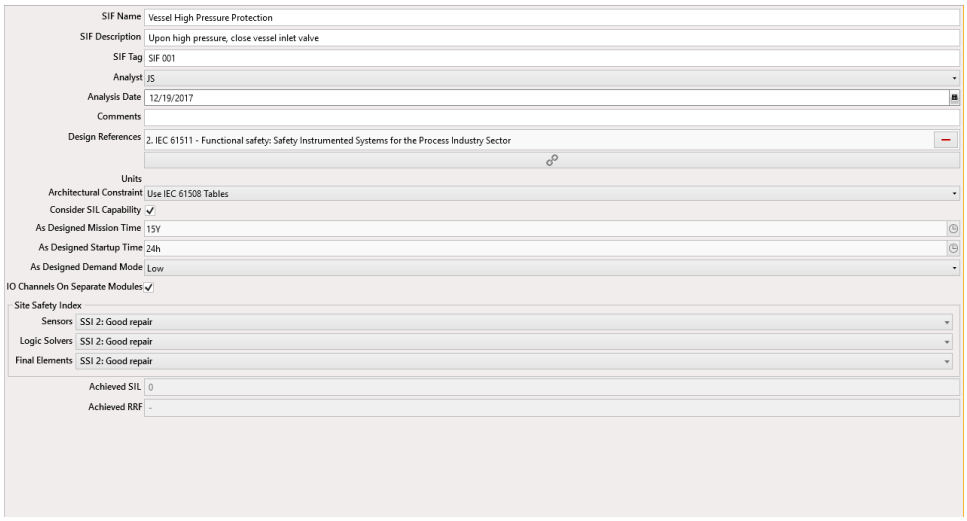
To delete a SIF:

- Select the SIF in the SIF navigation list
- Right click on the SIF and select ***Delete***, click on the ***Delete SIF*** button, or click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the SIF is really to be deleted

CAUTION: Deleting a SIF will delete all instances where the SIF was used. This will include any linking done in the PHAx™, LOPAx™, SILect™, and/or SRS tools.

G.3 SILver Worksheet - SIF Level

To start the modeling of a SIF's conceptual design in the SILver™ tool, select the SIF in the SIF list. The SILver™ workspace will now show the SIF level conceptual design information as shown in the figure below. The information to be recorded can be divided into general information and several specific parameters per the sections below.



G.3.1 General SIF Information

The General SIF Information in the SILver™ SIF level conceptual design includes the following properties that are part of the IPF Type Safeguard information and are therefore most likely already specified in the PHA, LOPA, SILect, and/or SRS tools.

- SIF Name
- SIF Description
- SIF Tag

In addition to these properties, there are specific items that are unique to the SILver™ tool

- Analyst
- Analysis Date
- Comments
- Design References

To define an Analyst, simply select a Team Member from the drop down box. See section *A.4 Members* for more information on specifying Team Members.

To specify the Analysis Date, enter the date directly into the date field or use the Calendar Icon to select the date from the calendar pop-up.

In the Comments field you can document any specific remarks or assumptions related to the SIL verification of this SIF.

The Design References item allows you to link specific project references to the SIL verification of this SIF. Click the Link Icon and select the applicable reference from the list that appears by double clicking that reference.

G.3.2 Architectural Constraints

You can indicate if Architectural Constraints should be considered in the conceptual design evaluation of this SIF. Architectural constraints place minimum Hardware Fault Tolerance (HFT) requirements on the elements in a Safety Instrumented Function. SILver™ provides the following architectural constraints options:

- None
- Use IEC 61508 Tables
- Use IEC 61511 Tables

If you select **None**, minimum hardware fault tolerance requirements are ignored when determining the achieved SIL level for this SIF.

If you select **IEC 61508 Tables**, the achieved SIL of the Safety Instrumented Function will be limited to the SIL supported by either Route 1_H or Route 2_H as defined in IEC 61508. Per clause 11.4.3 of IEC 61511 users can opt to follow the IEC 61508 tables instead of the IEC 61511 tables. Route 1_H architectural constraints are described in clause 7.4.4.2 and table 2 or 3 of IEC 61508-2:2010. These are based on Equipment Type, Safe Failure Fraction and Hardware Fault Tolerance. Route 2_H architectural constraints are described in clause 7.4.4.3 of IEC 61508-2:2010.

If you select **IEC 61511 Tables**, the achieved SIL of the SIF will be limited to the SIL supported by clause 11.4.5 to 11.4.9 of IE 61511:2016 clause 11.4 which includes table 6 of that standard.

The architectural constraints are set for each SIF individually. To specify the applicable architectural constraints, simply select your preferred method from the drop down box in the SILver™ SIF level workspace. To specify the default SSI values for this project, see section *6.10 SILver Project Parameters*.

G.3.3 Systematic Capability

You can indicate if Systematic Capability should be considered in the conceptual design evaluation of this SIF. Per IEC 61511, systematic failure robustness for equipment must be justified either by an assessment of that equipment per IEC 61508 or by documenting successful experience in the form of a Proven-In-Use/Prior-Use assessment. For equipment developed and assessed per IEC 61508, techniques and measures appropriate for the specified Safety Integrity Level have been used to prevent systematic faults. For equipment that was not developed and/or assessed per IEC 61508, a user can justify use of that equipment by means of a proven-in-use argument. In this case, the user is taking over the responsibility from the manufacturer in justifying that the equipment has a sufficiently low chance of having systematic faults. An appropriate plant operational experience tracking system needs to be in place to be able to make this argument.

When the Systematic Capability option is selected, SILver™ will take into account the IEC 61508 assessment levels and/or the Proven-In-Use justification levels (the Systematic Capability) of the equipment specified in determining the achieved SIL of a Safety Instrumented Function. In order to achieve a certain SIL level, all equipment used in a Safety Instrumented Function must either be assessed up to that SIL level and/or theProven-In-Use justification for the equipment must be up to that specific SIL level.

To specify the default Systematic Capability value for this project, see section *6.10 SILver Project Parameters*.

G.3.4 Mission Time

In the Mission Time field, the time period that the SIF is expected to be operational should be selected. For Low Demand applications, the PFD_{AVG} parameter, which determines the achieved Safety Integrity Level, is determined over this mission time. At the end of the mission time it is expected that all equipment in the SIF is either replaced or factory-new refurbished. The mission time is typically at least as long as the largest proof test interval. To account for different replacement or refurbishment intervals per sensor group/final element group/logic solver see section *G.5* , *G.7* , and *G.8* respectively.

To specify the default Mission Time value for this project, see section *6.10 SILver Project Parameters*.

G.3.5 Startup Time

In the Startup Time field you can list the number of hours it takes to *re-start* the process after a shutdown. This should be an integer number between 4 and 336 hours. The start up time is typically the sum of the repair time and any clean up time.

Note: It is a common misconception that the Startup Time should be greater than the mean repair time (MRT) as logic dictates that the sum of repair time and clean up time is always greater than the repair time assuming the clean up time is not 0. In conceptual design evaluation, a MRT is typically chosen such that there is an extra buffer of time that allows the user to make sure the replacement part is in place and/or the system is in a good state to shutdown. As such the mean repair time typically specified is the repair time plus a order part/wait time.

To specify the default Startup Time value for this project, see section *6.10 SILver Project Parameters*.

G.3.6 SIF Demand Mode

The SILver™ tool distinguishes between three modes of operation, i.e.

- Low Demand
- High Demand
- Continuous Demand

Using the Demand Mode drop down box you can specify which mode of operation you want to consider for the SIF. You can either explicitly select Low Demand, High Demand, or Continuous Demand or your can define that SILver™ should determine the mode of operation for the SIF based on the demand rate of the SIF. When you select the **Based On Demand Rate** option, an extra field will appear that allows you to enter the Demand Interval in months. SILver™ will subsequently determine the mode of operation per IEC 61511:2017.

For Low demand applications the average Probability of Failure on Demand (PFD_{AVG}) is calculated. For High and Continuous demand applications the Probability of a Dangerous Failure per Hour (PFH) is calculated. In High Demand applications credit for automatic diagnostics is taken whereas the automatic diagnostics are considered ineffective in Continuous demand applications.

Note: To indicate that the SIF is operating in continuous mode when using the **Based On Demand Rate** option, the demand interval should be specified as 0 month.

To specify the default Demand Mode value for this project, see section *6.10 SILver Project Parameters*.

G.3.7 I/O Channels on Separate Modules

The SILver™ tool allows you to indicate if individual I/O channels should be connected to the same or to different I/O modules for the relevant channels in this SIF. In a redundant configuration, if the channels are wired to the same I/O module, no voting is applied over this I/O module. If the channels are wired to different I/O modules, the voting applied to the sensor and final element groups will also be applied to the input and output modules respectively.

G.3.8 Site Safety Index

The Site Safety Index (SSI) model accounts for site specific operational practices. It allows a site with strong safety processes to take credit for that accomplishment while not masking issues at other sites. The Site Safety Index takes a variety of factors into consideration, including the maintenance capability which was used in exSILentia® v3. In addition to this, the SSI accounts for different overall failure behavior between sites, which is observed during field failure studies.

A total of 5 levels have been identified for the Site Safety Index (SSI), these are shown in the table below.

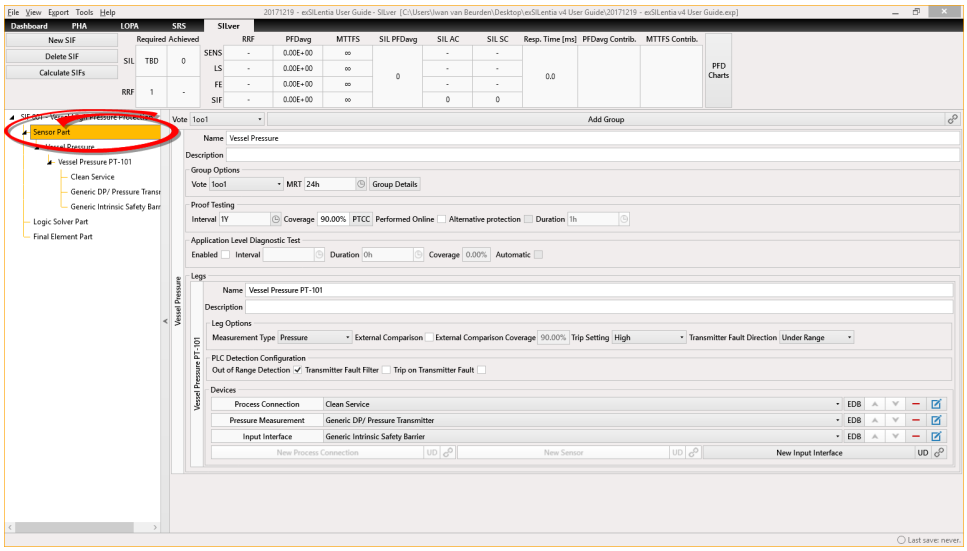
Level	Description
SSI 4	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, Equipment is always replaced before end of useful life, Equipment is always selected according to the specified environmental limits and process compatible materials, Electrical power supplies are clean of transients and isolated, Pneumatic supplies and hydraulic fluids are always kept clean, etc. This level is generally considered not possible but retained in the model for comparison purposes.

Level	Description
SSI 3	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, Equipment is replaced before end of useful life, Equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials, Electrical power supplies are normally clean of transients and isolated, Pneumatic supplies and hydraulic fluids are mostly kept clean, etc.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, Equipment is mostly replaced before end of useful life, Equipment is often selected according to the specified environmental limits and process compatible materials, Electrical power supplies may have transient voltage spikes and surges, Pneumatic supplies and hydraulic fluids are usually kept clean, etc.
SSI 1	Medium – Repairs are mostly correctly performed, Testing is done and often on schedule, Equipment is sometimes replaced before end of useful life, Equipment is sometimes selected according to the specified environmental limits and process compatible materials, Electrical power supplies have transient voltage spikes and surges, Pneumatic supplies and hydraulic fluids are sometimes kept clean, etc.
SSI 0	None - Repairs are not always done, Testing is not done, Equipment is replaced upon failure, Equipment is selected based on history, Electrical power supplies may drop out and have transient voltage spikes and surges, Pneumatic supplies and hydraulic fluids are sometimes kept clean, etc.

The Site Safety Index is a parameter that is specific for each SIF individually and can be specified for sensors, logic solvers, and final elements separately. To specify the applicable Site Safety Indexes for this SIF, simply select the appropriate level from the drop down boxes in the SILver™ SIF level workspace. To specify the default SSI values for this project, see section *6.10 SILver Project Parameters*.

G.4 SILver Worksheet - Sensor Part

To configure the SIF's Sensor Part in the SILver™ tool, select **Sensor Part** for the SIF in the SIF list. The SILver™ workspace will now show the sensor part conceptual design information as shown in the figure below.



As described in section *G.1 Introduction* a Sensor Part can consist of up to 4 Sensor Groups.

To add a new Sensor Group to the Sensor Part:

- Click on the ***Add Group*** button in the middle of the SILver™ workspace
- This will immediately add the Sensor Group to the SILver™ workspace
- This will also add the Sensor Group to the Sensor Groups library

To add a Sensor Group directly from the Sensor Groups Library:

- Click on the Link Sensor Group Icon
- Double Click the Sensor Group to add the group to the Sensor Part

After adding the applicable number of Sensor Groups to the Sensor Part, update the Sensor Part voting, i.e. the voting between groups, in the upper left hand corner of the SILver™ workspace. You can also specify the beta factor to account for common cause between groups. The beta factor must be entered as an integer between 0% and 100%. The default value for the common cause between groups is 0% as different groups are typically used to model independent equipment items. In case there is no complete independence however, i.e. there is common cause susceptibility, a beta factor other than 0% should be used. Use the beta factor estimator feature for assistance in determining an applicable beta factor by clicking the beta estimator icon BE, see also section *G.10 SILver Worksheet - Features*.

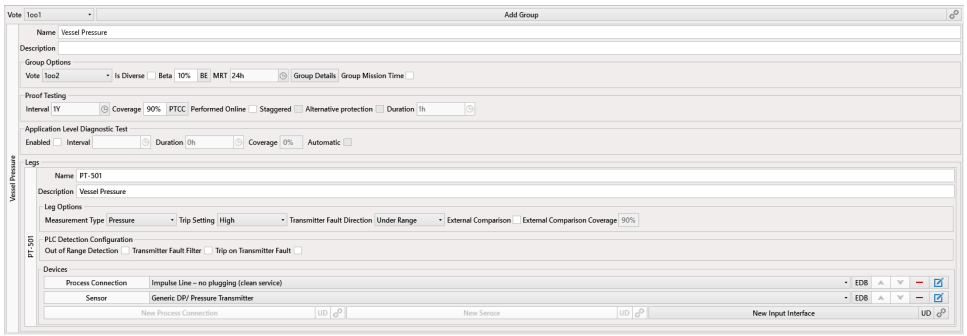
To delete a Sensor Group from the Sensor Part:

- Right click on the specific ***Sensor Group***
- Select ***Delete*** from the pop-up menu
- Click on ***Yes*** when asked if the Sensor Group is really to be deleted

Note: When a Sensor Group is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Sensor Group from the Library. Click **Yes** or **No** as applicable.

G.5 SILver Worksheet - Sensor Group

To configure a SIF's Sensor Group in the SILver™ tool you can either do this in the SILver™ workspace when you have selected the Sensor Part or by selecting the specific **Sensor Group** in the SIF list. The SILver™ workspace shows the sensor group conceptual design information as in the figure below.



As part of the Sensor Group conceptual design configuration, you can specify a ***Name*** and ***Description*** for the sensor group.

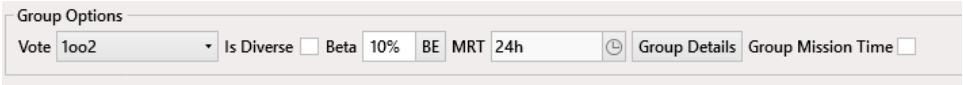
Note: Uniquely naming a Sensor Group is not essential to perform a SIL verification, however to efficiently use the full library aspects of exSILentia®, it is highly encouraged.

G.5.1 Group Options

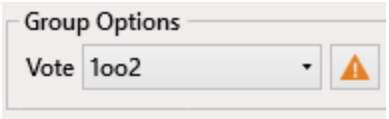
The group options for a Sensor Group allow you to specify:

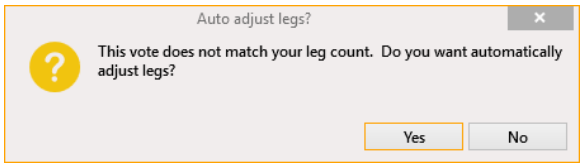
- The ***Voting*** within the sensor group, with standard options as defined in section *G.1 Introduction*
- The ***Voting Type*** for redundant voting options, i.e. are the redundant legs in the group identical or diverse
- The ***Beta Factor*** for redundant voting options, a percentage ranging from 0 and 100%. See section *G.10 SILver Worksheet - Features* for details on the Beta Estimator.
- The ***Mean Repair Time*** (MRT), the expected time to repair the equipment items in the group in case of a detected failure (failure detected by automatic equipment item diagnostics). The MRT is an integer between 4 and 336 hours.
- The ***Group Mission Time*** for this sensor group in case it has a different replacement or refurbishment interval than the entire SIF.

The Group Details button allows you to see the equipment that you selected for the Sensor Group including the associated failure rates. Click this button once you have completed the configuration of the Sensor Group.



When you change the Voting option within the Sensor Group, a Warning Icon will appear next to the Voting selection in addition to a message box. This icon indicates that after you change the voting option, the number of legs associated with the Sensor Group no longer matches the voting option. SILver™ can automatically adjust the number of legs or you can do this manually. The warning icon and message are shown in the next figure.





Note: Sensor Legs are also an exSILentia® Library item and can therefore be reused in multiple locations, not necessarily within the same Sensor Group.

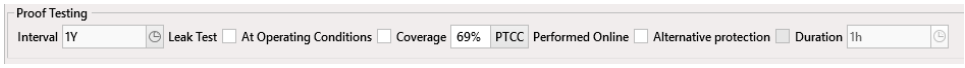
G.5.2 Proof Testing

To model the proof testing applied to the Sensor Group you need to specify:

- The ***Proof Test Interval*** for the sensor group, the time interval between two proof tests. The proof test is the periodic test performed to reveal failures undetected during normal operation. The interval ranges from 1 to 600 months and can be specified in years, months, and/or days.
- The ***Proof Test Coverage*** of the proof test specified for the sensor group. The Proof Test Coverage indicates the effectiveness of a proof test in revealing failures undetected during normal operation. A 100% proof test coverage would mean that ALL failures would be revealable by the test, which realistically is only feasible through replacement or complete refurbishment to an as new state. The proof test coverage must be a value between 0 and 100%. See section *G.10 SILver Worksheet - Features* for details on the Proof Test Coverage Calculator.

You can also indicate how the proof test is ***Performed***, either ***Online*** or ***Offline***. If a proof test is performed while online you can specify the following:

- For redundant configurations, is the testing done ***Staggered*** or not. Staggered indicates that only one of the redundant units is bypassed at a time, ensuring that the sensor configuration remains capable to react to a process demand.
- Is ***Alternate Protection*** available during the proof test. This indicates if during the bypassing of the sensor configuration other means are available to detect the hazard and bring the process to a safe state.
- The ***Duration*** of the proof test. This shows how long the sensor configuration is in bypass, the duration ranges from 1 to 24 hours.



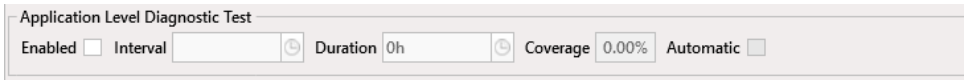
G.5.3 Application Level Diagnostic Test

Application Level Diagnostic Testing allows you to account for additional testing an end-user implements in addition to any automatic self-diagnostics that are part of a specific device. You should not select Application Level Diagnostic Test to account for standard device automatic self diagnostics as these are accounted for in the device's failure rates.

To model application level diagnostic testing to the Sensor Group, first select the "Enabled" check box for this option. Once enabled, you need to specify:

- The Application Level Diagnostic Test Interval for the sensor group, the time interval between two tests. This can be specified in months and years.
- The Application Level Diagnostic Test Duration. This can be specified in hours.
- The Application Level Diagnostic Test Coverage. This indicates the effectiveness of the application level diagnostic test in revealing failures. The test coverage must be a value between 0 and 100%.

You can also indicate if the test is automatic vs. manual, buy selecting the "Automatic" check box for this option. Only in the case of an automatically performed application test does this impact the safe failure fraction. The order of magnitude difference between the demand interval and diagnostic test interval is not considered in classifying a failure as detected or undetected by automatic diagnostics.



G.5.4 Legs

You can add Sensor Legs to your SIF by allowing SILver to automatically adjust the number of legs based on the Sensor Group voting. If you are modeling identical legs, you need only specify them once. If you have selected the "Is Diverse" check box, you will need to specify each separately. As part of the Sensor Leg conceptual design configuration, you can specify a ***Name*** and ***Description*** for the sensor leg.

Note: Uniquely naming a Sensor Leg is not essential to perform a SIL verification, however to efficiently use the full library aspects of exSILentia®, it is highly encouraged.

G.5.5 Leg Options

Once the Sensor Legs are created in SILver, you can select your Leg Options starting with the Measurement Type . The different measurement types include:

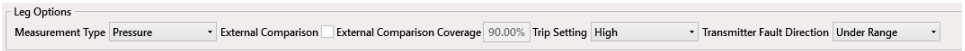
- Pressure
- FireGas
- Proximity
- Flow
- Temperature
- Level
- Other

The remaining Leg Options allow you to specify if the Trip Direction is High or Low, and if you have External Comparison. If you have selected and a sensor that uses analog signals, you will be able to specify if a Transmitter Fault drives the signal Over Range or Under Range.

Trip Setting: Specify whether a High Trip or Low Trip is configured in the application software. This is especially important for 4-20 mA operating devices. For such devices a failure resulting in an output below 4 mA is considered a Fail Low failure and a failure resulting in an output above 20 mA is considered a Fail High failure. Depending on the PLC Detection Configuration settings, Fail Low and Fail High failures will either be classified as safe or dangerous, detected or undetected.

External Comparison: External Comparison is an additional diagnostic implemented by the user. It indicates whether the device signal is compared with a similar second signal. External comparison is highly effective for analog signals since one can monitor differences in dynamic signals and see if something is wrong with one of the analog devices. It is very ineffective for digital signals since digital signals have a static output. IEC 61508 allows claims up to 99% diagnostic coverage on external signal comparison. In exSILentia the user can specify a value ranging from 0% to a more conservative 95% for the external comparison. The default value is 90% for analog signals and 0% for digital signals.

Transmitter Fault Direction: The Transmitter Fault Direction selection determines whether the analog output is driven Over Range or Under Range by the transmitter, upon detection of an internal failure (Fail Detected). This is typically done by setting a switch on the transmitter itself. This will determine how Fail Detected faults are classified, either Fail High or Fail Low. This will lead to subsequent classification into safe or dangers, detected or undetected.

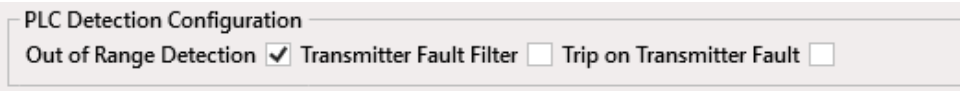


PLC Detection Configuration (Analog Devices Only). These options allow you to indicate the type of input signal diagnostics that are implemented in the logic solver connected to the devices selected in the Sensor Group. These options appear in the Sensor Group view after you choose an analog device.

Out of Range Detection: Select this option if the logic solver connected to the devices selected can detect out of range signals (>20 mA and <4 mA) and you programmed the logic solver to use this functionality, there is input range checking. If this is the case for your application, select the check box for Out of Range Detection.

Transmitter Fault Filter: Select this option if the logic solver performs a type of sampling, for example, the value communicated form the input card to the CPU is averaged or a median value is used. The effect here is that if there is an internal fault in, for example, a transmitter which drives the output over range (Fail High) and you would have a high trip this will not immediately lead to a trip on the application level as sudden input signal transitions are filtered. A next sampling of the input signal is very likely to show an over range signal rather than a signal in active scale above the trip point as internal failure transitions are typically very fast. If this is the case for your application, select the check box for Transmitter Fault Filter.

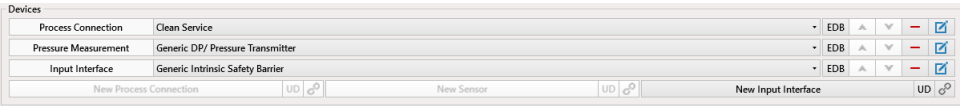
Trip on Transmitter Fault: Select this option if you would like to trip the plant in the event of a transmitter fault. In some cases, end-users do not want to cause any transmitter malfunction to result in a shutdown of a unit but simply have an alarm and perform maintenance on the specific unit that failed. Other end-users do not want to operate in such a degraded mode where, arguable, the SIF protection is lost. If this is the case in your application, select the check box for Trip on Transmitter Fault.



G.5.6 Devices

For each Sensor Group the following devices must be specified:

- **Process Connection** (1 per Sensor Leg): Select the "New Process Connection" button. exida's SERH database will open in a new window showing all available process connections for the measurement type selected. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Sensor** (1 per Sensor Leg): Select the "New Sensor" button. exida's SERH database will open in a new window showing all available sensors for the measurement type selected. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Input Interface** (Unlimited): Select the "New Input Interface" button. exida's SERH database will open in a new window showing all available interfaces for the measurement type selected. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.



Devices already specified in other SIF's can be re-used by selecting the link button and selecting the device in question. Keep in mind, this would mean the SIFs share this equipment. If you are re-using a Device Model used previously in the project, select the from the device drop down list. In this case, this is a new device in the safety instrumented system, but an identical device model.

To specify a User Defined device, select the UD button UD for the specific device type. This will open a new window that allows you to fill in the device information including applicable failure rates. Upon completing the information there, you can apply the device to your SIF by selecting the "Create" button.

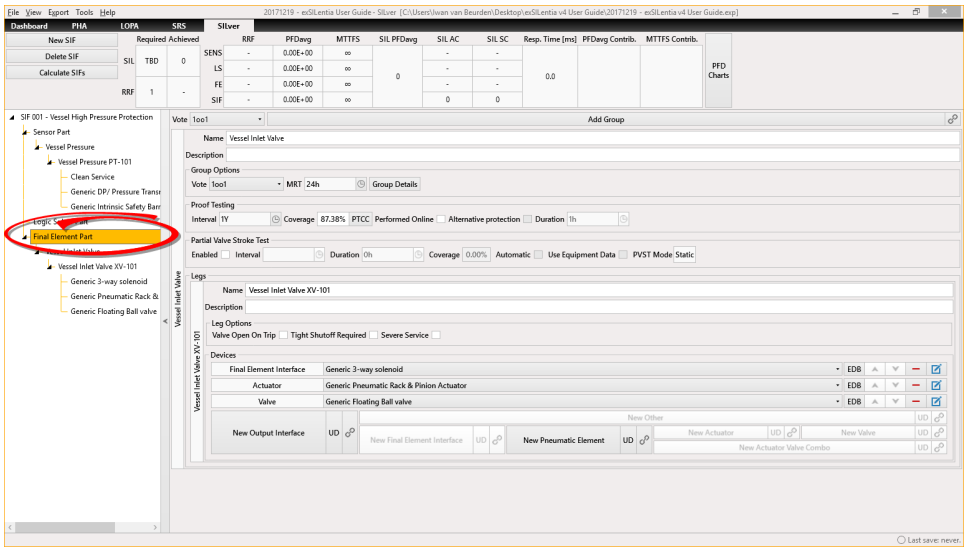
Note: If you specify an analog device for the Sensor Leg, additional Leg Options will appear that must also be specified.

Note: As part of the process connections in exida's SERH database, the following selections are available for Impulse lines:

- Clean Service: This selection means there is no plugging
- Impulse Line - plugging very unlikely: This selection means there is a low frequency of plugging (1 per 400 years).
- Impulse Line - plugging unlikely: This selection means there is a medium frequency of plugging (1 per 40 years).
- Impulse Line - plugging likely: This selection means there is a high frequency of plugging (1 per 4 years).

G.6 SILver Worksheet - Final Element Part

To configure the SIF's Final Element Part in the SILver™ tool, select **Final Element Part** for the SIF in the SIF list. The SILver™ workspace will now show the final element part conceptual design information as shown in the figure below.



As described in section *G.1 Introduction* a Final Element Part can consist of up to 4 Final Element Groups.

To add a new Final Element Group to the Final Element Part:

- Click on the ***Add Group*** button in the middle of the SILver™ workspace
- This will immediately add the Final Element Group to the SILver™ workspace
- This will also add the Final Element Group to the Final Element Groups library

To add a Final Element Group directly from the Final Element Groups Library:

- Click on the Link Final Element Group Icon
- Double Click the Final Element Group to add the group to the Final Element Part

After adding the applicable number of Final Element Groups to the Final Element Part, update the Final Element Part voting, i.e. the voting between groups, in the upper left hand corner of the SILver™ workspace. You can also specify the beta factor to account for common cause between groups. The beta factor must be entered as an integer between 0% and 100%. The default value for the common cause between groups is 0% as different groups are typically used to model independent equipment items. In case there is no complete independence however, i.e. there is common cause susceptibility, a beta factor other than 0% should be used. Use the beta factor estimator feature for assistance in determining an applicable beta factor by clicking the beta estimator icon BE, see also section *G.10 SILver Worksheet - Features*.

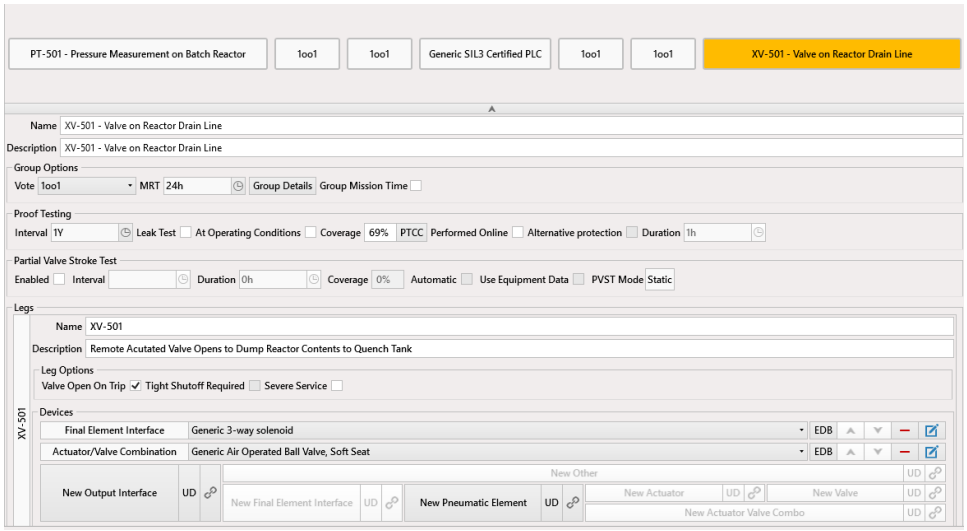
To delete a Final Element Group from the Final Element Part:

- Right click on the specific ***Final Element Group***
- Select ***Delete*** from the pop-up menu
- Click on ***Yes*** when asked if the Final Element Group is really to be deleted

Note: When a Final Element Group is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Final Element Group from the Library. Click **Yes** or **No** as applicable.

G.7 SILver Worksheet - Final Element Group

To configure a SIF's Final Element Group in the SILver™ tool you can either do this in the SILver™ workspace when you have selected the Final Element Part or by selecting the specific **Final Element Group** in the SIF list. The SILver™ workspace shows the final element group conceptual design information as in the figure below.



As part of the Final Element Group conceptual design configuration, you can specify a ***Name*** and ***Description*** for the sensor group.

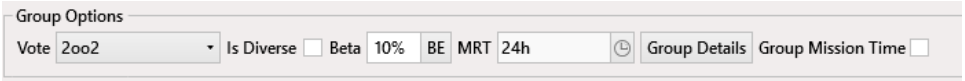
Note: Uniquely naming a Final Element Group is not essential to perform a SIL verification, however to efficiently use the full library aspects of exSILentia®, it is highly encouraged.

G.7.1 Group Options

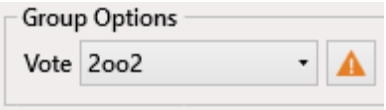
The group options for a Final Element Group allow you to specify:

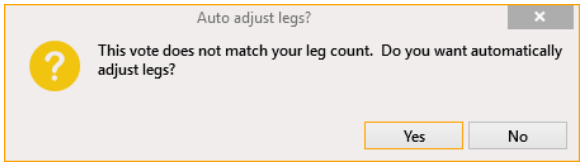
- The ***Voting*** within the final element group, with standard options as defined in section *G.1 Introduction*
- The ***Voting Type*** for redundant voting options, i.e. are the redundant legs in the group identical or diverse
- The ***Beta Factor*** for redundant voting options, a percentage ranging from 0 and 100%. See section *G.10 SILver Worksheet - Features* for details on the Beta Estimator.
- The ***Mean Repair Time*** (MRT), the expected time to repair the equipment items in the group in case of a detected failure (failure detected by automatic equipment item diagnostics). The MRT is an integer between 4 and 336 hours.
- The ***Group Mission Time*** for this final element group in case it has a different replacement or refurbishment interval than the entire SIF.

The Group Details button allows you to see the equipment that you selected for the Final Element Group including the associated failure rates. Click this button once you have completed the configuration of the Final Element Group.



When you change the Voting option within the Final Element Group, a Warning Icon will appear next to the Voting selection in addition to a message box. This icon indicates that after you change the voting option, the number of legs associated with the Final Element Group no longer matches the voting option. SILver™ can automatically adjust the number of legs or you can do this manually. The warning icon and message are shown in the next figure.





Note: Final Element Legs are also an exSILentia® Library item and can therefore be reused in multiple locations, not necessarily within the same Final Element Group.

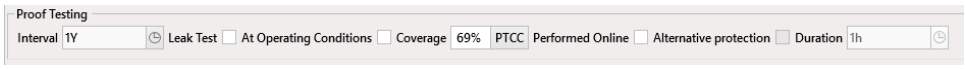
G.7.2 Proof Testing

To model the proof testing applied to the Final Element Group you need to specify:

- The ***Proof Test Interval*** for the final element group, the time interval between two proof tests. The proof test is the periodic test performed to reveal failures undetected during normal operation. The interval ranges from 1 to 600 months and can be specified in years, months, and/or days.
- Indicate if a ***Leak Test*** will be performed as part of the proof test by checking the associated checkbox.
- Indicate if the proof test will be performed ***At Operating Conditions*** by checking the associated checkbox.
- The ***Proof Test Coverage*** of the proof test specified for the final element group. The Proof Test Coverage indicates the effectiveness of a proof test in revealing failures undetected during normal operation. A 100% proof test coverage would mean that ALL failures would be revealable by the test, which realistically is only feasible through replacement or complete refurbishment to an as new state. The proof test coverage must be a value between 0 and 100%. See section *G.10 SILver Worksheet - Features* for details on the Proof Test Coverage Calculator.

You can also indicate how the proof test is ***Performed***, either ***Online*** or ***Offline***. If a proof test is performed while online you can specify the following:

- For redundant configurations, is the testing done ***Staggered*** or not. Staggered indicates that only one of the redundant units is bypassed at a time, ensuring that the final element configuration remains capable to react to a process demand.
- Is ***Alternate Protection*** available during the proof test. This indicates if during the bypassing of the final element configuration other means are available to detect the hazard and bring the process to a safe state.
- The ***Duration*** of the proof test. This shows how long the final element configuration is in bypass, the duration ranges from 1 to 24 hours.

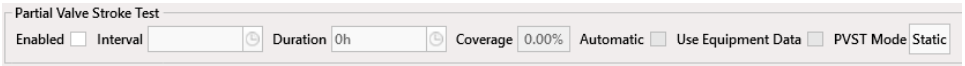


G.7.3 Partial Valve Stroke Test/Application Level Diagnostic Test

To model partial valve stroke testing to the Final Element Group, first select the "Enabled" check box for this option. Once enabled, you need to specify:

- The Partial Valve Stroke Test Interval for the sensor group, the time interval between two tests. This can be specified in months and years.
- The Partial Valve Stroke Test Duration. This can be specified in hours.
- The Partial Valve Stroke Test Coverage. This indicates the effectiveness of the partial valve stroke test in revealing failures. The test coverage must be a value between 0 and 100%.

You can also indicate if the test is automatic vs. manual, buy selecting the "Automatic" check box for this option.



G.7.4 Legs

You can add Final Element Legs to your SIF by allowing SILver to automatically adjust the number of legs based on the Final Element Group voting. If you are modeling identical legs, you need only specify them once. If you have selected the "Is Diverse" check box, you will need to specify each separately. As part of the Final Element Leg conceptual design configuration, you can specify a ***Name*** and ***Description*** for the final element leg.

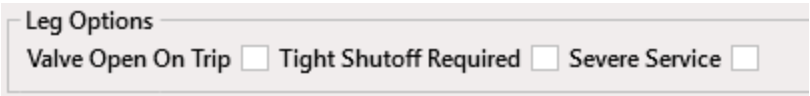
Note: Uniquely naming a Final Element Leg is not essential to perform a SIL verification, however to efficiently use the full library aspects of exSILentia®, it is highly encouraged.

G.7.5 Leg Options

Once the Final Element Legs are created in SILver, you can select your Leg Options. Here you must specify if:

- Tight Shutoff is Required. This option allows you to select if Tigh Shutoff is required for the valve or actuator-valve combination to achieve the safe state of the SIF. Based on the selection appropriate failure rates from exida's Safety Equipment Reliability Handbook database will be selected. If you have specified a User Defined device, the failure rates entered should reflect Tight Shutoff service.
- The application qualifies as Severe Service for your final element. This option allows you to indicate if a valve or actuator-valve combination will likely be used in severe service conditions. Severe Service is defined as the condition that exists when material through the valve has abrasive particles, as opposed to clean service where these particles are absent. Based on the selection appropriate failure rates from exida's Safety Equipment Reliability Handbook databse will be selected. If you have specified a User Defined device, the failure rates entered should reflect the Severe Service conditions.
- The Valve Opens on Trip. You will need to indicate if the valve or actuator-valve combination opens or closes to achieve the safe state. Based on the selection appropriate failure rates from exida's Safety Equipment Reliability Handbook databasewill be selected. If you have specified a User Defined device, the user is responsible for entering data that is representative for the open or close to trip situation.

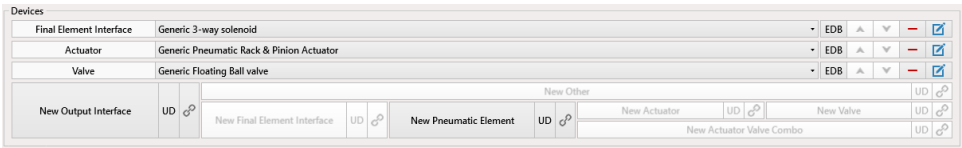
Note: Not all valves and actuator-valve combinations listed in exida's Safety Equipment Reliability Handbook database may have data specified for Open on Trip / Close on Trip, Tight Shutoff and Severe Service. Either the valve or actuator-valve combination cannot be used in one of these selections or additional study of the performance of the device still needs to be performed. If you select an option for which data is not currently available, an error message will be displayed. If this happens, please select a different device or enter a User Defined device.



G.7.6 Devices

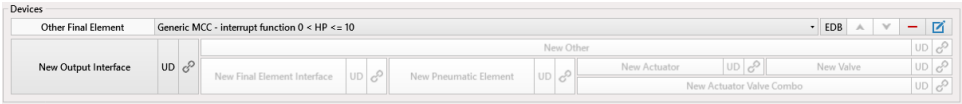
For each Final Element Group that includes a remote actuated valve, the following devices must be specified:

- **Output Interface** (Unlimited): Select the "New Output Interface" button. exida's SERH database will open in a new window showing all available output interfaces. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Final Element Interface** (1 per Final Element Leg): Select the "New Final Element Interface" button. exida's SERH database will open in a new window showing all available final element interfaces. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Pneumatic Element** (Unlimited): Select the "New Pneumatic Element" button. exida's SERH database will open in a new window showing all available pneumatic elements. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Actuator Valve Combo** (1 per Final Element Leg): Select the "New Actuator Valve Combo" button. exida's SERH database will open in a new window showing all available actuator valve combos. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button. Or you can also specify the actuator and valve separately by using the "New Actuator" and "New Valve" buttons.



For each Final Element Group that does not include a remote actuated valve, the following devices must be specified:

- **Output Interface** (Unlimited): Select the "New Output Interface" button. exida's SERH database will open in a new window showing all available output interfaces. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.
- **Other** (1 per Final Element Leg): Select the "New Other" button. exida's SERH database will open in a new window showing all available other final element options. These include alarm bells, relays, motor starters , general MCC's, among others. Scroll to the device of your choosing and double click to apply it to your SIF. You can also select the device once and click the "Add Device" button.

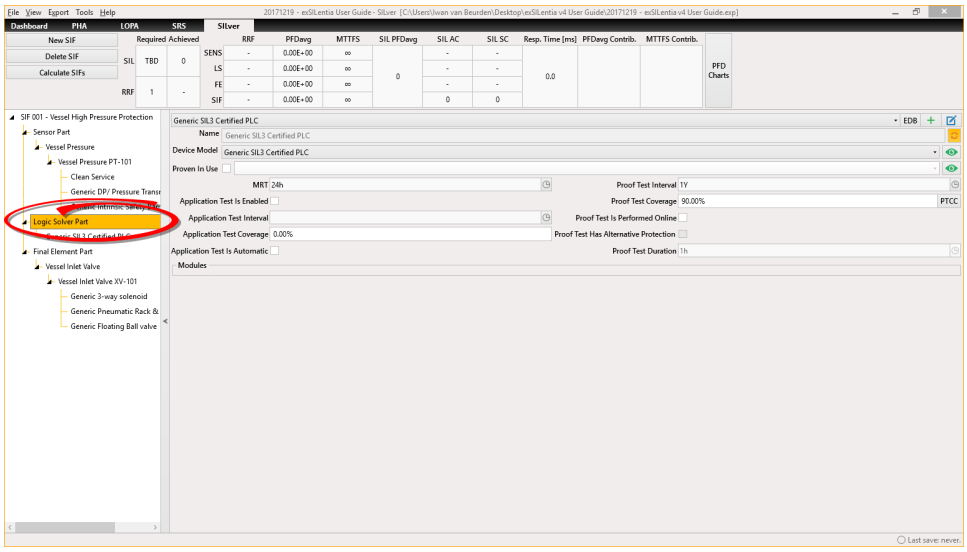


Devices already specified in other SIF's can be re-used by selecting the link button and selecting the device in question. Keep in mind, this would mean the SIFs share this equipment. If you are re-using a Device Model used previously in the project, select the from the device drop down list. In this case, this is a new device in the safety instrumented system, but an identical device model.

To specify a User Defined device, select the UD button UD for the specific device type. This will open a new window that allows you to fill in the device information including applicable failure rates. Upon completing the information there, you can apply the device to your SIF by selecting the "Create" button.

G.8 SILver Worksheet - Logic Solver Part

To configure the SIF's Logic Solver Part in the SILver™ tool, select **Logic Solver Part** for the SIF in the SIF list. The SILver™ workspace will now show the logic solver part conceptual design information as shown in the figure below.



As described in section *G.1 Introduction* a Logic Solver Part does not have any further division into groups like the Sensor and Final Element Parts.

To add a new Logic Solver to the Logic Solver Part:

- Click on the ***EBD*** button on the top right hand side of the SILver™ workspace
- exida's SERH database will open in a new window showing all logic solvers. Scroll to the logic solver of your choosing and double click to apply it to your SIF. You can also select the device once and click the link button .
- This will immediately add the logic solver to the SILver™ workspace
- This will also add the logic solver to the Logic Solvers library

To add a Logic Solver directly from the Logic Solver Library:

- Open the top drop down list in the SILver™ workspace
- Select the applicable logic solver to add it to the Logic Solver Part

To remove a Logic Solver from the Logic Solver Part:

- Click the EBD button and select a different logic solver from the exida SERH database, or
- Select a different logic solver from the drop down list

To permanently delete a Logic Solver from the exSILentia(R) Project:

- Open the project Library
- Select the specific logic solver from the Logic Solvers library
- Click the "-" button
- Confirm the action by clicking the Yes button

Caution: When a Logic Solver is deleted from the library, it will be deleted from all SIFs that it is being used in.

To further configure the Logic Solver you can specify:

- The ***Group Mission Time*** for this logic solver in case it has a different replacement or refurbishment interval than the entire SIF.
- The ***Mean Repair Time*** (MRT), the expected time to repair the logic solver in case of a detected failure (failure detected by automatic equipment item diagnostics). The MRT is an integer between 4 and 336 hours.

To model the proof testing applied to the Logic Solver you need to specify:

- The ***Proof Test Interval*** for the logic solver, the time interval between two proof tests. The proof test is the periodic test performed to reveal failures undetected during normal operation. The interval ranges from 1 to 600 months and can be specified in years and/or months.
- The ***Proof Test Coverage*** of the proof test specified for the logic solver. The Proof Test Coverage indicates the effectiveness of a proof test in revealing failures undetected during normal operation. A 100% proof test coverage would mean that ALL failures would be revealable by the test, which realistically is only feasible through replacement or complete refurbishment to an as new state. The proof test coverage must be a value between 0 and 100%. See section *G.10 SILver Worksheet - Features* for details on the Proof Test Coverage Calculator.

You can also indicate how the proof test is ***Performed***, either ***Online*** or ***Offline***. If a proof test is performed while online you can specify the following:

- For redundant configurations, is the testing done ***Staggered*** or not. Staggered indicates that only one of the redundant units is bypassed at a time, ensuring that the final element configuration remains capable to react to a process demand.
- Is ***Alternate Protection*** available during the proof test. This indicates if during the bypassing of the final element configuration other means are available to detect the hazard and bring the process to a safe state.
- The ***Duration*** of the proof test. This shows how long the final element configuration is in bypass, the duration ranges from 1 to 24 hours.

Application Level Diagnostic Testing allows you to account for additional testing an end-user implements in addition to any automatic self-diagnostics that are part of the logic solver. You should not select Application Level Diagnostic Test to account for standard device automatic self diagnostics as these are accounted for in the device's failure rates.

To model application level diagnostic testing to the Logic Solver, first select the "Enabled" check box for this option. Once enabled, you need to specify:

- The Application Level Diagnostic Test Interval for the sensor group, the time interval between two tests. This can be specified in months and years.
- The Application Level Diagnostic Test Duration. This can be specified in hours.
- The Application Level Diagnostic Test Coverage. This indicates the effectiveness of the application level diagnostic test in revealing failures. The test coverage must be a value between 0 and 100%.

You can also indicate if the test is automatic vs. manual, buy selecting the "Automatic" check box for this option. Only in the case of an automatically performed application test does this impact the safe failure fraction. The order of magnitude difference between the demand interval and diagnostic test interval is not considered in classifying a failure as detected or undetected by automatic diagnostics.

G.9 SILver Worksheet - Results

Once all of the parts of the Safety Instrumented Function are specified, SILver will display the overall SIF performance metrics in the header at the top. You can now review the results and see if the SIF meets the desired Safety Integrity Level. These metrics also include the RRF, PFDavg, MTTFS and the SIL level according to PFDavg, Architectural Constraints and Systematic Capability. For each SIF these metrics are shown for the sensor, logic solver and final element parts in addition to the overall SIF results. Also included are pie charts that indicate the contribution of each part to the overall SIF performance metrics for PFDavg and MTTFS respectively.

If the results do not meet the required SIL or if you want to try different selections, you can easily edit the configuration by clicking on the specific group you want to change in the navigation tree. Note that all SILver input and calculated results will be part of the exSILentia report for functional safety standard compliance.

PFD Charts: The PFD charts show the PFD as a function of mission time in combination with the PFDavg over the entire mission time. The clearly indicate the effects of the proof test interval and proof test coverage. For SIFs where the various parts of the SIF use different proof test intervals, the PFD graphs provide an indication of each parts proof test.

The PFD Charts can be viewed by selecting the "PFD Charts" button on the right side of the results header. A window will open showing four PFD charts, one for the sensor group, logic solver, final element group and overall SIF.

G.10 SILver Worksheet - Features

There are several features build in the SILver Worksheet. In most cases these are available for sensor groups, final element groups, and the logic solver.

G.10.1 Beta Estimator

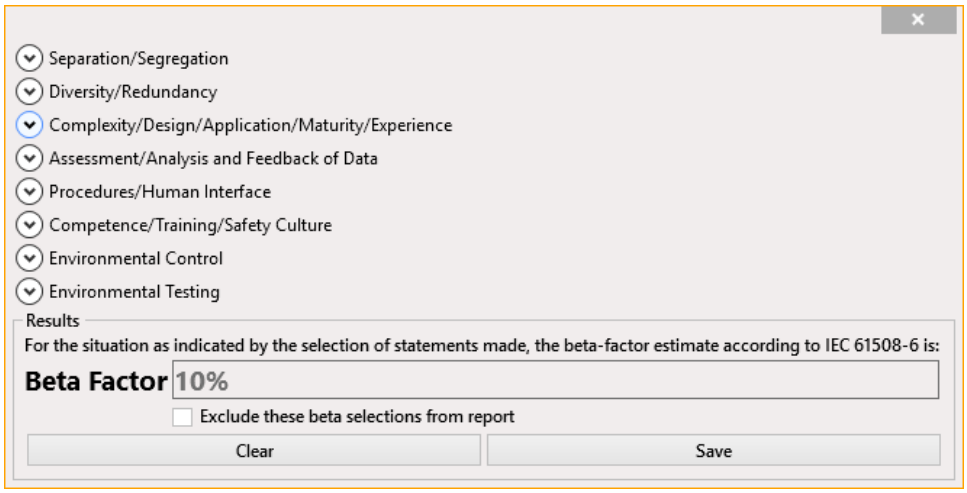
The beta factor is the common cause factor; this is the percentage of failures that is subject to common cause. The beta factor must be entered as an integer between 0 and 100%. For 1oo1 configurations, no beta factor needs to be entered.

Apart from the equipment selected for redundant configurations, the beta factor is the most dominant parameter when it comes to the behavior of the redundant configuration. Making the (unrealistic) claim that the beta factor is equal to 0% would indicate a true redundant behavior where no two failures can occur at the same time. The other extreme claim would be a beta factor of 100%. This would indicate that the redundant units of the configuration always fail at the same time, i.e. the configuration would behave as a single, non-redundant configuration.

If you are uncertain as to what beta factor to select you can use the Beta Estimator. Group Voting is selected in the Sensor Group or Final Element Group Views. If a redundant voting configuration is chosen, a beta factor window will appear with a default value of 10%. To launch the Beta Estimator, select the Beta Estimator button BE next to the beta factor window.

The Beta Estimator evaluates the beta factor to be used for common cause modeling based on the method presented in IEC 61508-6 for sensors and final elements. The tool presents statements about the measures that influence the occurrence of common cause failures and thus the value of the beta factor for the application. To estimate the beta factor one must ascertain which statements apply to the system in question and check the relevant boxes.

The scoring has been designed to allow for items that are not mutually exclusive. For example, a system with logic subsystem channels in separate racks is entitles to score for "Are the logic subsystem channels in separate cabinets?" and that for "Are the logic subsystem channels on separate printed circuit-boards?". A number of items relate to the operation of the system, which may be difficult to predict a the design time. In these cases, the designers should make reasonable assumptions and subsequently ensure that the eventual user of the system is made aware of these assumptions. You can either manually enter the resulting beta factor on the Sensor Group or Final Element Group views or have the beta estimate automatically copy the calculated beta factor.



G.10.2 Proof Test Coverage Calculator

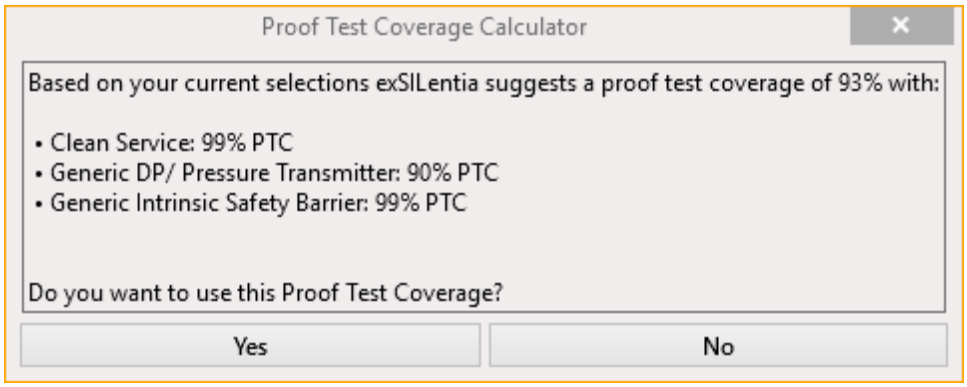
Proof test coverage is an indication of the amount (percentage) of failures that are revealed during a proof test that were not detected by automatic diagnostics. A proof test can be performed online or offline. Proof Test coverage, in combination with the mission time, can have a drastic effect of achieved PFDavg. The higher the proof test coverage the lower the calculated PFDavg; the lower the proof test coverage, the higher the calculated PFDavg will be for constant mission time intervals.

The proof test coverage factor ranges from 0 to 100%. Per IEC 61511, the analyst is allowed to make the assumption of a perfect proof test (proof test coverage is 100%). This would mean that all failures unrevealed during normal operation are revealed during the proof test and that the device is as new after the proof test. On contrast, a proof test factor of 0% would indicate that the proof test does not reveal any undetected failures or that the proof test is simply not performed.

Many manufacturers have published suggest proof tests with associated proof test coverage factors. This information is part of exida's Safety Equipment Reliability Handbook database. Based on the equipment selections made, and the associated proof tests and proof test coverages in the exida SERH database, the calculator will determine the overall proof test coverage for your sensor, logic solver, or final element.

To use the Proof Test Coverage Calculator, simply click the PTCC button next to the proof test window after completing your equipment selection. A Suggested Proof Test Coverage dialog box will appear. The dialog box show what proof test coverage factors will be used in the calculations for the individual equipment items. If exida's SERH database does not contain any suggested proof test coverage data, the calculations will use a coverage of 0%. If you have used a User Defined equipment item, the proof test coverage will also be 0% by default.

In this particular example a Proof Test Coverage factor of 95% is suggests. By clicking "Yes" you will copy the suggested value in the Proof Test Coverage window. If you click "No" no action will be taken and the dialog box will simply close.

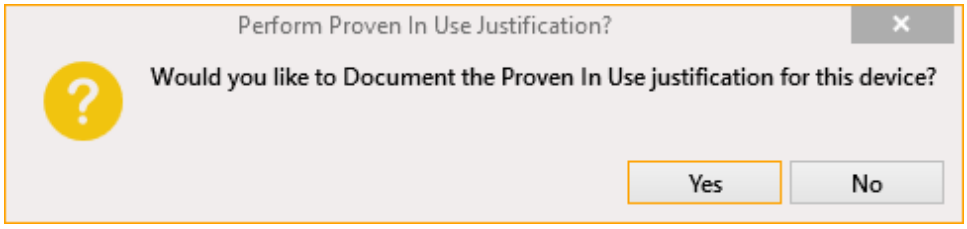


G.10.3 Proven In Use Justification

exSILentia allows you to identify if a specific equipment item is considered Proven in Use. The Proven In Use concept allows a user to justify the use of a specific component that has not been assessed per IEC 61508. The justification that the user is to provide along with the Proven In Use claim is intended to demonstrate that the product in that specific use does not have any systematic failures. With the Proven In Use Justification the end-user takes away the burden for the manufacturer to demonstrate that they followed good engineering practices while developing the product. This is a significant responsibility the end-user takes on themselves so exida urges you to be conservative in the use of the Proven In Use check box on these property dialog boxes.

Claiming Proven In Use will impact the SIL verification results in two ways. First, IEC 61511 architectural constraints allows reduction of the minimum Hardware Fault Tolerance by 1 if a device is proven in use (note that other requirements apply as well thought compliance with these requirements is trivial). Secondly, if you claim proven in use for a device you are able to specify its Systematic Capability, i.e. the SIL level up to which you claim that the systematic integrity of the proven in use is identical to that of a product developed per IEC 61508.

To complete the Proven In Use Justification in exSILentia, first specify your equipment selection. Once you have chosen your equipment, whether from exida's SERH database or a user defined device, you can then open the device details using the edit button . In the device details view, you can select the Proven In Use check box. A dialog box will open asking if you would like to document the Proven In Use Justification for this device. If so, select "Yes". This will open a new window. Select the edit button + and you will see a checklist appear.

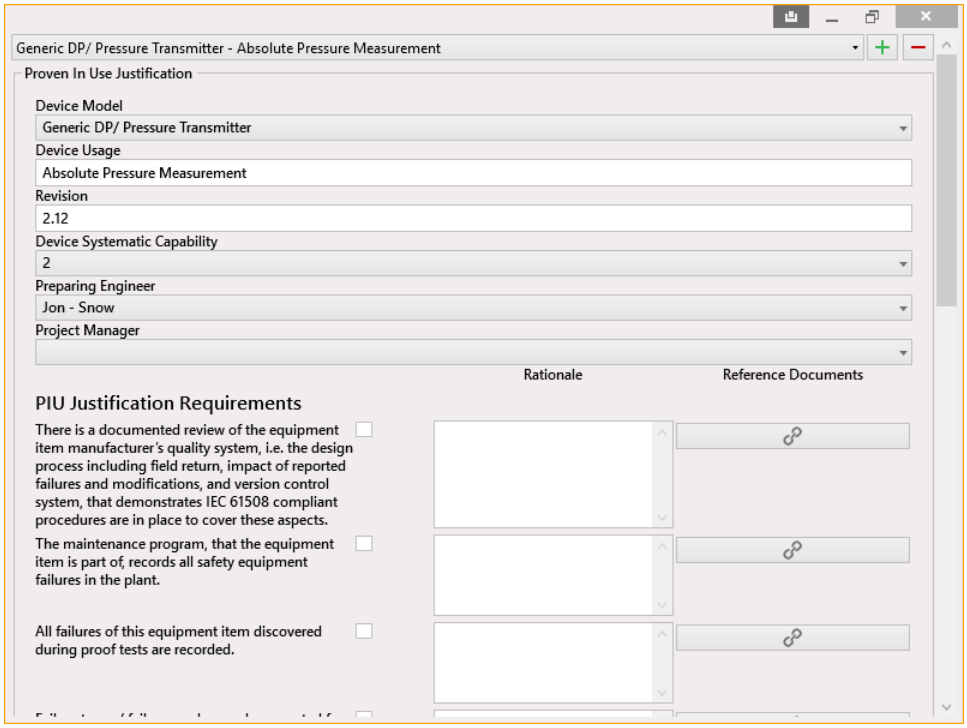


The Proven In Use Justification checklist will allow you to specify the application that the proven in use justification applies to. It also allows you to specify the specific revision of the product. The specific application is important to ensure that the proven in use justification actually applies to the proposed use of the equipment in the safety instrumented function, for example, proven experience in control (dynamic) environment may not suit safety (static) application use. The revision is especially important with regard to the software version of the product as this is usually the place with the majority of systemic failures.

exida has specified a set of Proven In Use Justification criteria based on the IEC 61508 and IEC 61511 functional safety standards. The intent of the justification is to provide a rationale and reference to reference documents why a criterion is met for the specific equipment item.

At the top of the dialog box, the Device Model and Device Usage should be automatically filled in. Then you can document the revision of the Proven In Use Justification documentation, input the Device Systematic Capability you are claiming, and list the Preparing Engineer and Project Engineer from the team members listed in the Library. Next you will see a list of PIU Justification Requirements. For each requirement that applies to your application, you select the adjacent check box. You can then document your rationale and link any references from the library that apply. For those requirements that are not met by the application, there is a space at the bottom to specify a basis for proven in use without those requirements.

Once you complete a Proven In Use Justification it will be stored as part of the exSILentia project. If you want to claim proven in use on the same device for a different SIF, simply choose the item from the drop down list at the top of the Proven In Use Justification window. The Proven In Use Justification documentation is stored in the Library for each Device Model.

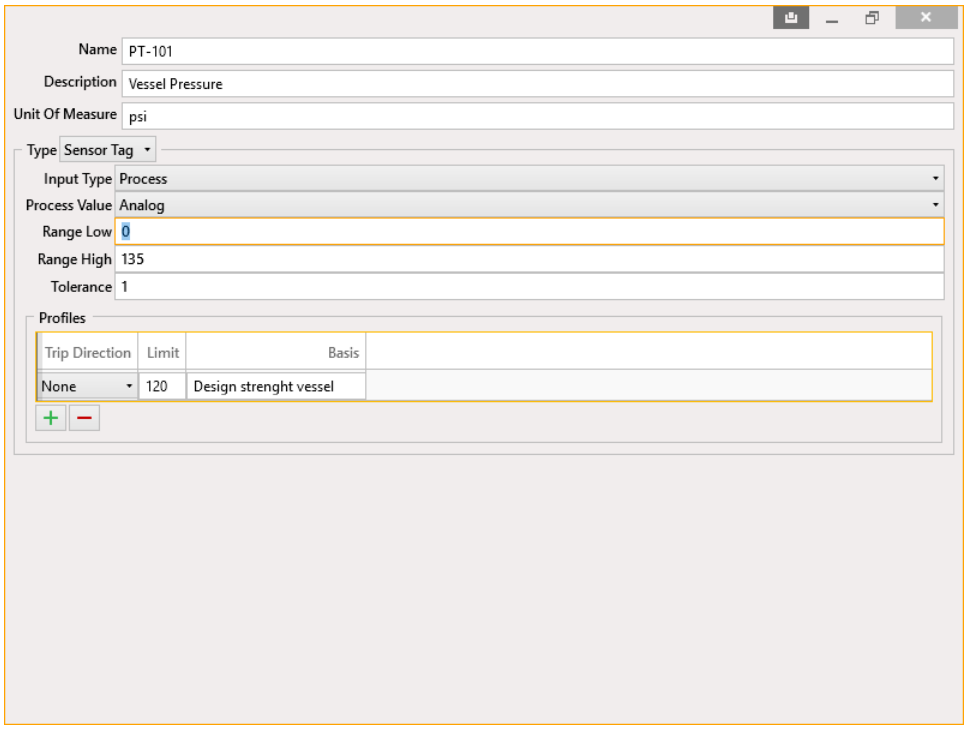


G.11 SILver Worksheet - Tags

Tag information can be applied to each sensor and final element legs. Though the tag information is not critical for the SIL Verification calculation, it can be used in the SRS, SILstat, the DeltaV SIS Configurator, and third party tools that interface with exSILentia.

To add tag information, select the sensor or final element leg in the navigation tree. At the bottom, there is a section labeled "Equipment Tag". On the far right there is a + button. If you select that + button, a window will open from the library that will allow you to enter the tag information. This includes:

- **Name:** Here you would type in the tag name to be used in your application logic.
- **Description:** Here the user can describe the sensor or final element leg and the impact it has on the system
- **Unit of Measure:** Input the unit of measure.
- **Type:** Chose from Sensor Type or Final Element Type.
- **Input Type (Sensor Type Only):** Chose from Process or Discrete
- **Process Value (Sensor Type Only):** Chose from Analog or Digital
- **Range Low (Analog Sensor Type Only):** Input the process value at 4 mA in the unit of measure specified above.
- **Range High (Analog Sensor Type Only):** Input the process value at 20 mA in the unit of measure specified above.
- **Tolerance (Analog Sensor Type Only):** Input the tolerance for the Range Low/High values.
- **Profiles:** Multiple profiles can be assigned to each tag.
    - **For Sensor Type, Analog:** Input the trip direction, the limit (or set point), and the basis of the limit.
    - **For Sensor Type, Digital:** Input the trip direction, and the basis.
    - **For Final Element Type, Remote Actuated Valve:** Input the action, fail position and if tight shutoff is required.
    - **For Final Element Type, Non-Remote Actuated Valve:** Input trip action and fail position.



Note: If you plan to use this information in your safety logic configuration this must match the nomenclature used in the application program.

G.12 SILver Data Transfer

Delete this text and replace it with your own content.

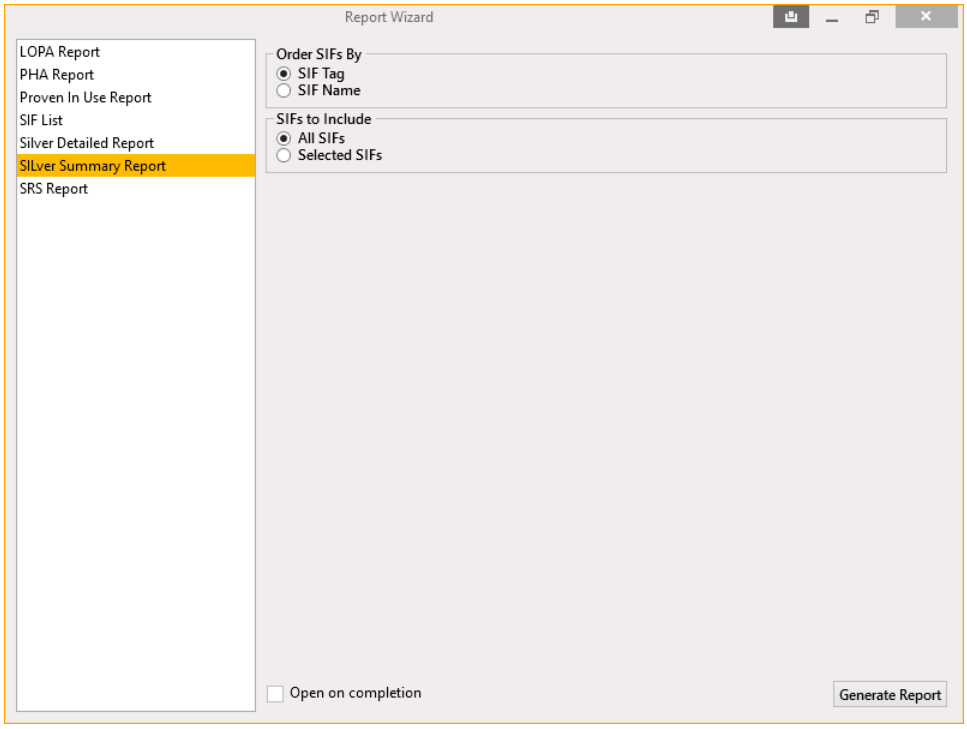
G.13 SILver™ Reports

There are several SILver™ specific reports in exSILentia®. These are

- Proven In Use Report: Documents the Proven In Use justification for a device entered into the SILver module.
- SIF List: Provides an overview of all the safety instrumented functions that are associated with the current project. Details include the tag, name, description, status, required SIL and RRF, and achieved SIL and RRF.
- SIF Detailed Report: Documents all required information for functional safety standard conformance.
- SIF Summary Report: Provides a one page summary of key SIL Verification selections and results of each SIF. Details include achieved SIL, calculated PFDavg, RRF and MTTFS results, as well as a graphical representation of the SIF as modeled in SILver.

For the SILver Summary Report there are several report options which allow you to specify the order of the SIFs as which SIFs to include in the summary report.

In order to generate one of the SILver™ reports select the *Proven In Use Report*, *SIF List*, *SILver Detailed Report*, or *SILver Summary Report* option from the Report Wizard. The Report Wizard will show applicable Report Options.



G.14 SILver™ Data Export

SILver allows you to export SIL verification data into excel including.

The SILver Summary Export documents SIF information in an excel format. Includes:

- Project
- Unit Name
- SIF Name
- SIF Tag
- SIF Description
- Required SIL
- Achieved SIL
- Achieved RRF
- Achieved PFDavg
- SIL (Arch. Const.)
- SIL Capability
- MTTFS
- Proof Test Interval and Coverage for each device
- Limiting Subsystem

The SILver Tags Export documents information in an excel format including:

- SIF Name
- SIF Parts
- Part Tags
- Part Group
- Achieved SIL

In order to generate one of the SILver™ exports, navigate to the top menu and select Export and Export Data, them choose from SILver Summary Export and SILver Tags Export.

Appendix H Design SRS

The Design SRS tab navigates to the exSILentia® v4 detailed design Safety Requirements Specification tool Design SRS. Availability of the Design SRS tab, and therefore the Design SRS tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The Design SRS tool allows detailed design specification of functional requirements for each Safety Instrumented Function (SIF) identified in the exSILentia® project. The detailed design requirements are a result of the conceptual design evaluation performed using the SILver™ tool.

H.1 Introduction

The Design Safety Requirements Specification functionality in the DSRS tool uses a template type interface that enables the specification of general SIS, general SIF, and SIF specific requirements.

In the subsequent sections the DSRS worksheet, its template structure and integrated relationship between general SIS, general SIF, and SIF specific requirements, and its reporting capability will be explained. The available interfaces with the SILect™ and SILver™ tools will also be addressed.

H.2 Design SRS Worksheet

The Design Safety Requirements Specification functionality in the Design SRS tool uses a template type interface that enables the specification of general SIS, general SIF, and SIF specific requirements. The output of the Design SRS tool is a detailed Design Safety Requirements Specification document meant to communicate the conceptual SIF design to the implementation team. Much of the information needed in the DSRS will already be specified in the SILver tool. Any changes to the SILver twool will automatically update the DSRS template. The work flow is setup such that you define general requirements first and then transfer those requirements to the individual SIF specific requirements. The SRS worksheet consists of three main areas: the SIF navigation tree, and the SIF Worksheet and System Level Worksheet.

H.2.1 Creating Safety Instrumented Functions

Within exSILentia® v4 Safety Instrumented Functions (SIF) are Safeguards of Safeguard Category Type IPF (Instrumented Protection Function) where the *"Is SIF"* property is checked. The exSILentia® v4 SIFs therefore comprise of many related data fields inherited from Safeguards, IPFs, and SIF specific fields. Each SIF has a unique Safeguard ID which is automatically generated and assigned to ensure relational data integrity. SIFs should be specified in the library or in PHA, LOPA, SILect, SRS or SILver. You should complete your SIL Verification calculations for each SIF before working on the Design SRS.

To edit the SIF properties:

- Right click on the SIF in the SIF navigation list and select view, or
- Edit the SIF Name and SIF Tag directly in the toolbar

To delete a SIF:

- Select the SIF in the SIF navigation list
- Right click on the SIF and select ***Delete***, click on the ***Delete SIF*** button, or click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the SIF is really to be deleted

CAUTION: Deleting a SIF will delete all instances where the SIF was used. This will include any linking done in the PHAx™, LOPAx™, SILect™, and/or SILver tools.

H.2.2 General SIF Requirements

The General SIF Requirements section allows you to specify requirements that are valid for all SIFs. You will be able to copy these general requirements to the individual SIF Specific Requirements.

To edit the DSRS General SIF Requirements:

- Select ***General SIF Requirements*** tab on the right hand panel of the DSRS.
- Edit the relevant information in this tab.

H.2.3 SIF Specific Requirements

The SIF Specific Requirements are, as their name already indicates, specified for each SIF individually. Though some requirements for different SIFs may be identical, and therefore specified in the General SIF Requirements section, it is essential that each SIF is addressed individually to ensure that each SIF is properly implemented. The SIF Specific Requirements are specified in the left hand area of the DSRS worksheet. Simply select a SIF from the SIF navigation tree and edit the applicable fields.

There are two ways to copy specifications from the General SIF Requirements to SIF Specific Requirements. You can copy data from the general SIF requirements to SIF specific requirements

- for all SIFs at once
- for one SIF at a time

To transfer data for all SIFs at once:

- Click on the ***Load data from General SIF Requirements to SIF Specific Requirements for all SIFs*** button

To transfer data for one SIF at a time:

- Select the desired SIF in the SIF Navigation List
- Click on the ***Load data from General SIF Requirements to SIF Specific Requirements for current SIF*** button

When transferring data, you will receive a warning that advises you that the General SIF Requirements data will be merged into the existing SIF(s) Specific Requirements which could delete information that you specified previously.

H.2.4 Sensor Legs, Auxiliary Input Legs, and Auxiliary Input Parameters

Legs

The DSRS automatically accounts for the Sensor Legs specified in the SILver module. For each leg, the leg type (analog or digital) is determined from the selections in the SIL Verification calculation. In addition, the PID number, Model/Datasheet, Action, Comparison Tag and Maintenance Override can be documented in the DSRS.

Auxiliary Input Legs can also be added to a SIF in the DSRS. To add a new Auxiliary Input Leg, select 'Add Auxiliary Leg' in the SIF Specific Sensor Section of the DSRS. Here you can enter Name, Description ,Type, PID number, Model/Datasheet, Action, Comparison Tag and Maintenance Override.

Finally Auxiliary Input Parameters can be added to a SIF in the DSRS. To add a new Auxiliary Input Parameter, select 'Add Auxiliary Parameter' in the SIF Specific Sensor Section of the DSRS. Here you can enter the Name, Description, Type, Security, Unit of Measure, Range, Setpoint and Trip Direction.

H.2.5 Final Element Legs, Auxiliary Output Legs, and Auxiliary Output Parameters

The DSRS automatically accounts for the Final Element Legs specified in the SILver module. For each leg, the leg type is determined from the selections in the SIL Verification calculation. In addition, the PID number, Model/Datasheet, Action, Resent Options and ETT or DTT selection can be documented in the DSRS.

Auxiliary Output Legs can also be added to a SIF in the DSRS. To add a new Auxiliary Output Leg, select 'Add Auxiliary Leg' in the SIF Specific Sensor Section of the DSRS. Here you can enter Name, Description, Type, the PID number, Model/Datasheet, Action, Resent Options and ETT or DTT selection.

Finally Auxiliary Input Parameters can be added to a SIF in the DSRS. To add a new Auxiliary Input Parameter, select 'Add Output Parameter' in the SIF Specific Sensor Section of the DSRS. Here you can enter the Name, Description, and Type.

H.3 Design SRS Data Transfer

The exSILentia® v4 integration of Process Safety / Functional Safety software tools allows for seamless data exchange between the different phases of the Lifecycle. The Design SRS is meant to document the conceptual design based on SIL Verification. Much of the information input into the SILver module will be included in the Design SRS report. This will be done automatically, and any changes to the SILver tool will update in Design SRS without any prompt from the user.

H.4 Design SRS Reports

In order to generate a Design SRS report select the Design SRS Report option from the Report Wizard. There are no Report Options for the Design SRS report.

Appendix I Proof Test Generator

The Proof Test Generator tab navigates to the exSILentia® v4 proof test generator tool. Availability of the PTG tab, and therefore the Proof test generator tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The proof test generator tool provides and easy way to generate a proof test plan for the equipment items specified as part of your Conceptual Design verification using the SILver™ tool.

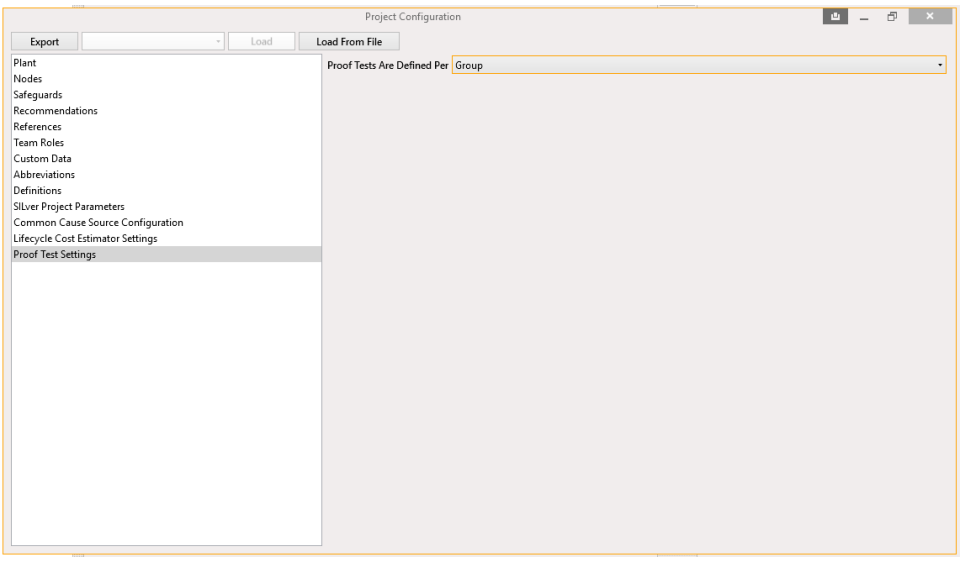
I.1 Introduction

Proof Test Generator is an automated way to create a draft proof test plan for inclusion in your mechanical integrity program. The Proof Test Generator can save you hours of engineering time as it will provided specific proof test for each equipment item specified as part of your Conceptual Design verification using the SILver™ tool. The proof tests are directly obtained from the exida Safety Equipment Reliability Handbook (SERH) database which contains both the proof test steps as well as the associated proof test coverage.

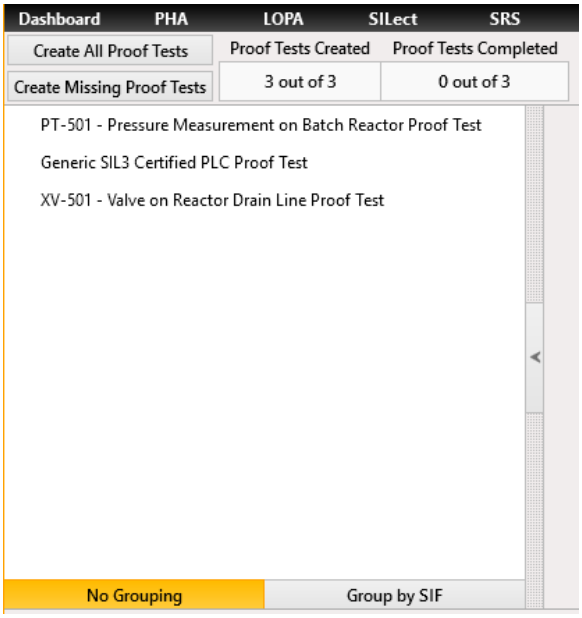
A proof test is a manual test designed to reveal equipment item failures undetected by automatic diagnostics during normal operation. This includes both safe and dangerous undetected failures as well as diagnostic failures. The proof test interval in combination with the comprehensiveness of the proof test, expressed through the proof test coverage, can have a dramatic impact on the achieved Safety Integrity Level for the SIF that the equipment item is part of.

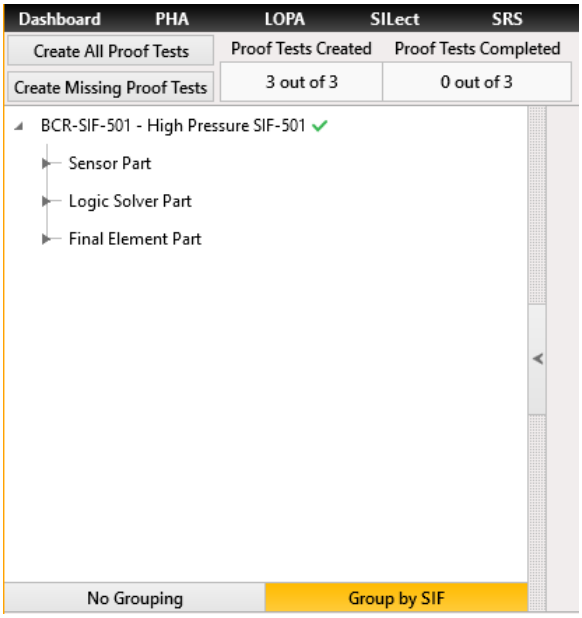
I.2 Proof Test Generator Worksheet

The PTG module should be used to create proof test procedures on the SIF devices modeled during SIL Verification. Once the conceptual design for a SIF is finalized, open the PTG module and select 'Create all Proof Tests' button. If you have already created some proof tests but want to add more to the module, select the 'Create Missing Proof Tests' button instead. Proof Tests can be defined per SIF, Group, or Leg. This is a project wide setting that can be made in the Project Configuration under the Proof Test Settings entry.



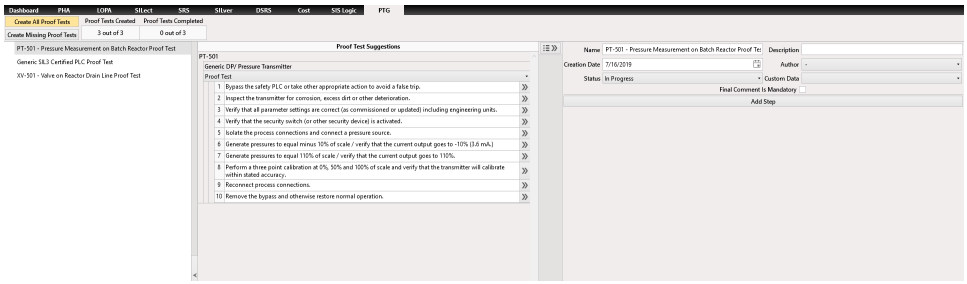
In the Proof Test Generator (PTG) module, the navigation tree view options include organizing the proof tests per SIF (Group by SIF), or simply listing the proof tests (No Grouping). For proof tests organized per SIF, the proof test can be created on the same level the the proof test is defined. The other levels are shown as reference, but are not used to build the proof test. In this case, the proof test pane will indicate 'No proof test on this level'. Simply navigate to the level on which the proof test will be defined.



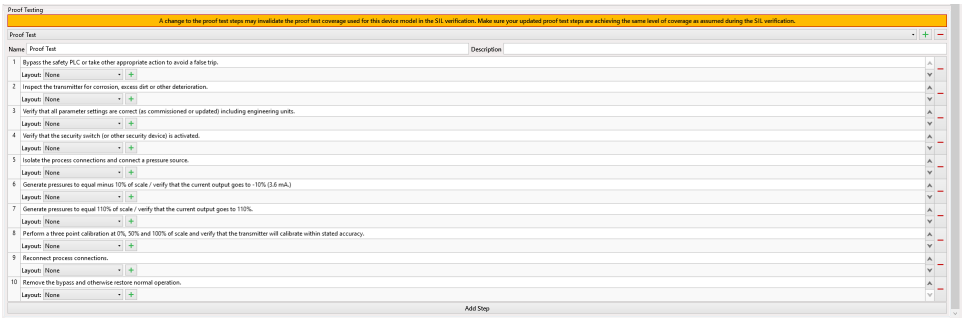


I.2.1 Proof Test Suggestions

Many SIF devices specified using exida's SERH have associated proof test steps that help to determine the proof test coverage used in the SIL Verification calculation. These steps are not application specific and are often provided from the manufacturer. In the 'Proof Test Suggestions' pane, to the right of the navigation tree, the PTG module automatically populates these suggestions for the user to apply to the proof test procedure. This can be done by selecting the arrow button next to each step to apply steps one at a time. To apply all steps at once select the apply all suggestions button in the column between the suggestions and the proof test.

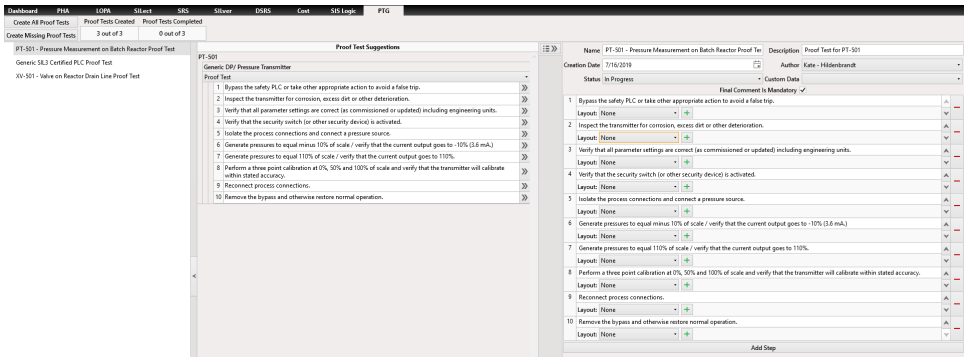


Proof Test suggestions can be modified in the library in the Device Model view. Before making changes remember that the steps provided correlate to the proof test coverage used in the SIL Verification calculation. Changing the procedure to exclude steps would affect this coverage, rendering your results invalid. However, information specific to the application or site may be added without affecting the coverage. User defined steps may also be added to the Device Model library and will automatically populate along with steps provided by the SERH.



I.2.2 Proof Test Procedure

In the far right pane the proof test procedure can be customized. Each proof test can be given a Name, Description, Creation Date, Author and Status. You can indicate if a Final Comment is mandatory for each proof test and add custom data as needed.



Steps can be added directly to the proof test using the 'Add Step' button. If any suggestions were applied, they will appear in the Proof Test Procedure as well. Here the steps can be specified further. This includes editing the text to add any application or site specific information to this procedure. They can be re-ordered or deleted using the arrow and delete buttons to the far right of each step. The layout can be specified to indicate the response or result required by the recorder of the proof test. Passing criteria can also be specified. Child steps can be added by selecting the plus button next to the layout for each step.

The different layouts include:

Text - In this case no passing criteria need be specified. The recorder is expected to write in results.

Boolean - In this case a checkbox will appear. The user can indicate if the box should be checked or left unchecked for passing criteria.

Number - In this case you can indicate that the result should be a value greater than, less than, greater than or equal to, less than or equal to, equal to, not equal to or greater than or equal to AND less than or equal to the specified value. A tolerance can be added for passing criteria, and unit of measure can be indicated.

None - In this case a checkbox will appear to show that the step is completed, and nothing more.

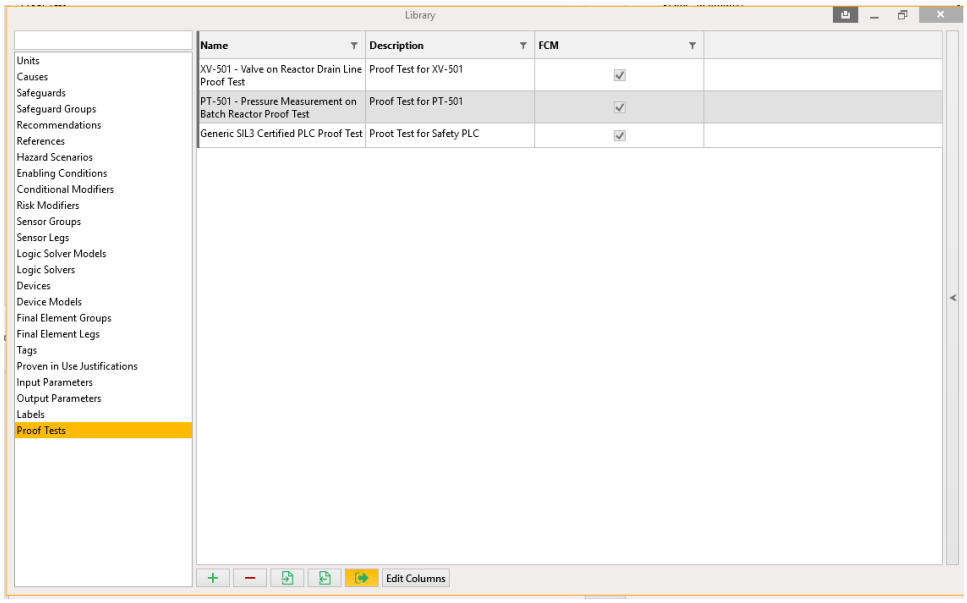
Name	PT-501 - Pressure Measurement on Batch Reactor Proof Tes	Description	Proof Test for PT-501
Creation Date	7/16/2019	Author	Kate - Hildenbrandt
Status	In Progress	Custom Data	

Final Comment Is Mandatory ☑

1	Bypass the safety PLC or take other appropriate action to avoid a false trip.				
	Layout: None				
2	Inspect the transmitter for corrosion, excess dirt or other deterioration.				
	Layout: Boolean	Pass Criteria: ☑			
3	Verify that all parameter settings are correct (as commissioned or updated) including engineering units.				
	Layout: Boolean	Pass Criteria: ☑			
4	Verify that the security switch (or other security device) is activated.				
	Layout: Boolean	Pass Criteria: ☑			
5	Isolate the process connections and connect a pressure source.				
	Layout: None				
6	Generate pressures to equal minus 10% of scale / verify that the current output goes to -10% (3.6 mA.)				
	Layout: Number	Pass Criteria: 3.6	=	Tolerance: 0.1	UOM: mA
7	Generate pressures to equal 110% of scale / verify that the current output goes to 110%.				
	Layout: Number	Pass Criteria: 21.5	=	Tolerance: 0.1	UOM: mA
8	Perform a three point calibration at 0%, 50% and 100% of scale and verify that the transmitter will calibrate within stated accuracy.				
	Layout: Text				
9	Reconnect process connections.				
	Layout: None				
10	Remove the bypass and otherwise restore normal operation.				
	Layout: None				

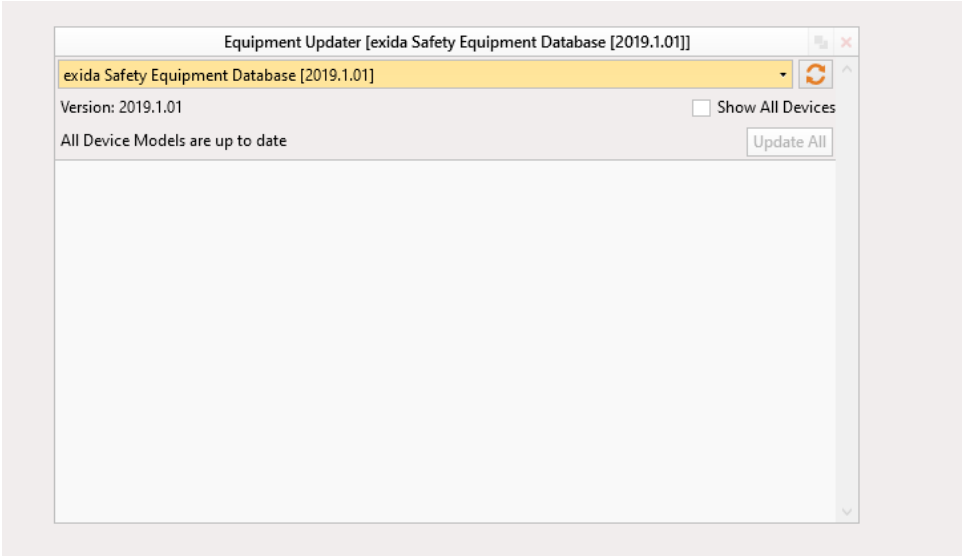
Add Step

Upon completion of each proof test the status can be changed to 'Complete'. A green checkmark will appear in the navigation tree to show which proof tests are complete. The header at the top of the module shows number of 'Proof Tests Created' and 'Proof Tests Completed'. All proof tests created are saved in the library, under Proof Tests.



I.2.3 Starting PTG with an Existing Project File

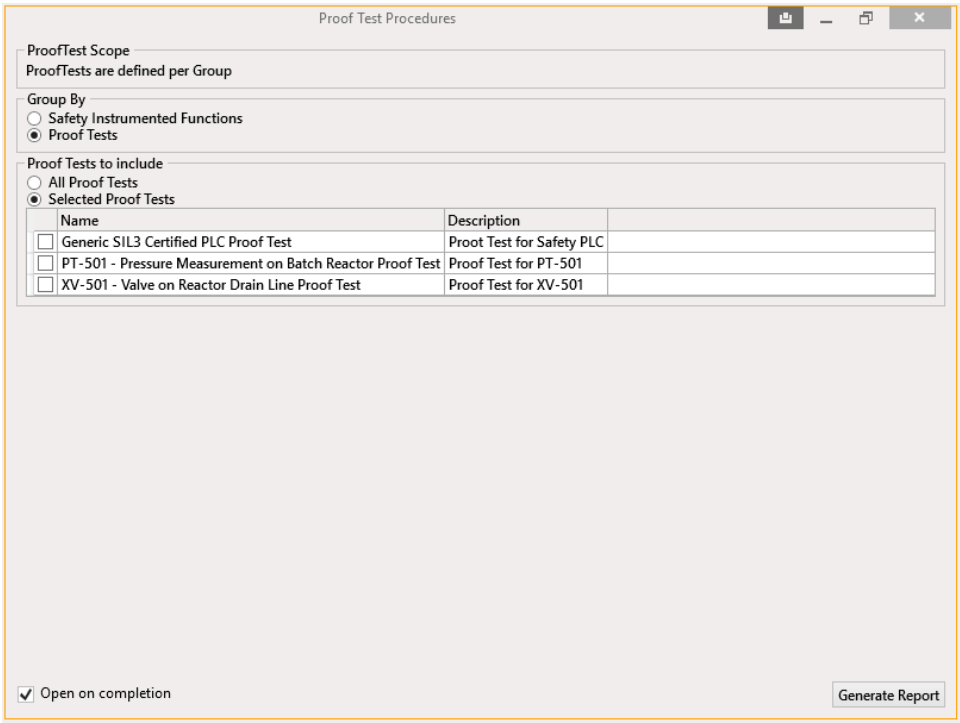
If the SIL Verification was completed in a project file 4.7 or earlier, the SERH may need to be updated before starting with the PTG. This will ensure the proper suggestions are given in the PTG module. To update the SERH, use the SERH widget on the Dashboard. This can be found by navigating to the Dashboard tab, and selecting the green plus button on the far right hand side. This shows all the widgets available for the dashboard. Select the widget titled 'exida Safety Equipment Database'. The widget will open on the dashboard. Select the checkbox that says show all devices. Make sure all are highlighted and then select the 'Update All' button. This will populate the proof test suggestions needed to create your proof test.



I.3 Proof Test Generator Reports

In order to generate a Proof Test report select the *Proof Test Procedures* option from the Report Wizard. The Report Wizard will show applicable Report Options.

The Report Option allows you to choose a report organized per SIF or per Proof Test. For each you can choose to include all defined in the project, or select individual tests to be included.



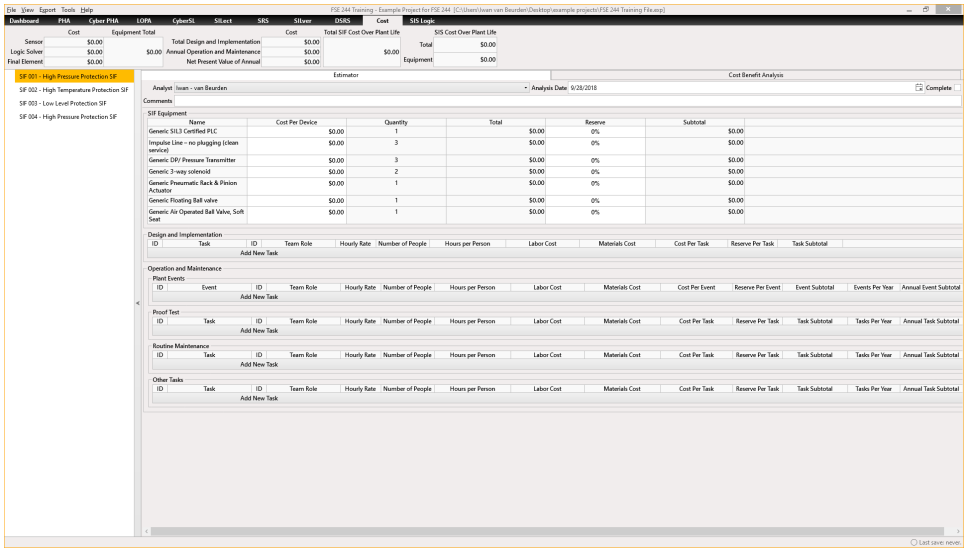
Appendix J Lifecycle Cost Estimator

The Cost tab navigates to the exSILentia® v4 Lifecycle Cost Estimator tool. Availability of the Cost tab, and therefore the Lifecycle Cost Estimator tool, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The Lifecycle Cost Estimator tool supports the evaluation of a Safety Instrumented Function's conceptual design on the basis of expected overall lifecycle cost, accounting for aspects such proof test cost and proof test frequency. The Lifecycle Cost Estimator tool can assist in making an economical justification why a particular conceptual design may be better than an alternate conceptual design where both meet the same functional and integrity requirements. The Lifecycle Cost Estimator takes many aspect into consideration, including spurious trip rates, frequency of proof tests, maintenance requirements, installation cost etc., and determines based on a discount rate what the net current cost is of a proposed Safety Instrumented Function. Many of the parameters that impact overall lifecycle cost are automatically obtained from the conceptual SIF design as modeled in the SILver™ tool.

In addition, the exSILentia® v4 Lifecycle Cost Estimator tool allows you to perform a cost benefit analysis for a particular SIF, determining the financial impact of a SIF on overall plant risk.

J.1 Introduction

The lifecycle cost estimation functionality in the Cost tool use s a spreadsheet type interface to allow you to specify SIF equipment, Design and Implementation, and Operation and Maintenance cost.



In the subsequent sections the Cost worksheet for both Lifecycle Cost Estimation and Cost Benefit Analysis will be explained, as wells as the reporting capability. Interactions with the library regarding items as Device Models and Team Members will also be addressed.

J.2 Lifecycle Cost Estimator Worksheet

The Lifecycle Cost Estimator worksheet consists of two sub-worksheets, the Estimator worksheet and the Cost Benefit Analysis worksheet. The cost benefit analysis relies on information specified as part of the estimator work, so always start with the estimator.

J.2.1 Estimator worksheet

The estimator worksheet is divided into several sections to make specifying the individual cost aspects easy.

SIF equipment

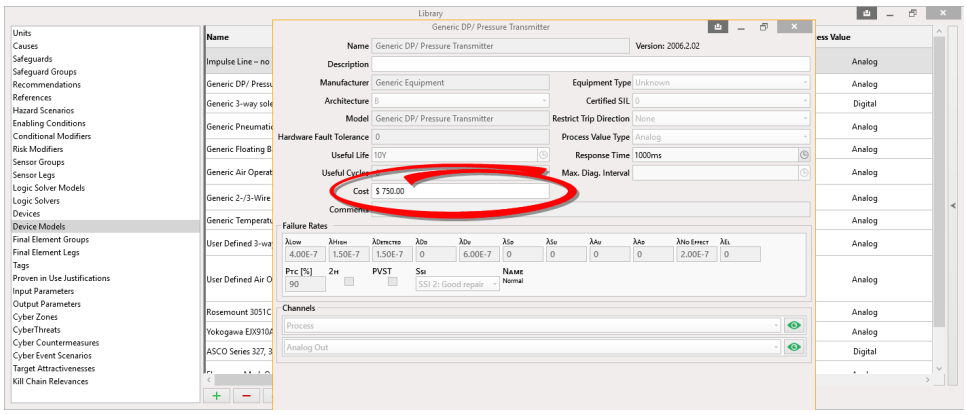
The SIF Equipment area shows all device models that are part of the specific SIF. The Cost tool automatically determines the total quantity of device used for each device model as specific in the SILver™ tool. For each device, you can specify:

- Cost per Device
- Reserve

The cost per device is automatically associated with the specific device model, meaning that if you specify a cost for a device model here, it will automatically be used for all estimations that use the same device model. This also means that you can specify the cost per device in the Device Model library.

SIF Equipment

Name	Cost Per Device	Quantity	Total	Reserve	Subtotal
Generic SIL3 Certified PLC	$ 75,000.00	1	$ 75,000.00	5%	$ 78,750.00
Impulse Line – no plugging (clean service)	$ 50.00	3	$ 150.00	5%	$ 157.50
Generic DP/ Pressure Transmitter	$ 750.00	3	$ 2,250.00	5%	$ 2,362.50
Generic 3-way solenoid	$ 2,000.00	2	$ 4,000.00	5%	$ 4,200.00
Generic Pneumatic Rack & Pinion Actuator	$ 5,000.00	1	$ 5,000.00	5%	$ 5,250.00
Generic Floating Ball valve	$ 15,000.00	1	$ 15,000.00	5%	$ 15,750.00
Generic Air Operated Ball Valve, Soft Seat	$ 20,000.00	1	$ 20,000.00	5%	$ 21,000.00



Design and Implementation

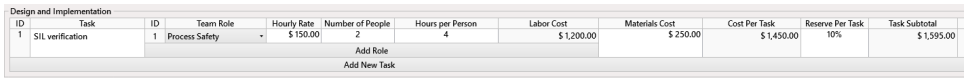
Design and Implementation cost are specified on a task basis.

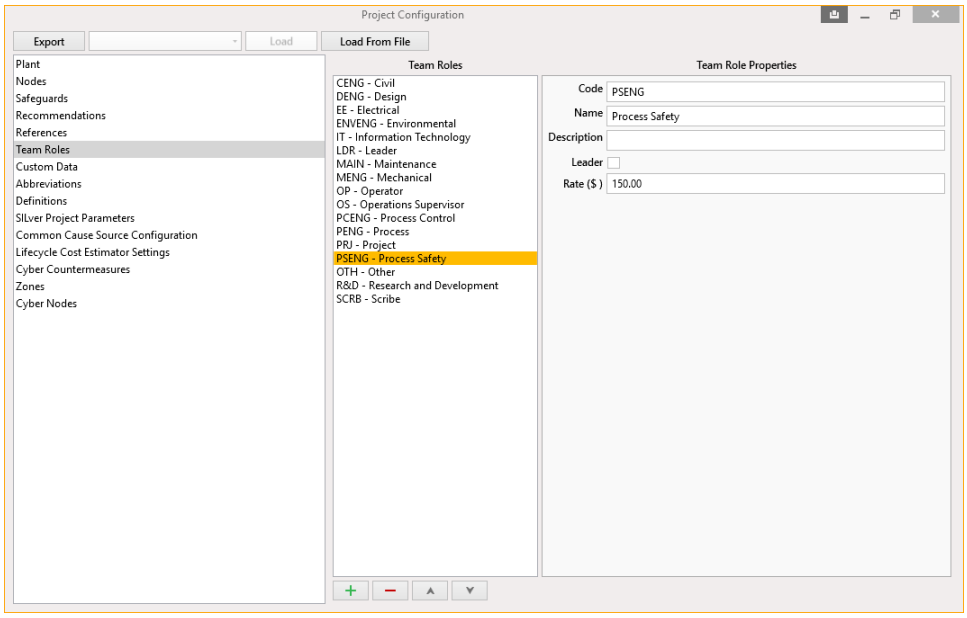
To add a design and implementation task click the ***Add New Task*** button. You can now specify a description for the task, e.g. SIL verification. You can then add a Role to the task by clicking on the ***Add Role*** button. Once a role is added to a task you can select the team role from the drop down list. The roles available are specified in the Project Configuration, see section *6.6 Team Roles*. For each role you can then calculate the Labor Cost by specifying:

- Hourly Rate
- Number of People
- Hours per Person

The hourly rate is automatically associated with the specific team role, meaning that if you specify an hourly rate for a team role here, it will automatically be used for all estimations that use the same team role. This also means that you can specify the hourly rate in the Team Roles section of the Project Configuration.

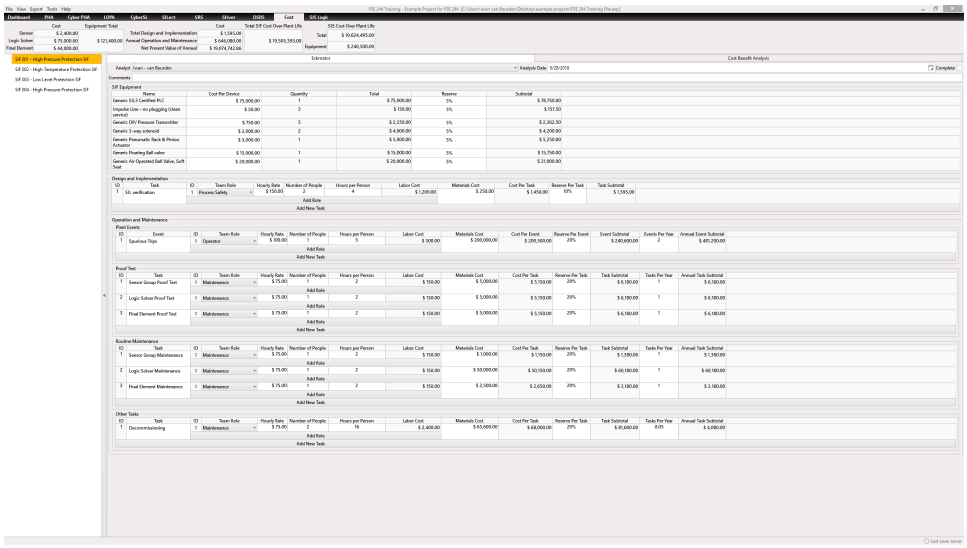
Next you can specify Materials Cost and a Reserve per Task to determine the Task Subtotal.





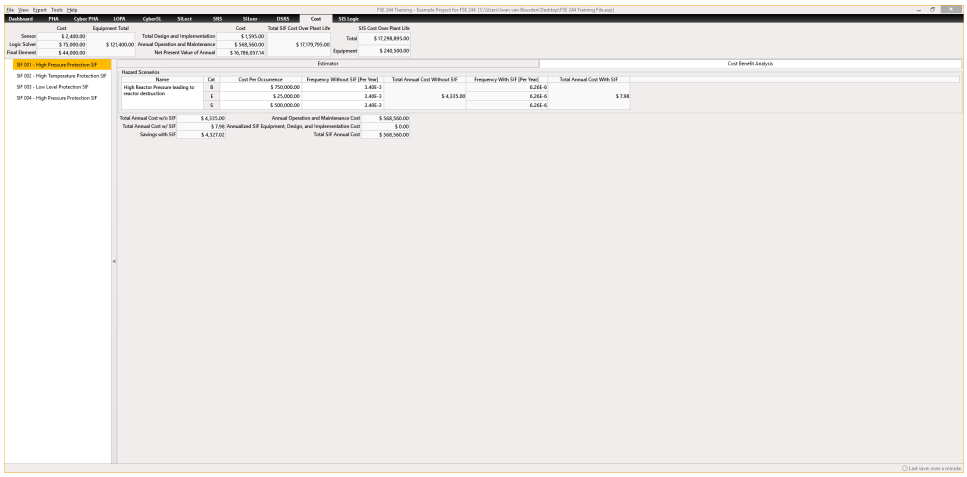
Operation and Maintenance

Operation and Maintenance Cost are further divided into Plant Events, Proof Tests, Routine Maintenance, and Other Tasks. For each section events can be defined similar to the tasks in the Design and Implementation cost section. In addition to the fields available for the Design and Implementation tasks, the Operation and Maintenance section also include a field to specify the frequency of the event per year.



J.2.2 Cost Benefit Analysis worksheet

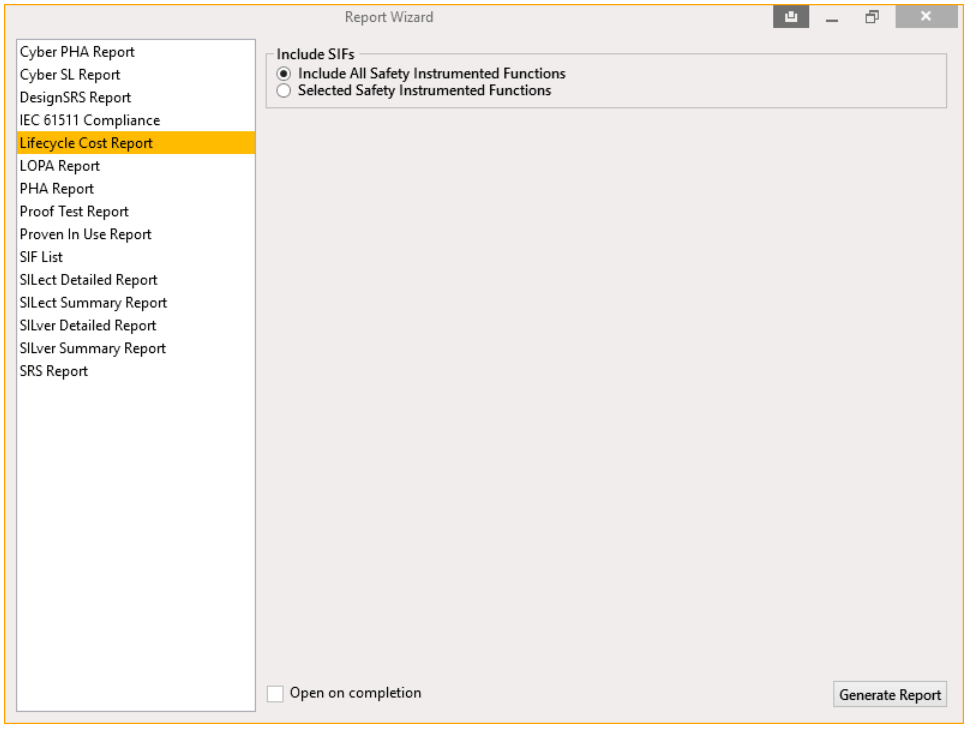
The cost benefit analysis worksheet shows all hazard scenarios that the current SIF is protection against. You can specify the cost per occurrence of the hazard scenario for each severity category. If you used exSILentia™ LOPA tool on this project the frequency of occurrence of the hazard without the SIF will be automatically calculated. Given the probability of failure of the SIF as calculated in SILver and the SIF cost as determined in the estimator portion of the Cost tool, the annualized cost of the hazard scenario with and without the SIF is calculated.



J.3 Lifecycle Cost Estimator Reports

In order to generate a Lifecycle Cost Estimator report select the *Lifecycle Cost Report* option from the Report Wizard. The Report Wizard will show applicable Report Options.

The Report Option allows you to include or exclude SIFs in your Lifecycle Cost report.



Appendix K exSILentia® Cyber

The CyberPHA tab navigates to the exSILentia® v4 cyber process hazard analysis tool CyberPHAx™ whereas the CyberSL™ tab navigates to the exSILentia® v4 cyber security level tool CyberSL™. Availability of the CyberPHA and CyberSL tabs, and therefore the exSILentia® Cyber tools CyberPHAx™ and CyberSL™, is based on your exSILentia® v4 license (see *Chapter 1 Introduction* for an overview of the exSILentia® v4 license options). The CyberPHAx™ tool allows cyber risk assessment to be performed based on the process industry Hazard and Operability (HAZOP) methodology. The CyberSL™ tool allows for a security level evaluation to be performed on the various countermeasures identified for a particular threat.

K.1 CyberPHAx™

The CyberPHAx™ tool allows cyber risk assessment to be performed based on the process industry Hazard and Operability (HAZOP) methodology.

K.1.1 Introduction

Since the cyber risk assessment approach is based on the HAZOP methodology, CyberPHAx™ shows many similarities with exSILentia® PHAx™, see *Appendix C PHAx™*. The CyberPHAx™ tool uses a spreadsheet type interface with defined columns for the various cyber risk assessment items.

In the subsequent sections the CyberPHAx™ tool hierarchy, the worksheet, and its reporting capability will be explained.

K.1.2 Hierarchy

The hierarchical top level for an exSILentia® v4 project is a plant. Within the plant level several cyber zones can be defined and within the cyber zone level, cyber nodes can be defined. Threat vectors which are the cornerstone of the cyber risk assessment are defined for each cyber node.

- **Plant (exSILentia® v4 project)**
  - **Cyber Zones**
    - **Cyber Nodes**
      - **Threat Vector**

Cyber Zones

A cyber zone allows division of an exSILentia® v4 project plant.

To add a Cyber Zone:

- Click on the green plus (**+**) symbol in the Cyber Zone row
- Edit the Cyber Zone Properties, i.e. *Name*, select the *Plant Type* from the drop down box (optional), and select the *Process Type* from the drop down box (optional)
  - See section *6.1* for more information on Plant and Process Types

Note: The default value for Plant Type is *Unknown*. The Process Type field will remain blank without drop down box selections until a Plant Type has been defined.

Upon completion of all study items associated with a particular cyber zone, the *Complete* check box can be checked. The box to the far right of the unit will turn orange and show a green bold check mark.

To navigate between cyber zones you can use the navigation tree in the left hand side bar, click the Cyber Zone drop down box and select the desired Cyber Zone, or click on the up or down icons until the applicable Cyber Zone is selected.

To modify a Cyber Zone:

- Highlight the Cyber Zone
- Click the icon
- Edit the Cyber Zone Properties, i.e. *Name*, select the *Plant Type* from the drop down box (optional), and select the *Process Type* from the drop down box (optional)

To delete a Cyber Zone:

- Highlight the Cyber Zone
- Click on the red minus (**-**) symbol in the Cyber Zone row
- Click *Yes* to confirm you want to delete the Cyber Zone
- This will remove that Cyber Zone, its Cyber Zone Properties, and all associated data

Cyber Nodes

A HAZOP Cyber Node represents a specific section of the cyber zone system in which threat vectors are evaluated.

To add a Cyber Node:

- Select the Cyber Zone where the node will be added
- Click on the green plus (**+**) symbol in the Cyber Node row
- Edit the Cyber Node Properties, i.e. *Name*, *Node Intention*, and *Comments* (optional)
- To take advantage of Smart Threat Vectors:
    - Check the Smart Threat Vectors check box
    - Within the Cyber Node Window, select the cyber node type from the drop down box

Upon completion of all study items associated with a particular Cyber node, the *Complete* check box can be checked. The box to the far right of the node will turn orange and show a green bold check mark.

To navigate between cyber nodes you can use the navigation tree in the left hand side bar, click the Cyber Node drop down box and select the desired Cyber Node within a Cyber Zone, or click on the up or down icons until the applicable Cyber Node is selected for the selected Cyber Zone.

To modify a Cyber Node:

- Highlight the Cyber Node
- Click the icon
- Edit the Cyber Node Properties, i.e. *Name*, *Node Intention*, and *Comments* (optional)

To delete a Cyber Node:

- Highlight the Cyber Node
- Click on the red minus (-) symbol in the Cyber Node row
- Click *Yes* to confirm you want to delete the Cyber Node
- This will remove that Cyber Node, its Cyber Node Properties, and all associated data

You can link references from the reference library (see section *7.4* for more information on the Reference Library) to a Cyber Node by clicking on the link Icon and selecting a reference from the list of available references. Once a reference is linked, you can click on the red minus (-) symbol to remove the link.

Threat Vectors

A Threat Vector is a way in which the process conditions may depart from its design/process intent. It is created by evaluating the susceptibility of the specific Cyber Node.

If you selected the Smart Threat Vectors check box when defining the Cyber Node the threat vectors associated with the specific Cyber Node Type will be automatically defined for the Cyber Node. The following steps can be used if you did not use Smart Threat Vectors or want to add or modify the Smart Threat Vectors. You will also be able to delete a smart threat vector if it is not applicable to the Cyber Node, however to document that you considered the specific threat vector it is better to leave it in the project and mark it as not applicable.

To add a Threat Vector:

- Select the Cyber Node where the threat vector will be added
- Click on the green plus (+) symbol in the Threat Vector row
- Edit the Threat Vector Properties, i.e. *Name* and *Design Intent*

Upon completion of all study items associated with a particular threat vector, the *Complete* check box can be checked. The box to the far right of the threat Vector will turn orange and show a green bold check mark.

If for a threat vectors no threats or consequences of no significance are found, then the “No Issues” check box can be checked. This will document “No Issues Found ” on the worksheet.

To navigate between threat vectors you can use the navigation tree in the left hand side bar, click the Threat Vector drop down box and select the desired Threat Vector within a Cyber Node, or click on the up or down icons until the applicable Threat Vector is selected for the selected Cyber Node.

To modify a Threat Vector:

- Highlight the Threat Vector
- Click the icon
- Edit the Threat Vector Properties, i.e. *Name* and *Design Intent*

To delete a Threat Vector:

- Highlight the Threat Vector
- Click on the red minus (-) symbol in the Threat Vector row
- Click *Yes* to confirm you want to delete the Threat Vector
- This will remove that Threat Vector, its Threat Vector Properties, and all associated data

K.1.3 CyberPHA Worksheet

The CyberPHAx™ tool worksheet uses columns for the selected Threat Vector in a spreadsheet type interface. This allows the Threat data to be viewed quickly so one Threat-Consequence pair can be compared to another Threat-Consequence pair within the same Threat Vector. Within the worksheet columns buttons exist for adding Threats, Consequences, Countermeasures, and Recommendations. For Threats and Consequences content can be edited directly from within the worksheet. Content for the Countermeasures and Recommendations can also be directly edited from within the worksheet, however as they are part of the Project Libraries (see *Chapter 7 Project Libraries*) additional functionality is available. Within the worksheet you will be able to add a new Countermeasure or Recommendation. When you begin typing a new name for a Countermeasure or Recommendation the auto-complete feature will display a list of Countermeasures or Recommendations which match the entered text. You can double click on an item in the list to create a link between the relevant Countermeasure or Recommendation and the current Threat-Consequence pair.

Threats

CyberPHAx™ threats are comprised of four related data fields, i.e. ID, Description, Threat Category, and Threat Likelihood. The Threat ID is automatically generated and assigned to ensure relational data integrity. If more than one Likelihood Category was defined in the Risk Matrix, a drop down list will allow you to select the applicable Threat Category. The Threat Likelihood is intended to be the likelihood with NO Countermeasures or the scenario where all countermeasures have failed. When combining the Threat Likelihood with the Consequence Severity a Risk Without Countermeasures is obtained from the Risk Matrix. The Threat Likelihood is selected from a drop down list of likelihoods configured within the Risk Matrix. The list that appears is based on the associated Threat Category.

To add a Threat :

- Click on the ***Add Threat*** button at the bottom of the CyberPHA worksheet
- Edit the Threat Properties, i.e. *Description*, *Threat Category*, and *Threat Likelihood*
- Once a Threat Description has been entered you can click the ***Enter*** key on your keyboard to add a new Threat

To delete a Threat :

- Highlight the Threat ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Threat is really to be deleted

CAUTION: Deleting a Threat will delete all consequences, countermeasures, and recommendations that are related to it.

Consequence

CyberPHAx™ consequences are comprised of five related data fields, i.e. ID, Description, Consequence Category, Severity, and Risk. The Consequence ID is automatically generated and assigned to ensure relational data integrity. If more than one Consequence Category was defined in the Risk Matrix, a drop down list will allow you to select the applicable Category. The Consequence Severity is selected from a drop down list that is based on the Consequence Category selected. The Risk, representing the risk without countermeasures, is automatically determined based on the Risk Matrix given the Threat Likelihood and Consequence Severity selected.

To add a Consequence:

- Click on the ***Add Consequence*** button that is in line with the Threat that you want to add the Consequence to
- Edit the Consequence Properties, i.e. *Description*, *Consequence Category*, *Severity*, and *Risk*
- Once a Consequence Description has been entered you can click the ***Enter*** key on your keyboard to add a new Consequence

To delete a Consequence:

- Highlight the Consequence ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Consequence is really to be deleted

CAUTION: Deleting a Consequence will delete all countermeasures and recommendations that are related to it.

Countermeasures

CyberPHAx™ countermeasures are comprised of four related data fields, i.e. ID, Description, Countermeasure Tag, and Countermeasure Category. The Countermeasure ID is automatically generated and assigned to ensure relational data integrity. The Countermeasure Tag can be used to uniquely identify a specific Countermeasure within a process plant. The Countermeasure Tag also enables links to the Countermeasures from other applications. The Countermeasure Category is selected from a drop down list. Categorizing Countermeasures allows for enhanced Countermeasure reporting. Furthermore Countermeasure Category specific process safety information can be specified by clicking on the Countermeasure Icon. In addition to the four data fields identified above, Custom Data/process safety information data fields can be configured in the Custom Data section within the Project Configuration (see section *6.7*).

To add a New Countermeasure:

- Click on the ***Add Countermeasure*** button that is in line with the Consequence that you want to add the Countermeasure to
- Edit the Countermeasure Properties, i.e. *Description*, *Countermeasure Tag*, and *Countermeasure Category*
- Once a Countermeasure Description has been entered you can click the ***Enter*** key on your keyboard to add a new Countermeasure

To add a Countermeasure directly from the Countermeasure Library:

- Click on the Link Countermeasure Icon
- Highlight the Countermeasure to add
- Click on ***Add***

To delete a Countermeasure :

- Highlight the Countermeasure ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Countermeasure is really to be deleted

Note: When a Countermeasure is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Countermeasure from the Library. Click **Yes** or **No** as applicable.

To edit the Custom Data/process safety information for a Countermeasure, click on the CD icon. The applicable Custom Data entry form will appear.

Likelihood with Countermeasures

The Likelihood with Countermeasures is intended to reflect the Threat Likelihood assuming ALL Countermeasures are successful. The Likelihood is selected from a drop down list of likelihoods configured within the Risk Configuration. The list that appears is based on the associated Threat Category.

Risk with Countermeasures

The Risk with Countermeasures is automatically determined based on the Risk Matrix given the Likelihood with Countermeasures and Consequence Severity selected.

Recommendations

CyberPHAx™ recommendations are comprised of six related data fields, i.e. ID, Description, Category, Assigned to, Due Date, and Status. The Recommendation ID is automatically generated and assigned to ensure relational data integrity. The Recommendation Category is selected from a drop down list. Categorizing Recommendation allows for easy recommendation sorting and reporting. The Assigned to is selected from a drop down list. The list is populated with Member names that can be configured from the Dashboard (see section *A.4*). The Due Data is selected from the pop-up calendar. The Status is selected from a drop down list where *Open* is the default value.

To add a New Recommendation:

- Click on the ***Add Recommendation*** button that is in line with the Consequence that you want to add the Recommendation to
- Edit the Recommendation Properties, i.e. *Description*, *Category*, *Assigned to*, *Due Date*, and *Status*
- Once a Recommendation Description has been entered you can click the ***Enter*** key on your keyboard to add a new Recommendation

To add a Recommendation directly from the Recommendation Library:

- Click on the Link Recommendation Icon
- Highlight the Recommendation to add
- Click on ***Add***

To delete a Recommendation:

- Highlight the Recommendation ID
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Recommendation is really to be deleted

CyberSL

The CyberSL column allows the CyberPHA team to record if a detailed Cyber Security Level Verification is required for a specific Threat-Consequence pair scenario. The drop down list allows a *Yes*, *No*, or *N/A* (default) selection. When a Threat-Consequence pair scenario is to be further evaluated it can be assigned to a Cyber Event Scenario. To add, edit, or remove a Cyber Event Scenario click on the Cyber Event Scenario icon .

Note: The Threat-Consequence pair will only be available for further evaluation in the CyberSL™ worksheet if the CyberSL drop down box selection is ***Yes***, even when the Threat-Consequence pair is assigned to a Cyber Event Scenario.

To create a new Cyber Event Scenario for a Threat-Consequence pair:

- Click on the green **+** symbol
- Edit the Cyber Event Scenario Properties, i.e. *Name* (the Cyber Event Scenario ID is automatically generated and assigned to ensure relational data integrity)
- Once a Consequence Description has been entered you can click the ***Enter*** key on your keyboard to add a new Consequence

To add a Cyber Event Scenario to a Threat-Consequence pair:

- Highlight the applicable Cyber Event Scenario
- Click on the ***Left*** arrow

To remove a Cyber Event Scenario from a Threat-Consequence pair:

- Highlight the assigned Cyber Event Scenario
- Click on the ***Right*** arrow

Comments

Comments can be edited directly in the Comments text box. A Comment is associated with a single Threat. To delete a comment, highlight the text and click on the ***Delete*** key on your keyboard.

K.1.4 CyberPHAx Reports

In order to generate a CyberPHAx report select the *Cyber PHA Report* option from the Report Wizard. There are no additional Report Options for the CyberPHAx report.

K.2 CyberSL™

The Cyber SL tool SL Verification analysis worksheet uses a spreadsheet type interface for the evaluation of each Cyber Event Scenario. This provides a clear overview of the applicable cyber threats and countermeasures for the respective Severity Categories. Within the worksheet interface buttons exist for adding Threats (T), Countermeasures (CMR), Target Attractiveness (TA), Kill Chain Relevance (KCR), and Conditional Modifiers (CM) to the Cyber SL Worksheet for a specific Cyber Event Scenario. Applicability of a CMR, TA, KCR, and/or CM can be edited directly in the worksheet. As the Cyber Threats, Cyber Countermeasures, Cyber Event Scenarios, Target Attractiveness, Kill Chain Relevance and Conditional Modifiers are part of the Project Libraries (see *Chapter 7 Project Libraries*) they can be linked to existing items. The Cyber SL worksheet consists of three main areas: the toolbar, the Cyber Event Scenario list, and the workspace.

An example of the LOPAx™ tool layer of protection analysis worksheet is shown in the figure below.

K.2.1 Creating Cyber Event Scenarios

Cyber SL Cyber Event Scenarios are comprised of two related data fields, i.e. ID and Name. The Cyber Event Scenario ID is automatically generated and assigned to ensure relational data integrity. Cyber Event Scenarios can be defined manually within the tool or obtained from the work previously done using the Cyber PHAx tool.

To add a Cyber Event Scenario:

- Click on the ***Add Cyber Event Scenario*** button in the upper left hand corner of the toolbar
- This will immediately add the Cyber Event Scenario to the Cyber Event Scenario list

To edit the Cyber Event Scenario Name:

- Right click on the Cyber Event Scenario in the Cyber Event Scenario list and select edit, or
- Double click the Cyber Event Scenario name in the upper left hand corner of the worksheet

To delete a Cyber Event Scenario:

- Select the Cyber Event Scenario in the Cyber Event Scenario list
- Click on the ***Delete*** key on your keyboard
- Click on ***Yes*** when asked if the Cyber Event Scenario is really to be deleted

CAUTION: Deleting a Cyber Event Scenario will delete all instances where the Cyber Event Scenario was used. This will include any linking done in the Cyber PHAx tool.

K.2.2 Specifying Target Likelihood

Cyber SL uses Target Likelihood to help determine if the likelihood of a cyber event is tolerable. In case the Likelihood of Success is higher than the Target Likelihood a Remaining Cyber Risk will be determined that must be implemented to bring the likelihood to a tolerable level. For Cyber Event Scenarios that are manually defined within the Cyber SL worksheet, Cyber SL will define a target likelihood of 1.00E-5 events per year. You can update these target likelihood by directly editing in the Cyber SL worksheet toolbar. The target likelihood should be defined on a per year basis. Note that the target likelihoods do not need the same for all Severity Categories.

When transferring data from Cyber PHA to Syber SL, the target likelihood will be automatically defined based on the severity level selections related to the Cyber Event Scenario. The target likelihoods that are used in this case were defined earlier in the Cyber Risk Configuration.

K.2.3 Cyber Threats (T)

A cyber threat represents the start of a cyber event scenario sequence. Some threats will already be defined from the Cyber PHA, and are stored in the library.

To add a new Threat:

- Click on the ***Add T*** button at the upper left hand corner of the toolbar
- This will immediately add the Threat to the Cyber SL Worksheet
- This will also add the Threat to the Cyber Threats library

To edit the Threat Name:

- Double click the threat name in the worksheet, or
- Right click on the threat in the worksheet and select edit

To add a Threat directly from the Cyber Threats Library:

- Click on the Link Threat Icon
- Highlight the Threat(s) to add
- Click on ***Link Selected***

To delete a Threat:

- Highlight the Threat
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Threat Event is really to be deleted

Note: When a Threat is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Threat from the Library. Click **Yes** or **No** as applicable.

When you add a threat a default threat likelihood of attack of 1 per year is associated with the threat. This value can of course be update as needed, directly in the workspace.

To directly edit the likelihood within the workspace:

- Highlight the Threat Likelihood value
- Type in the applicable value (likelihood must be per year)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon

Note: When a Threat is used in multiple locations, changing its properties (including the Threat Likelihood) will impact all locations where that initiating event is used.

K.2.4 Target Attractiveness

The Target Attractiveness is a factor applied to the SL Verification calculation that accounts for the attractiveness of the target of a cyber event. This will add a factor of 1 through 5, indicating that an attack would be more for some plant or organization types than for others.

To add a new Target Attractiveness:

- Click on the ***Add TA*** button at the upper left hand corner of the toolbar
- This will immediately add the Target Attractiveness to the Cyber SL Worksheet
- This will also add the Target Attractiveness to the Target Attractiveness library

To edit the Target Attractiveness Name:

- Double click the Target Attractiveness name in the worksheet, or
- Click on the Edit icon when hovering over the Target Attractiveness, or
- Right click on the Target Attractiveness in the worksheet and select edit

To add a Target Attractiveness directly from the Target Attractiveness Library:

- Click on the Link Target Attractiveness Icon
- Highlight theTarget Attractiveness(s) to add
- Click on ***Link Selected***

To delete a Target Attractiveness:

- Highlight the Target Attractiveness
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Target Attractiveness is really to be deleted

Note: When an Target Attractiveness is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Target Attractiveness from the Library. Click **Yes** or **No** as applicable.

When you add a Target Attractiveness, a default factor of 1 is associated with the Target Attractiveness. In addition the Target Attractiveness is set to be Not Applicable (NA) to all Cyber Threats in the Cyber SL Worksheet. Applicability and probability of the situation occurring can be update as needed. To change the applicability of an Target Attractiveness to a specific threat, simply double click the intersection of Target Attractiveness and Cyber Threat. The NA will then change to the factor associated with theTarget Attractiveness.

To manually edit the Target Attractiveness factor:

- Click on the Edit icon when hovering over the Target Attractiveness or right click on the Target Attractiveness in the worksheet and select edit
- Type in the applicable value (probability must range from 1 to 5)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon

K.2.5 Countermeasures

A Countermeasure (SMR) is a device, system, or action that is capable of preventing a cyber event scenario from proceeding to its undesired consequence independent of the threat or the action of any other countermeasure associated with the scenario.

To add a new Countermeasure:

- Click on the ***Add CMR*** button at the upper left hand corner of the toolbar
- This will immediately add theCountermeasure to the Worksheet
- This will also add the Countermeasure to the Cyber Countermeasures library

To edit the Countermeasure Name:

- Double click the Countermeasure name in the worksheet, or
- Click on the Edit icon when hovering over the Countermeasure, or
- Right click on the Countermeasure in the worksheet and select edit

To add an Countermeasure directly from the Cyber Countermeasure Library:

- Click on the Link Countermeasure Icon
- Highlight the Countermeasure(s) to add
- Click on ***Link Selected***

To delete an Countermeasure:

- Highlight the Countermeasure
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Countermeasure is really to be deleted

Note: When a Countermeasure is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Countermeasure from the Library. Click **Yes** or **No** as applicable.

When you add an Countermeasure a default probability of failure of 1 is associated with the Countermeasure. In addition the Countermeasure is set to be Not Applicable (NA) to all Cyber Theats in the Worksheet. Applicability and probability of failure can be update as needed. To change the applicability of a Countermeasure to a specific cyber threat, simply double click the intersection of Countermeasure and Cyber Threat. The NA will then change to the probability associated with the Countermeasure.

To manually edit the Countermeasure:

- Click on the Edit icon when hovering over theCountermeasure or right click on theCountermeasure in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon

K.2.6 Conditional Modifiers (CM)

To add a new Conditional Modifier:

- Click on the ***Add CM*** button at the upper left hand corner of the toolbar
- This will immediately add the Conditional Modifier to the Worksheet
- This will also add the Conditional Modifier to the Conditional Modifiers library

To edit the Conditional Modifier Name:

- Double click the Conditional Modifier name in the worksheet, or
- Click on the Edit icon when hovering over the Conditional Modifier, or
- Right click on the Conditional Modifier in the worksheet and select edit

To add a Conditional Modifier directly from the Conditional Modifier Library:

- Click on the Link Conditional Modifier Icon
- Highlight the Conditional Modifier(s) to add
- Click on ***Link Selected***

To delete a Conditional Modifier:

- Highlight the Conditional Modifier
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Conditional Modifier is really to be deleted

Note: When a Conditional Modifier is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Conditional Modifier from the Library. Click **Yes** or **No** as applicable.

When you add a Conditional Modifier a default probability of 1 is associated with the Conditional Modifier. In addition the Conditional Modifier is set to be Not Applicable (NA) to all Cyber Threats in the Cyber SL Worksheet. Applicability and probability can be update as needed. To change the applicability of an conditional modifier to a specific Cyber Threat, simply double click the intersection of conditional modifier and Cyber Threat. The NA will then change to the probability associated with the conditional modifier.

To manually edit the probability:

- Click on the Edit icon when hovering over the Conditional Modifier or right click on the Conditional Modifier in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon

K.2.7 Kill Chain Relevance

The Kill Chain Relevance is a factor applied to the SL Verification calculation that accounts for the required steps that a threat agent must complete before initiating a given Cyber Threat. This approach is developed from the Lockheed Martin Cybersecurity Kill Chain® and accounts for the fact that prior steps such as detailed system reconnaissance or the compromise of other devices within the IACS are necessary for certain engineered attacks. This will add a factor of 1 or less, indicating that an engineered attack requiring previous successful attacks may be to some extent less likely than an attack that does not require any previous actions.

To add a new Kill Chain Relevance:

- Click on the ***Add KCR*** button at the upper left hand corner of the tool bar
- This will immediately add the Kill Chain Relevance to the Cyber SL Worksheet
- This will also add the Kill Chain Relevance to the Kill Chain Relevance library

To edit the Kill Chain Relevance Name:

- Double click theKill Chain Relevance name in the worksheet, or
- Click on the Edit icon when hovering over the Kill Chain Relevance, or
- Right click on the Kill Chain Relevance in the worksheet and select edit

To add a Kill Chain Relevance directly from the Kill Chain Relevance Library:

- Click on the Link Kill Chain Relevance Icon
- Highlight the Kill Chain Relevance(s) to add
- Click on ***Link Selected***

To delete a Kill Chain Relevance:

- Highlight the Kill Chain Relevance
- Click on the ***Delete*** key on your keyboard (or right click and select Delete)
- Click on ***Yes*** when asked if the Kill Chain Relevance is really to be deleted

Note: When a Kill Chain Relevance is deleted and it is the last place where it is used, you will be asked if you want to permanently delete the Kill Chain Relevance from the Library. Click **Yes** or **No** as applicable.

When you add a Kill Chain Relevance, a default factor of 1 is associated with the Kill Chain Relevance. In addition the Kill Chain Relevance is set to be Not Applicable (NA) to all Cyber Threats in the Cyber SL Worksheet. Applicability and probability of the situation occurring can be update as needed. To change the applicability of an Kill Chain Relevance to a specific threat, simply double click the intersection of Kill Chain Relevance and Cyber Threat. The NA will then change to the factor associated with the Kill Chain Relevance.

To manually edit the Kill Chain Relevance factor:

- Click on the Edit icon when hovering over the Kill Chain Relevance or right click on the Kill Chain Relevance in the worksheet and select edit
- Type in the applicable value (probability must range from 0 to 1)
- Manually add the applicable assumptions, comments, and reference by clicking on the notes icon

K.2.8 Calculating Remaining Cyber Risk

The Cyber SL Worksheet determines a Mitigated Likelihood for each Cyber Threat in a Cyber Event Scenario. This Mitigated Likelihood is calculated by multiplying the Cyber Threat Likelihood with the probabilities and factors associated with the applicable Countermeasures, Conditional Modifiers, Kill Chain Relevance, and Target Attractiveness. The calculated Mitigated Likelihood is displayed on the right hand side of the worksheet for each Cyber Event.

The Likelihood of Success is calculated by adding the Mitigated Likelihood for each Cyber Threat across the Cyber Event Scenario. This Cyber Event Scenario Likelihood of Success is displayed in the menu bar of the worksheet for each severity Category.

Cyber Event Scenario Remaining Cyber Risk

Given the Target Likelihood specified and the Likelihood of Success calculated, a Remaining Cyber Risk (RCR) is calculated for the Cyber Event Scenario. If theLikelihood of Success is less than or equal to the Target Likelihood, the Remaining Cyber Risk will state a NA for not applicable, indicating no further risk reduction is required.

K.2.9 Comments

Comments can be edited directly in the Comments text box. A Comment is associated with a single Cyber Threat. To delete a comment, highlight the text and click on the ***Delete*** key on your keyboard. Note that Cyber SL Comments are independent of the Cyber PHA Comments.

Disclaimer and Assumptions

Limitations and assumptions associated with the use of exSILentia® v4 are documented in the following sections.

Disclaimer

The user of the exSILentia® v4 software is responsible for verification of all results obtained and their applicability to any particular situation. Calculations are performed per guidelines in applicable international standards. *exida.com L.L.C.* accepts no responsibility for the correctness of the regulations or standards on which the software tool is based.

In particular, *exida.com L.L.C.* accepts no liability for decisions based on the results of the exSILentia® v4 software. The *exida.com L.L.C.* guarantee is restricted to the correction of errors or deficiencies within a reasonable period when such errors or deficiencies are brought to exida's attention in writing. *exida.com L.L.C.* accepts no responsibility for modifications made by the user to the automatically generated reports.

Assumptions exida LOPA Database

exida has compiled a proprietary initiating event frequency and protection layer probability of failure database. This database is a compilation of failure data collected from a variety of public and confidential sources and presents an industry average. The database is available in the LOPAx™ module of exSILentia® v4.

The user is responsible for determining the applicability of the initiating event frequencies and protection layer probabilities of failure to any particular application. Accurate plant specific data (historic data) is preferable to general industry average data. Industrial plant sites with high levels of stress must use initiating event and protection layer data that is adjusted to a higher value to account for the specific conditions of the plant.

Assumptions exida SERH Database

exida has compiled a proprietary equipment failure database. This database is a compilation of failure data collected from detailed predictive analysis performed through Failure Modes, Effects, and Diagnostics Analysis (FMEDA) for specific manufacturer specific products and a variety of public and confidential sources. The failure rate data presents an average worst-case estimate of failure rates to be expected during normal operation of a particular equipment item. The database is published as the "Safety Equipment Reliability Handbook, fourth edition" ISBN 978-1-934977-15-6. The reliability data collection process is described in the SERH book.

The user is responsible for determining the applicability of the failure data to any particular environment. The stress levels assumed to determine the equipment failure rate are average worst-case for an industrial environment and are documented in the SERH book. Accurate plant specific data is preferable to general industry average data. Industrial plant sites with high levels of stress must use failure rate data that is adjusted to a higher value to account for the specific conditions of the plant.

Assumptions LOPA

The following assumptions apply to the LOPA Worksheet calculations.

- The severity level translation into tolerable frequencies is based on the user specified risk configuration
- Unmitigated event frequencies are directly calculated from initiating event frequencies and probabilities for enabling conditions, independent protection layers, and conditional modifiers using algebraic formulas.
- LOPA calculations assume that there is no correlation between an initiating event and the associated enabling condition(s), independent protection layer(s), and/or conditional modifier(s).
- The required Risk Reduction Factor is obtained directly from the relation between tolerable frequency and unmitigated frequency.

Assumptions SILect

The following assumptions apply to the SILect Worksheet calculations.

- The Target Safety Integrity Level is obtained from the relation between required Risk Reduction Factor and Safety Integrity Level boundaries.
- The SIL boundaries are adjusted based on the Target SIL Threshold Ratio specified

Assumptions SILver - Reliability Modeling

The SILver Worksheet calculations are based on many of the assumptions that are identified in IEC 61508-6, Annex B. Specific assumptions on which the calculations within SILver Worksheet are based are listed below.

- The sensor part ranges from the actual sensing element up to and including the logic solver input channel or the logic solver input module depending on logic solver I/O channel configuration by the user
- The logic solver part ranges from the logic solver input module to the logic solver output module or includes just the CPU based on the logic solver I/O channel configuration by the user.
- The final element part ranges from the logic solver output channel or the logic solver output module depending on the I/O channel logic solver configuration by the user up to and including the final actuating element within the safety instrumented function
- Equipment item failure rates are constant over the useful life of the equipment item
- Only a single failure can occur within one independent part of a configuration
- The embedded diagnostic test time is much shorter than the average repair time
- The proof test interval is at least two orders of magnitude greater than the embedded diagnostic test interval
- Limited coverage of failures during a proof test is modeled using the proof test coverage factor, it is assumed that the proof test coverage has effect on all states, undetected and detected
- For each sensor, logic solver, and final element group there is a single proof test interval and Mean Time To Repair
- Multiple repair teams are available to work on all known failures
- Repair rates are constant
- The Mean Time To Repair (MTTR) is an order of magnitude less than the expected demand rate
- Common cause failures are assumed to be the same in redundant units

Assumptions SILver - Proof Test Coverage Calculator

The SILver Worksheet Proof Test Coverage Calculator determines a suggested Proof Test Coverage factor based on a manufacturer identified proof test and the effectiveness of that proof test. If you use the suggested proof test coverage, you must ensure that the actual test(s) performed is (are) at least as effective as the manufacturer suggested test(s).

Software License Agreement – exida exSILentia®

IMPORTANT – READ CAREFULLY: This Software License Agreement is the legal agreement ("Agreement") between you, the customer who has acquired the software ("You") and exida.com LLC ("exida") with offices at 80 North Main Street, Sellersville, PA, 18960, USA. Please read this agreement carefully before completing the installation process and using the exida exSILentia® tool (together with its accompanying documentation, the "Software"). This agreement provides a license to use the Software and contains warranty information and liability disclaimers.

BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT INSTALL OR USE THE PRODUCT.

IF YOU DID NOT ACQUIRE THE SOFTWARE FROM exida, THEN YOU MAY NOT ENTER INTO THIS AGREEMENT OR USE THE SOFTWARE. NO OTHER PARTY HAS THE RIGHT TO TRANSFER A COPY OF THE SOFTWARE TO YOU.

The Software is owned by exida and is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. **THE SOFTWARE IS LICENSED, NOT SOLD.**

If you have any questions or concerns about this agreement, please contact exida at the above listed address.

1. **DEFINITIONS**
   a. "Affiliates" means any company or entity controlled by, controlling, or under common control with You or exida. For the purposes of this definition, "control" shall mean the power to cause the direction of the management of such company or entity, directly or indirectly, whether through ownership of voting securities or otherwise, it being understood that ownership of 50% or more of the voting securities of another shall in all circumstances constitute control.
   b. "exida" means exida.com LLC and its Affiliates
   c. "You", "Your" means you, your company, and your company's Affiliates
   d. "Documentation" means the user manuals and any other materials in any form or medium customarily provided by exida to You which will provide sufficient information to operate, diagnose, and maintain the Software properly, safely and efficiently
   e. "Software" means the product provided to You, which includes the exSILentia® tool and the associated media, printed materials, and "online" or electronic documentation. The Software includes any updates or new versions that may be provided to You.
   f. "Maintenance" is defined in the Maintenance and Support Article, section 4 of this agreement
   g. "Proprietary Information" means all of Your and your affiliates plans, processes, products, business information, data, technology, Information Resources, computer programs and documentation and the like. It includes any information or material that (a) is marked "Confidential", "Restricted", or "Proprietary Information" or other similar marking, (b) is known by the parties to be considered confidential and proprietary, or (c) should be known or understood to be confidential or proprietary by an individual exercising reasonable commercial judgment.
2. **OWNERSHIP.** The Software is owned and copyrighted by exida. The license granted to You confers no title or ownership in the Software and is not a sale of any rights in the Software. exida

warrants that it has full power and authority to grant the licenses and rights granted under this License Agreement without the consent or approval of any third party.

a. All information, artwork, graphics, text, copy, data, software, and other material included in the Software are exida's exclusive intellectual property.

3. **LICENSE**
    1. **GRANT OF LICENSE.** exida grants You the following rights provided You comply with all terms and conditions of this agreement. For each license You have acquired for the Software:
        a. You are granted a non-exclusive, non-transferable, license during the term of this Agreement to install and use for your business purposes the Software on an unlimited number of Your workstations. If the Software is a software suite or bundle with more than one specified Software product, this license applies to all such specified Software products.
        b. You are granted a non-exclusive, non-transferable, right to apply quarterly updates to the Safety Equipment Reliability Handbook database for the duration of 1 year
        c. The USB license key(s) restricts use to a specified number of concurrent users only
        d. You may make one copy of the Software for backup, disaster recovery, or archival purposes
    2. **DOCUMENTATION.** You are hereby granted the right to reproduce the user manuals and other written materials created by exida to describe the functionality and use of the Software (the "Documentation") and to distribute a single copy of the Documentation in soft form or in print to each user over Your internal network.
    3. **LICENSE RESTRICTIONS.** You shall not grant access to the Software to any persons or entities other than those of Your employees and on-site contractors who are located at Your facilities nor shall You sell, lease or distribute the Software to any person or entity as a standalone or bundled product or make any other commercial use thereof. You shall not modify, reverse engineer, decompile, or disassemble the Software. You shall not adapt, translate, or create derivative works based on the Software or the Documentation without the prior written approval of exida. You shall not exceed the scope of the license granted in Sections 3.1 and 3.2 above. You shall not export the Software or Documentation, or any copies thereof, to any user in violation of applicable laws and regulations.
    4. **COPYRIGHT.** exida owns the Software and related Documentation and their copyrights that are protected by United States copyright laws and international treaty provisions. This Agreement does not and shall not be construed as transferring ownership rights of the Software, Documentation, any modifications thereto or any related materials to You or to any third party. exida owns and shall retain all right, title and interest in the Software, including all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. You shall retain all copyright and trademark notices on the Software and Documentation and as otherwise necessary to protect exida intellectual property rights.
    5. **YOUR RESPONSIBILITY.** You expressly agree to be fully responsible for compliance by Your employees and on-site contractors with the applicable terms of this Agreement.
    6. **COPIES.** You are permitted to copy the Documentation and written materials for distribution to employees using the Licensed Software, and to make and retain a copy of the Software for archival purposes.

4. **MAINTENANCE AND SUPPORT.**
    1. **SUPPORT.**
        a. Limited Technical Support. During the term of this agreement You are entitled to limited technical support. exida will provide technical support via its support website http://support.exida.com. Safety Instrumented Function Consultancy is excluded from the exida support under this agreement.
        b. Upon payment of the Annual Maintenance Fee, You shall be entitled to 2 hours of technical support per year for each concurrent user license. Bug reporting and resolution is not counted towards your technical support allotment.
    2. **MAINTENANCE AND UPDATES.**
        a. Definitions. For the purposes of this section, the following shall apply:
            i. Bug Fix: The term "Bug Fix" means any engineering patch intended to fix bugs and errors in the Software.
            ii. Functionality Update: The term "Functionality Update" means any new release of the Software. Functionality Updates are issued provided that maintenance and support is in good standing, i.e. maintenance period is active and no lapses have occurred in the maintenance period. Updates do not include any exida software, which constitutes a separate product by virtue of different features or functionality. Updates do not include standalone products that can be integrated with the Software.
            iii. Equipment Database Update: The term "Equipment Database Update" means any new version of the Safety Equipment Reliability Handbook Database embedded in the Software. Equipment Database Updates are issued quarterly.
            iv. Maintenance: The term "Maintenance" means technical support, Functionality Updates, and Equipment Database Updates, provided during the Maintenance Period.
            v. Maintenance Period. The term "Maintenance Period" for the Software means any period commencing at the date of sale of the Software, or any anniversary thereof, for which You have paid the Maintenance Fee for each license of the Software you purchased.
        b. Delivery of Updates. For any period in which You have paid the Maintenance Fee (or the relevant pro-rated portion thereof in accordance with section 4.3), exida shall provide automatic download of functionality, and Equipment Database updates.
        c. License to Updates. exida hereby grants You a nonexclusive; nontransferable license during the term of this Agreement to use the Updates delivered under this section.
    3. **RENEWAL.** If exida continues to offer support and updates for the Software, You may renew Maintenance by delivering exida a purchase order referencing this Agreement on or before the expiration of the Paid Maintenance Period. If You elect to renew the Maintenance, You must do so for all copies of the Software licensed hereunder. As a courtesy, exida agrees to notify you via automated message 30 days prior to the expiration of the Maintenance Period to allow ample time for renewal. exida assumes no responsibility for lapses in the Maintenance Period that occurs as a result of You failing to renew the Maintenance Period before its expiration. If Maintenance is not renewed, maintenance fees must be paid for the time of the maintenance lapse, in order to obtain full Functionality and Equipment Database updates.

5. **RESTRICTED USE.**
    a. You agree to use reasonable efforts to prevent unauthorized copying of the Software
    b. You may not disable any licensing or control features of the Software or allow the Software to be used with such features disabled
    c. You may not share, rent, or lease Your right to use the Software
    d. You may not modify, sublicense, copy, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement
    e. You may not reverse engineer, decompile, translate, create derivative works, decipher, decrypt, disassemble, or otherwise convert the Software to a more human-readable form for any reason
    f. You may not use the Software for any purpose other than to perform safety lifecycle tasks in accordance with the accompanying documentation
    g. You may not remove, alter, or obscure any confidentiality or proprietary notices (including copyright and trademark notices) of exida on, in or displayed by the Software
    h. You will return or destroy all copies of the Software if and when Your right to use it ends
    i. You may not use the Software for any purpose that is unlawful
6. **PROPRIETARY INFORMATION.**
    1. **EXIDA SHALL**
        a. Not use or disclose Proprietary Information to any third party except as is clearly necessary to provide the Services, provided such party is bound by a written confidentiality agreement with terms no less stringent than the terms herein.
        b. Not attempt to access any portion of Information Resources without authorization of You. If unauthorized access is nevertheless obtained, whether inadvertently or otherwise, exida shall have a duty to promptly report to You, in writing, each instance thereof, setting out the extent and circumstances of such access.
        c. Not attempt to defeat any security provisions maintained by You for the protection of Information Resources or information contained therein.
        d. Not remove, copy, alter, or install any software or information or data on any of Your computers unless specifically authorized by You in connection with the Services or make any attempt to learn or document passwords or other information which could facilitate unauthorized access to Information Resources.
        e. Require each of its employees, contractors and agents needing access to Information Resources to obtain passwords from Your authority responsible for the security of Information Resources, to use and protect passwords as required by You, and to follow such protocols governing access as may be set out by You.
    2. **CONFIDENTIALITY.** Neither party shall, during the term of this Agreement or thereafter, disclose, make commercial or other use of, give or sell to any person, firm, or corporation, any information of the other party that is treated and identified in writing as confidential, except either party may disclose such information if (i) required to do so pursuant to applicable law; (ii) it was rightfully in their possession from a source other than the other party prior to the time of disclosure of said information; (iii) it was in the public domain prior to the time of receipt; (iv) it became part of the public domain after the time of receipt by any means other than an unauthorized act or omission by such party; (v) it is supplied after the time of receipt without restriction by a third party who is under no obligation to maintain such information in confidence; or (vi) it was independently developed prior to the time of receipt. Both parties will use at least the same standard of care as they do to protect their own Proprietary Information to ensure that their employees, agents or consultants do not disclose or make any unauthorized use of such

Proprietary Information. Both parties will promptly notify the other party upon discovery of any unauthorized use or disclosure of the Proprietary Information.

3. **TERMINATION OF exida's RIGHT TO POSSESS PROPRIETARY INFORMATION.** Upon final acceptance or earlier termination of this Agreement for any reason, exida's rights to possession and use of any of the Proprietary Information in connection with the performance of its obligations hereunder or otherwise shall terminate and exida shall immediately deliver to You all of the Proprietary Information and all copies of any portion thereof. exida shall, upon completion of such delivery, certify in writing to You that it has fulfilled its obligations under this Article. exida will keep one copy of all Proprietary Information provided for future reference and legal liability requirements.

7. **DISCLAIMER OF WARRANTY.** The Software is provided on an "AS IS" basis, without warranty of any kind, including, without limitation, the warranties of merchantability, fitness for a particular purpose, non-infringement title, and results. The entire risk as to the quality and performance of the Software is borne by You. If the Software is intended to link to, extract content from or otherwise integrate with a third party product, exida makes no representation or warranty that Your particular use of the Software is or will continue to be authorized by law in Your jurisdiction or that the third party product will continue to be available to You. This disclaimer of warranty constitutes an essential part of the agreement.
    1. **WARRANTY.** exida warrants that the Software does not infringe the intellectual property rights of any third party.
8. **LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL exida BE LIABLE TO YOU OR ANY OTHER PERSON OR SHALL YOU BE LIABLE TO exida OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR WORK STOPPAGE, COMPUTER FAILURE OR LOSS OF REVENUES, PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE OR ECONOMIC LOSSES. IN NO EVENT WILL exida BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT PAID TO LICENSE THE SOFTWARE, EVEN IF YOU OR ANY OTHER PARTY SHALL HAVE INFORMED exida OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM. NO CLAIM, REGARDLESS OF FORM, MAY BE MADE OR ACTION BROUGHT BY YOU MORE THAN ONE YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO THE PARTY ASSERTING IT.**
9. **TERM AND TERMINATION.**
    1. **TERM.** This Agreement shall continue for an indefinite period of time so long as the License Fee is paid and use of the license as documented in this contract is not violated. Maintenance and Support is defined in section 4 of this Agreement. You may choose to renew the Maintenance Agreement upon expiration.
    2. **TERMINATION.** exida may terminate Your license if You do not abide by the license terms. Upon termination of license, You shall immediately discontinue the use of the Software and shall within ten (10) days return to exida the USB License Key(s) and all copies of the Software or confirm that You have destroyed all copies of it. Your obligations to pay accrued charges and fees, if any, shall survive any termination of this Agreement. You agree to indemnify exida for reasonable attorney fees in enforcing its rights pursuant to this license. Sections 2, 5, 7, 8, 9 and 15 will survive expiration or termination of this Agreement for any reason.
10. **exSILentia® USE.** You are required to perform any verification activities when using the software as described in the Documentation.

11. **REGISTRATION.** The software will only function if You are using a valid "License Key". The License Key will be provided by exida. Software registration is required.
12. **UPGRADES.** If this copy of the software is an upgrade from an earlier version of the software, it is provided to You on a license exchange basis. Your use of the Software upgrade is subject to the terms of this license, and You agree by Your installation and use of this copy of the Software to voluntarily terminate Your earlier license and that You will not continue to use the earlier version of the Software or transfer it to another person or entity.
13. **ADDITIONAL SOFTWARE.** This license applies to updates, upgrades, options and any other additions to the original Software provided by exida, unless exida provides other terms along with the additional software.
14. **THIRD PARTY PRODUCTS.**
    a. This Software may make use of 3rd party content. This 3rd party content will be used per the usage agreements and other restrictions set forth by the 3rd party. exida agrees to bear all responsibility for the proper implementation of embedded 3rd party content.
    b. This Software may have the ability to make use of, link to, or integrate with 3rd party content. The availability of the content is at the sole discretion of the 3rd party content providers and may be subject to usage agreements and other restrictions. You agree to indemnify and hold harmless exida from all claims, damages, and expenses of whatever nature that may be made against exida by 3rd party content providers as a result of Your use of the Software.
15. **GENERAL.**
    1. **SERVICES.** There are no services provided under this Agreement. Support, maintenance, and other services, if available, must be purchased separately from exida
    2. **APPLICABLE LAW.** This license shall be interpreted in accordance with the laws of the State of Pennsylvania, USA without giving effect to any choice of law principles that would require the application of the laws of a different state or country. Any disputes arising out of this license shall be adjudicated in a court of competent jurisdiction in Pennsylvania, USA. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act (USA) do not apply to this Agreement.
    3. **GOVERNING LANGUAGE.** Any translation of this License is done for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this License shall govern.
    4. **COMPLIANCE WITH LAWS.** You will comply with all applicable export and import control laws and regulations in your use or re-exportation of the Software and, in particular, you will not export or re-export the Software without all required United States Bureau of Export and Administration licenses. You will defend, indemnify, and hold harmless exida and its suppliers from and against any violation of such laws or regulations by You.
    5. **RELATIONSHIP BETWEEN THE PARTIES.** The parties are independent contractors and neither party is the agent, partner, employee, fiduciary, or joint venture of the other party under this Agreement. You may not act for, bind, or otherwise create or assume any obligation on behalf of exida. There are no third party beneficiaries under this Agreement.
    6. **EXPORT OF TECHNICAL DATA.** Neither party shall export, directly or indirectly, any technical data acquired from the other party or any of its affiliated companies, or any direct product of that technical data, to any other country for which the United States Government or any agency of that government at the time of export requires an export license or other governmental approval without first obtaining that license or approval, when required by applicable United States law.

7. **ASSIGNMENTS.** You may not assign or transfer, by operation of law or otherwise, your rights under this Agreement (including your licenses with respect to the Software) to any third party without exida's prior written consent. Any attempted assignment or transfer in violation of the foregoing will be void. exida may freely assign its rights or delegate its obligations under this Agreement.
8. **SEVERABILITY.** If any provision of this Agreement is held unenforceable by a court, such provision may be changed and interpreted by the court to accomplish the objectives of such provision to the greatest extent possible under applicable law and the remaining provisions will continue in full force and effect. Without limiting the generality of the foregoing, you agree that Section 8 will remain in effect notwithstanding the unenforceability of any other provision of this Agreement.
9. **TRADEMARKS AND TRADE NAMES.** Nothing in this Agreement shall confer on You any right to use any trademark or trade name belonging to exida.

16. **ENTIRE AGREEMENT.** This license constitutes the entire agreement between the parties relating to the Software and supersedes any proposal or prior agreement, oral or written, and any other communication relating to the subject matter of this license. Any conflict between the terms of this License Agreement and any Purchase Order, invoice, or representation shall be resolved in favor of the terms of this License Agreement. In the event that any clause or portion of any such clause is declared invalid for any reason, such finding shall not affect the enforceability of the remaining portions of this License and the unenforceable clause shall be severed from this license. Any amendment to this agreement must be in writing and signed by both parties.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto as of the date first below written.

exida.com LLC

By:	_____	By:	_____
(Print):	Iwan van Beurden	(Print):	_____
Title:	CTO / Director of Product Development	Title:	_____
Date:	_____	Date:	_____

exida exSILentia® Software License Agreement v1.7 (June 17, 2014)

Copyright © 2000-2017 exida.com LLC
80 North Main Street
Sellersville, PA 18960
USA

exSILentia®, SILect™, SILver™, PHAx™, and LOPAx™ are trademarks of exida.com LLC

Open Source Disclosure

Effective date: March 22, 2019

exida products include third-party code licensed to exida for use and redistribution under open-source licenses. Below is a list of disclosures and disclaimers in connection with exida's incorporation of certain open-source licensed software into its products. Notwithstanding any of the terms and conditions of your license agreement with exida, the terms of certain open-source licenses may be applicable to your use of exida's products, as set forth below.

This list of open-source code was compiled with reference to third-party software incorporated into the products as of the date the list was generated. This list may be updated from time to time and may not be complete.

ALL INFORMATION HERE IS PROVIDED "AS IS". exida AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THIS LIST OR ITS ACCURACY OR COMPLETENESS, OR WITH RESPECT TO ANY RESULTS TO BE OBTAINED FROM USE OR DISTRIBUTION OF THE LIST. BY USING OR DISTRIBUTING THIS LIST, YOU AGREE THAT IN NO EVENT SHALL EXIDA BE HELD LIABLE FOR ANY DAMAGES WHATSOEVER RESULTING FROM ANY USE OR DISTRIBUTION OF THIS LIST, INCLUDING, WITHOUT LIMITATION, ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR OTHER DIRECT OR INDIRECT DAMAGES.

Castle Core

Copyright © 2004-2018 Castle Project - http://www.castleproject.org/

You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html

CommandLineParser

Copyright © 2005 - 2018 Giacomo Stelluti Scala & Contributors

You may obtain a copy of the license at https://opensource.org/licenses/MIT

CoreCLR-NCalc

Copyright © Sebastian Klose

You may obtain a copy of the license at https://opensource.org/licenses/MIT

MathNet.Numerics

Copyright © 2002-2018 Math.NET Project

You may obtain a copy of the license at https://numerics.mathdotnet.com/License.html

Morelinq

Copyright © 2008 Jonathan Skeet.

Portions Copyright © 2009 Atif Aziz, Chris Ammerman, Konrad Rudolph.

Portions Copyright © 2010 Johannes Rudolph, Leopold Bushkin.

Portions Copyright © 2015 Felipe Sateler, "sholland".

Portions Copyright © 2016 Andreas Gullberg Larsen, Leandro F. Vieira (leandromoh).

Portions Copyright © 2017 Jonas Nyrup (jnyrup).

Portions Copyright © Microsoft. All rights reserved.

You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html

Prism.Core

Copyright © .NET Foundation

You may obtain a copy of the license at https://opensource.org/licenses/MIT

protobuf-net

Copyright © 2008 Marc Gravell

You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html

Serialize.Linq

Copyright © 2012-2018 Sascha Kiefer

Copyright © 2007 Free Software Foundation, Inc. - http://fsf.org/

You may obtain a copy of the license at https://www.gnu.org/licenses/gpl-3.0.en.html

Index

A

Action Items 112
Architectural Constraints 186

C

Cause 127
  Library 61
Column Visibility 136
Conditional Modifier 156
  Library 68
Consequence 128, 234
  Category 73
Continuous Editing 136
Countermeasures 235
Custom Data 50
Cyber Event Scenario 236
Cyber Node 232
Cyber Security Checklist 33
Cyber Zone 231

D

Data Export 85
  PHAx 146
Data Import 83
Data Transfer
  LOPA to SILect 169
  PHA to LOPA 161
  Safeguard to SRS 179
Database
  LOPA 87
  SERH 89
Deviation 38, 43, 125

E

Enabling Condition 152
Library 67

H

Hardware Fault Tolerance 186
Hazard Scenario 28, 132
Library 66
Hierarchy
Cyber Project 231
Project 123, 133

I

I/O Channel to Module Connection 188
IEC 61511 Checklist 34
Independent Protection Layers 153
Initiating Event 150
Instrumented Protection Function 167

L

Library 61
Causes 61, 150
Conditional Modifier 156, 241
Conditional Modifiers 68
Countermeasure 235
Enabling Condition 152
Enabling Conditions 67
Final Element Groups 196
Hazard Scenarios 66
Independent Protection Layer 154
Kill Chain Relevance 242
Logic Solver 202
Recommendations 63, 132, 236
References 65
Safeguards 62, 129
Sensor Groups 190

Likelihood 127, 234
Category 74
Likelihood Matrix 75
LOPA Database 87
exida 88
Generic 88
User Defined Data 88

M

Members 110
Mission Time 187

N

Navigation
Dashboard 27, 109
PHAx™ 133
Node 124
Types 38

P

Parking Lot Items 113
Plant Types 35
Prior-Use 187
Project
Configuration 35
Hierarchy 123
Information 33
Project Abbreviations 55
Project Definitions 56
Proof Test 217
Proof Test Coverage 30, 217
Proof Testing 192, 198
Proven-In-Use 187

R

Recommendation 131, 236
Category 46
Library 63
Reference
Library 65
Type 47
Report Generation 81
CyberPHAx 237
Lifecycle Cost Estimator 229
LOPAx 162
PHAx 137
SILect 169
SILver 210
SRS 179
Required Risk Reduction Factor 157
Risk Matrix 73, 76, 131, 236

S

Safeguard 129
Category 44
Labels 130
Library 62
Sessions 111
Severity Category Visibility 159
Severity Matrix 74
SIF Demand Mode 188
SIL Threshold 78
Site Safety Index 188
Smart Deviations 38, 124-125
Smart Threat Vectors 232-233
SRS
SIF General 176
SIF Specific 177
SIS General 173

Startup Time 187
Systematic Capability 187

T

Target Frequency 149
Target Safety Integrity Level 168
Team Roles 49
Threat 234
Threat Vector 233

U

Unit 123
Upgrading 93