exSILentia
Integrated Safety Lifecycle Tool

exida
Functional Safety, Security, & Reliability
www.exida.com

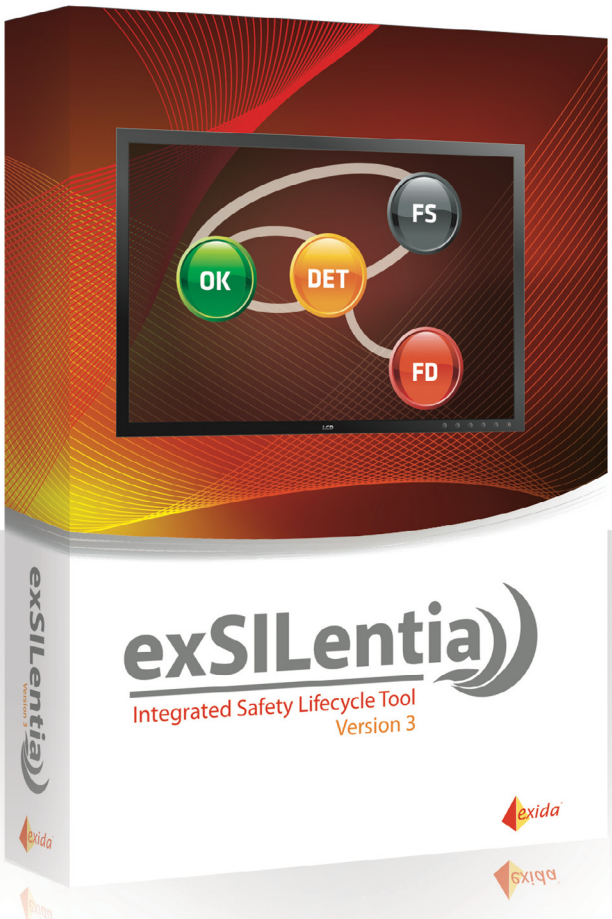
Is it Time to Upgrade Your Process Safety Tools to exSILentia® Version 3?

Design, operation and maintenance of Safety Instrumented Systems (SIS) just got easier

exSILentia Version 3 adds capabilities that will help users achieve a new level of consistency and productivity in the design of their Safety Instrumented Systems (SIS). This release enhances the existing suite of tools, including the industry leading tool for Safety Integrity Level (SIL) verification (SILver®). All-new functionality allows users to follow the entire IEC 61511/ISA 84 functional safety lifecycle for the first time using a single tool. It also supports compliance with regulations such as OSHA PSM 1910.119 (USA) and Seveso II (Europe).

Enhancements to the Existing exSILentia Suite

- New Graphical User Interface (GUI)
- Create user-defined risk graphs
- Required SIL based upon LOPA calculation (uses detailed frequency based target)
- Multiple risk calibrations can be used for SIL selection within a single project
- Specify partial stroke test intervals
- Support for MooN (M-out-of-N) architectures
- Required SIL based upon LOPA calculation (uses detailed frequency based target)
- Define proof testing to account for SIF deadtime (during bypass)



All New Functionality

- Process Hazard Analysis (PHA) - HAZOP Tool
- Import PHA results from 3rd party tools
- Alarm rationalization
- Automatic generation of proof test specifications
- Lifecycle cost evaluator
- Failure & demand data collection / evaluation
- Critical device list
- Viewer for exida's Safety Equipment Reliablity Handbook (SERH) - (reliability database)
- Checklist to demonstrate compliance with the IEC 61511 / ISA 84 standard

Follow the entire IEC 61511 / ISA 84 functional safety lifecycle using a single tool

The use of a single tool for the whole safety lifecycle reduces total cost of ownership and helps ensure SIS applications are not over-designed or under-designed. It improves traceability while also making it easier to manage change, assess the impact of design changes, and audit the overall design as required by industry regulations. exSILentia Version 3 is a modular suite of tools available in four different bundles:

- **Standard**
- **Analysis**
- **Operations**
- **Ultimate**

This allows users to select the package that best meets their functionality requirements, budget, and addresses their specific engineering tasks.

exSILentia Version 3 Options

			exSILentia v3.0 Packages			
Safety Lifecycle Phase / Activity	**exSILentia® Module**	**Module Functionality**	Standard	Analysis	Operation	Ultimate
Functional Safety Management, Auditing and Assessment	IEC/ISA 61511 Compliance Documentation	Checklist for Documenting Compliance with IEC / ISA 61511 Standard	✓	✓	✓	✓
Safety Lifecycle Structure & Planning	N/A					
Hazard & Risk Assessment (Process Hazard Analysis)	PHAx *	Record results of Process Hazards Analysis (PHA) / Hazard and Operability Study (HAZOP)		✓		✓
	PHA Import	Import HAZOP results from 3rd party tools		✓		✓
Allocation of Safety Functions to Protection Layers (SIL Target Selection)	SILect	Safety Integrity Level (SIL) Selection (Risk Graph Hazard Matrix, LOPA)	✓	✓	✓	✓
	SILAlarm *	Alarm Rationalization per ISA18.2, EEMUA 191				✓
Safety Requirements Specification (SRS)	SIF SRS	Basic Safety Instrumented Function Safety Requirements Specification	✓	✓	✓	
	SRS C&E --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 Database (over 1700 devices)	✓	✓	✓	✓
	Lifecycle Cost Estimator	Evaluate Lifecycle cost of proposed SIF designs			✓	✓
	SRS C&E --Design SRS	Detailed Design level Safety Requirements Specification, creation of Cause & Effect matrices				✓
Installation, Commissioning and Validation	N/A					
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				
Decommissioning	N/A					
Verification	Built--in	Peer review capability based on login allows review / approval of tool output	✓	✓	✓	✓
Cost			$	$$	$$	$$$

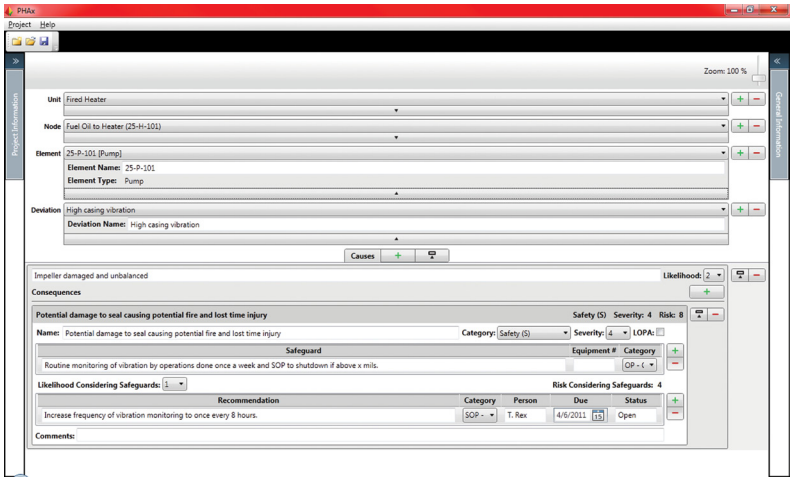
* Also Available Seperately

Advanced GUI improves the workflow process

A new Graphical User Interface (GUI) provides a fresh look and feel to exSILentia, enhancing its usability and the compatibility between software modules. It allows resizing of SIF windows and provides zoom capabilities to accommodate a large variety of screen sizes / resolutions. This is ideal for presentation and review of SIS design results in a conference room with a group of people. A spreadsheet-like overview is also provided to allow a quick comparison of data between Safety Instrumented Functions (SIFs) gaining an overview of the SIS design, and managing the exSILentia project with ease.

Identify and document process hazards with a new integrated tool

The new PHAX tool guides users through the HAZOP process, facilitating effective identification of hazards, hazardous events, and associated sequence of events, simplifying the task of documenting the results. Safeguards and recommendations identified as potential SIFs or alarms can be recorded in a standard format. PHAX supports seamless exchange of the PHA data to subsequent tasks in the safety lifecycle (SIL selection) and alarm management lifecycle (rationalization) via integration with the exSILentia modules such as SILect and SILAlarm. This provides traceability and auditability by helping manage changes that may impact compliance with corporate risk criteria. The tool helps users meet industry regulations such as the Process Hazard Analysis requirement within OSHA PSM.

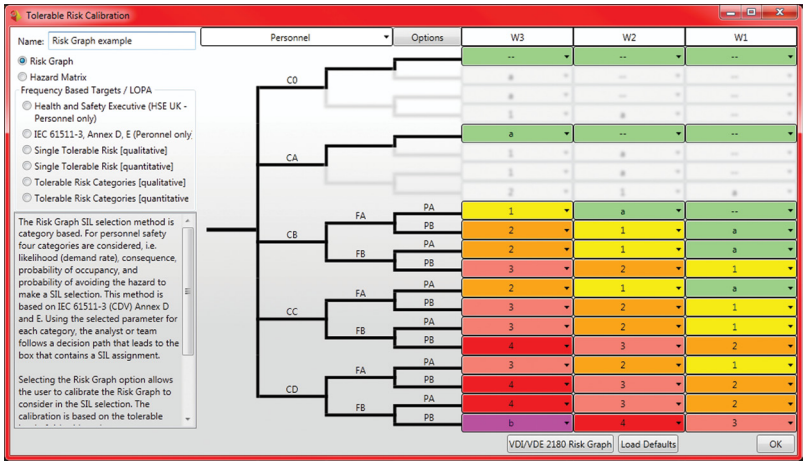


Documenting HAZOP results in PHAX

If you already have a HAZOP tool, this is not a problem. exSILentia provides the ability to import HAZOP results from 3rd party tools (e.g., PHAWorks and PHA-Pro) allowing the data to be used for subsequent SIS design tasks such as SIL selection or alarm rationalization.

Mix and match tolerable risk criteria during SIL Selection

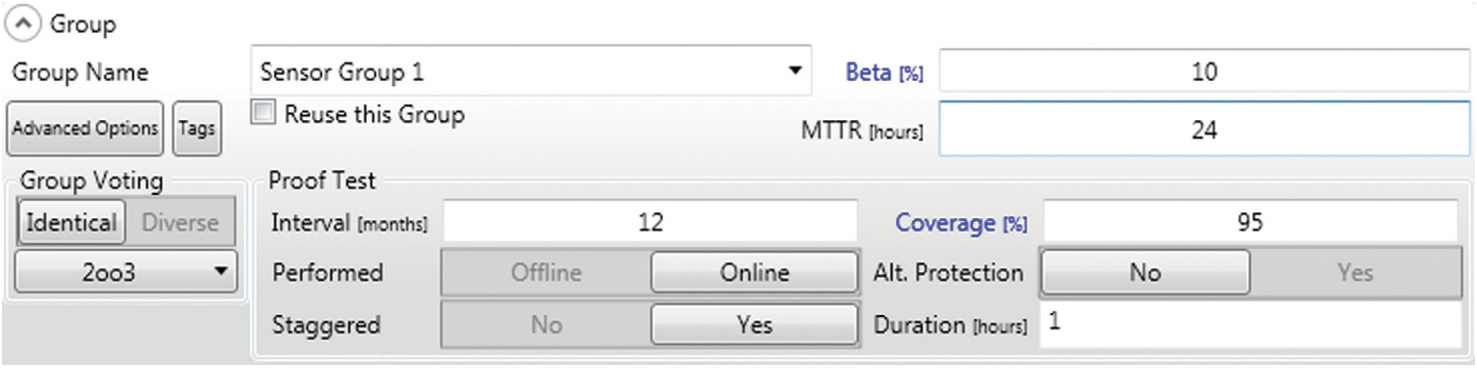
The exSILentia SILect tool now includes the ability to make use of different tolerable risk calibrations on a single project. It is now possible, for example, to use a mixture of risk graph, hazard matrix, and frequency based target (LOPA) approaches within one project. Also, SILect allows a user to create their own risk graph or frequency-based targets, thus incorporating the functionality of the SILClass product.



Using the Risk Graph Calibration wizard for SIL Selection

Enhanced SIL verification

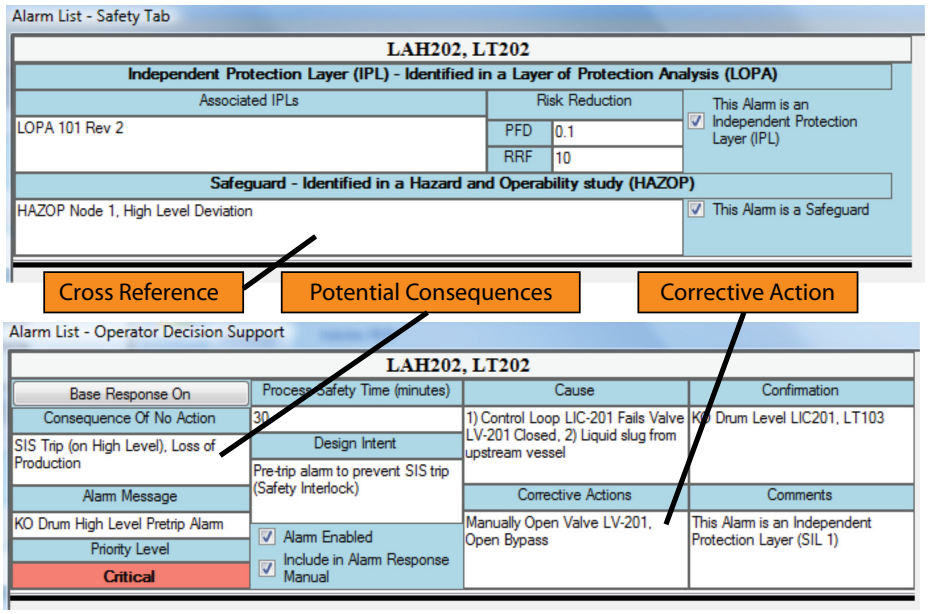
With exSILentia Version 3, the industry leading tool for SIL Verification (SILver) became even better by adding capabilities requested by our users. The test interval of application level diagnostics like Partial Stroke Testing can now be specified. This helps address situations where partial stroke testing is not performed ≥ 10X more frequently than the proof test. SILver can now also account for SIF dead time, which is important in situations where the SIF is completely bypassed during normal operation to execute a proof test. The ability to specify MooN (M-out-of-N) configurations during occasions when a standard architecture does not apply is another new feature of this product.



Accommodating proof test deadtime in SIL Verification calculations

Maximize the risk reduction of the operator and alarm system protection layer through alarm rationalization

Available with exSILentia Ultimate, the SILAlarm™ tool guides users through the alarm rationalization process ensuring that every alarm is justified, properly prioritized, and has a defined operator response as required by ISA-18.2 and EEMUA 191. Alarm rationalization can eliminate alarm overload, reduce the effect of alarm floods, eliminate nuisance alarms, and ensure that the operator has sufficient time to respond (all of which helps achieve the expected level of risk reduction for this type of IPL). SILAlarm allows HAZOP and LOPA results to be cross-referenced during the alarm rationalization process ensuring that safety-critical alarms are treated appropriately.



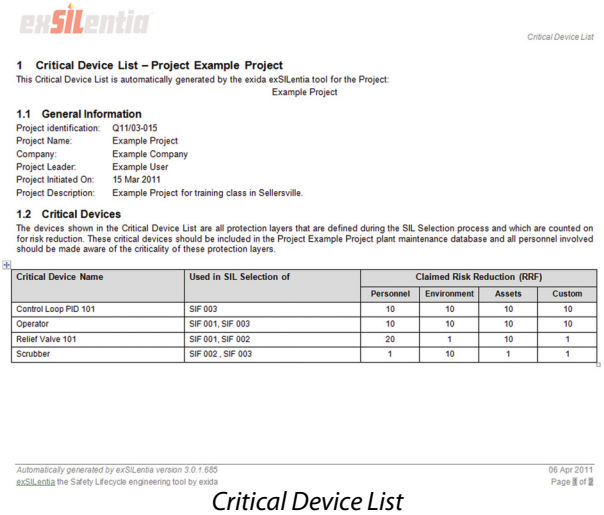
Documenting operator response and creating HAZOP & LOPA cross references in SILAlarm

Critical Device List provides increased visibility into IPLs

Have you ever wondered if a particular relief valve was considered an Independent Protection Layer (IPL) somewhere in the SIL selection activity? This new feature generates a list of all devices defined in a project and cross references all IPLs where they are used, even non SIS risk-reduction measures.

Built-in viewer for failure database simplifies gathering / comparing failure rate data

exSILentia includes the world's most extensive reliability database of instrumentation and control equipment for use in Safety Instrumented Systems, the Safety Equipment Reliability Handbook (SERH). Reliability data for over 1700 sensors, logic solvers, interface modules, and final elements can be referenced directly during SIL verification, eliminating the time-consuming task of gathering reliability data. This data can also be accessed through the SERH viewer, which allows users to compare reliability data by product, manufacturer, or type of assessment. The database is continuously updated as new products are introduced and assessed. Common uses of the SERH include:



exSILentia — Critical Device List

1 Critical Device List – Project Example Project

This Critical Device List is automatically generated by the exida exSILentia tool for the Project: Example Project

1.1 General Information

Project identification: Q11/03-015
Project Name: Example Project
Company: Example Company
Project Leader: Example User
Project Initiated On: 15 Mar 2011
Project Description: Example Project for training class in Sellersville.

1.2 Critical Devices

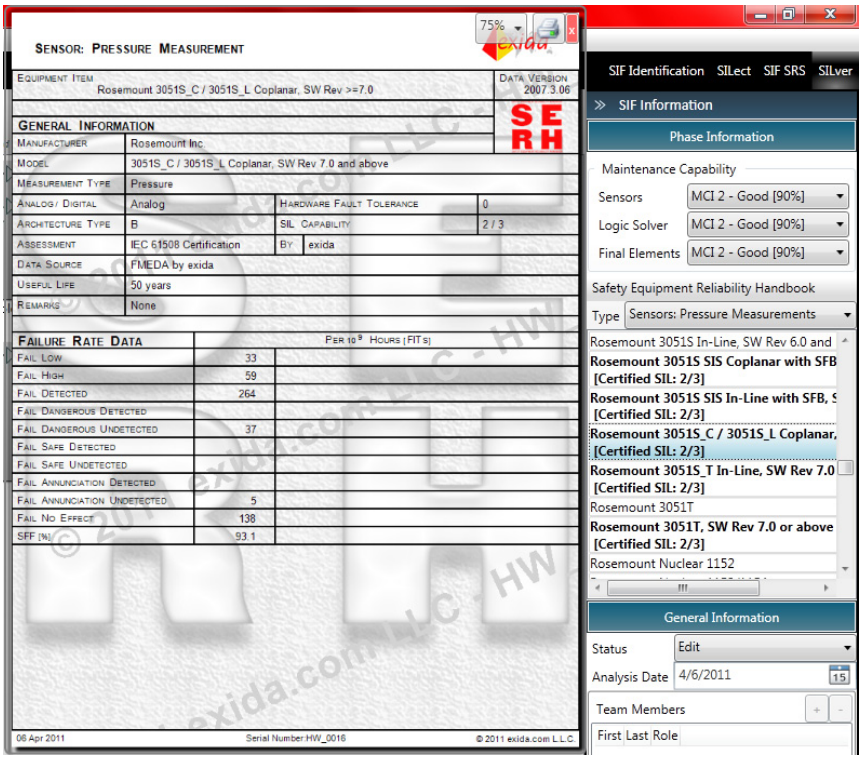
The devices shown in the Critical Device List are all protection layers that are defined during the SIL Selection process and which are counted on for risk reduction. These critical devices should be included in the Project Example Project plant maintenance database and all personnel involved should be made aware of the criticality of these protection layers.

Critical Device Name	Used in SIL Selection of	Claimed Risk Reduction (RRF)			
		Personnel	Environment	Assets	Custom
Control Loop PID 101	SIF 003	10	10	10	10
Operator	SIF 001, SIF 003	10	10	10	10
Relief Valve 101	SIF 001, SIF 002	20	1	10	1
Scrubber	SIF 002 , SIF 003	1	10	1	1

Automatically generated by exSILentia version 3.0.1.685 — 06 Apr 2011
exSILentia the Safety Lifecycle engineering tool by exida — Page 1 of 2

Critical Device List

- Source of equipment reliability data for calculating the SIL of a safety instrumented function (sensor – logic solver – final control element).
- A database that can be used to standardize reliability evaluations across a company
- A tool for evaluating suppliers and equipment to create a preferred vendor list for SIS applications
- As a reference during SIL selection to estimate typical PFDs for common types of equipment (e.g., valves).



SENSOR: PRESSURE MEASUREMENT

Equipment Item	Rosemount 3051S_C / 3051S_L Coplanar, SW Rev >=7.0
Data Version	2007.3.06

General Information

Manufacturer	Rosemount Inc		
Model	3051S_C / 3051S_L Coplanar, SW Rev 7.0 and above		
Measurement Type	Pressure		
Analog / Digital	Analog	Hardware Fault Tolerance	0
Architecture Type	B	SIL Capability	2 / 3
Assessment	IEC 61508 Certification	By	exida
Data Source	FMEDA by exida		
Useful Life	50 years		
Remarks	None		

Failure Rate Data — Per 10^9 Hours (FITs)

Fail Low	33
Fail High	59
Fail Detected	264
Fail Dangerous Detected	
Fail Dangerous Undetected	37
Fail Safe Detected	
Fail Safe Undetected	
Fail Annunciation Detected	
Fail Annunciation Undetected	5
Fail No Effect	138
SFF [%]	93.1

06 Apr 2011 — Serial Number HW_0016 — © 2011 exida.com L.L.C.

SIF Identification | SILect | SIF SRS | SILver

SIF Information

Phase Information

Maintenance Capability

Sensors: MCI 2 - Good [90%]
Logic Solver: MCI 2 - Good [90%]
Final Elements: MCI 2 - Good [90%]

Safety Equipment Reliability Handbook

Type: Sensors: Pressure Measurements

Rosemount 3051S In-Line, SW Rev 6.0 and
Rosemount 3051S SIS Coplanar with SFB [Certified SIL: 2/3]
Rosemount 3051S SIS In-Line with SFB, S [Certified SIL: 2/3]
Rosemount 3051S_C / 3051S_L Coplanar, [Certified SIL: 2/3]
Rosemount 3051S_T In-Line, SW Rev 7.0 [Certified SIL: 2/3]
Rosemount 3051T
Rosemount 3051T, SW Rev 7.0 or above [Certified SIL: 2/3]
Rosemount Nuclear 1152

General Information

Status: Edit
Analysis Date: 4/6/2011
Team Members
First Last Role

Viewing device failure rate data from the SERH database

Document compliance with the IEC 61511 / ISA 84 standard

A checklist for evaluating/demonstrating that your SIS design, operation, and maintenance activities comply with the IEC 61511 / ISA 84 standard is another addition. A comprehensive compliance matrix can be generated automatically by exSILentia, with compliance arguments pre-entered for the requirements that are addressed based on usage of the tool. The remaining compliance arguments can be completed by the user. The resultant document can be used to demonstrate to an auditor, assessor, or regulator how the requirements of the standard have been fulfilled. It can also be used as part of operating plant hazard reviews.

exSILentia

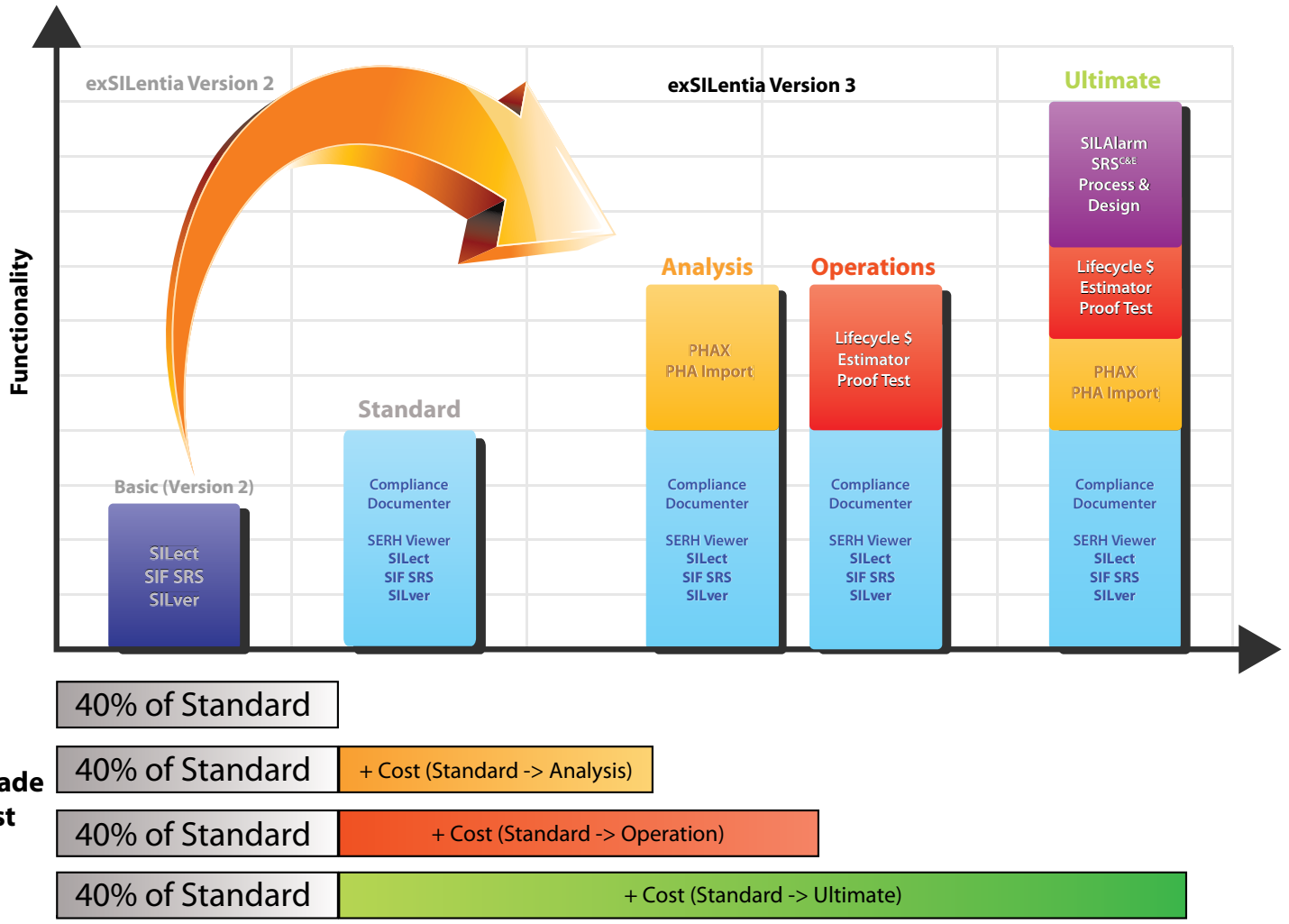
IEC 61511 Compliance Requirements & Arguments

2.4 Risk Assessment

Item	Requirement	Reference IEC 61511	Compliance Argument
01	Process design should be as inherently safe as possible, in accordance to economic objectives and benefits. To bridge the gap between remaining process risk and tolerable risk criteria, additional layers of protection, in the form of mechanical and safety instrumented systems, must be added to the process design	8.1 (p 46) NOTE 2	It is exida policy to strive for as few as possible SIFs by ensuring the process design is as inherently safe as possible. Any SIFs that result in an initial risk reduction requirement greater than SIL 2 require additional study
02	After the process conceptual design, a process hazard and risk analysis must be performed to identify the hazardous events associated with the operations and maintenance of the process. Along with the hazard identification, its associated risk, i.e. its likelihood and potential consequences, must be evaluated (when evaluating the risk posed by the process, human factors, e.g. errors, training, awareness, etc., should be considered in the overall results), and all mechanisms and layers of protection must be identified, including basic process control actions and operator interventions. All these hazard protections must be individually and collectively evaluated for their effectiveness against the hazard (it is important to identify at this time, or later when a more complete design is available, all sources of failures that could lead to a defeat of more than one protection at the same time. These are known as common cause failures and they must be properly accounted, for them having a greater impact on the safety integrity analysis). As a result, the appropriate risk reduction achieved must be stated. This activity will lead to a complete safety functions definition for the process, with the associated degree of risk reduction and remaining risk, for each one of them. Finally, a required or target safety integrity level must be defined for each safety function identified.	8.2.1 (pp 46-47) 3.2.54 (p 30) NOTE 3	For the Example Project project exida is using the exSILentia® sub-tool PHAX. PHAX allows the user to perform a detailed process hazard and risk analysis that can be used to flag potential and existing SIFs as well as functional safety critical alarms. The potential and existing SIFs can be further evaluated using the exSILentia® sub-tool SILect. Functional safety critical alarms can be linked to the exSILentia® sub-tool SILAlarm for alarm management and rationalization. For the Example Project project exida is using the exSILentia® PHA Import functionality. This PHA Import functionality allows users to import potential and existing SIFs identified during a PHA for further evaluation using the exSILentia® sub-tool SIL etc.
03	Whenever a BPCS, not designed as per the requirements of this standard, places a demand on the protection layers, it must be considered that at least once every 100,000 hours a dangerous demand will occur.	8.2.2 (p 47)	The exSILentia® sub-tool SILect contains an embedded Initiating Event (IE) and Independent Protection Layer (IPL) database with industry accepted levels of effectiveness. BPCS loops & interlocks listed in this database comply with this requirement. User to Complete

Making upgrades cost effective and easy

The modular design of exSILentia Version 3 supports an easy and cost-effective upgrade path from version 2 based on your current level of functionality and the functionality desired. Project files created in earlier versions of exSILentia can be automatically converted for use in the new version, ensuring no loss in productivity.



Upgrade paths from exSILentia Version 2 to Version 3

If your current exSILentia package includes optional plug-ins (SRS C&E, PHA Import, Proof Test Generator, or Life- cycle Cost Estimator), then your upgrade path is defined below based on keeping equivalent functionality.

SRS C&E	PHA Import	Proof Test Generator	Lifecycle Cost Estimator	Comparable exSILentia Version 3 Package	Upgrade Cost to Version 3 (Equivalent Functionality)
●	—	—	—	Ultimate	40% of Ultimate Purchase Price
❍	●	❍	❍	Analysis	40% of Analysis Purchase Price
❍	❍	●	❍	Operation	40% of Operation Purchase Price
❍	❍	❍	●	Operation	40% of Operation Purchase Price
❍	❍	●	●	Operation	40% of Operation Purchase Price
❍	●	❍	●	Ultimate	40% of Ultimate Purchase Price
❍	●	●	❍	Ultimate	40% of Ultimate Purchase Price
❍	●	●	●	Ultimate	40% of Ultimate Purchase Price

Flexible licensing to support a variety of applications and project teams

Four different licensing options for exSILentia are available in order to accommodate your safety engineering team, whether co-located or distributed around the world. It also allows for temporary usage (subscriptions for 3, 6, and 12 month online access) or long-term usage allowing users to support projects of different durations.

exSILentia Option	Description
Standalone	License for a single user. Requires no special connectivity (can be used in the office or remotely)
Site	Multiuser license for 5 or 10 concurrent users. Users must be connected to the same network (subnet) as the license server for the application to run.
Online	Application is hosted remotely on an exida server. Users must have a web browser on their local machines and the Citrix® interface client installed to be able to access the application, as well as an internet connection. Projects can be stored on the exida servers as well as locally.
Server	Application and database(s) are hosted on the customer's Citrix® Presentation Server. Users must have a web browser on their local machines and the Citrix® interface client installed to be able to access the application.

For more information or to request a quote:

Contact your local exida representative or visit our website at www.exsilentia.com

Germany	USA	South Africa	Asia Pacific
exida.com GmbH Birkensteinstr. 53 83730 Fischbachau PHONE: +49-89-49000547	exida.com LLC 64 North Main Street Sellersville, PA 18960 PHONE: +1-215-453-1720	exida South Africa PTY LTD Suite 1003, 34 Essex Terrace Westville, 3629, KZN PHONE: +27 31 2671564	11 Collyer Quay #10-13, The Arcade Singapore 049317 PHONE: +65 6222-5160
Switzerland	**Canada**	**Mexico**	**United Kingdom**
exida Certification SA Chemin de Champ-Poury 2 1272 Genolier PHONE:+41 22 364 14 34	exida Canada Ltd. 2nd Floor 3003 - 23rd Street NE Calgary, Alberta T2E 7A4 Canada PHONE: +1-403-475-1943	exida Consulting Mexico Giorgione No. 6 Col. Nonoalco Mixocac Mexico, D.F. 03700 Mexico PHONE: 52-55-5-6-11-98-58	8 Hotchkiss Way Binley Industrial Estate Coventry CV3 2RL UK Phone: +44 (0) 24 76 456 195 +44 (0) 24 76 456 195