


## Assessment Report of the SILver™ tool

<b>Revision No.:</b>	1.0
<b>Date:</b>	2005-07-20
<b>Report Number:</b>	701-002/2005A
<b>Product:</b>	SILver™
<b>Customer:</b>	exida.com 64 N. Main Street Sellersville, PA 18960 USA
<b>Order Number:</b>	20670753
<b>Inspection Authority:</b>	RWTÜV Systems GmbH Member of TÜV NORD Group Safety Approval Service – SAS Hübnerstr. 3 86150 Augsburg Germany
<b>Responsible:</b>	Author:  _____ (Josef Neumann)  Reviewer:  _____ (Gerhard M. Rieger)

This document is only valid in it's entirety and separation of any part is not allowed.

Content	Page
<b>1 Subject of the report .....</b>	<b>3</b>
<b>2 Basis of the assessment .....</b>	<b>3</b>
<b>3 Standards.....</b>	<b>4</b>
<b>4 Definitions.....</b>	<b>5</b>
<b>5 Overview about the system configuration .....</b>	<b>6</b>
<b>6 Software identification.....</b>	<b>7</b>
<b>7 Documentation .....</b>	<b>7</b>
<b>8 Assessment activities and results.....</b>	<b>9</b>
8.1 Functional Safety Management Audit .....	9
8.2 Software Development Process.....	11
8.3 Safety Requirements and Software Architecture .....	12
8.4 Software Design and Implementation .....	13
8.5 Verification and Validation.....	13
8.6 Modifications for the calculation of the S7-400FH.....	14
8.7 User Manual.....	15
<b>9 Summary.....</b>	<b>15</b>

## 1 Subject of the report

This report compiles the results of the assessment of the SILver™ tool of exida.com. The independent services of RWTÜV Systems GmbH (thereafter known as RWTÜV) was ordered by exida.com to assess the SILver™ tool because of its use in safety-relevant applications by the process industry (e.g. oil & gas, chemical industry, etc.) with the goal of achieving a successful assessment of the SILver™ in the framework of the IEC 61508.

## 2 Basis of the assessment

An effective assessment in order to meet all the requirements for a complete project requires the following testing segments to be successfully completed:

- Functional Safety Management
- Development process
- Safety requirements and system architecture
- Software design and implementation
- Safety verification steps and the validation tests
- Test specification and test results

Including the following principal functional safety considerations:

- Software failure-avoidance
- Safety Manual

### 3 Standards

Because of the application area of the SILver™, the following standards are relevant:

List of standards	
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems SIL 2 capability; To verify SIS in Low Demand Mode
IEC 61508-1:1998	Part 1: General Requirements
IEC 61508-3:1998	Part 3: Software requirements

## 4 Definitions

FSM	Functional Safety Management
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-check frequency
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency
SF	Safety Function
SFF	Safety Failure Fraction
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
SIL	Safety Integrity Level.
SRS	Safety Requirements Specification

## 5 Overview about the system configuration

SILver™ is a software tool created to calculate reliability metrics needed for safety system design. It can be used as an engineering tool that calculates the average Probability of Failure on Demand (PFDavg) of Safety Instrumented Functions, as required by functional safety standards like IEC 61508 and IEC 61511, in order to verify that designs meet the target safety integrity level requirement. SILver also calculates the Mean Time to Fail Spurious (MTTFS). SILver™ includes a built-in equipment failure rate database, a full Markov calculation engine, and either IEC 61508 or IEC 61511 architecture constraints consideration.

The SILver™ tool covers two main features:

- First the tool provides an accepted standard method and set of procedural guidelines for executing the SIL verification tasks.
- Second, the tool provides an automatic documentation of the results from this key lifecycle task that helps streamlining the front end of the safety lifecycle.

Typical use of the SILver™ tool will be during conceptual design phases of Safety Instrumented System projects.

The exSILentia web based version of the exida SILver™ tool will be accessible through the internet after a user logs in using a unique username and password. The web based version will be designed to work on a Windows server 2000 (and up) platform and using the Microsoft Internet Explorer 5.5 (and up) browser.

The exSILentia standalone version of the exida SILver™ tool will be designed to work with Microsoft Windows 2000 and up. The SILver™ engine part of this tool will be identical to the proven web based SILver engine.

SILver™ will be based on many of the assumptions that are in IEC 61508-6, Annex B. These assumptions on which the calculations within SILver are based are listed in the SILver™ Requirements Specification [D2].

## 6 Software identification

The following revision is considered for the assessment:

SILver™ Software:           Version 3.0

## 7 Documentation

- [D1] SILver Functional Safety Management Plan, Rep.no.: EX SILver R001, V1.2, April 05, 2005
- [D2] SILver Requirements Specification, Rep.no.: EX SILver R003, V1.3, April 04, 2005
- [D3] SILver Architectural Design Document, Rep.no.: EX SILver R005, V1.1, February 16,2005
- [D4] SILver Validation Test Plan Template, Rep.no.: EX SILver R002, V0.3, January 28, 2005
- [D5] SILver Test Strategy Plan, Rep.no.: EX SILver R011, V1.1, April 15, 2005
- [D6] SILver Coding Guidline, Rep.no.: EX SILver R004, V1.2, February 17, 2005
- [D7] SILver Engine COM object Test Plan, Rep.no.: EX SILver R006, V1.1, February 17, 2005
- [D8] SILver Test Results Evaluation Report, Rep.no.: EX SILver R007, V1.1, February 18, 2005
- [D9] SILver Validation Test Plan Template, Rep.no.: EX SILver R002, V0.3, February 17, 2005
- [D10] SILver Code/Peer Review, Rep.no.: EX SILver R008, V0.1, February 22, 2005
- [D11] SILver Validation Test Plan, Rep.no.: EX SILver R009, V1.1, February 23, 2005
- [D12] SILver Logic Solver Part Options Test Report, Rep.no.: EX SILver R012, April 25, 2005
- [D13] SILver Generic Part / Group Options Test Report, Rep.no.: EX SILver R012-3, April 26, 200
- [D14] SILver Structured Equivalence Testing, SILver TSP SET, April 12, 2005

- [D15] SILver User Manual, February, 2005
- [D16] Listing SilverFuncs.asp, February 16, 2005
- [D17] S7-400FH modification Issue; June 10, 2005
- [D18] Modification of S7-400FH Markov Models, V01; May, 03, 2005
- [D19] Project\_3477 Engine Compare Modification S7-400FH Markov Models.xls;  
June 10, 2005
- [D20] SILver Test Strategy Plan V12, June 09, 2005
- [D21] SILver engine S7 Modifications Test Report, June 10, 2005
- [D22] SILver Markov Models Test Report V12, June 10, 2005
- [D23] SILver Logic Solver Part Options Test Report V12, June 10, 2005
- [D24] SILver Structured Equivalence Testing - Addendum 1, June 10, 2005



## 8 Assessment activities and results

Assessment of the Functional Safety Management

### 8.1 Functional Safety Management Audit

In the assessment process for the SILver™ tool a safety management audit has been performed to cover the relevant requirements of the IEC 61508, in respect of the fulfilment of the requirements to the safety quality procedures. The audit of the Functional Safety Management was based on the SILver™ Functional Safety Management Plan [D1]. Review activities were performed on a visit at exida together with interviews together with project engineers. The functional management system is based on the existing quality system designed per ISO9000:2000.

#### **Scope of the Assessment of the SILver tool:**

The scope of the Functional Safety Management Audit covers the specified Safety Lifecycle Phases of the IEC61508 Part 3 for software development.

The scope is as follows:

**For managing and development of a software tool to be used for safety relevant SIF calculations.**

For the Functional Safety Management Audit according to IEC 61508 it was essential that the functional safety management and the software development process meet SIL 2 requirements in order to qualify for SIL 3 applications of a safety-related product. The FSM procedures are used to reduce the systematic failure rate.

**The Functional Safety Management Audit covered the following areas:**

- Overall safety planning (regarding quality)
- Overall Quality Management System
- Company FSM procedure
- Requirement specifications
- Software design and development method
- Verification & Validation activities (test planning and testing)
- Change and Configuration management
- Feedback control and improvement of safety processes
- Safety Manual

An important part of the audit was to discuss safety aspects of the project with the participants and to ask for the relevant documents and the access to the relevant information. Also the specific knowledge about safety processes and internal review activities were reviewed. Actual documentation was reviewed and the statements of the participants were compared with the relevant parts of the documents.

**Result:**

The audits, interviews and document reviews performed at January, 2005 have shown that the Functional Safety Management System defined in the listed documents complies with the applicable sections of the IEC 61508.

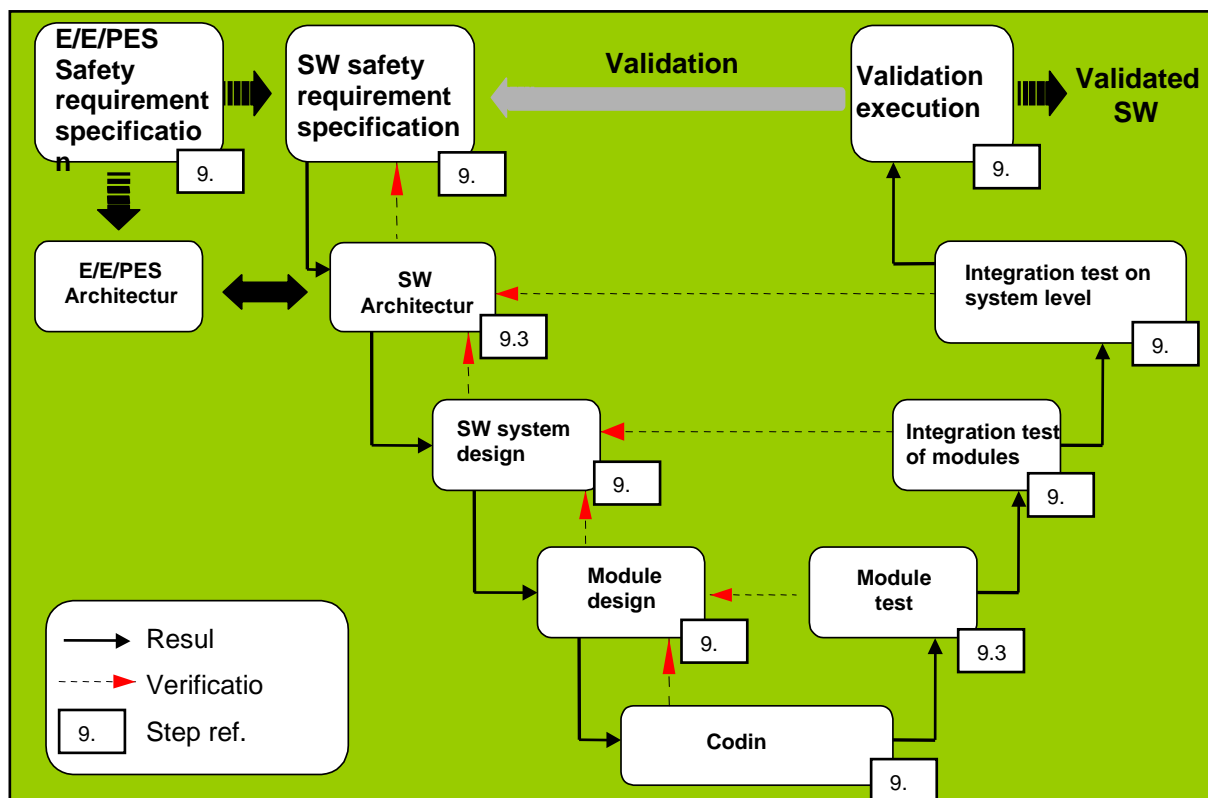
No major findings were detected in the audit.

If changes to the Safety Management Systems are performed than RWTÜV must be informed.

## 8.2 Software Development Process

The assessment of the software development process has been performed based on the documentation listed in section 7 “Documentation” and on interviews with project engineers regarding the life cycle phases of the IEC 61508.

In general the standard defines the V-Model as a development process deviated into different phases for the software development.



Picture 1: V-Model (taken from IEC 61508)

### Structuring of the development process:

The document SILver™ Functional Safety Management Plan [D1] describes the exida.com development processes and procedures as well as the defined techniques and measures listed in the IEC 61508 part 3. The aim of the assessment was to show that the defined procedures are not only defined but also used and lived in the project.

The principal parts of design, verification & validation, implementation and test activities have been reviewed and discussed with the development engineers.

**Result:**

The review of the software development process has shown that the definitions in the Functional Safety Management Plan [D1] of the SILver™ tool together with additional documents as [D2, D3 and D4] is consistent according the requirements of the IEC 61508. The specifications in the documentation are consistent and complete and clearly presented. The overall concept with the chosen architecture design [D3] and the selected techniques and measures are able to fulfil the Safety Integrity Level 2.

### **8.3 Safety Requirements and Software Architecture**

The software requirements document [D2] and the software architecture document [D3] have been reviewed to verify compliance of the system architecture with the IEC 61508.

Based on the set of requirements RWTÜV has evaluated whether the implemented fault detection for random and interference failures and fault control measures which are defined for the SILver™ tool were sufficient to meet the requirements. The software architecture was evaluated in regards to completeness and correctness against the Safety Requirements Specification.

Probable deviation from the specified function of the unit was also considered to be a malfunction.

**Result:**

The review from RWTÜV has shown that the Software Architectural Design of the SILver™ is consistent against the Safety Requirements Specification. The specifications in the documentation are consistent and complete and clearly presented. The overall concept with the chosen architecture design and the selected measures of fault detection and fault control is able to fulfil the Safety Integrity Level 2.

## 8.4 Software Design and Implementation

The software design of the SILver™ was based on the architectural definitions and followed up the specific coding guidelines [D6]. A high level language was used to develop the SILver™ software. RWTÜV has reviewed the relevant documentation and has interviewed the project engineers about the implementation procedures.

### **Result:**

The software design and Implementation is compliant to IEC 61508 part 3 for the required SIL.

## 8.5 Verification and Validation

The test specifications defined in the Validation Test Plan [D4] from exida have been reviewed. The list of validation tests are referenced to the Requirement Specification [D2]. The review has shown that the requirements are covered by the validation plan. After the execution of the validation tests by the manufacturer, the test results have been reviewed by RWTÜV.

Additional sample testing of the SILver™ software functions have been defined by RWTÜV and a separate list of test items has been generated. The defined tests have been executed at exida by RWTÜV. The definition and results are documented in the RWTÜV Fault Injection Test Report.

### **Result:**

The review of the Validation Test Plan and the various test reports from exida and the performing of the sample tests by RWTÜV have shown, that the defined tests are consistent to the software functions and the tested results can be compared to the tests of exida. The test definitions are sufficient to prove compliance with the standard.

## 8.6 Modifications for the calculation of the S7-400FH

After some RWTÜV activities exida introduced some modifications made to the SILver™ engine to more accurately calculate the Siemens S7-400FH logic solver. The documentation is listed in section 7 “Documentation” [D17 to D24]. The descriptions of the modifications and the test documentation have been reviewed by RWTÜV. The modified test plans and the test results are consistent and cover the documented modifications.

### **Result:**

The reviews of the Test Strategy Plan [D5] and the various test reports from exida have shown that the defined tests are consistent to the software modifications and the tested results can be compared with the test plans of exida. The test definitions are sufficient to prove compliance with the standard.

## 8.7 User Manual

The user manual has been reviewed to fulfil the requirements of the considered standard. Specifically the section about “Using SILver™” has been checked according the defined procedures to maintain the safety aspects of the tool by using the necessary configurations for a safety handling of the tool.

### **Result:**

The review has shown that the safety manual meets the requirement of the IEC 61508. Detailed descriptions are included for the end user to operate the SILver™ tool in the required safety level.

## 9 Summary

The assessment of the SILver™ tool has shown that the Functional Safety Management, the defined development process as well as the software structure, the software design, implementation and testing are compliant with the IEC 61508, SIL 2 requirements in order to qualify for SIL 3 applications of a safety-related product. The definitions for software modifications together with the coding guidelines are in accordance with SIL 2 requirements.

The validation and testing activities have shown the compliances between the realised SILver™ implementation and the safety requirements specification.

The actual version of the Safety Manual [D12] must be considered for the use in safety relevant applications.