RiskCATs V6.2
Product Description

16th October 2011

RiskCATs

Requirements on High Quality Embedded Systems and their Software

- Requirements Capturing from IEC 61508, ISO 26262, …
- Checklist Production
- Export to requirements management tools and to development tools
- Means for company specific frames and interpretations

A Tool of the

Code ***A***nalyzer ***T***ool ***S***et

Product Description

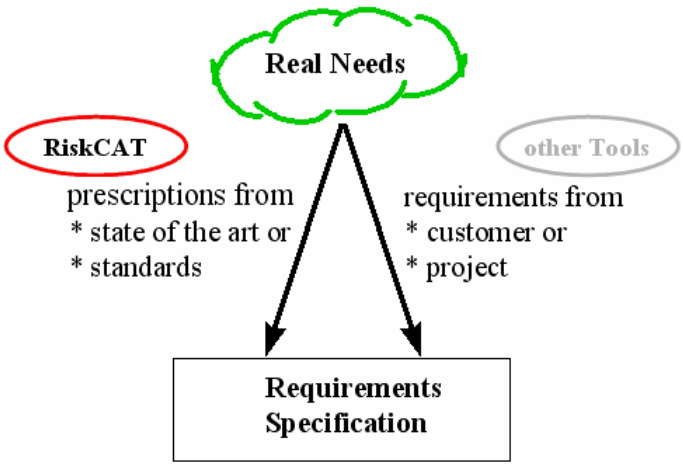
CATS Software Tools GmbH, Hamburg
www.cats-tools.de

List of Contents

Quality First 2
A suggestion for the efficient handling of standards 3
Usage of RiskCAT 4
Short description of RiskCAT 4
Application Area of RiskCAT 8
Benefits of RiskCAT 8
RiskCAT Components 8
Installation of RiskCAT 9
Input to RiskCAT 9
Result data of RiskCAT 9
Integration of RiskCATs with other Tools 11
Tools of the RiskCAT family 14
Back ups 15
Maintenance 15
Quality Assurance for RiskCATs 16
RiskCAT xxxxx — Data Sheet 17
Abbreviations 18

Quality First

Prerequisite to produce and certify high quality software is to know about the functional and non functional requirements imposed on the software. These requirements generally result from two different sources. One source are the specific requirements of the customer or producer e.g. based on their applications or marketing strategy. The other source are prescriptions imposed on software by the state of the art represented e.g. by national or international standards.



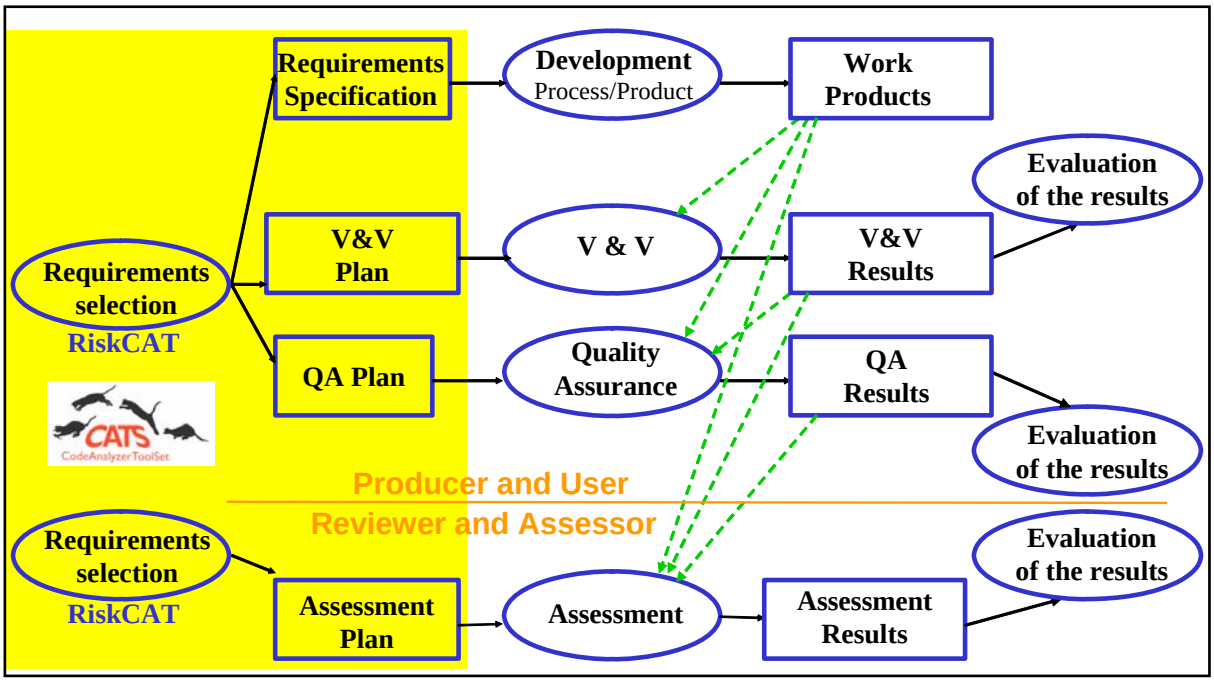
RiskCAT is a tool family of Code Analyzer Tool Set (CATS) for requirements capturing from standards thereby providing the starting point for high quality software development and products. The state of the art in quality of electrical / electronic / programmable electronic systems is provided to a large extent by IEC 61508 as well as the application sector specific derivates from IEC 61508 as for example IEC 61511, EN 50128, ISO 13848 or ISO 26262.

A suggestion for the efficient handling of standards

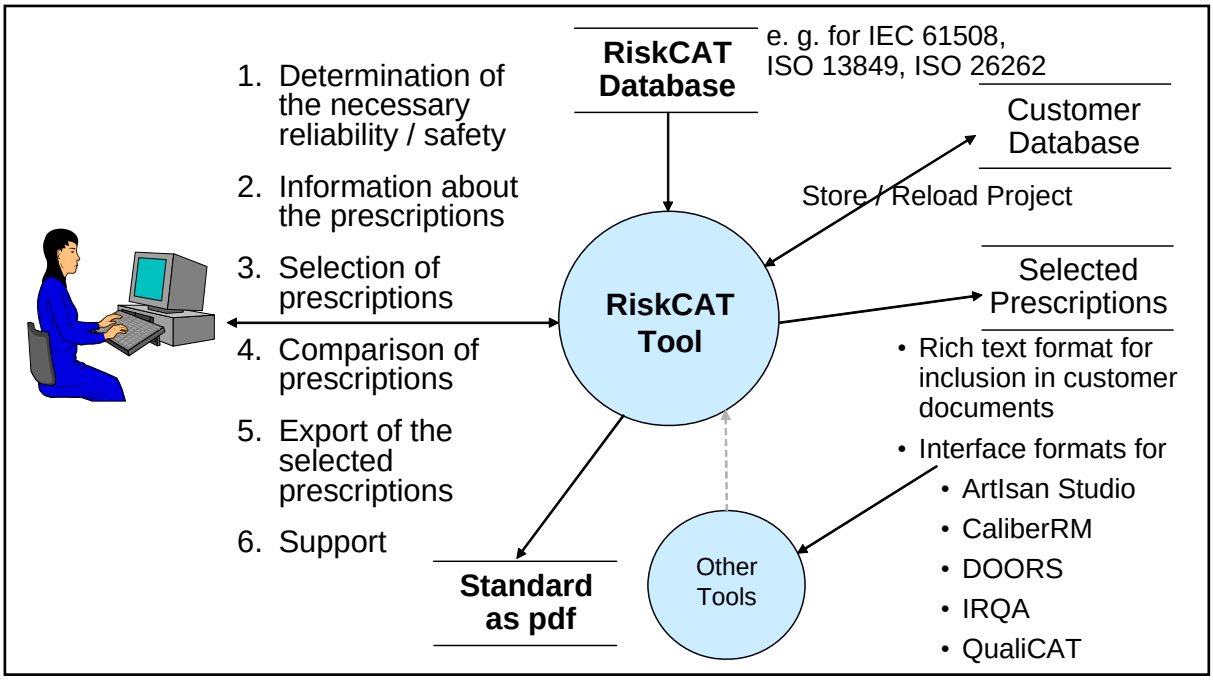
<table>
<tr><th colspan="2">For all activities</th></tr>
<tr><td colspan="2">1 Before starting the real work an overview on the considered standard should be achieved. This may be achieved e. g. in technical discussions or in seminars.
2a Selection of the prescriptions from the considered standard relevant for the next working step which needs to be accomplished OR
2b assurance that the standard does not provide guidance for the working step.
3a Generation of a checklist from the selected prescriptions OR
3b transfer of the prescriptions into requirements management.
4 In case relevant prescriptions are not selected for a working step a note about the motivation for omitting the prescription should be made in the checklist respectively the requirements management.
RiskCATs provide efficient help for this approach.</td></tr>
<tr><th>For the preparation of processes and the development of products</th><th>For V&V and QA as well as Assessment of products and processes</th></tr>
<tr><td>5 Taking into account the prescriptions which have been selected during preparation of the respective processes
6 Taking into account the prescriptions which have been selected during product development
RiskCATs generate checklists and provide interfacing to development tools.</td><td>7 Logging compliance with the prescription in the checklists or the requirements management.
8 Referencing the work product which provides the compliance (detailed to the relevant chapter / page)
9 Compliance evaluation for the individual prescriptions, the themes of the standard and the standard as a whole.
QualiCAT provides efficient help.</td></tr>
</table>

Usage of RiskCAT

RiskCATs may be used to determine those requirements which shall be applied during process development, development of a whole embedded system or just specific work products, verification & validation, or assessment for purpose of compliance with state of the art given in standards.



Short description of RiskCAT



RiskCAT supports

- the determination of the necessary Safety Integrity Level (SIL)
- information about the prescriptions required by the standard under consideration
- selection of those prescriptions relevant for the actual step of work
- the export of the selected prescriptions for further work as well as for integration of RiskCATs into our customers development environment

Besides this RiskCAT offers some support functions.

The work tasks assisted by RiskCAT are:

1. Determination of the necessary Safety Integrity Level (SIL)
   - determination of the normative prescriptions for determination of the necessary SIL,
   - manual pre-selection of the SIL,
   - the informative SIL determination via the necessary risk reduction,
   - the informative SIL determination via a risk graph.
   - (This may be different between the standards supported, especially the informative means may vary. The list given here is valid for IEC 61508.)

2. Information about prescriptions[1]
   - the structured overview on the recommended prescriptions,
   - retrieval in the original standard (or the relevant parts of it as e. g. for IEC 61508),
   - the context related presentation of the original standards clause,
   - the context related presentation of explanations to the clause given in the supported standard itself,
   - the context related presentation of terms used in the prescription texts given in the supported standard, e. g. part 4 of IEC 61508 or part 1 of ISO 26262.

3. Selection of prescriptions
   - the selection of individual prescriptions,
   - the selection of groups of prescriptions according to the degree of obligation,
   - the selection of prescriptions related to documents,
   - the selection of prescriptions related to activities (life cycle phases),
   - the selection of prescriptions related to key words.

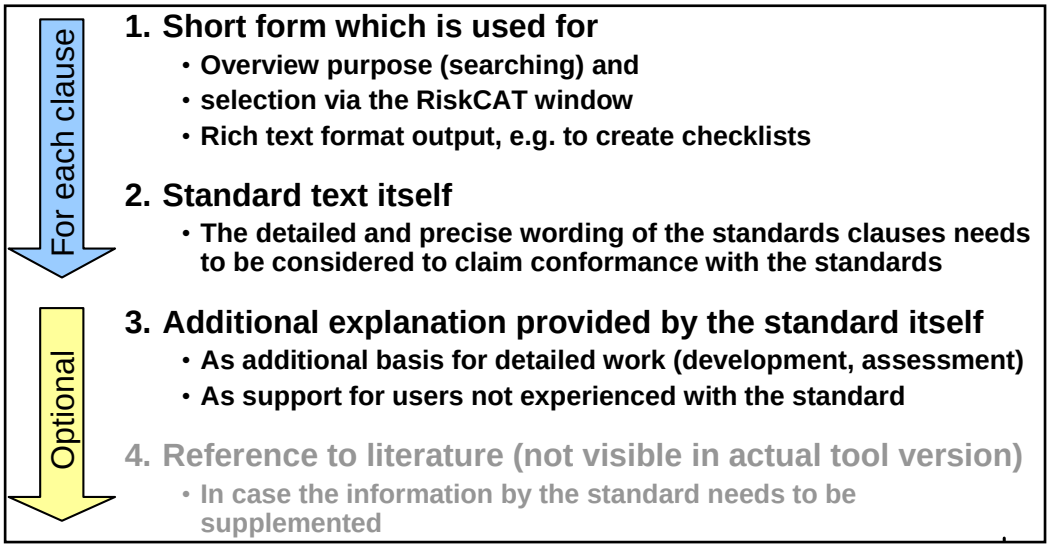
4. Comparison of prescriptions
   - Comparison of the degree of obligation of a prescription at different quality levels (not available for standards which deal with one quality level only as e. g. IEC 60880 which is for Category A only)

[1] The demands of a standard are called professionally „requirements“. With embedded systems – especially their software – the term „requirements“ is used as well. With that results from the standard requirements e.g. on (software-) requirements. Because that makes communication difficult, RiskCAT uses for the requirements of the IEC 61508 the term „ prescriptions “.

- Comparison of a prescription in the actual standard (e. g. ISO/DIS 2 62 62 in RiskCAT 2 62 62) to the basic safety standard IEC 61508.
  (available only with a "RiskCAT Modul for Requirements Comparison between different standards")

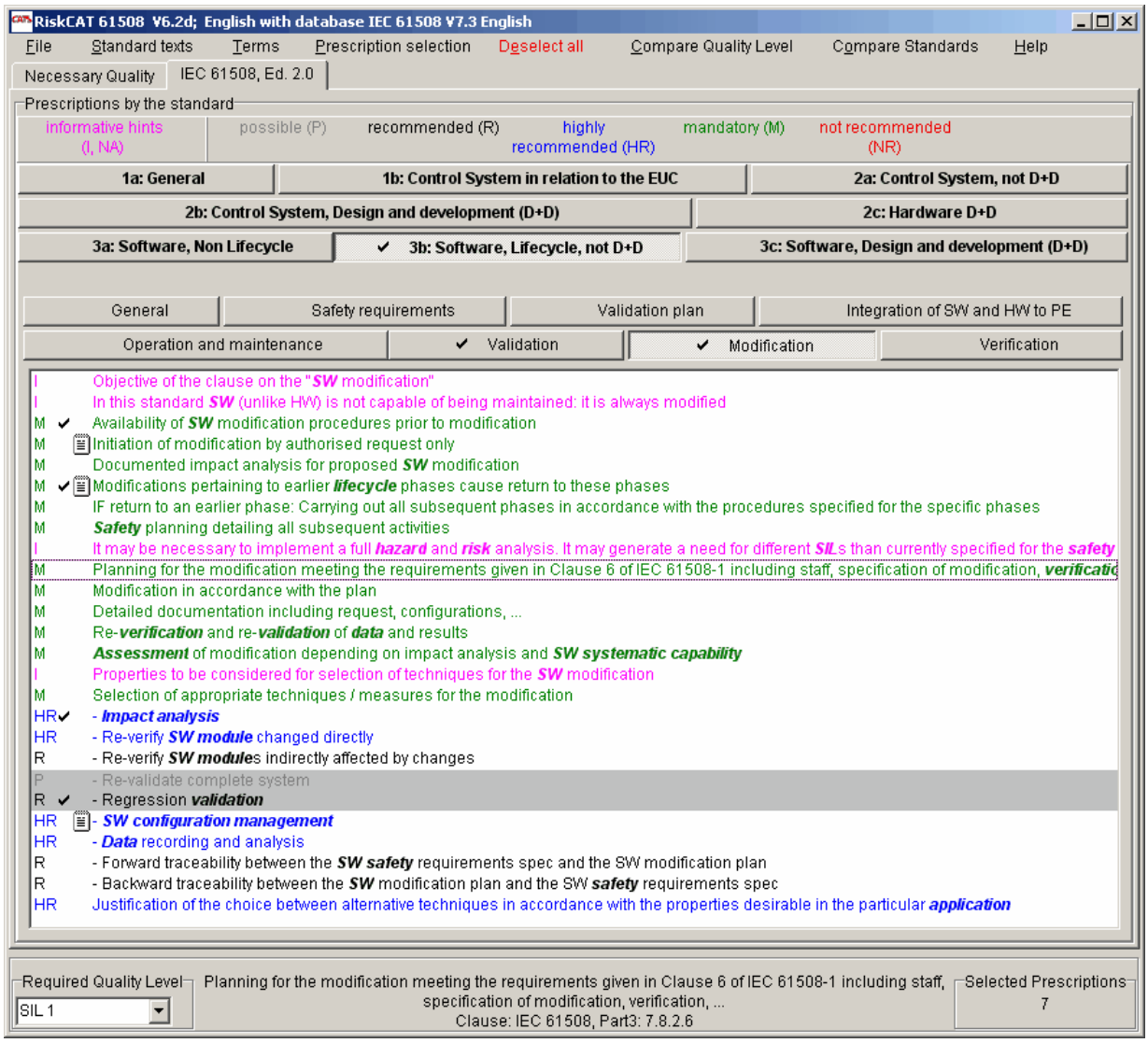
5. Export
   - the result storage as simple text file for further processing by the customer
   - the result storage as formatted text file (Rich Text Format, RTF) providing a ready checklist
   - the result export to Artisan Studio
     (available only with an "RiskCAT Interface to Requirements Management Tools").
   - the result export to CaliberRM
     (available only with an "RiskCAT Interface to Requirements Management Tools").
   - the result export to DOORS
     (available only with an "RiskCAT Interface to Requirements Management Tools"),
   - the result export to IRQA
     (available only with an "RiskCAT Interface to Requirements Management Tools"),
   - the result export to QualiCAT which is the CATS tool for evaluation of the compliance with standards.

6. Support function
   - the possibility to edit simple notes for each individual prescription,
   - the possibility to edit comprehensive notes for each individual prescription,
   - the overview on the terms defined by the considered standard which are used in the prescription presentations,
   - the copy function for actually marked prescription into the clipboard,
   - the copy function for standard texts into the clipboard,
   - the storage of prescription profiles as project or company templates in a project file (project storage),
   - the reloading of prescription profiles.



Important advantage of the tool supported approach is the possibility to vary interactively risk parameters, risk classes and sets of process and realization prescriptions defining alternative or optimized sets of prescriptions to reach specified quality, safety or reliability targets.

The purpose of RiskCAT is to assist the user in application of the IEC 61508. However, it is of course not the purpose of the tool to replace the standard. Anyhow the detailed and precise wording of the standards clauses needs to be considered to claim conformance with the standards. RiskCAT's condensed presentation of the standards contents has been established for the purpose of ease of work, overview and general navigation.



RiskCAT offers an interface for full text browsing as well as context sensitive browsing in original standards. To use this interface the XpdfViewer™ ActiveX Control needs to be installed and licensed standard files need to be available. Both are supplied with RiskCAT.

RiskCAT is designed for use by embedded systems software professionals. Experience of using WINDOWS on PCs is required.

Application Area of RiskCAT

Main activities supported by **RiskCAT** are:

- to capture the prescriptions available from the considered standard, e. g. IEC 61508, for high quality software and high quality software production
- to support retrieval in the standard
- to assist in identification of the prescriptions to be applied in development
- to produce checklists for the purpose of quality control
- to provide a means for
    - company specific templates of prescriptions as well as
    - company specific interpretations of prescriptions

Benefits of RiskCAT

For the occasional user of standards, **RiskCAT** provides a qualified database containing the relevant prescriptions for development, verification and validation. These are accessible for use on the current project and can be exported for use in future projects.

For frequent users, **RiskCAT** with its wide range of options and features, provides a targeted method of matching tasks to specific steps and provides a mechanism for evaluating the impact of changes on quality levels. **RiskCAT** can also link the explanations in the standard to tasks.

RiskCAT Components

The **RiskCAT** components are:

- The executable runtime image RiskCAT_xxxxx[2]_V62x.exe,
- the help file RiskCAT_xxxxx_V62x.hlp,
- XpdfViewer™ ActiveX Control,
- pdf files of the supported standard or just the relevant parts of it, e. g. parts 1, 2, 3, 4 and 7 for IEC 61508. These pdf files are protected by pass word and to be used together with RiskCAT only, and
- the user's manual as a pdf file.

All these files are available on the **RiskCAT** USB memory stick.

RiskCAT is executable from the RiskCAT USB memory stick only.

By contract with the German Chapter of the IEC (DKE) CATS has been asked to declare with RiskCAT[3]:

> „The data from the international standards series IEC 61508 are in use with permission of the IEC International Electrotechnical Commission, Geneva. They have not been checked by IEC or their deputies.
>
> Authoritative for the application of the standard are the versions with newest edition which may be received

[2] xxxxx is the number (normally 5 digits) of the supported standard, e. g. 61508

[3] The original clause is in German language. Because no official translation has been available this translation is by CATS.

from VDE VERLAG GMBH, Bismarckstr. 33, D-10625 Berlin (www.vde-verlag.de). The user shall pay attention to the national standards.

CATS declares that texts used correspond to the actual state of the IEC-standards. 2001-09-24, CATS“

By email from 2011-08-03 CATS has been asked to declare with RiskCAT:

“CATS Software Tools GmbH thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standard IEC 61508 ed.2.0 (2010). All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein. ”

Installation of RiskCAT

RiskCAT is supplied as executable code on USB memory stick. RiskCAT itself does not need any installation. So just run the executable file from the USB memory stick.

RiskCAT uses the XpdfViewer™ ActiveX Control which needs installation. This installation is automatically during the first run. Prerequisite for this are administrator rights.

For earlier versions of RiskCAT the experience showed that the automatic installation of XpdfViewer™ ActiveX Control sometimes failed. Than it needs to be installed.

Input to RiskCAT

File input to RiskCAT are project files which may be used

- to restore recent tool sessions or
- to start with the company specific or project specific set of requirements.

All other input is interactively by the user.

Result data of RiskCAT

Besides interactive results RiskCAT produces on demand

- project files,
- simple text result files which are intended for further processing by the user.
- rich text format (rtf) files which establish checklists ready for use. An example for a short result from an IEC 61508 session is given on the next page.
- Interface files to third party tools (options at extra expense) as well as to QualiCAT

Example for RiskCAT's formatted text output

Prescriptions of IEC 61508, Ed. 2.0 for SIL 1 on 2011-04-25, 14:26, elaborated with RiskCAT 61508 V6.2d; English with database IEC 61508 V7.3 English

Structure of this table:

Prescription for Area – Topic			
Nr.	Prescription	Reference	Obligation

The selected prescriptions are:

1b: Control System in relation to the EUC - Modification and retrofit			
1	Planning of modification or retrofit activities prior to carrying out	IEC 61508, Part1: 7.16.2.1	M
2	Initiation of modification and retrofit by authorised request only	IEC 61508, Part1: 7.16.2.2	M
3	Request determines affected hazard, proposed change, reason	IEC 61508, Part1: 7.16.2.2	M
4	Impact analysis including assessment of the impact	IEC 61508, Part1: 7.16.2.3	M
5	Documentation of impact analysis	IEC 61508, Part1: 7.16.2.4	M
6	Authorization of modification or retrofit depending on impact analysis	IEC 61508, Part1: 7.16.2.5	M
7	Modifications impacting safety cause repetition of earlier phases	IEC 61508, Part1: 7.16.2.6	M
8	NO usage of test procedures for initial installation and commissioning for operations without checking	IEC 61508, Part1: 7.16.2.6/Note 2	HR
9	Chronological documentation of modifications, analysis, re-verification, ...	IEC 61508, Part1: 7.16.2.7	M
2a: Control System, not D+D - Modification			
10	Maintained documentation including detailed spec of change, ...	IEC 61508, Part2: 7.8.2.1	M
11	Maintenance of a system initiating changes and informing users	IEC 61508, Part2: 7.8.2.2	M
12	Level of expertise, tools, ... for modifications at least that of initial development	IEC 61508, Part2: 7.8.2.3	M
13	Re-verification and re-validation after modification	IEC 61508, Part2: 7.8.2.4	M

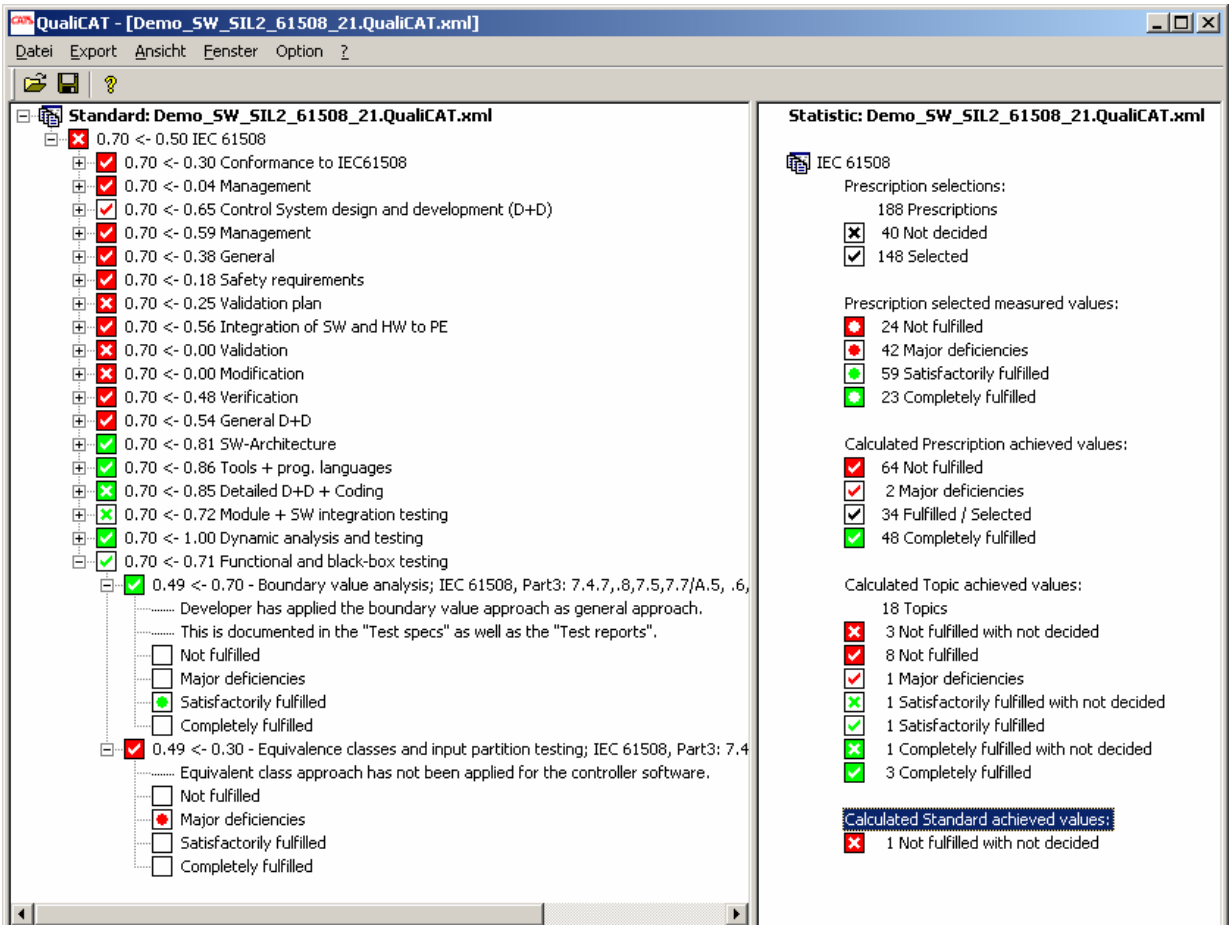
Integration of RiskCATs with other Tools

The RiskCAT export interfaces offer

- to export the prescriptions actually selected to and
- to integrate RiskCAT into your development environment together with
  - **Artisan Studio™** (Model based development by Artisan Software Tools Ltd.)
  - **CaliberRM™** (Requirements Management by Borland Software Corporation).
  - **DOORS®** (Requirements Management by IBM Rational)
  - **IRQA** (Requirements Management by VISURE SOLUTIONS) as well as
  - **QualiCAT** (Evaluation of standard compliance by CATS Software Tools)

The RiskCAT export interfaces are packages of its own and need an extra licence (except for the QualiCAT interface).

QualiCAT is the CATS tool to evaluate compliance with standards as a whole, the topics of the standards as well as the individual prescriptions during verification & validation as well as assessment. The QualiCAT example shown below based on the RiskCAT export is concerned with 188 prescriptions selected from IEC 61508.

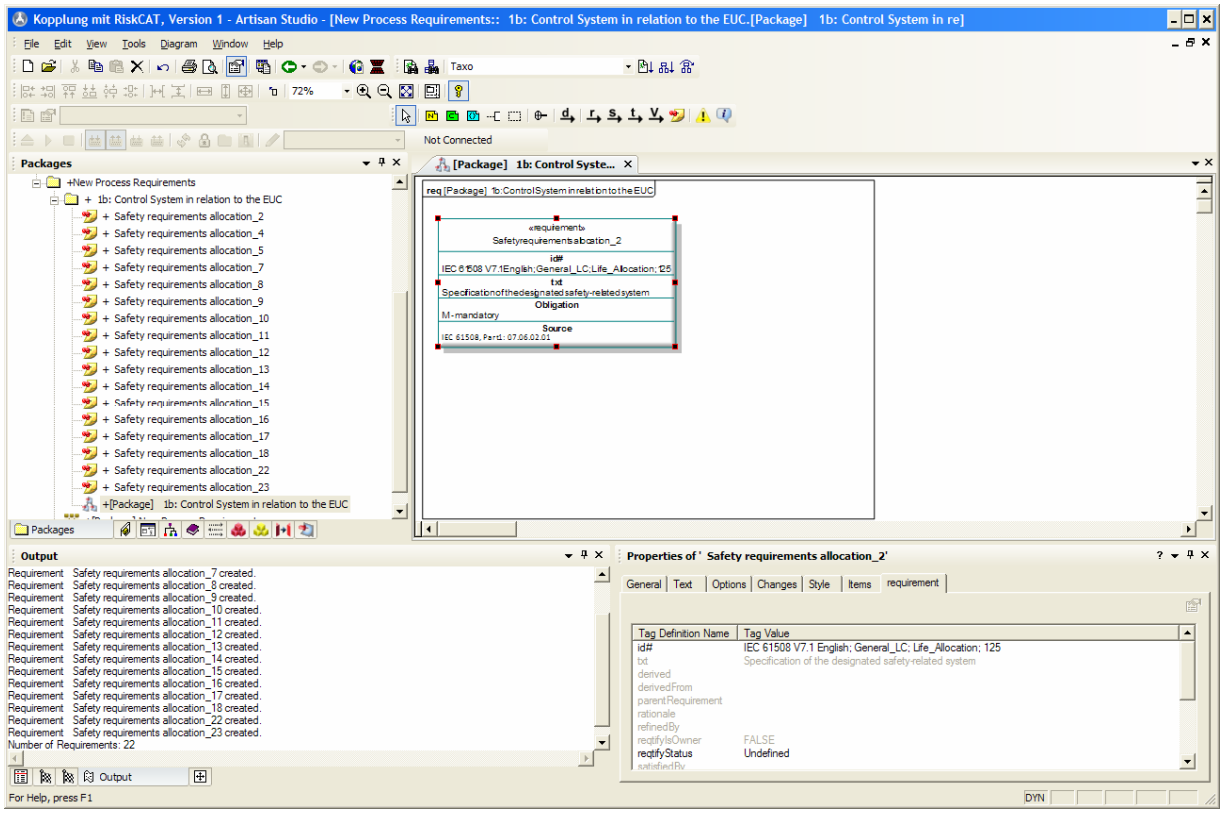


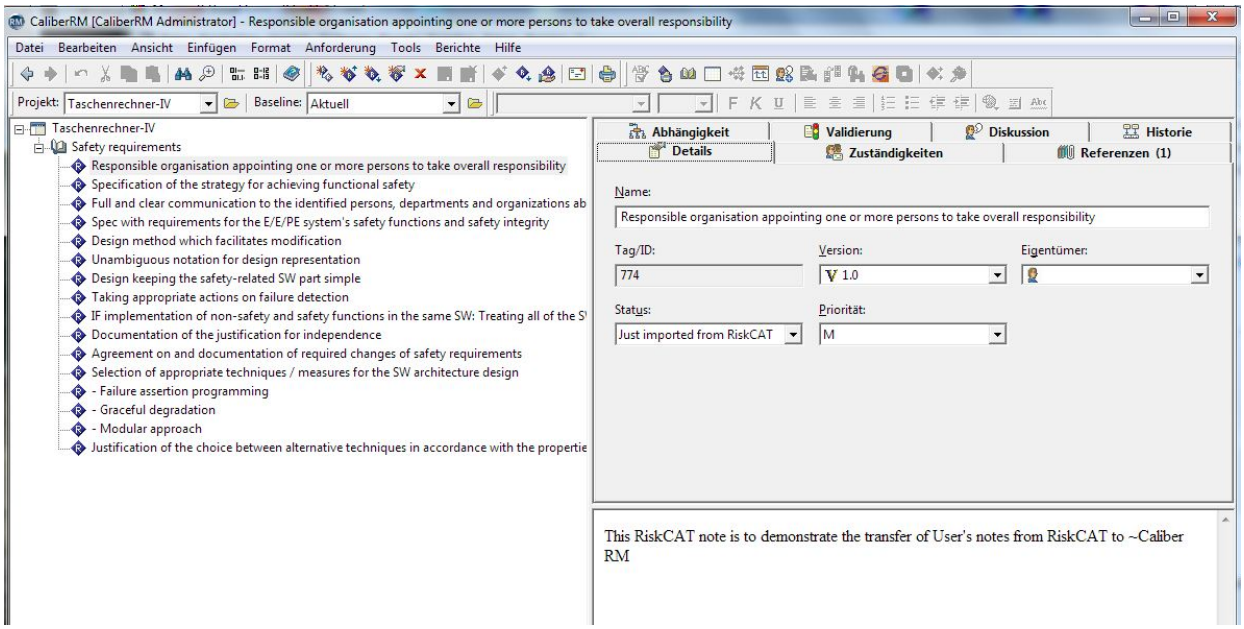
The left column numbers in the left window give the quality targets. These targets are calculated e.g. from the Safety Integrity Level (SIL) and the degree of obligation.

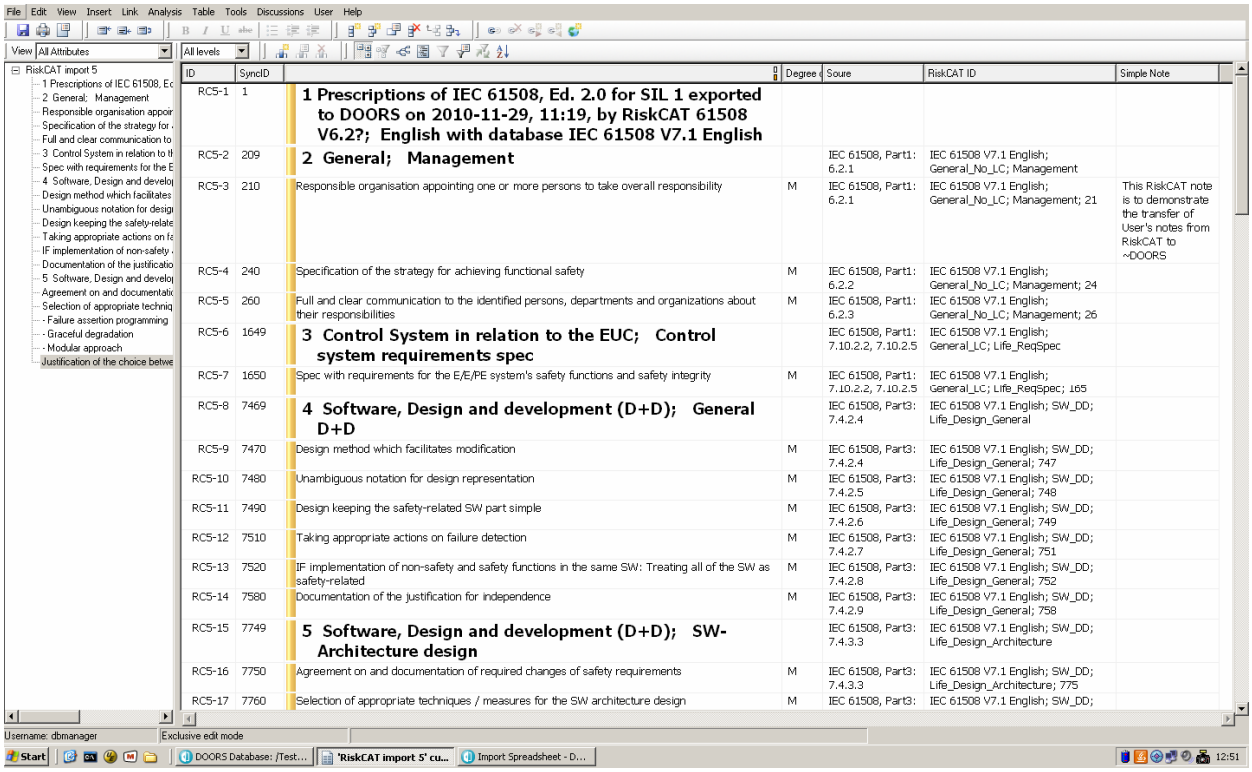
The right column number present the achieved quality which is calculated from test or

assessment results and the degree of obligation of the respective prescription.

The figures below illustrate the import from RiskCAT interface data by Artisan Studio, Caliber RM, DOORS, and IRQA.







Code	Name	Degree ...	RiskCAT Ex...	Source	Simple Note
EN50128_A0003 (59)	Design and development (D+D)				
EN50128_T0303 (4)	SW design and implementation				
EN50128_T0304 (34)	SW design and implementation; techniques				
EN50128_0500 (33)	Choice of a suitable set of techniques for SW...	M	SWSIL 2	IEC 62279: Table A.4	
EN50128_0501	> Formal Methods including for example CC...	R	SWSIL 2	IEC 62279: Table A.4.1	Although it's just recommended we should take special care on this.
EN50128_0502	> Semi-Formal Methods [is detailed in the Ri...	HR	SWSIL 2	IEC 62279: Table A.4.2	
EN50128_0503	> Structured Methodology including for exa...	HR	SWSIL 2	IEC 62279: Table A.4.3	
EN50128_0504	> Modular Approach	M	SWSIL 2	IEC 62279: Table A.4.4	
EN50128_0505 (5)	> Choice of a suitable set of techniques for ...	M	SWSIL 2	IEC 62279: Table A.4 / Table A.20	
EN50128_0506	>> Module Size Limited	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.20.1	
EN50128_0507	>> Information Hiding/Encapsulation	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.20.2	
EN50128_0508	>> Parameter Number Limit	R	SWSIL 2	IEC 62279: Table A.4 / Table A.20.3	Not important to us.
EN50128_0509	>> One Entry/One Exit Point in Subroutines ...	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.20.4	
EN50128_0510	>> Fully Defined Interface	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.20.5	
EN50128_0511	> Design and Coding Standards	HR	SWSIL 2	IEC 62279: Table A.4.5	
EN50128_0512 (7)	> Choice of a suitable set of techniques for ...	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.12	
EN50128_0513	>> Coding Standard Exists	HR	SWSIL 2	IEC 62279: Table A.4 / Table A.12.1	

Tools of the RiskCAT family

Standard	Tool	Language of User Interface, User Manual, and Help	
		English	German
The Basic Standard			
IEC / DIN EN 61508	RiskCAT 61508	✓	✓
Process Industries			
DIN EN 61511	RiskCAT 61511	---	✓
Railways			
IEC 62279 / DIN EN 50128	RiskCAT 50128	✓	✓
DIN EN 50129	RiskCAT 50129	✓	✓
Nuclear			
IEC 60880 : 2006	RiskCAT 60880	✓	---
IEC 61513	RiskCAT 61513	✓	---
IEC 62138	RiskCAT 62138	✓	---
IEEE 323	RiskCAT IEEE323	✓	---
IEEE 344	RiskCAT IEEE344	✓	---
IEEE 387	RiskCAT IEEE387	✓	---
IEEE 7-4.3.2	RiskCAT IEEE7432	✓	---
YVL 5.5	RiskCAT YVL 5.5	✓	---
RCC-E, Section C5000	RiskCAT R5000	✓	---
Machinery			
DIN EN ISO 13849	RiskCAT 13849	---	✓
IEC 62061	RiskCAT 62061 (planned)	✓	---
Automotive			
ISO 25119	RiskCAT 25119 (planned)	✓	---
ISO FDIS 26262	RiskCAT 26262	✓	---
Customer Standards			
According to user's choice, time, and competence	RiskCAT Customer	✓	✓

Back ups

For saving and reproducibility of the results achieved with RiskCAT we suggest to back up the project files and the history file related to the project.

Maintenance

Besides warranty CATS offers

- maintenance and
- upgrading.

Maintenance is on improvement of the CATS tools themselves. It includes those new tool versions created to improve the tool capabilities. Examples are improvements in the human machine interface or improvements with respect to keywords in the database.

Upgrading is on adoption of RiskCATs to revised standards. Examples are the adoption from IEC 61508 Edition 1 to Edition *2.0* or from ISO DIS 26262 to ISO *F*DIS 26262.

Quality Assurance for RiskCATs

RiskCAT consists of two mayor components which are

- the **tool** providing the interface to the user and
- the **database** representing the contents of the considered standard, e. g. IEC 61508.

All parts (units) of the **tool** except those for determination of the necessary SIL are general for the whole series of RiskCATs.

A thorough testing of the first tools of this series which have been RiskCAT 61508 V 1.x and RiskCAT 61508 V 3.x took place by CATS by a person independent from the development in March 2000 (V1.0) and June 2001 (V3.0). Since then each version is checked by a short regression test by CATS by a person independent from the development.

From the users of the RiskCATs series of tools we get few complaints. However, those we get are used to improve all tools of the series.

All **databases** are created by CATS in a way such that CATS may reproduce on demand the relation from the standard clauses to the database and vice versa.

The tracing from the database to the standard is feasible for the RiskCAT customers as well. The RiskCAT function “Prerequisite in the standard” which is available for each prerequisite contained in the database may be used for this purpose.

IEC 61508 database

Each data set of the initial database for IEC 61508 (English) has been validated by CATS by a person independent from the development.

Creating the RiskCAT 61508 V5 databases (English as well as German) the database developer made a complete check of the databases with respect to the related standard.

From the users of RiskCAT 61508 we get very few complaints with respect to the database. However, those we get are used to improve the English database as well as the German one.

2004 the German working group concerned with the automotive sector standard based on IEC 61508 (VDA FAKRA AA-I3 AK16) started to use **RiskCAT 61508** for its work which has been introduced to the ISO TC22 SC3 WG16 project on ISO 26262. No incompleteness or inconsistency of RiskCAT has been recognized during all of this work.

EN 5012x databases

Each data set of the initial database for EN 50126, EN 50128 as well as EN 50129 (German) has been validated by CATS by a person independent from the development.

RiskCAT xxxxx — Data Sheet

Program name	RiskCAT xxxxx
Program version	6.2x
Program size	between 4 MByte and 5 MByte depending on the forms for determination of the necessary quality and on the databases used
Programming Environment	DELPHI 2006
Hardware	PC
Operating system	®WINDOWS; Execution as administrator is required.
Main memory	128 MByte; 32 MByte available for RiskCAT
Mass store	20 MByte free disk space
Video subsystem	Screen resolution 1280 x 1024 or higher
Language of screens, supported standard, help and user manual:	
• **for the English versions**	English
• **for the German versions**	German
License types	RiskCAT licenses are provided as “Stick bounded license” or as “Server based license”

Additional third party software supplied on RiskCAT USB memory stick:

- XpdfViewer™ ActiveX Control; Version 3.0 or a newer one
- pdf files of the standards supported by the actual RiskCAT

Obligatory software not supplied on the RiskCAT USB memory stick:

- text processor to read the user’s manual which is in pdf format

Optional software not supplied on the RiskCAT USB memory stick:

- text processor to process RiskCAT’s text and rich text format (RTF) result files
- tools as Artisan Studio™, CaliberRM™, DOORS® or IRQA

Options included in RiskCAT at extra expense:

- modules for requirements comparison between different standards
- export interfaces for export to Artisan Studio™, CaliberRM™, DOORS® and / or IRQA

Abbreviations

AK	Arbeitskreis
CATS	Code Analyzer Tool Set
DIN	Deutsches Institut für Normung
DKE	Deutsche Kommission Elektrotechnik Elektronik und Informationstechnik im DIN und VDE
FAKRA	Normenausschuss Kraftfahrzeuge im DIN
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PC	Personal Computer
RTF	Rich Text Format
SIL	Safety integrity level
TC	Technical Committee
USB	Universal Serial Bus
VDA	Verband der Automobilindustrie
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
V&V	Verification & Validation
WG	Working Group

For information about CATS tools please contact

- info@cats-tools.de

or

- CATS Software Tools GmbH
  Günter Glöe
  Koboldweg 36
  21077 Hamburg
  Germany