

RiskCAT 61508 V5, Normal Version
Product Description

07. October 2006



RiskCAT

Requirements Derivation from ***Risk*** Classes

a Tool of the

Code ***A***nalyzer ***T***ool Set

Product Description

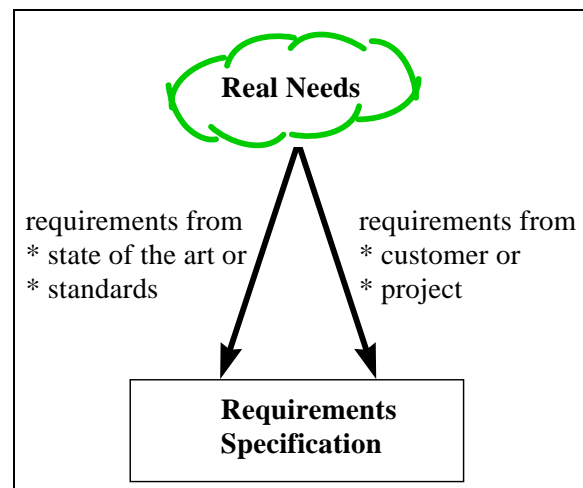
Günter Glöe & Ernst-Ulrich Mainka, Hamburg

List of Contents

Short description of RiskCAT	1
Application Area of RiskCAT.....	5
RiskCAT Components	5
Input to RiskCAT	5
Result data of RiskCAT	6
Usage of RiskCAT Results with other Tools.....	6
Quality Assurance for RiskCAT.....	7
RiskCAT for IEC 61508 — English Version — Data Sheet	8
RiskCAT for IEC 61508 — German Version — Data Sheet.....	9
Abbreviations.....	10

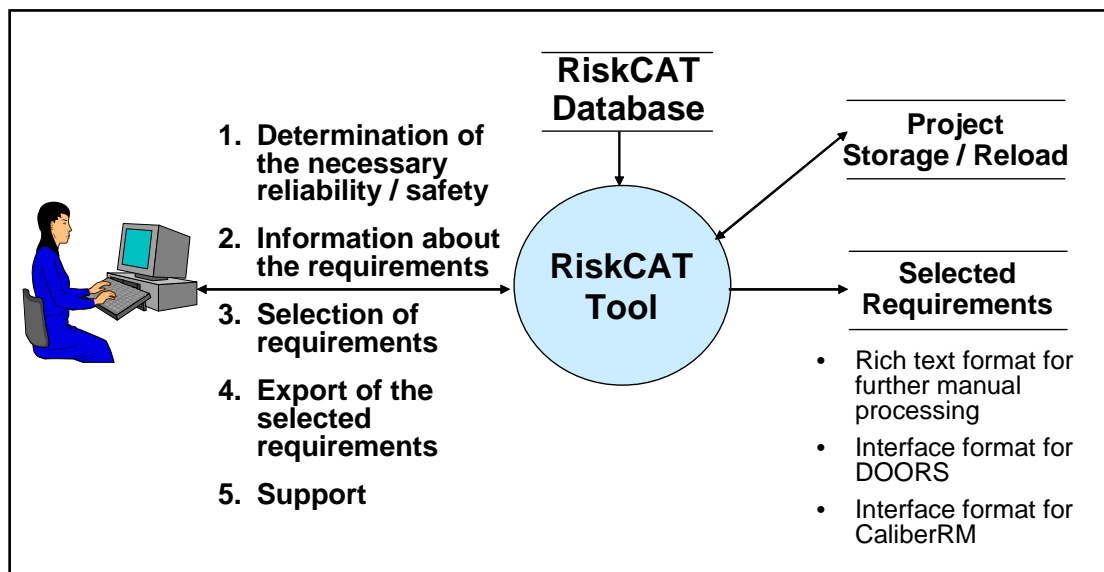
Short description of RiskCAT

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 requirements imposed on software by the state of the art represented e.g. by national or international standards.



RiskCAT is a tool 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.

The design of RiskCAT is modular and widely configurable. It is possible to adopt the tool to modifications and enhancements of the standards applied as well as the extension to alternative standards or other technical rules.



RiskCAT supports

- the determination of the necessary Safety Integrity Level (SIL)
- information about the measures required by IEC 61508
- selection of those measures relevant for the actual step of work
- the export of the selected measures for further work

Besides this RiskCAT offers some support functions.

The work tasks assisted by RiskCAT are:

1. Necessary Safety Integrity Level (SIL)

- the selection of risk parameters,
- the evaluation of risk classes based on the risk parameters selected,
- manual pre-selection of risk class.

2. Information about measures

- the structured overview on the recommended measures,
- retrieval in parts 1 to 4 and 7 of the original standard,
- the context related presentation of the original standards clause,
- the context related presentation of explanations to the clause given in IEC 61508 itself,
- the context related presentation of terms used in the measure texts given in IEC 61508, part 4.

3. Selection of measures

- the selection of individual measures,
- the selection of groups of measures according to the degree of obligation,

- the selection of measures related to documents¹,
- the selection of measures related to activities (life cycle phases)²,
- the selection of measures related to key words.

4. Export

- the result storage as text file (Rich Text Format, RTF) consisting of
 - selected risk parameters and risk class,
 - selected measures and the notes related to the selected measures, e.g. to create checklists or test plans
- the result export to DOORS (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”).

5. Support function

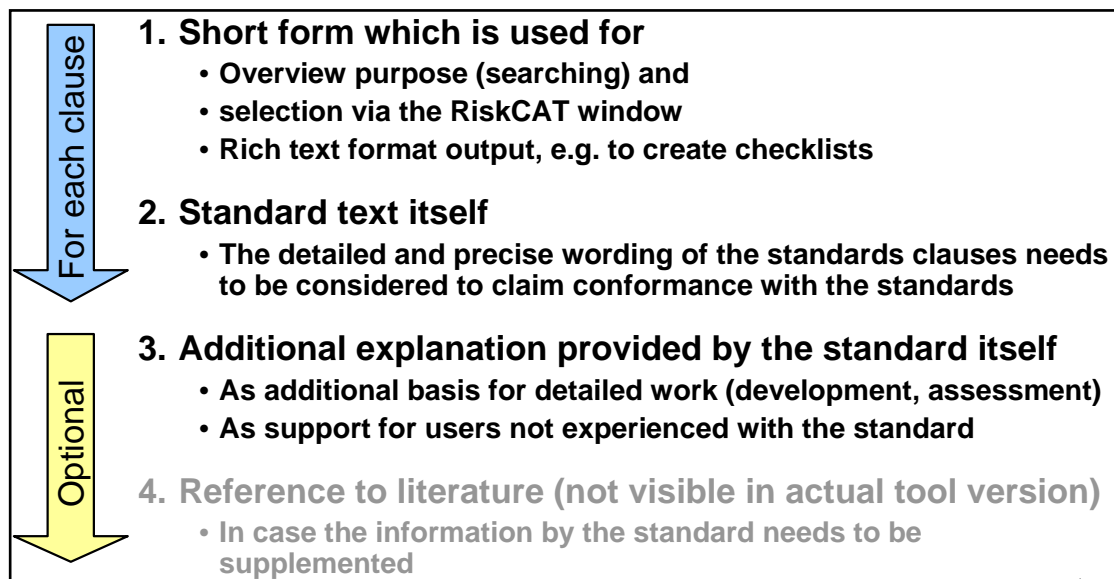
- the possibility to edit notes for each individual measure,
- the copy function for actually marked measure into the clipboard,
- the copy function from standards into the clipboard,
- the storage of measure profiles as project or company templates in a project file (project storage),
- the reloading of measure profiles.

Important advantage of the tool supported approach is the possibility to vary interactively risk parameters, risk classes and sets of process and realization measures defining alternative or optimized sets of measures 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.

¹ The set of documents used is based on Tables A.1 to A.3 of IEC 61508, Part 1

² The set of life cycle phases used is based on Tables A.1 to A.3 of IEC 61508, Part 1



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 requirements available from IEC 61508 for high quality software and high quality software production
- to support retrieval in the standard
- to assist in identification of the requirements to be applied in development
- to produce checklists for the purpose of quality control
- to provide a means for
 - company specific templates of prescribed measures as well as
 - company specific interpretations of measures

RiskCAT Components

The RiskCAT components are:

- The executable runtime image RiskCAT_V5x.exe,
- The help file RiskCAT_V5x.hlp,
- XpdfViewer™ ActiveX Control, and
- IEC 61508 parts 1, 2, 3, 4 and 7
(protected by pass word and to be used together with RiskCAT only)

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

By contract with the German Chapter of the IEC (DKE) CATS has been asked to declare with RiskCAT³:

„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 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“

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.

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

Result data of RiskCAT

Besides interactive results already mentioned above in the short description, RiskCAT V5 produces

- project files (on demand) and
- text result files (rtf format). An example for a (very short) result from an IEC 61508 session is given below. To produce the figure few editing work took place.

IEC 61508 results		
Risk parameters: <ul style="list-style-type: none"> • Consequences: <i>Death to several people</i> • Frequency of, and exposure time in, the hazardous zone: <i>Frequent to permanent exposure in the hazardous zone</i> • Possibility of avoiding the hazardous event: <i>Possible under certain conditions</i> • Possibility of the unwanted occurrence: <i>A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely</i> 		
Safety Integrity Level: 3; Value is valid		
Measures selected:		
Requirement	Reference	Comment
Detailed SW architecture design description	IEC 61508, Part1: 7.4.3.2	
Fault detection and diagnosis	IEC 61508, Part1: 7.4.3 / Table A.2	
Error detecting and correcting codes	IEC 61508, Part1: 7.4.3 / Table A.2	
Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	IEC 61508, Part1: 7.4.3 / Table A.2	Actual choice is SADT.

Usage of RiskCAT Results with other Tools

The “RiskCAT Interfaces to Requirements Management Tools” offers to export the measures actually selected to the requirements management tools DOORS® (by Telelogic AB) as well as CaliberRM™ (by Borland Software Corporation). The “RiskCAT Interfaces to Requirements Management Tools” are a package of its own and need an extra licence.

Quality Assurance for RiskCAT

RiskCAT consists of two mayor components which are

- the **tool** providing the interface to the user and
- the **database** representing the contents of the IEC 61508.

Most parts (units) of the **tool** are general for the series of RiskCATs consisting besides RiskCAT 61508 e.g. of RiskCAT 61511, RiskCAT 50128, RiskCAT 50129 as well as RiskCAT Nuclear.

A thorough testing of the first tools of this series which have been RiskCAT 61508 V1.x and RiskCAT 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.

The **database** has been 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 “context related presentation of the original standards clause” which is available for each requirement contained in the database may be used for this purpose.

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.

RiskCAT for IEC 61508 — English Version — Data Sheet

Program name	RiskCAT 61508
Program version	5
Program size	about 1,6 MByte
Hardware	PC
Operating system	®WINDOWS 2000, ®WINDOWS NT, ®WINDOWS XP
Main memory	128 MByte; 32 MByte available for RiskCAT
Mass store	20 MByte free disk space
Video subsystem	Screen resolution 1024 x 768 or higher
Language of screens, help and user manual	English

Additional third party software supplied on RiskCAT USB memory stick:

- XpdfViewer™ ActiveX Control; Version 3.0 or a newer one
- pdf files of IEC 61508, parts 1, 2, 3, 4 and 7. To improve readability of the standard the French language pages have been deleted. (These pdf files are protected by pass words. They are for usage with RiskCAT only.)

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 rich text format (RTF) export
- tools for requirements capturing as DOORS® or CaliberRM™
- scripts to interface with development environments as Real-time Studio®

RiskCAT for IEC 61508 — German Version — Data Sheet

Program name	RiskCAT 61508
Program version	5
Program size	about 2,6 MByte
Hardware	PC
Operating system	WINDOWS® 2000, WINDOWS® NT, WINDOWS® XP
Main memory	128 MByte; 32 MByte available for RiskCAT
Mass store	20 MByte free disk space
Video subsystem	Screen resolution 1024 x 768 or higher
Language of screens, help and user manual	German

Additional third party software supplied on RiskCAT USB memory stick:

- XpdfViewer™ ActiveX Control; Version 3.0 or a newer one
- pdf files of DIN EN 61508, parts 1, 2, 3, 4 and 7. (These pdf files are protected by pass words. They are for usage with RiskCAT only.)

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 rich text format (RTF) export
- tools for requirements capturing as DOORS® or CaliberRM™
- scripts to interface with development environments as Real-time Studio®

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
RiskCAT	Requirements Derivation from Risk Classes, a Tool of the Code Analyzer Tool Set
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
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