RiskCAT Nuclear

Requirements derivation from Risk classes

A Tool of the

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

User's Manual

Günter Glöe & Ernst-Ulrich Mainka, Hamburg
www.cats-tools.de

Contents

Figures

Acknowledgements and trademarks

All trademarks used in this manual are acknowledged.

Windows 9*, NT, 2000 and XP are trademarks of Microsoft

PDF is a trademark of Adobe Corporation USA

XpdfViewer is a trademark of Glyph & Cog.

InstallShield is a trademark of Macrovision Corporation.

DOORS is a trademark of Telelogic AB.

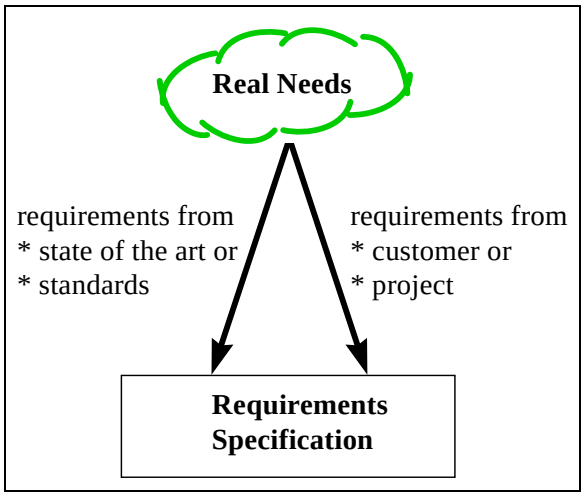
CaliberRM is a trademark of Borland Software Corporation.

CATS Software Tools GmbH would like to thank our UK distributor PhaedruS Systems Ltd for proof reading & editing the English version of this manual. www.phaedsys.org

CATS Software Tools GmbH thanks the DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE and the IEC International Electrotechnical Commission for permission to reproduce extracts from International Standard IEC 61508.

1 Overview

Prerequisite to produce and certify high quality embedded systems including their software is to know about the functional and non functional requirements imposed on the embedded system. These requirements generally result from two different sources. One source is the specific requirements of the customer or producer e.g. based on their applications or marketing strategy. The other sources are the requirements imposed on the embedded system and its 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 development and products in the area of embedded systems and their software. The state of the art in quality of Instrumentation and control for systems important to safety is provided to a large extent by IEC 61513 as well as IEC 62138.

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

The work tasks assisted by RiskCAT Nuclear are:

1. Selection of the functions to be performed,
2. manual pre selection of the category,
3. the structured overview on the recommended measures,
4. the selection of individual measures,
5. the selection of groups of measures according to the degree of obligation,
6. the selection of measures related to documents[1],
7. the selection of measures related to activities (life cycle phases)[2],
8. the selection of measures related to key words,
9. the copy function for actually marked measure into the clipboard,
10. the possibility to edit notes for each individual measure
11. overview on defined terms in the measures texts

[1] The set of documents used is given in Appendix 7.1, "List of Documents"

[2] The set of life cycle phases used is given in Appendix 7.2, "List of Activities"

12. retrieval in the original standards (available only if user has installed pdf files of the concerned standard in the RiskCAT target installation directory),
13. the context related presentation of the original standards clause,
14. the context related presentation of explanations to the clause given by IEC 61513 or IEC 62138 themselves
15. the context related presentation of terms used in the measure texts given in IEC 61513 or IEC 62138 themselves
16. the storage of measure profiles as project or company templates in a project file (project storage),
17. the reloading of measure profiles
18. the result storage as text file (Rich Text Format, RTF) consisting of
    - selected risk parameters,
    - risk class,
    - selected measures and
    - the notes related to the selected measures,
19. the result export to DOORS
    (available only with an "RiskCAT Interface to Requirements Management Tools"),
20. the result export to CaliberRM
    (available only with an "RiskCAT Interface to Requirements Management Tools")

An 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 Nuclear is to assist the user in application of the IEC 61513 as well as IEC 62138. 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.

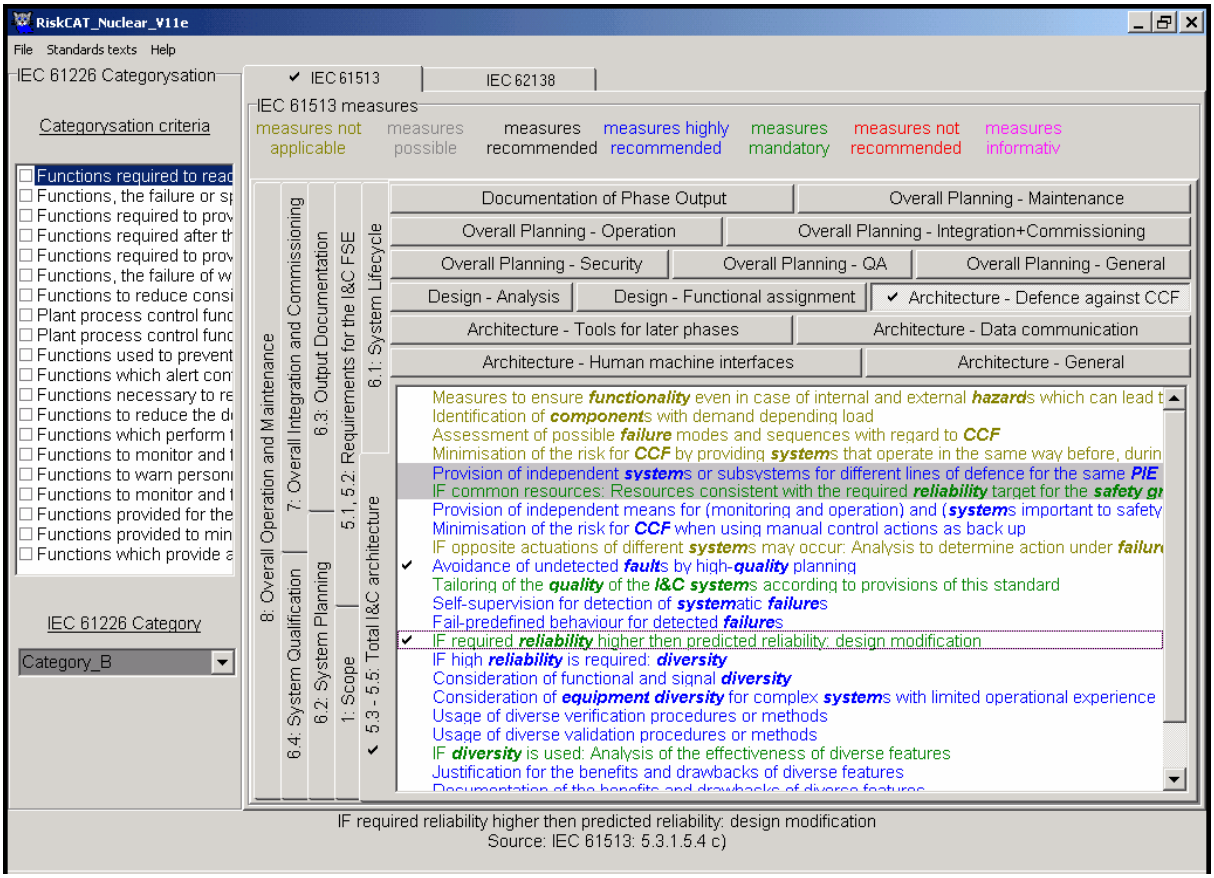


Figure 1: RiskCAT Nuclear screen

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

2 Installation / First Start / Deinstallation

2.1 The components of RiskCAT

RiskCAT is an application for Windows 2000/ NT/ XP®. It is distributed on an **USB memory stick**.

The **USB memory stick** has the following directory structure:

- RiskCAT_Nuclear with the subdirectory
  - XPDF
- Tool_Documentation
- CATS_Information

The directory RiskCAT_Nuclear contains besides other files:

- The RiskCAT executable **RiskCAT_Nuclear_V11e.exe**.
- The help file **RiskCAT_Nuclear_V11e.hlp**.
- The help content file RiskCAT_Nuclear_V11e.cnt.
- The standard files
  - IEC61226_GB_1.pdf
  - IEC61513_GB_1.pdf
  - IEC62138_GB_1.pdf

The subdirectory XPDF of directory RiskCAT_Nuclear contains:

- The XpdfViewer™ ActiveX Control, Version 3.0, **XpdfViewerCtrl.ocx**.

The sub-subdirectory t1fonts in the subdirectory XPDF contains

- the fonts needed by the XpdfViewer

The directory Tool_Documentation contains:

- This user manual **RiskCAT_Nuclear_UserManual_11e.pdf**

The directory CATS_Information contains:

- The product description **RiskCAT_61508_V5_Product_4.pdf**
- The product description **RiskCAT_50128_V411_Product.pdf**
- The description of the Static Analyzers of the Code Analyzer Tool Set, Overview and Motivation, **StaticAnalyzers_5.pdf**.

Because of licensing conditions the standard files

- IEC61226_GB_1.pdf,
- IEC61513_GB_1.pdf and
- IEC62138_GB_1.pdf

are for use with RiskCAT only.

2.2 Local Operation on a PC

RiskCAT Nuclear does not need any installation. Just run the executable file RiskCAT_Nuclear_V11e.exe from the directory RiskCAT Nuclear on the USB memory stick.

CAUTION: The execution of **RiskCAT_Nuclear_V11e** is possible only from the original USB memory stick. For backup purpose the stick contents may be copied to any backup device. However, RiskCAT_Nuclear_V11e will operate from the memory stick only.

CAUTION: The first execution of **RiskCAT_Nuclear_V11e** will install the XpdfViewer™ ActiveX Control, Version 3.0, on the local PC. In case of version conflicts with a XpdfViewer already installed please contact CATS via info@cats-tools.de.

2.3 Uninstallation on a local PC

As RiskCAT Nuclear does not need any installation so it does neither need any uninstallation.

Uninstallation of XpdfViewer is accomplished by running WINDOWS-System-Control > Software > Installation/Uninstallation > selecting the XpdfViewer control.

2.4 Network Installation of RiskCAT

RiskCAT offers two different possibilities for network installations:

- You may access RiskCAT_Nuclear_V11e on the CATS USB memory stick network wide or
- you may use a server disk drive based installation. This option needs an extra licence.

For both types of network installation a single RiskCAT executable is relocated on the server USB / disk drive. Additionally one XPDF Viewer is installed on each client.

CAUTION: The number of simultaneous usage is limited by the licensed number of users.

The installation procedure for the two installation types differs.

In case of **CATS USB memory stick usage**

- The stick just needs to be connected to the server and
- the local XPDF-Viewer installation needs to be performed by calling the **XpdfViewerCtrl-3[1].00.04.exe** located in the stick directory XPDF_Installation before the first RiskCAT Nuclear client session is started.

For a **server disk drive based installation**

- The contents of the **CATS USB memory stick** (or of the CATS CD) need to be copied into a suitable RiskCAT target directory on the server disk **or**
- the minimum runtime environment for RiskCAT Nuclear needs to be to installed on the server by running the **Setup.exe** from the root of the USB memory stick (or of the CATS CD). In this case the XPDF subdirectory must be copied manually into the RiskCAT Nuclear target directory created by the Setup.
- As for the USB memory stick usage the local XPDF-Viewer installation needs to be performed by calling the **XpdfViewerCtrl-3[1].00.04.exe** located in the stick directory XPDF_Installation before the first RiskCAT Nuclear client session is started.

Please contact us for further information via info@cats-tools.de.

2.5 Network Uninstallation

The network uninstallation is performed by

- uninstallation of client based XPDF-Viewers by calling **XpdfViewerCtrl-3[1].00.04.exe**

and in case of server disk drive based installations additionally by

- deletion of the RiskCAT Nuclearcomponents copied on the server **or** (in case of having used **Setup.exe** for installation of the minimum runtime environment for RiskCAT Nuclear on the server**)**
- using **WINDOWS system control** or **Setup.exe** to remove the minimum runtime environment for RiskCAT Nuclear from the server.

3 Basics

3.1 Screen parts

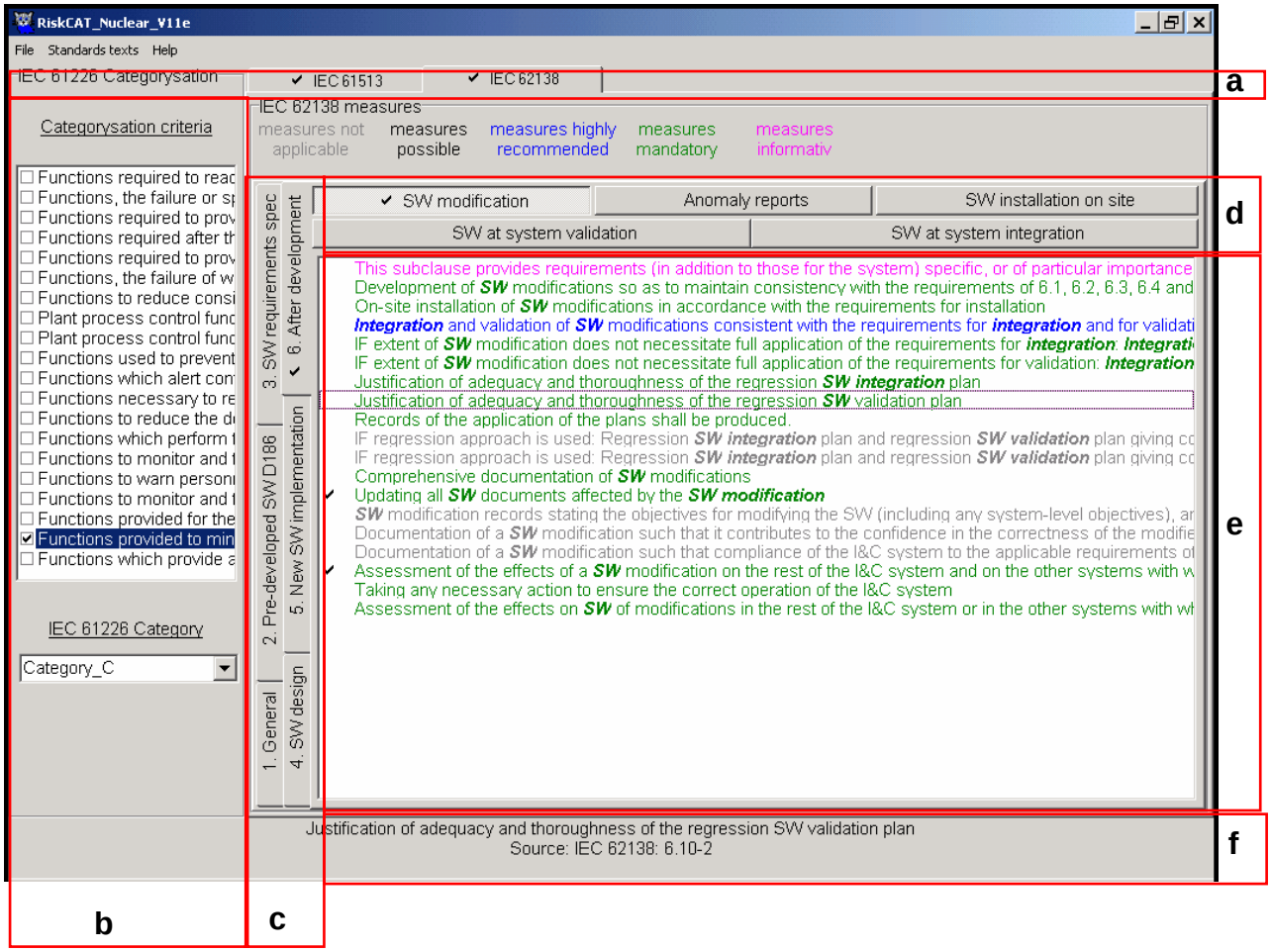


Figure 2: RiskCAT screen parts

a: Standard tabs

b: Risk window

c: Area tabs

d: Topic tabs

e: Measure window

f: Information line

3.2 Interrelationship between the screen parts

The screen parts c, d and e are used to present the measures.

The Safety Integrity Level (SIL) selected in screen part b controls the degree of obligation of the measures given in screen part e.

However, the two screen parts are largely independent from each other. The screen relationship between the measures group (parts c, d & e) and the SIL block on the left may be adjusted. This is accomplished by a single left mouse button click on the boarder line between the screen parts b and c and moving the mouse afterwards

CAUTION: The measures selected in screen part e are consistent with the safety integrity level shown in screen part b only if the RiskCAT usage is according to chapter 4.5, "Selection of groups of measures according to the degree of obligation", of this manual.

3.3 Measure states

RiskCAT applies a three dimensional state to each measure. The three state dimensions are

- marked / unmarked
- selected / deselected
- with comment / without comment

The state "marked" may be assigned to one measure only at any time. Marking of a measure is by a single left mouse button click. It is visible by a box around the text describing the measure.

The state "selected" may be assigned to one, several or even all measures at the same time. Manual election of a measure is by a single left mouse button click. It is visible by a tick ✓ left of the text describing the measure. Automatic selection is discussed later in this manual (see chapters 4.5, "Selection of groups of measures according to the degree of obligation", to 4.8, "Selection of measures related to key words").

The state "with comment" may be assigned to one, several or even all measures at the same time. Adding comments to a measure is via context menu (depress of right mouse button) in the measure list boxes. It is visible by a  left of the text describing the measure.

3.4 Measure colours

The measures in screen part "e" are dynamically coloured depending on their level, Not applicable (olive), Possible (grey), Recommended (black), Highly recommended (red), Mandatory (green), NOT recommended (red) and informative (pink) as indicated by the SIL selected in screen area "b".

CAUTION: The screen shown in Figure 2 has all levels, Recommended, Highly recommended, Mandatory, NOT recommended and informative. All users who may be colour blind should go to "7. Software, Design and development (D+D)" and Tab "SW-Architecture" and set the SIL to 3. Then select in turn each of the measure settings to get the check mark ✓ by the relevant measures.

3.5 Structure of the measures presentation used with RiskCAT

RiskCAT starts from standards. So the original sets of measures are the **standards** represented by the standard tabs (marked with "a" in Figure 2).

A standard may consist of different parts as e.g. IEC 61508 has 7 parts. The standard or even its parts may be such voluminous that it is not appropriate to use all measures as an entity. This has been the reason to break down some standards into **areas** represented by the area tabs (marked with "c" in Figure 2). Depending on the standard an area may consist of a part of a standard, some clauses of a standard or some clauses of a part of a standard. For details see the standard specific descriptions in this manual.

Most standards cover a variety of **topics** represented by the topic tabs (marked with "d" in Figure 2). The approach has been to have an assignment between standards chapters and RiskCAT topics. However, in some cases standard chapters have been further split up, because of a high number of measures or because of different matters covered in the same chapter.

A further structuring is by grey shaded areas in the measure window. This presentation indicates that the marked requirements are alternatives to each other.

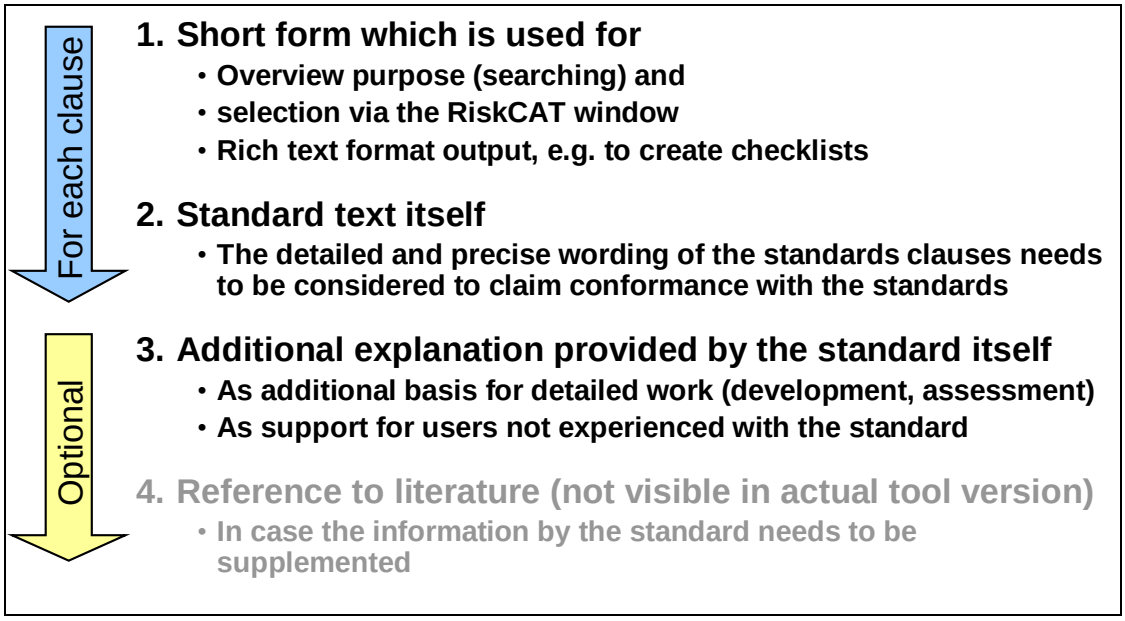
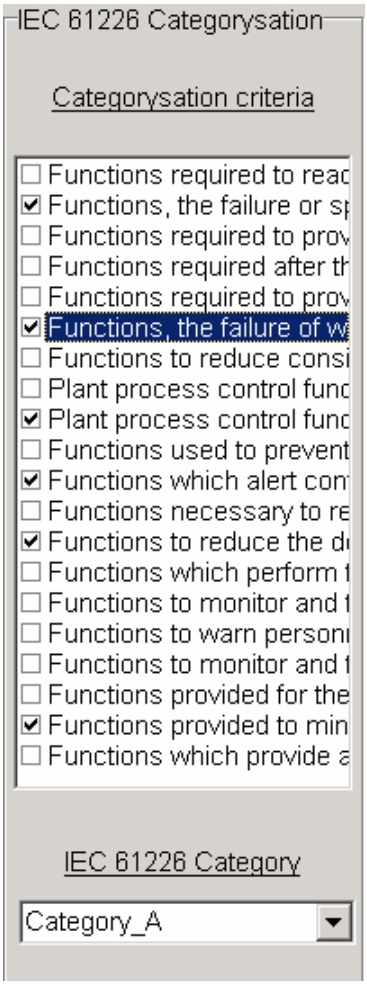


Figure 3: Presentation of the standard clauses in four levels

4 Tasks



4.1 Selection of the functions to be performed

The categorisation of the functions to be performed by the I&C system and its software is based on IEC 61226.

It is by selection of the function to be performed. Several functions may be selected in parallel.

The resulting category is the maximum of the categories of the selected functions.

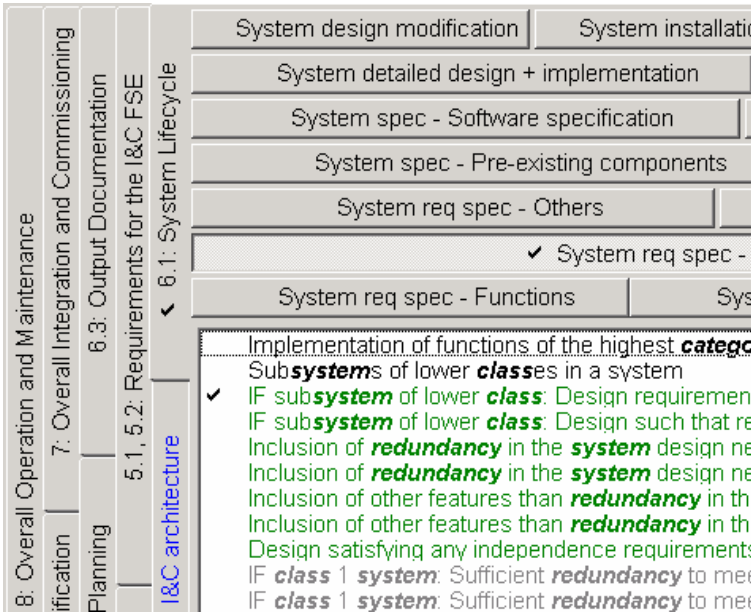
4.2 Manual pre selection of the category

The category applied to the measures can be modified directly and independently from selection of the functions by using the up/down switches of the IEC 61226 Category control. In this case the background for the category is greyed to indicate there is a mismatch between the category used and the selected functions.

4.3 Structured overview on the recommended measures

Each of the area tabs represents an important theme within the scope of embedded controllers and their software. And each of the topic tabs represents a coherent set of measures. Just by selection of corresponding tabs RiskCAT provides an overview about the measures with respect to the topic given as tab text.

4.4 Selection of individual measures

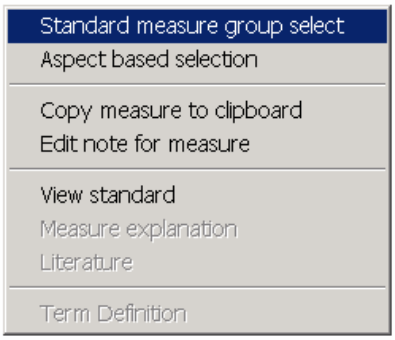


Individual measures are selected / deselected by a double click with left mouse button. Selection is visible by

- A check mark ✓ to the left of the measure itself
- A check mark ✓ to the left of the corresponding topic tab
- a check mark ✓ to the left of the corresponding area tab

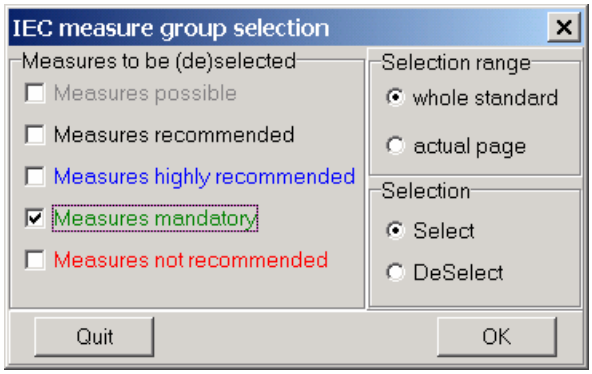
The selection is in addition to already selected measures. If the real interest is just to concentrate on the measures actually selected; precautions need to be applied to de-select any measures that may have been selected previously. See next chapter of this manual for global selection/ de-selection of measures.

4.5 Selection of groups of measures according to the degree of obligation



The selection of groups according to the degree of obligation3, under the currently selected SIL, of the measures is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).

[3] For the degree of obligation please refer as well to chapter 6.1, "Presentation of the degree of obligation of the requirements".



After choice of "Standard measure group selection" the selection form shown on the left appears.

If the "whole standard" is activated the selection will be for all measures in all areas for all topics.

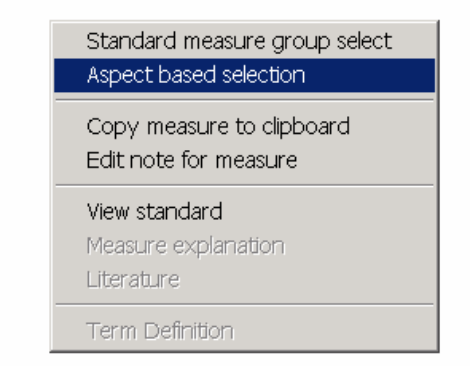
If the "actual page" is activated the selection will be just for the measures in visible topic tab.

The visibility of the selection is same as for individual measures selection.

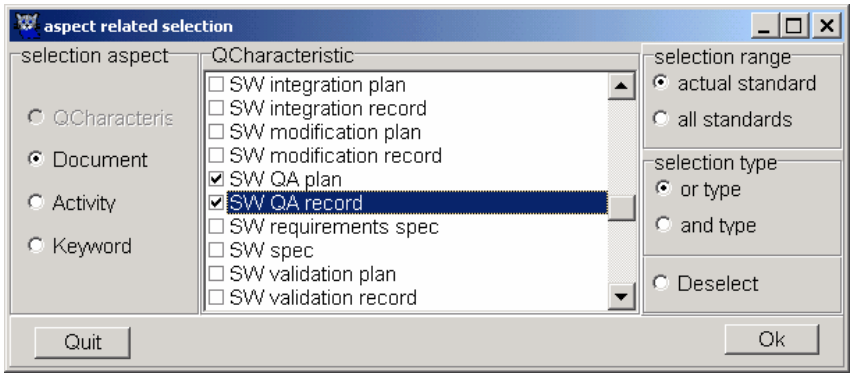
CAUTION: If you change the SIL between group selection and the "DeSelect" the set of deselected measures may be different from the selected set. So here "DeSelect" is only the inverse function to "Select" if SIL is the same for both actions.

The selection is in addition to already selected measures. If the real interest is just to concentrate on the measures you are about to select then precautions need to be applied that at on starting measure selection no measures are already selected.

4.6 Selection of measures related to documents



The document related selection functionality is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).



After choice of "Aspect based selection" the selection form shown on the left appears.

The set of documents is listed in Appendix 7.1 "List of Documents", page 29, of this manual.

Apart from the possibility to select according to the documents list RiskCAT offers selection according to activity (life cycle phase). Of course "documents" and "life cycle phases" are related to each other. However, a phase may result in several documents and on the other hand a document may be used for different phases. Therefore RiskCAT uses documents as well as activities.

If you are interested in a specific selection you should just apply a single document or activity.

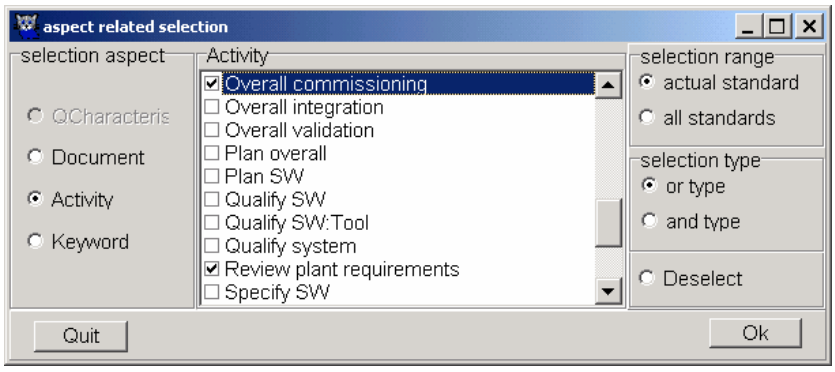
If your interest is to get a complete view you should run two selections after each other:

- In one "or type" selection choose the *document* of your specific interest as well as "All". Terminate it with "Ok".
- In the other "or type" selection choose the *activity* related to the document of your specific interest as well as "All". Terminate it again with "Ok".

The selection is in addition to already selected measures. So precautions need to be applied that at starting no measures are selected.

4.7 Selection of measures related to activities (life cycle phases)

As the with the "document" related selection functionality the "activity" related selection is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).



After choice of "Aspect based selection" the selection form shown on the left appears.

The set of activities is listed in Appendix 7.2, "List of Activities", page 31, of this manual.

The selection is in addition to already selected measures. So precautions need to be applied that at starting no measures are selected.

4.8 Selection of measures related to key words

The "Keyword" related selection functionality is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).

The set of keywords has been created based on work with and discussion about quality of embedded systems and their software by the authors.

The selection is in addition to already selected measures. So precautions need to be applied

that at starting no measures are selected.

4.9 Copying the actually marked measure into the clipboard

The copy to clipboard functionality is activated via context menu in the measure window (screen part "e" in Figure 2).

The steps are:

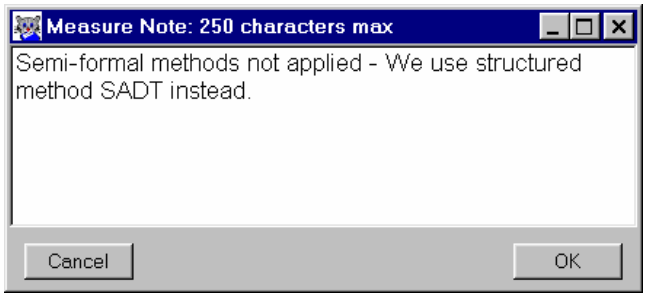
- Mark the measure to be copied by a single left mouse button click. (Otherwise no measure will be found on the clipboard later on.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Copy selected measure to clipboard" to copy contents of the state line
- Use an application with clipboard functionality
- Insert or paste clipboard contents

4.10 Edit notes to the marked measure

Purpose of edit notes is to provide:

- Space for comments on a specific project, e.g. to log the reasoning for not selecting particular measures for the project
- Company specific frames of prescribed measures as well as company specific interpretations of measures
- Log results from audits, reviews, or tests.

The edit measure note functionality is activated via context menu in the measure window.



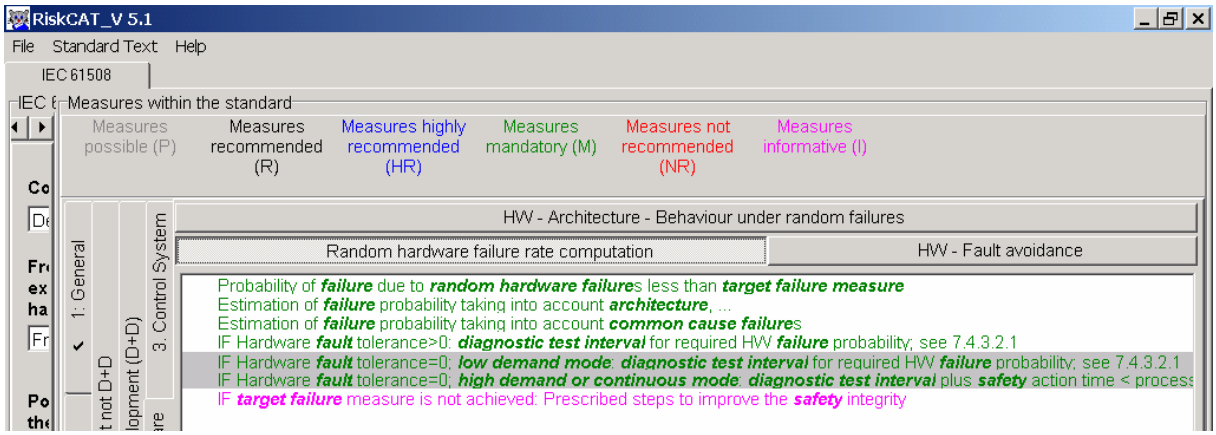
The steps are:

- Mark the measure for which the item note shall be edited by a single left mouse button click. Otherwise nothing visible to the user will occur.
- Activate context menu. Depress right mouse button while the pointer is in the measure window (screen part "e" in Figure 2).
- choose „Edit note for measure"

For looking to existing notes or modifying them choose "Edit note for measure" again. Notes are saved via Project storage (see chapter 4.16, "Project (session) storage in a file" of this manual). They may be reloaded by Project reload.

4.11 Overview on defined terms in the measures texts

As shown in the figure below terms defined in IEC 61513 or IEC 62138 are highlighted in **bold type** in the presentation of the measure texts.

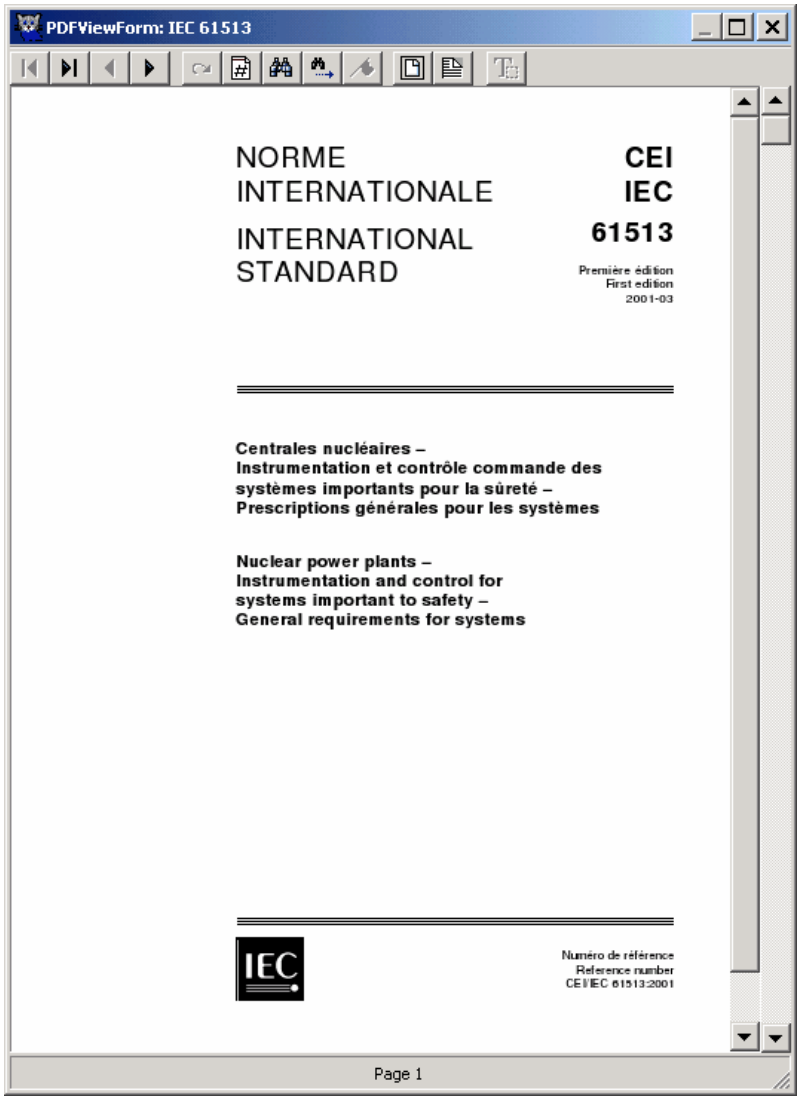


Just scrolling through the measures provides an overview about the defined terms used in the measures texts.

4.12 Retrieval in the original standards

RiskCAT offers an interface for viewing the original standards. For this the XpdfViewer™ XpdfViewerCtrl.ocx library is implemented. Prerequisite for the retrieval is the availability of licensed standard files. With RiskCAT Nuclear IEC 61513 as well as IEC 62138 are available.

Retrieval is started via "Standard Text" menu. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.

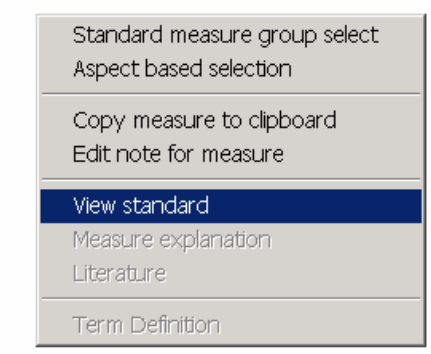


The XpdfViewer™ provides the following functions:

- First page
- Last page
- Previous page
- Next page
- Back to selection
- Go to page
- Find
- Find next
- Add page to hotlist
- Adjust to page height
- Adjust to page width
- Copy text to clipboard

4.13 Context related retrieval in the original standards

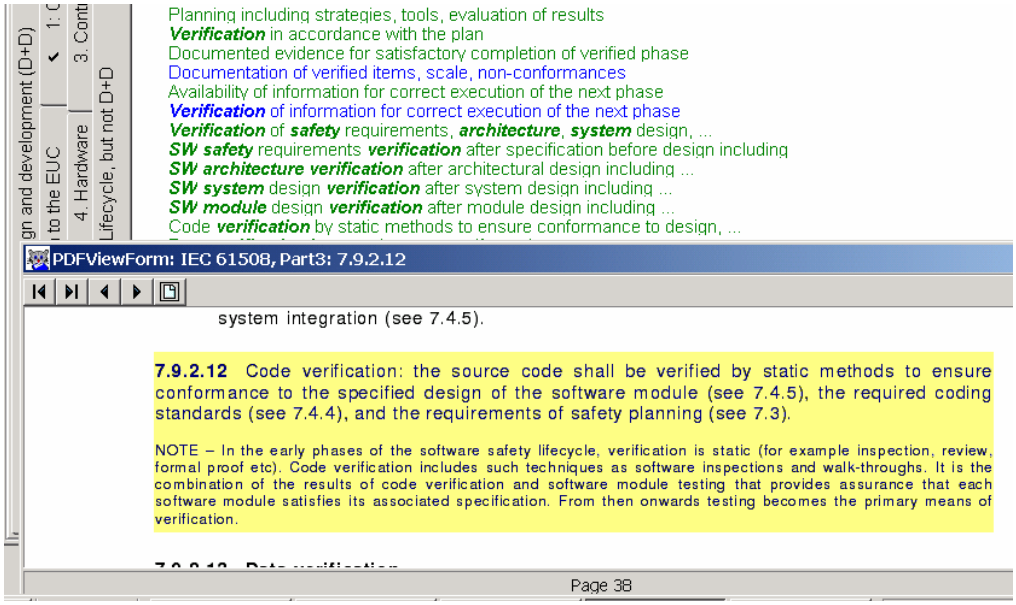
Besides the interface for full text browsing RiskCAT offers an interface for context sensitive browsing in original standards. Again prerequisite for this task is the availability of licensed standard files. With RiskCAT Nuclear IEC 61513 as well as IEC 62138 are available.



The context related retrieval is activated via context menu in the measure window (screen part "e" in Figure 2). The steps are:

- Mark the measure establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "View standard"

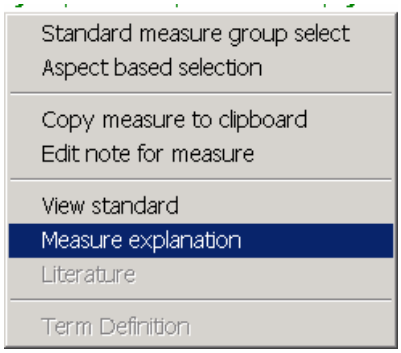
RiskCAT will show the page of the standard highlighting the clause in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it



If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

4.14 The context related presentation of explanations to the clause provided by IEC 61513 or IEC 62138 themselves

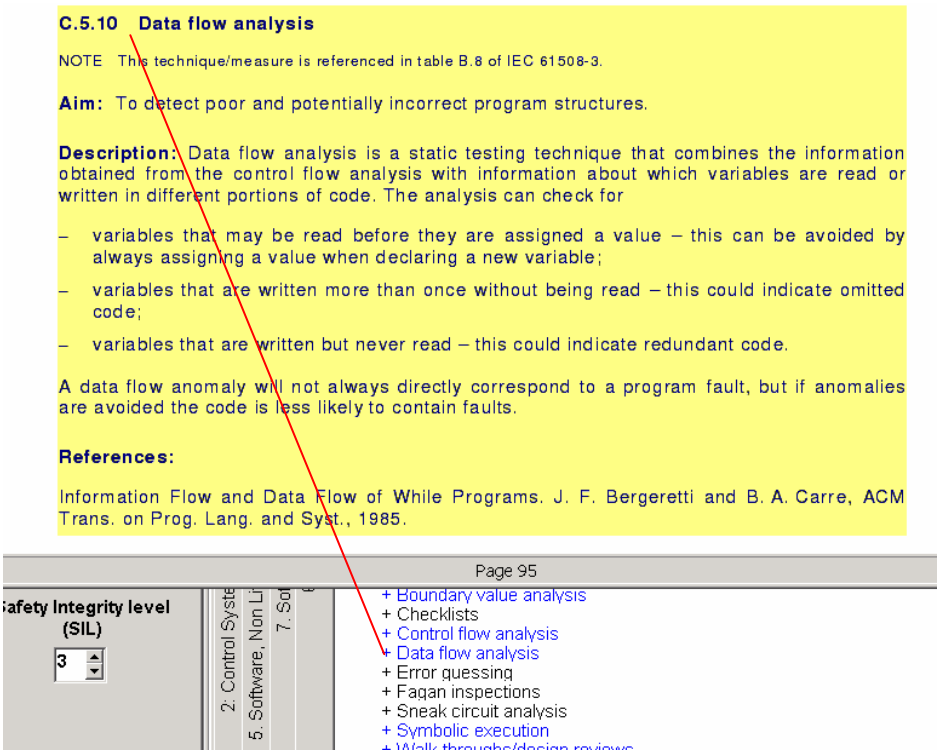
For certain clauses IEC 61513 or IEC 62138 themselves provides additional explanations. RiskCAT offers an interface for context sensitive browsing the explanations from the original standard.



The context related explanation is activated via context menu in the measure window. The steps are:

- Mark the measure establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Measure explanation"

RiskCAT will show the page of the standard highlighting the explanation in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.

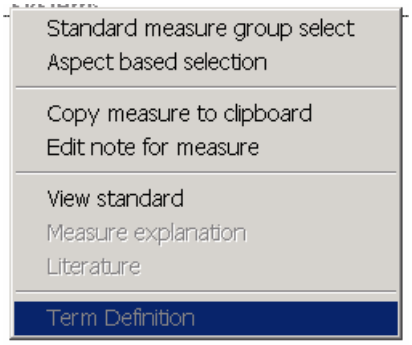


If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools

4.15 The context related presentation of terms used in the measure texts given in IEC 61513 or IEC 62138 themselves

For certain terms IEC 61508 or IEC 62138 themselves provide definitions. RiskCAT offers an interface for context sensitive browsing the definitions from the original standard.

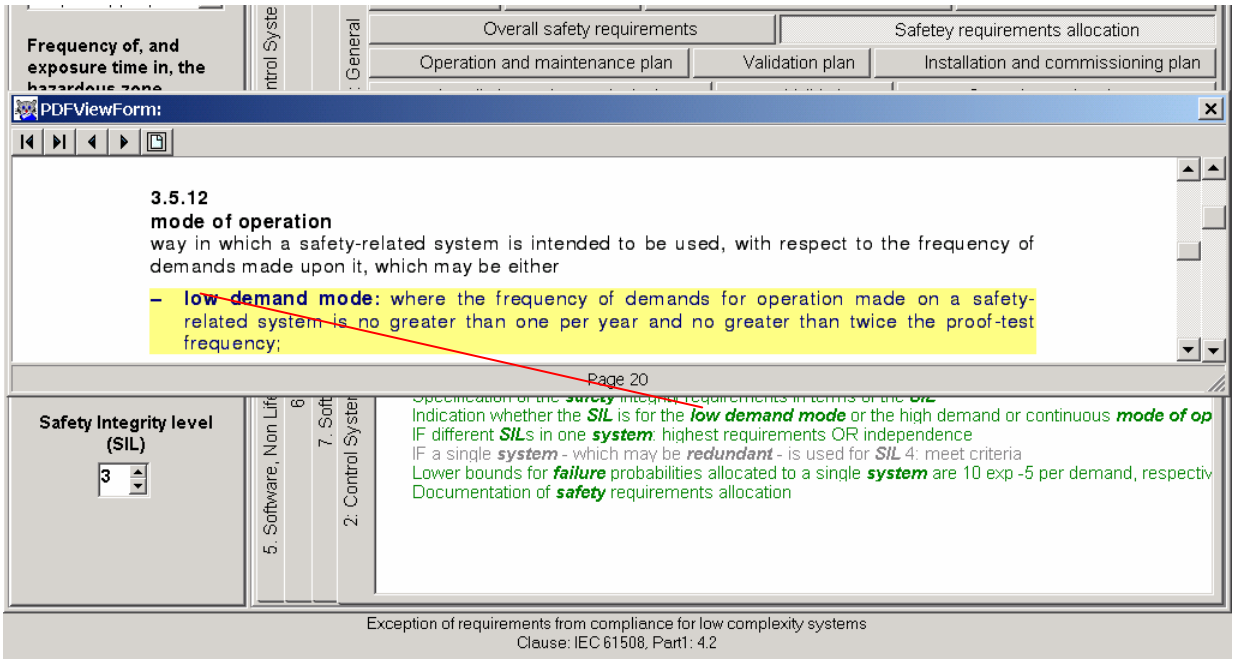
The defined terms used in the measures presentation are presented in bold.



The context related term definition is activated via context menu in the measure window. The steps are:

- Go with the cursor to a defined (**bold**) term. The type of the cursor which normally is ↖ then will change to ☝
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Term Definition"

RiskCAT will show the page of the standard highlighting the definition in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.



If other PDF versions of the standards have been installed than those supplied by CATS, RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

4.16 Project (session) storage in a file

Project storage has two distinct purposes one for the 'normal' user and another for the project leader or the quality manager.

- For the *'normal' user* it offers the possibility to interrupt and resume RiskCAT tool sessions. For this purpose the actual status is stored in binary RiskCAT project files.
- For the *project leader* or the quality manager it offers the possibility to fill in the comments to the measures. Thereby advice may be given to the 'normal' user by which means (e.g. tools, procedures, forms) compliance with the measure shall be achieved in a specific project. If certain measures are not applicable in a specific project or for a specific part of a project background for this may be supplied as comment as well. So the comments result in a company or project specific framework. This framework - or requirements capture - may be stored and used as a starting point by the 'normal' users.

The storage function is chosen by item "Store project" in "File" menu.

4.17 Project (session) reload from a file

- For a new session the framework prepared by the project leader or the quality manager may be loaded.
- An interrupted and stored tool session may be resumed.

The restore function is chosen by item "Load project" in "File" menu.

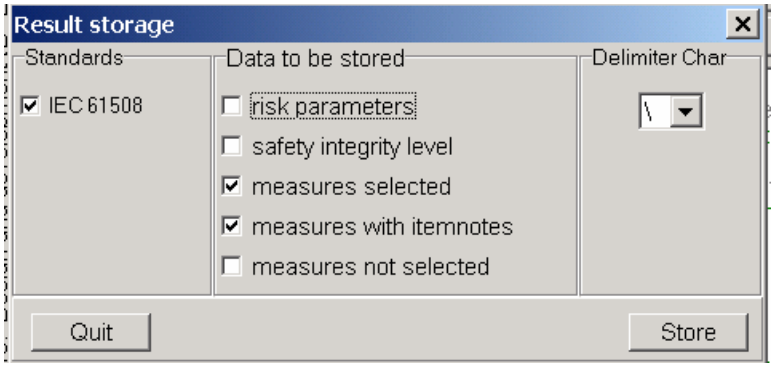
4.18 Result storage as RTF-file

For further documentation, e.g. creation of checklists or test plans, RiskCAT offers storage as text file (Rich Text Format, RTF) of:

- The selected risk parameter,
- The Safety Integrity Level (SIL) as shown in the risk window (that is either the SIL resulting from risk parameters or the manually pre selected one)
- Three sets of measures
    - Measures contained in more than one set are stored once only

For each measure following items are stored

- The measure text (text of the level 1 presentation),
- The reference to the standard as well as to the clause,
- The degree of obligation,
- The note.



Result storage is started via the menu "File". For result storage there are some options given in the menu in a self-explaining manner. The option to select a delimiter character supports an import of the stored data in tables by a text processor.

RiskCAT Nuclear Results

IEC 61226 category: Category_B

Criteria checked:

IEC 61513 measures selected:

IC_Architecture	Design_CCF	Avoidance of undetected faults by high-quality planning	x	M
IC_Architecture	Design_CCF	IF required reliability higher then predicted reliability: design modification	x	P

IEC 62138 measures selected:

Requirements	Content	SW requirements spec stating the SW quality objectives	x	M
Requirements	Content	SW requirements spec stating the constraints to be respected by SW design and implementation because of correctness	x	P

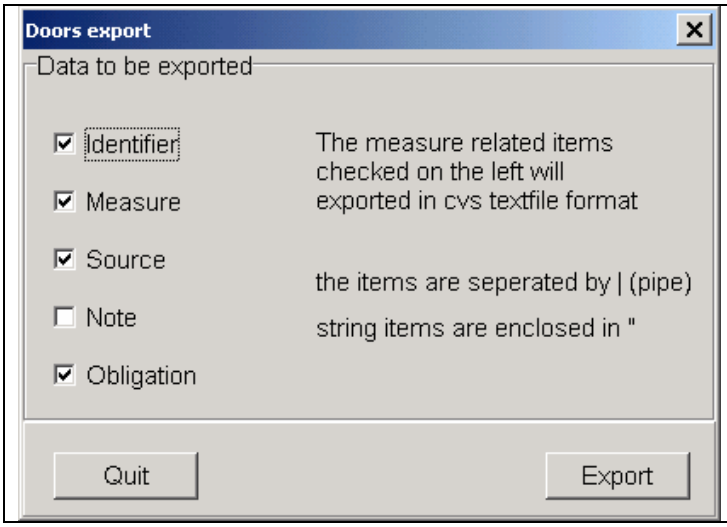
4.19 DOORS export

The "RiskCAT Interfaces to Requirements Management Tools" offer to export the measures actually selected to the requirements management tool DOORS (by Telelogic AB). The "RiskCAT Interfaces to Requirements Management Tools" are a package of its own and need an extra licence.

Export for each selected measure consists of:

- The identifier of the measure
- The measure text (text of the level 1 presentation),
- The reference to part as well as clause of IEC 61508.
- The note the user may have issued with respect to the measure
- The degree of obligation for the measure.

First step to export measures from RiskCAT to DOORS is the selection of the measures to be exported. Then the export itself is started via the menu "File".



For the export itself there are some options given in the menu in a self-explaining manner.

Finally the "Export" button needs to be pushed to choose the name of the export file and to start its generation.

Export of RiskCAT for DOORS is one file:

- "*.cvs" with the information selected on the "Doors export" form.

The import by DOORS is specified in the DOORS user documentation. Please, apply that for the further procedure.

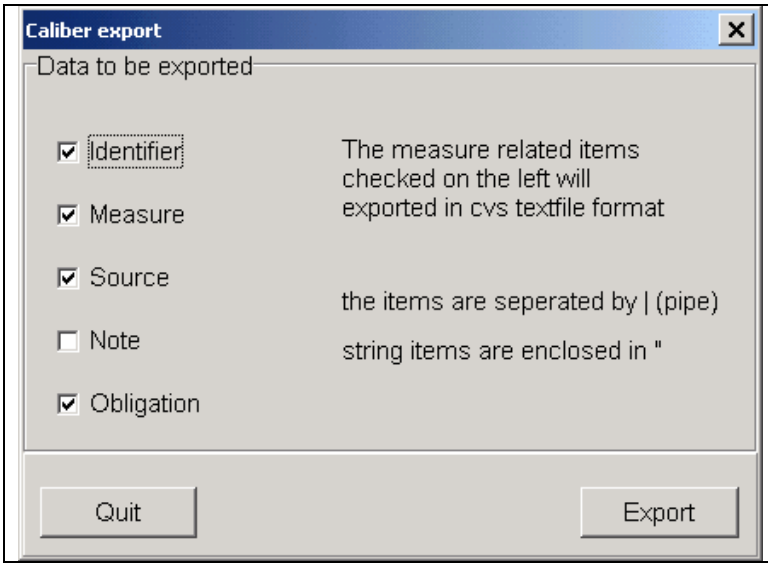
4.20 CaliberRM export

The "RiskCAT Interfaces to Requirements Management Tools" offer to export the measures actually selected to the requirements management tool CaliberRM (by Borland Software Corporation). The "RiskCAT Interfaces to Requirements Management Tools" are a package of its own and need an extra licence.

Export for each selected measure consists of:

- The identifier of the measure
- The measure text (text of the level 1 presentation),
- The reference to part as well as clause of IEC 61508.
- The note the user may have issued with respect to the measure
- The degree of obligation for the measure.

First step to export measures from RiskCAT to CaliberRM is the selection of the measures to be exported. Then the export itself is started via the menu "File".



For the export itself there are some options given in the menu in a self-explaining manner.

Finally the "Export" button needs to be pushed to choose the name of one of the export files and to start their generation.

Export of RiskCAT for CaliberRM are two files:

- "Export_Info.txt" with
  - the items delimiter character (|) and
  - the text enclosure character (") used for the export
- "*.cvs" with the information selected on the "Caliber export" form.

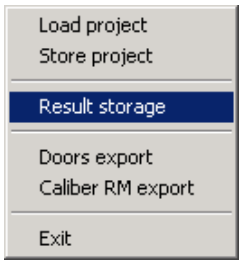
These files are inputs for the Caliber RM tools

- Import factory and
- Import utility.

The import by CaliberRM is specified in the CaliberRM user documentation. Please, apply that for the further procedure.

5 Menu functions

5.1 "File" menu



Functions within file menu are:

- Load project – see chapter 4.17, "Project (session) reload from a file"
- Store project – see chapter 4.16, "Project (session) storage in a file"
- Result storage – see chapter 4.18, "Result storage as RTF-file"
- Doors export – see chapter 4.19, "DOORS export"
- CaliberRM export – see chapter 4.20, "CaliberRM export"
- Exit – closes RiskCAT.

5.2 "Standard Text" menu

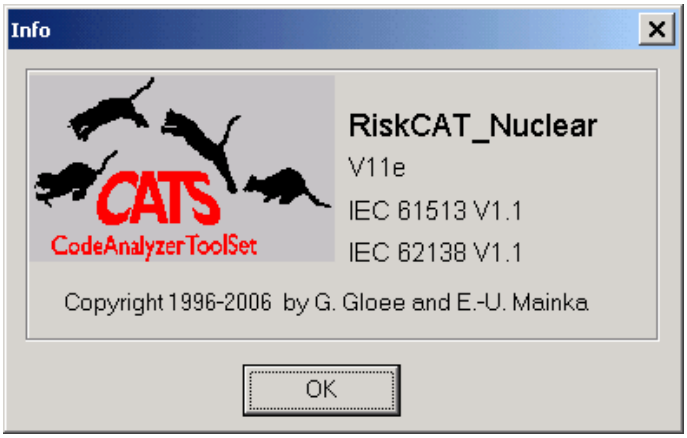
Functions within standards text menu are:

- Standard view by XpdfViewer™ – see chapter 4.12, "Retrieval in the original standards"

5.3 "Help" menu

Functions within help menu are:

- Help – Main texts of this user's manual are supplied as help.
- About – Informs about RiskCAT version and copyright



The upper line in the besides figure identifies the version of RiskCAT Nuclear (V1.1e).

The lower line identifies the versions of the databases (IEC 61513 V1.1 and IEC 62138 V1.1), which are included in RiskCAT.

6 IEC 61513 and IEC 62138 specific features

6.1 Presentation of the degree of obligation of the requirements

Up to date IEC standards as IEC 61513 and 62138 use four key words to identify their requirements (the first three explanations are from of the introduction to IEC 61226):

shall indicates requirements that are mandatory for compliance with the standard

should indicates requirements that are not mandatory for compliance with the standard but are strongly recommended

may indicates that compliance with the recommendation is optional

must not / shall not
indicates requirements that are mandatory for compliance with the standard

Within the RiskCAT tools family only one set of key words is used for the degree of obligation. To realize this

- shall requirements are classified as 'mandatory'
- should requirements are classified as 'highly recommended'
- may recommendations are classified as 'possible'
- must not requirements are classified as 'not recommended'

for all categories.

Contents from notes and informative annexes have not been adopted to RiskCAT generally.

6.2 About the license for the standards supplied with RiskCAT

By contract with the German Chapter of the IEC (DKE) CATS has been asked to declare with RiskCAT[5]:

> "The data from the international standards 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"

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

6.3 About some Key-Words in the individual measure presentation in RiskCAT

To a certain extent IEC 61513 or IEC 22138 clauses themselves give a condition for their applicability. To ease identification of these conditionally applicable clauses RiskCAT presents the respective individual measures starting with the Key-Word "***IF***". The end of the condition is denoted by "***:***".

To a certain extent again within a single IEC 61513 or IEC 22138 clause there is a choice between different measures. To present this situation without splitting up the clause into too many individual measures, RiskCAT uses the Key-Word "***OR***" in its presentation.

To a certain extent again within a single IEC 61513 or IEC 22138 clause several measures are required, e.g. several documents. To present this situation without splitting up the clause into too many individual measures RiskCAT may give some of the measures (the most important ones, hopefully) ending up with "**…**".

6.4 About the IEC 61513 presentation by RiskCAT

IEC 61513 is concerned with the functions to be implemented as well as with the systems providing the functions. Based on IEC 61226 the IEC 61513 uses **categories** for the functions. However, for the systems IEC 61513 uses **classes**. RiskCAT Nuclear uses **categories** to control the degree of obligation of the IEC 61513 clauses.

As usual the scope of IEC 61513 is not intended to provide requirements on I&C systems and their software. However, there is one basic statement about the safety lifecycle in the scope. So CATS decided to include the scope into RiskCAT Nuclear.

As already explained in the chapter above in some cases the RiskCAT short presentation of the clauses indicates by … that the original clause has much more information then the RiskCAT short form. For IEC 61513 this happens about 30 times.

Dedicated to efficient work other RiskCATs, e.g. RiskCAT 61508, tend to combine related requirements into one presentation. Because of the nuclear focus this has not been felt to be appropriate for RiskCAT Nuclear. So the presentation of IEC 61513 may seem to be more detailed than that e.g. in RiskCAT 61508 resulting in a higher number of measures.

6.5 About the IEC 62138 presentation by RiskCAT

IEC 62138 is concerned with the functions to be implemented as well as with the software providing the functions. Based on IEC 61226 the IEC 62138 uses **categories** for the functions. However, for the software IEC 62138 uses **classes**. RiskCAT Nuclear uses **categories** to control the degree of obligation of the IEC 62138 clauses.

IEC 62138 has chapters of its own for category C and category B. The category B chapter involves the category C chapter (see IEC 62138 at the beginning of chapter 6), partly in a slightly modified manner. For purpose of the "Context related retrieval in the original

standards" (see chapter 4.13) in IEC 62138, RiskCAT Nuclear references the chapter for category B (chapter 6) as well for category B as for category C.

IF

- the degree of obligation for category C differs from that for category B AND
- the degree of obligation for category C is not "not applicable" AND
- there are no real explanation by IEC 62138 for the measure

THEN RiskCAT will give reference at "The context related presentation of explanations to the clause provided by IEC 61513 or IEC 62138 themselves" (see chapter 4.14) to the respective clause in the chapter for category C (chapter 5).

As already explained in the chapter above in some cases the RiskCAT short presentation of the clauses indicates by … that the original clause has much more information then the RiskCAT short form. For IEC 62138 this happens about 20 times.

Dedicated to efficient work other RiskCATs, e.g. RiskCAT 61508, tend to combine related requirements into one presentation. Because of the nuclear focus this has not been felt to be appropriate for RiskCAT Nuclear. So the presentation of IEC 62138 may seem to be more detailed than that e.g. in RiskCAT 61508 resulting in a higher number of measures.

6.6 Abbreviations

Abbreviations used in CATS database of IEC 61513 and/or IEC 62138:

AFTS	Assigning application functions important to safety to systems and subsystems
DB	Database
IF	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"
HW	Hardware
SQAP	System quality assurance plan
NPP	Nuclear power plant
OR	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"
QA	Quality assurance
SOP	System operation plan
SVAP	System validation plan
SVP	System verification plan
SW	Software
…	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"

7 Appendix

7.1 List of Documents

RiskCAT Nuclear uses the documents from IEC 61513, First Edition, 2001-03, which are

Document	Reference	Document	Reference
Overall requirements spec	5.2		
Detailed I&C architecture design	5.5.1		
System requirements spec	5.5.2, 6.3.1		
Overall QA plan	5.4.1		
Overall security plan	5.4.2		
Overall integration plan	5.4.3.1	Overall integration doc	7.2
Overall commissioning plan	5.4.3.2		
Overall operation plan	5.4.4		
Overall maintenance plan	5.4.5		
Overall user doc	8		
System spec	6.3.2		
SW spec	6.3.2.1.d		
System design doc	6.3.3		
System QA plan	6.2.1		
System verification plan	6.2.1.1		
System configuration management plan	6.2.1.2		
System security plan	6.2.2		
System integration plan	6.2.3	System integration report	6.3.4
System validation plan	6.2.4	System validation report	6.3.5
System installation plan	6.2.5	System installation report	Table 3 / 6.1.6
System operation plan	6.2.6		
System maintenance plan	6.2.7	System modification request	6.3.6
		System modification record	6.3.6
System qualification plan	6.4.1		

For RiskCAT Nuclear following documents have been added to those given by IEC 61513 :

- All
- All: Overall plans
- All: System plans
- Communication link
- HW
- NA (not applicable)
- SW
- System
- System: Interconnected

Additionally RiskCAT Nuclear uses the documents from IEC 62138, First Edition, 2004-01, which are

Document	Reference	Document	Reference
SW QA plan	6.1.1-1	SW QA record	6.1.1-11
SW configuration management plan	6.1.3-1		
Security assurance plan	6.1.6-1		
SW verification plan	6.1.2-1	SW verification record	6.5.4-2
SW requirements spec	6.1.2-4; 6.3		
SW design spec	6.1.2-4; 6.4		
Doc for Safety	6.2		
Development tools instruction	6.1.5-4	Development tools log	6.5.1-2
Code: Executable	6.5.1-3		
Program doc	6.5.1-2; 6.5.2-1		
Coding rules	6.5.3-4		
SW integration plan	6.6-3	SW integration record	6.6-4
Regression SW integration plan	6.10-2		6.10.2
SW validation plan	6.1.2-4	SW validation record	6.7-5
Regression SW validation plan	6.10-2		6.10-2
SW installation plan	6.8-1		
Anomaly report	6.9-1		
SW modification plan	6.10	SW modification records	6.10-4

7.2 List of Activities

RiskCAT Nuclear uses the documents from IEC 61513, First Edition, 2001-03, table 1 (page 47) and table 3 (page 83) which are

----------Table 1 ----------

- Review plant requirements
- Design I&C architecture
- Assign functions
- Plan overall
- Overall validation
- Overall integration
- Overall commissioning

----------Table 3 ----------

- Specify system requirements
- Specify system
- Design system
- Implement system
- Integrate system
- Validate system
- Install system
- Modify system
- Qualify system
- Qualify SW

For RiskCAT Nuclear following activities have been added to those given by IEC 61513 :

- All
- Assess
- NA (not applicable)
- Evaluate
- Inspect
- Operate
- Test
- Verify

Additionally RiskCAT Nuclear uses the activities from IEC 62138, First Edition, 2004-01, which are

Activity	Reference	Remarks
Plan SW	6.1.6	
Specify SW	6.3	
Design SW	6.4	Development (6.1.1-1) is Design plus Implementation (see Figure 3)
Implement SW	6.5	
Coding	6.5.1	
Integrate SW	6.6	
Validate SW	6.7	
Install SW	6.8	
Modify SW	6.10	

For RiskCAT following activity has been added to those given by IEC 62138 :

- Manage Safety