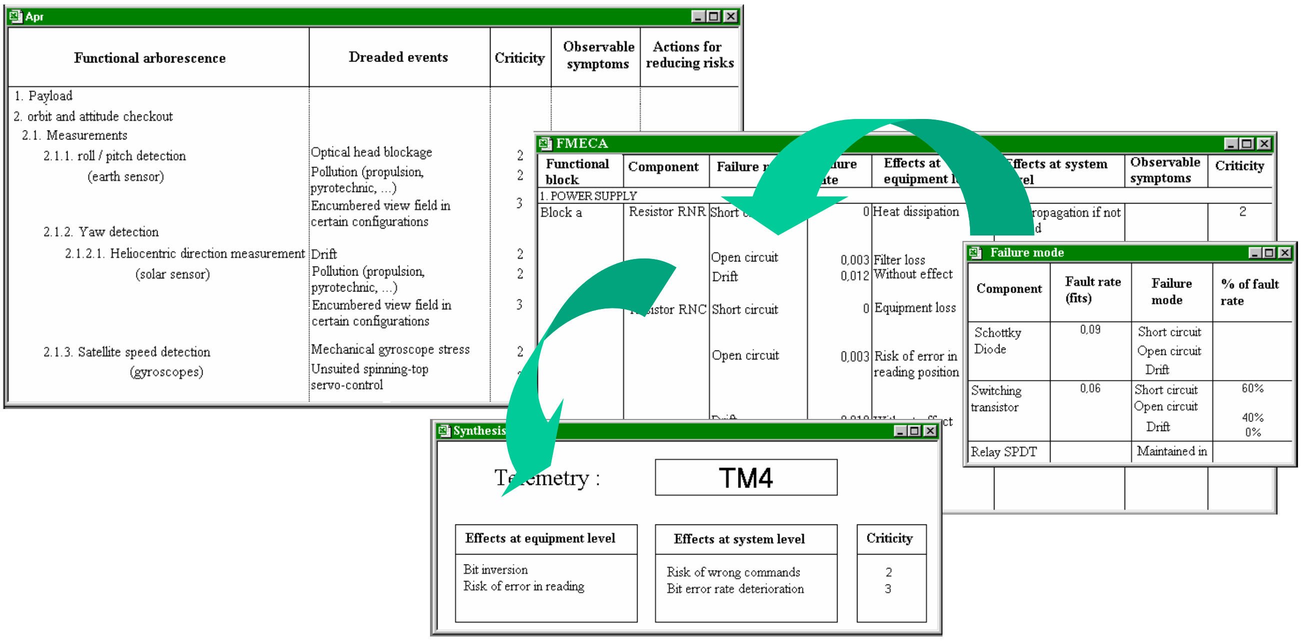
Cab Innovation

3 rue de la Coquille
31500 Toulouse
Tel. 33 (0)5 61 54 68 08
Fax. 33 (0)5 61 54 33 32
Mail : Contact@cabinnovation.com
Web : www.cabinnovation.com

FAILCAB Version 7

using Microsoft EXCEL®



Apr

Functional arborescence	Dreaded events	Criticity	Observable symptoms	Actions for reducing risks
1. Payload				
2. orbit and attitude checkout				
2.1. Measurements				
2.1.1. roll / pitch detection (earth sensor)	Optical head blockage Pollution (propulsion, pyrotechnic, ...) Encumbered view field in certain configurations	2 2 3		
2.1.2. Yaw detection				
2.1.2.1. Heliocentric direction measurement (solar sensor)	Drift Pollution (propulsion, pyrotechnic, ...) Encumbered view field in certain configurations	2 2 3		
2.1.3. Satellite speed detection (gyroscopes)	Mechanical gyroscope stress Unsuited spinning-top servo-control	2		

FMECA

Functional block	Component	Failure r	ure te	Effects at equipment l	ffects at system el	Observable symptoms	Criticity
1. POWER SUPPLY							
Block a	Resistor RNR	Short c	0	Heat dissipation	ropagation if not d		2
		Open circuit Drift	0,003 0,012	Filter loss Without effect			
	istor RNC	Short circuit	0	Equipment loss			
		Open circuit	0,003	Risk of error in reading position			

Failure mode

Component	Fault rate (fits)	Failure mode	% of fault rate
Schottky Diode	0,09	Short circuit Open circuit Drift	
Switching transistor	0,06	Short circuit Open circuit Drift	60% 40% 0%
Relay SPDT		Maintained in	

Synthesis

Telemetry : TM4

Effects at equipment level	Effects at system level	Criticity
Bit inversion Risk of error in reading	Risk of wrong commands Bit error rate deterioration	2 3

Risks analysis and FMECA

User's Manual

FOREWORD

The software FAILCAB BASIC version 2 includes some of the FAILCAB version 7 features. It is not the subject of a specific user manual

The Programming Protection Agency (A.P.P.) references ***FAILCAB*** at the I.D.D.N. (Inter Deposit Digital Number) index, with the following reference:

IDDN.FR.001.070017.00.R.P.2000.000.20600

CONTENTS:

1 The *FAILCAB* Software

1.1 General Presentation

FAILCAB helps achieving and operating FMECA (Failure Mode Effect And Criticity Analysis) and PRA (Preliminary Risks Analyses) according to specific or standard formats (Standards X 60-510, CEI 812-1985 and MIL-STD-1629A).
It automatically controls the material or functional product arborescence and offers various supports to user to relieve him from a major part of typing activity.
So, this allows to supplement automatically the FMECA from nomenclatures, lists of fault modes, effect synthesis, or any other database.
Furthermore, such supports foster the standardization of words used so as to facilitate the subsequent performance of analyses using multiple-criterion sorting.
From FMECA or PRA, ***FAILCAB*** allows also to automatically generate synthesis documents such as the risks control manual intended for the product operators.

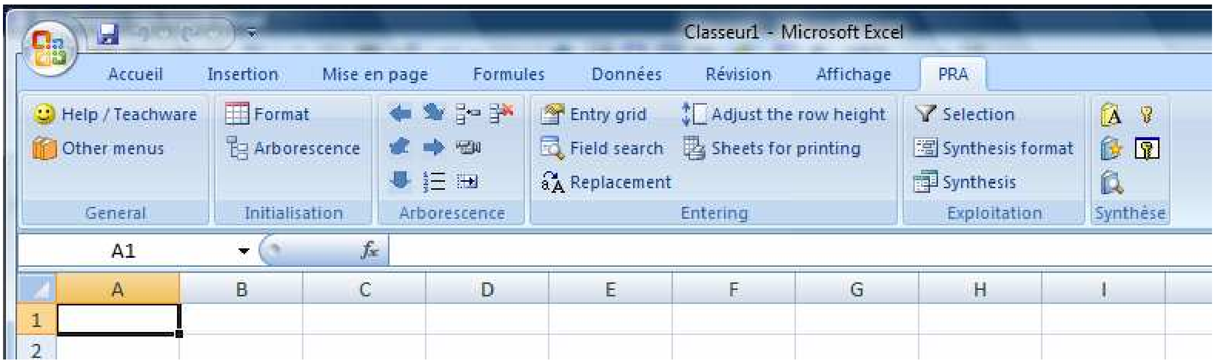
1.2 Installing *FAILCAB* on Hard Disk

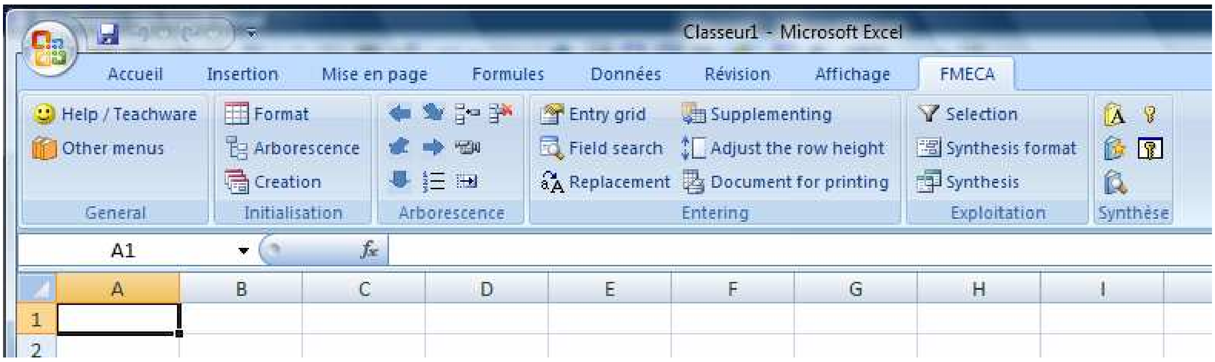
Please comply with instructions shown in CD-ROM.

1.3 To Start *FAILCAB*

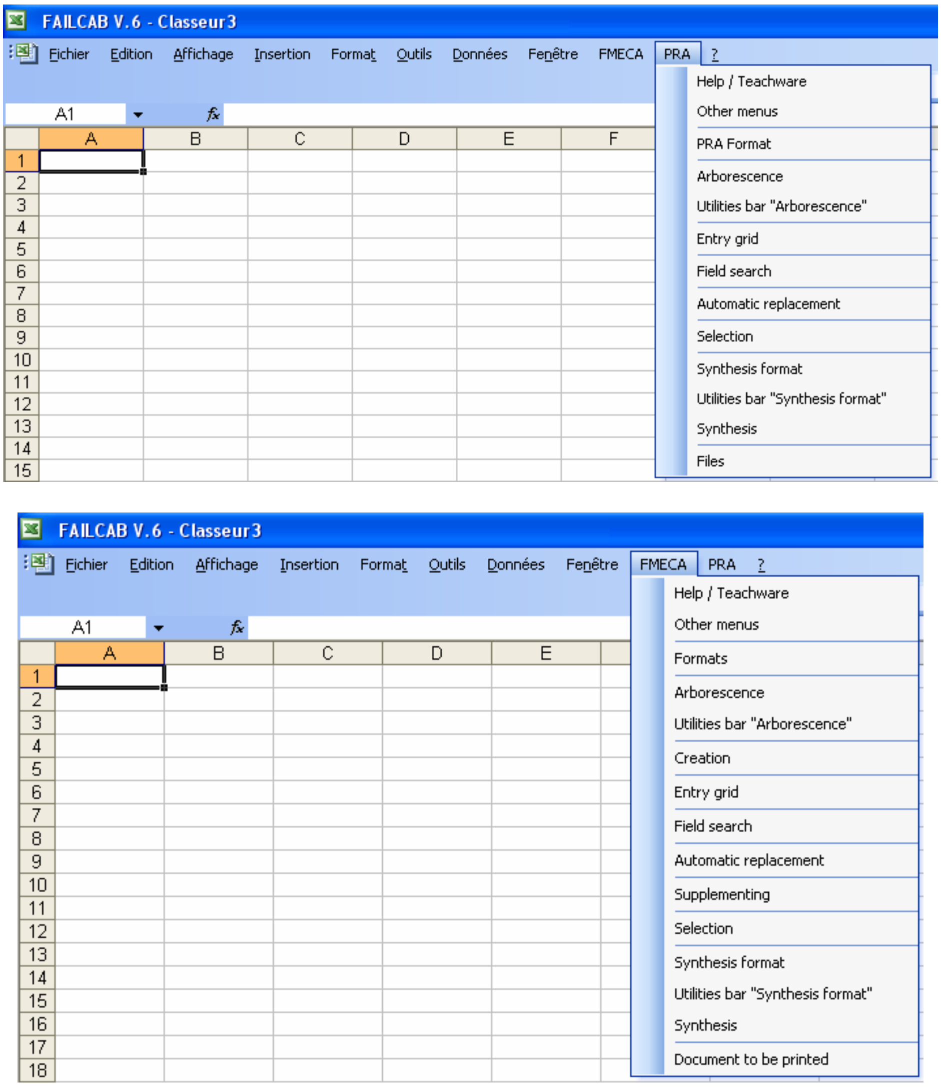
In EXCEL, open file **FAILCAB.xla**.

Software's functionalities are then accessible using "PRA" or "FMECA" menus, spreadsheet functionalities remaining always available. The command "Others menus" allows to change the menu.





Bannrsr on Excel versions after 2007



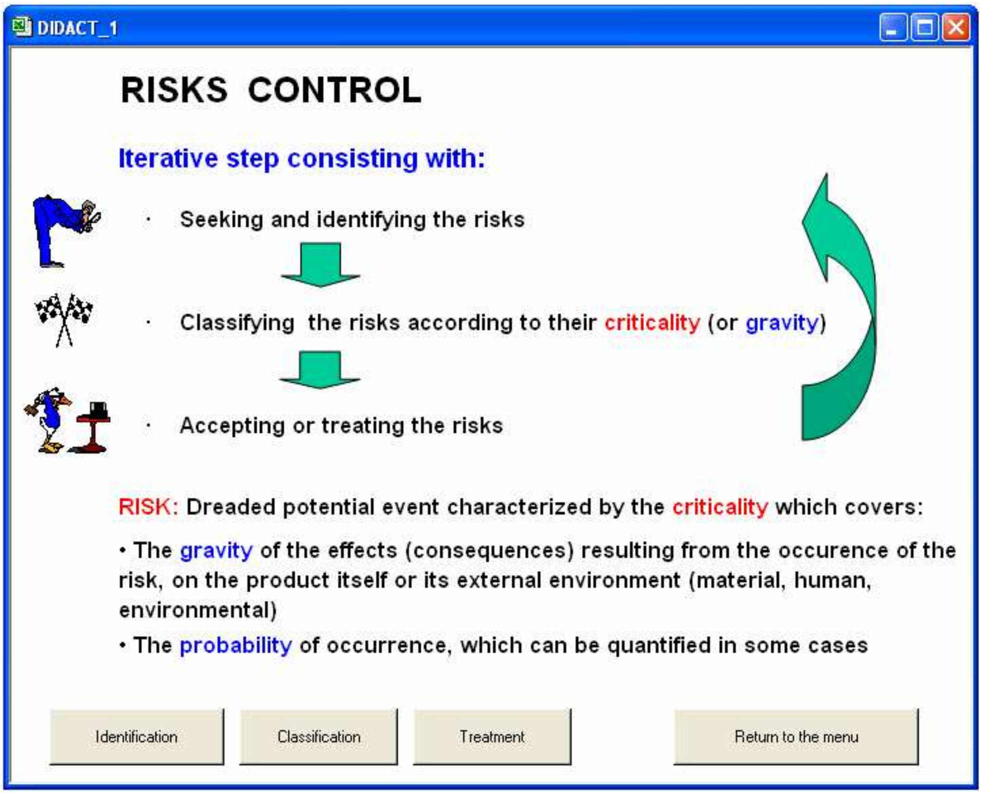
Menus on Excel versions prior to 2007

A help and a teachware are proposed in the menu.

2 Teachware

The teachware presents the risks control methods by means of various tables and demonstrations.

2.1 Risks control



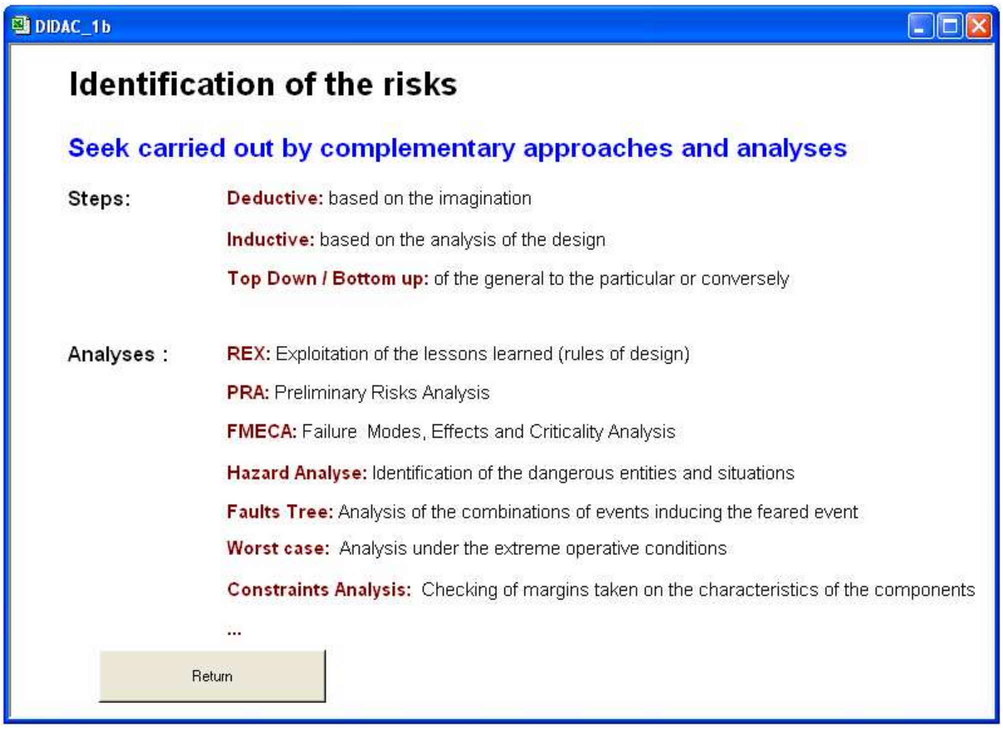
RISKS CONTROL

Iterative step consisting with:

- Seeking and identifying the risks
- Classifying the risks according to their criticality (or gravity)
- Accepting or treating the risks

RISK: Dreaded potential event characterized by the criticality which covers:

- The gravity of the effects (consequences) resulting from the occurence of the risk, on the product itself or its external environment (material, human, environmental)
- The probability of occurrence, which can be quantified in some cases



Identification of the risks

Seek carried out by complementary approaches and analyses

Steps:

Deductive: based on the imagination

Inductive: based on the analysis of the design

Top Down / Bottom up: of the general to the particular or conversely

Analyses :

REX: Exploitation of the lessons learned (rules of design)

PRA: Preliminary Risks Analysis

FMECA: Failure Modes, Effects and Criticality Analysis

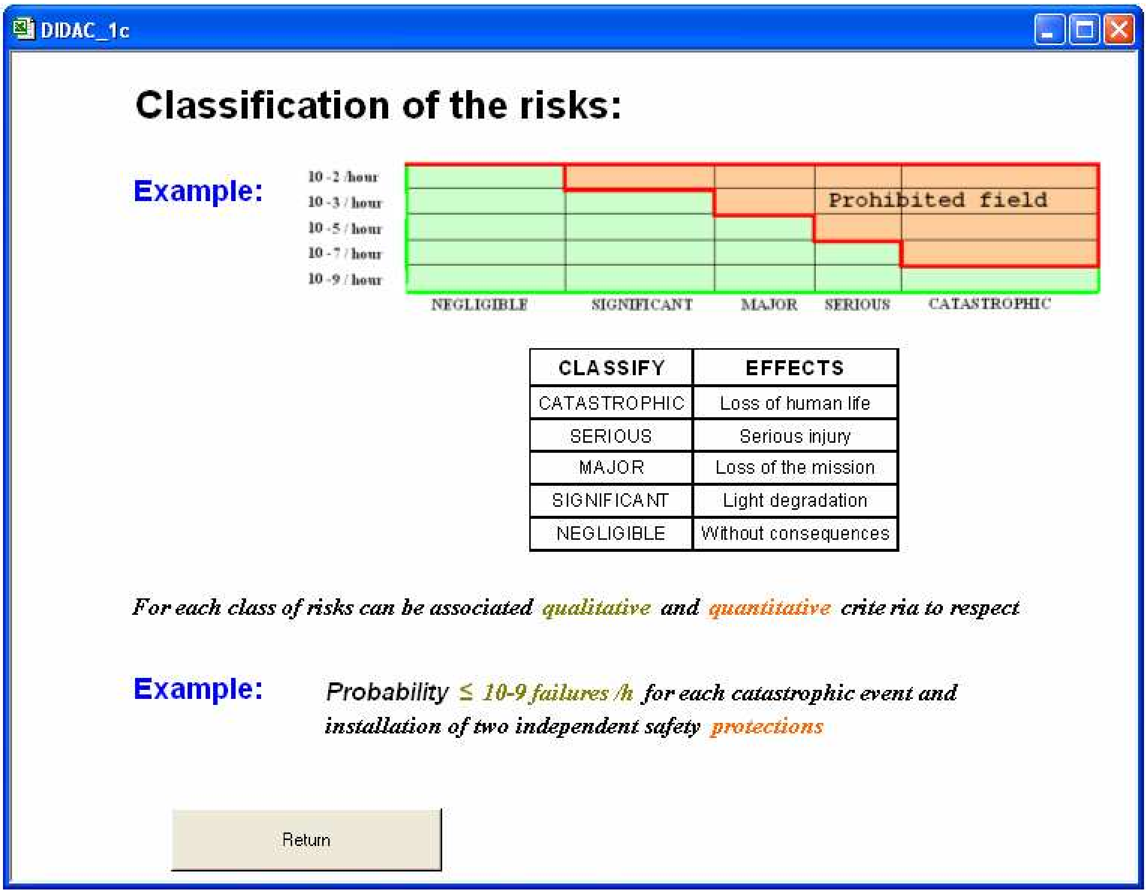
Hazard Analyse: Identification of the dangerous entities and situations

Faults Tree: Analysis of the combinations of events inducing the feared event

Worst case: Analysis under the extreme operative conditions

Constraints Analysis: Checking of margins taken on the characteristics of the components

...



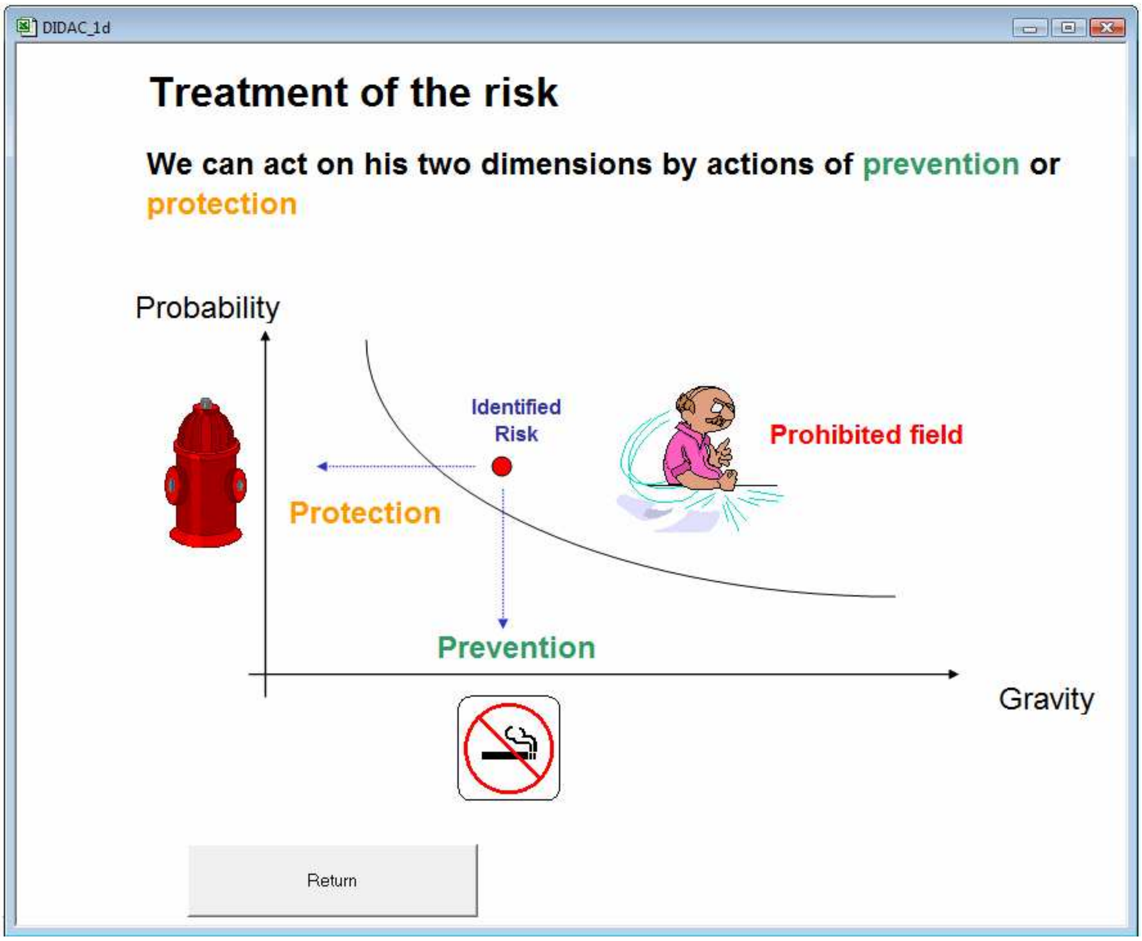
Classification of the risks:

Example:

CLASSIFY	EFFECTS
CATASTROPHIC	Loss of human life
SERIOUS	Serious injury
MAJOR	Loss of the mission
SIGNIFICANT	Light degradation
NEGLIGIBLE	Without consequences

For each class of risks can be associated qualitative and quantitative crite ria to respect

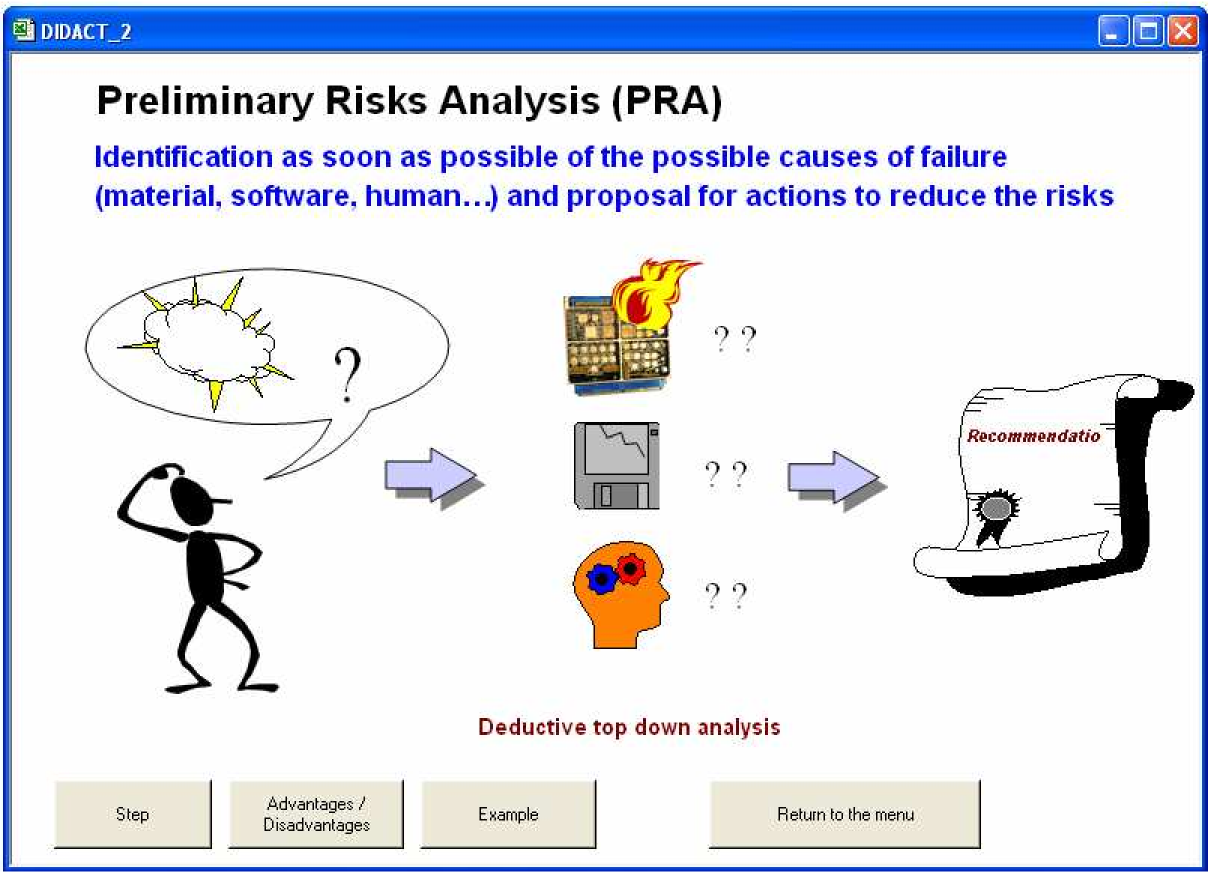
Example: Probability ≤ *10-9 failures /h for each catastrophic event and installation of two independent safety protections*



Treatment of the risk

We can act on his two dimensions by actions of prevention or protection

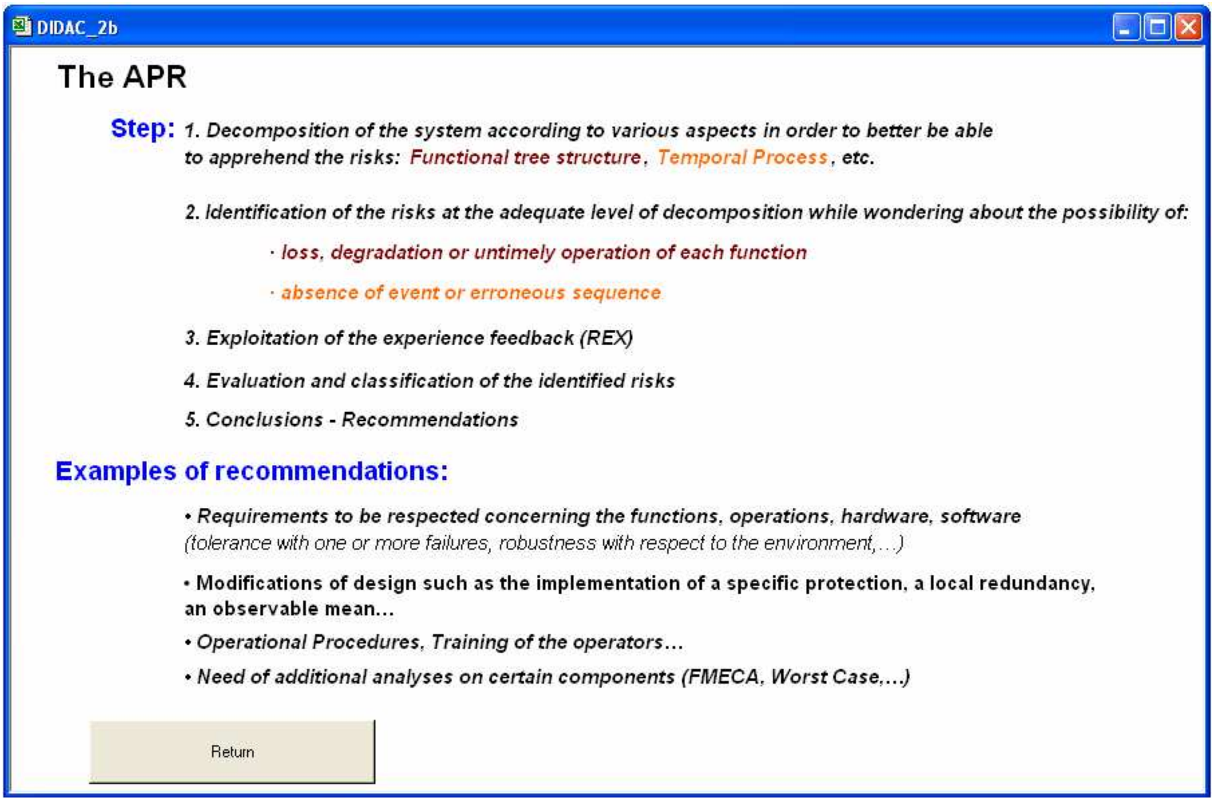
2.1 Preliminar Risks Analysis (PRA)



Preliminary Risks Analysis (PRA)

Identification as soon as possible of the possible causes of failure (material, software, human…) and proposal for actions to reduce the risks

Deductive top down analysis



The APR

Step: *1. Decomposition of the system according to various aspects in order to better be able to apprehend the risks: Functional tree structure, Temporal Process, etc.*

2. Identification of the risks at the adequate level of decomposition while wondering about the possibility of:

- *loss, degradation or untimely operation of each function*
- *absence of event or erroneous sequence*

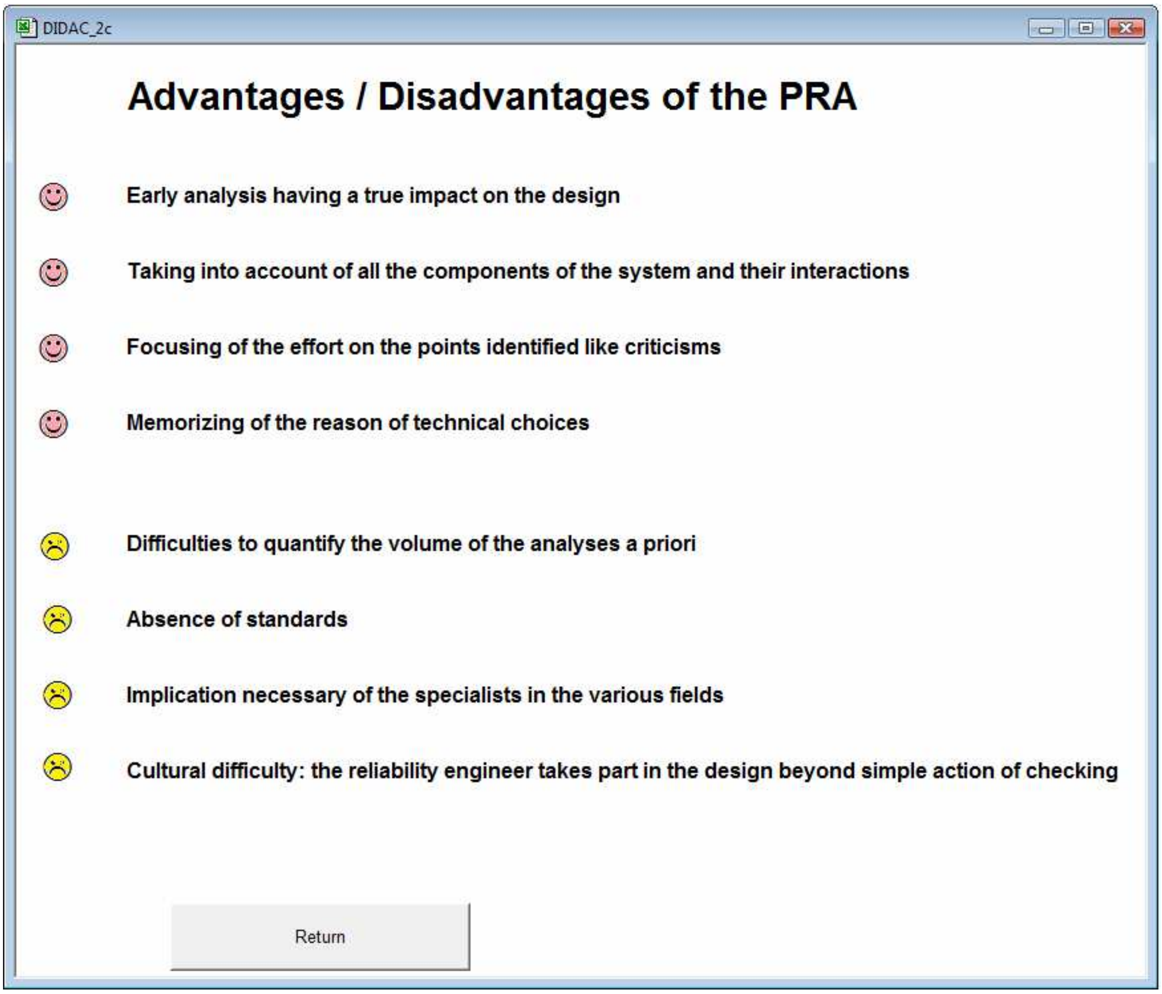
3. Exploitation of the experience feedback (REX)

4. Evaluation and classification of the identified risks

5. Conclusions - Recommendations

Examples of recommendations:

- *Requirements to be respected concerning the functions, operations, hardware, software* *(tolerance with one or more failures, robustness with respect to the environment,…)*
- Modifications of design such as the implementation of a specific protection, a local redundancy, an observable mean…
- *Operational Procedures, Training of the operators…*
- *Need of additional analyses on certain components (FMECA, Worst Case,…)*



Advantages / Disadvantages of the PRA

☺ Early analysis having a true impact on the design

☺ Taking into account of all the components of the system and their interactions

☺ Focusing of the effort on the points identified like criticisms

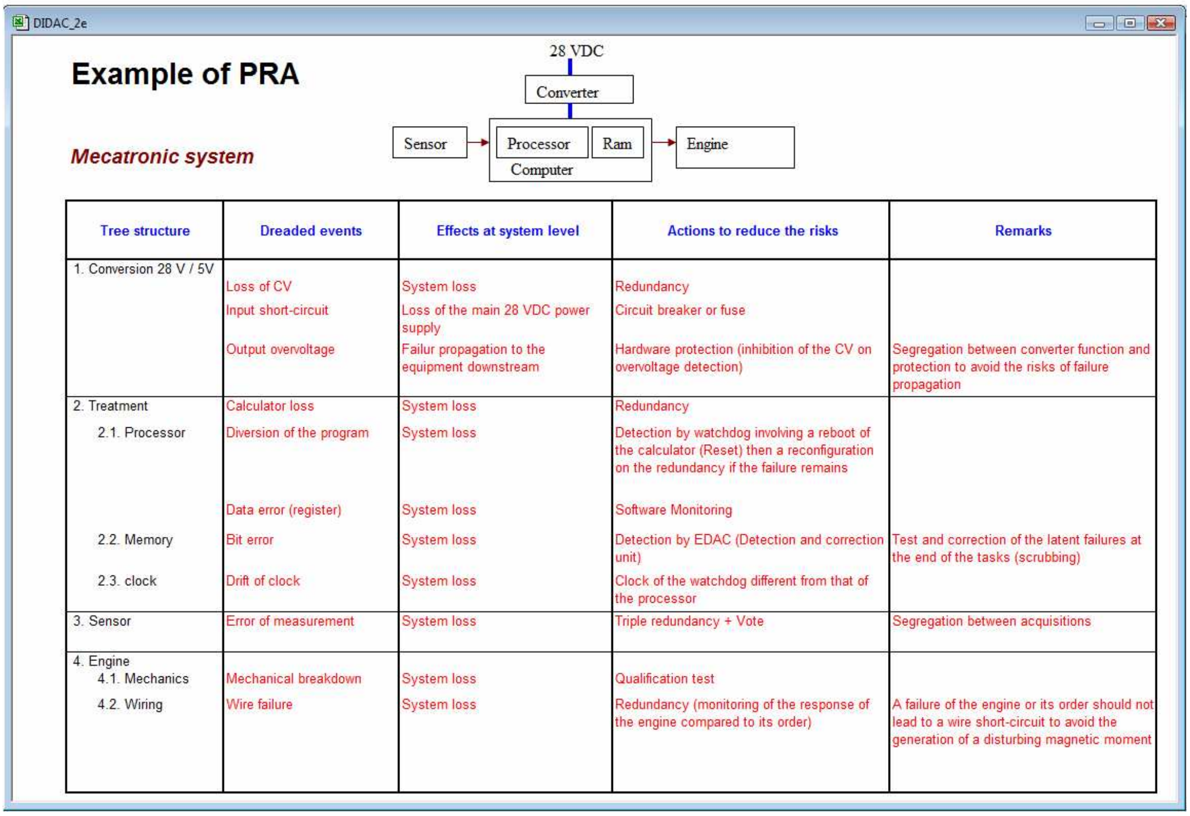
☺ Memorizing of the reason of technical choices

☹ Difficulties to quantify the volume of the analyses a priori

☹ Absence of standards

☹ Implication necessary of the specialists in the various fields

☹ Cultural difficulty: the reliability engineer takes part in the design beyond simple action of checking

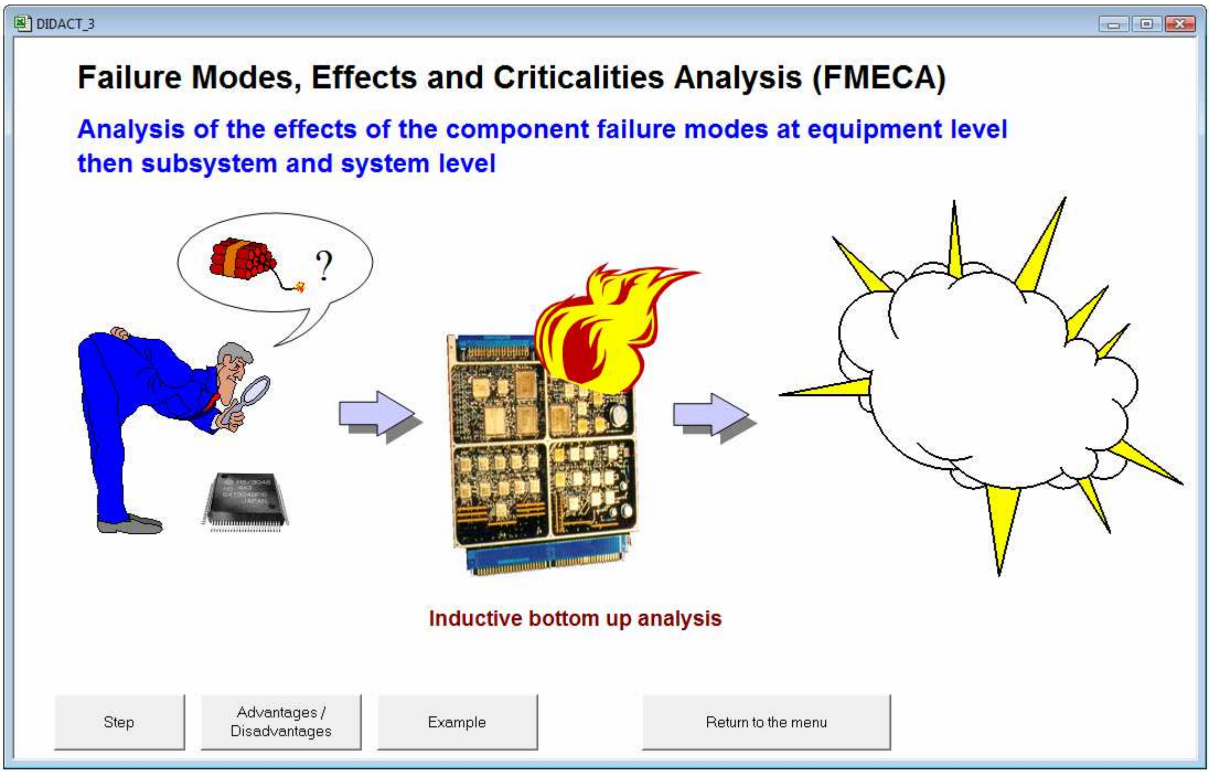


Example of PRA

Mecatronic system

Tree structure	Dreaded events	Effects at system level	Actions to reduce the risks	Remarks
1. Conversion 28 V / 5V	Loss of CV	System loss	Redundancy	
	Input short-circuit	Loss of the main 28 VDC power supply	Circuit breaker or fuse	
	Output overvoltage	Failur propagation to the equipment downstream	Hardware protection (inhibition of the CV on overvoltage detection)	Segregation between converter function and protection to avoid the risks of failure propagation
2. Treatment	Calculator loss	System loss	Redundancy	
2.1. Processor	Diversion of the program	System loss	Detection by watchdog involving a reboot of the calculator (Reset) then a reconfiguration on the redundancy if the failure remains	
	Data error (register)	System loss	Software Monitoring	
2.2. Memory	Bit error	System loss	Detection by EDAC (Detection and correction unit)	Test and correction of the latent failures at the end of the tasks (scrubbing)
2.3. clock	Drift of clock	System loss	Clock of the watchdog different from that of the processor	
3. Sensor	Error of measurement	System loss	Triple redundancy + Vote	Segregation between acquisitions
4. Engine 4.1. Mechanics	Mechanical breakdown	System loss	Qualification test	
4.2. Wiring	Wire failure	System loss	Redundancy (monitoring of the response of the engine compared to its order)	A failure of the engine or its order should not lead to a wire short-circuit to avoid the generation of a disturbing magnetic moment

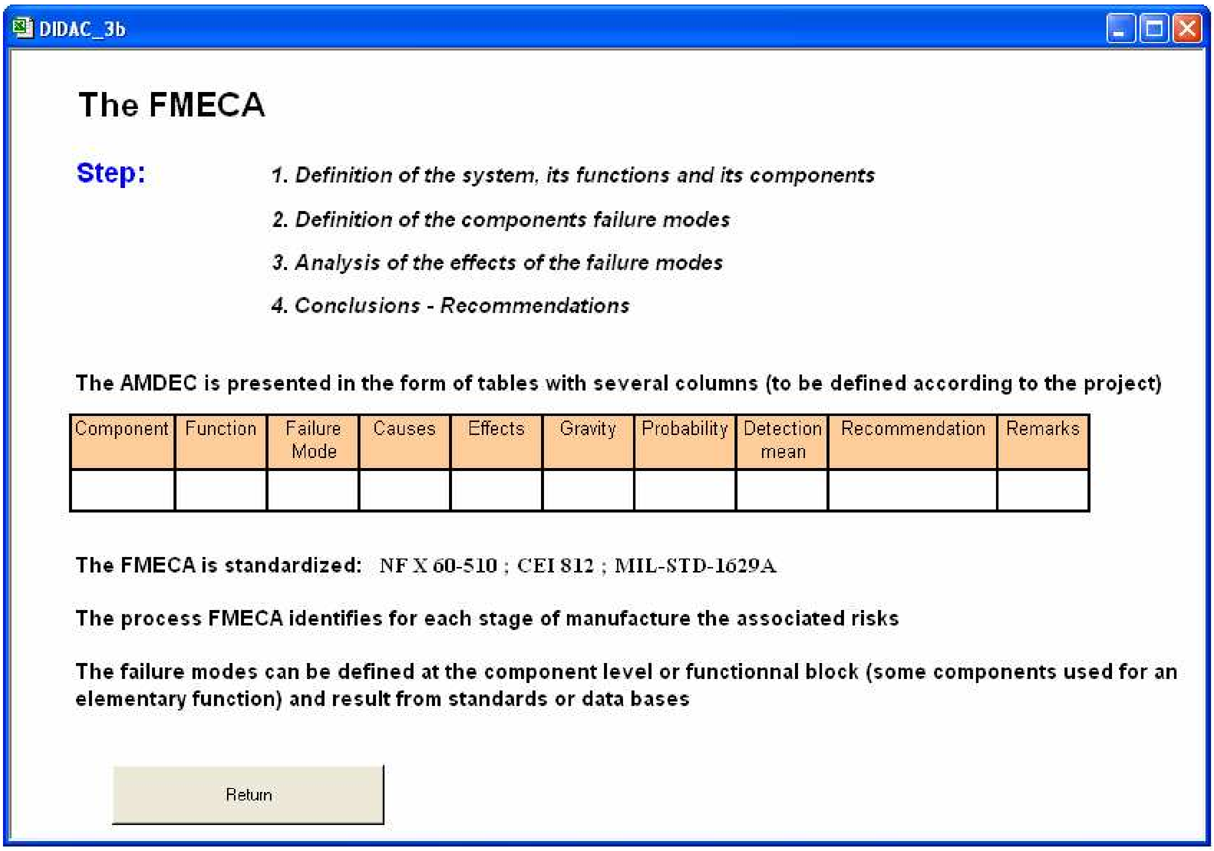
2.1 Failure Modes, Effects and Criticalities Analysis (FMECA)



Failure Modes, Effects and Criticalities Analysis (FMECA)

Analysis of the effects of the component failure modes at equipment level then subsystem and system level

Inductive bottom up analysis



The FMECA

Step:

1. Definition of the system, its functions and its components

2. Definition of the components failure modes

3. Analysis of the effects of the failure modes

4. Conclusions - Recommendations

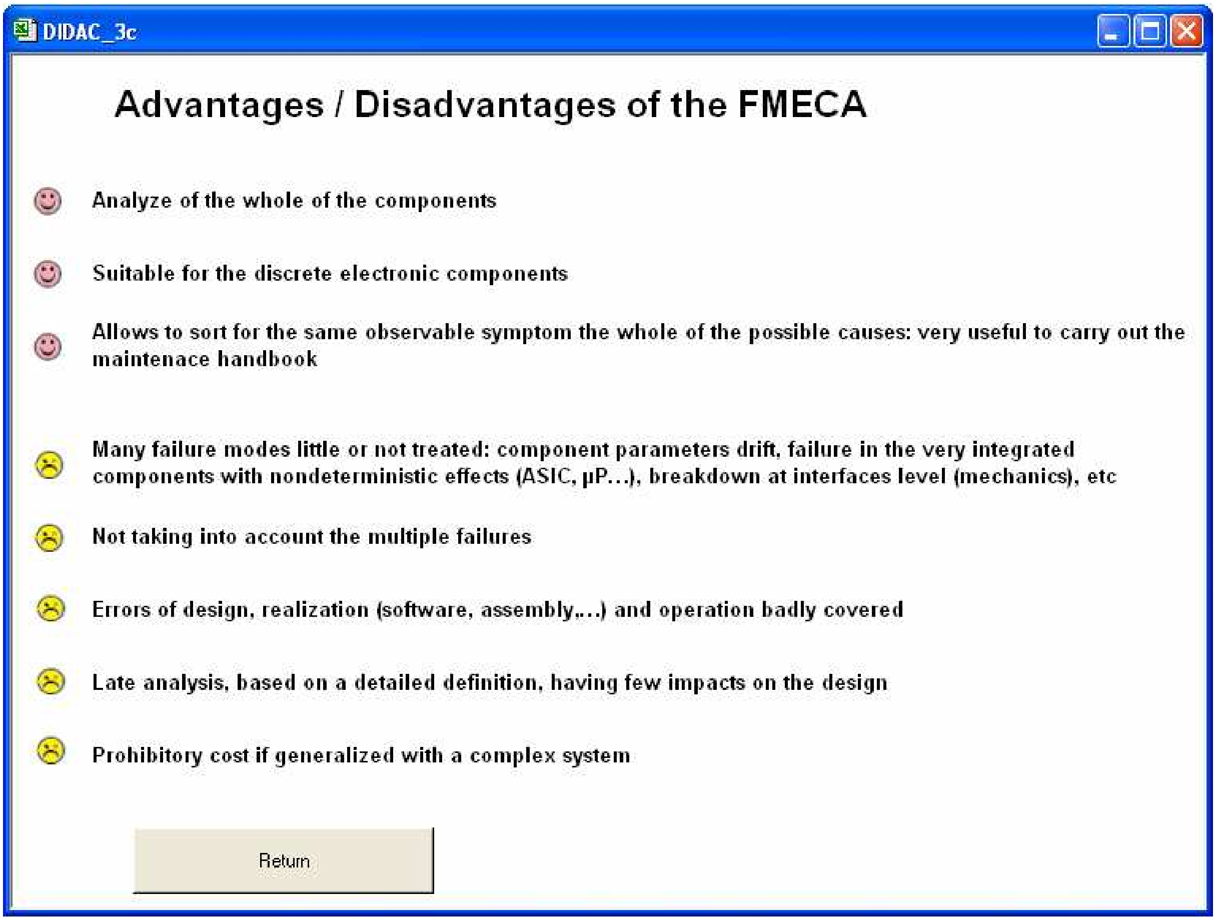
The AMDEC is presented in the form of tables with several columns (to be defined according to the project)

Component	Function	Failure Mode	Causes	Effects	Gravity	Probability	Detection mean	Recommendation	Remarks

The FMECA is standardized: NF X 60-510 ; CEI 812 ; MIL-STD-1629A

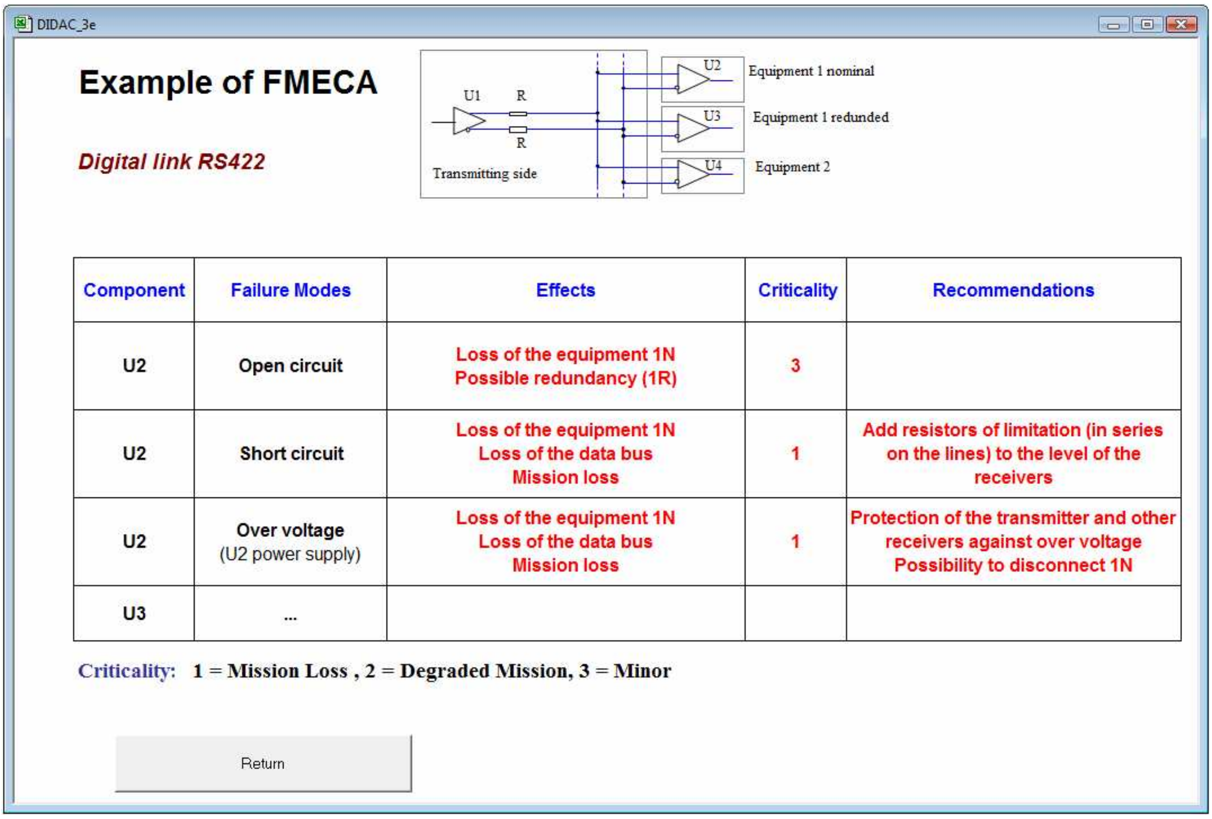
The process FMECA identifies for each stage of manufacture the associated risks

The failure modes can be defined at the component level or functionnal block (some components used for an elementary function) and result from standards or data bases



Advantages / Disadvantages of the FMECA

- ☺ Analyze of the whole of the components
- ☺ Suitable for the discrete electronic components
- ☺ Allows to sort for the same observable symptom the whole of the possible causes: very useful to carry out the maintenace handbook
- ☹ Many failure modes little or not treated: component parameters drift, failure in the very integrated components with nondeterministic effects (ASIC, µP…), breakdown at interfaces level (mechanics), etc
- ☹ Not taking into account the multiple failures
- ☹ Errors of design, realization (software, assembly,…) and operation badly covered
- ☹ Late analysis, based on a detailed definition, having few impacts on the design
- ☹ Prohibitory cost if generalized with a complex system



Example of FMECA

Digital link RS422

Component	Failure Modes	Effects	Criticality	Recommendations
U2	Open circuit	Loss of the equipment 1N Possible redundancy (1R)	3	
U2	Short circuit	Loss of the equipment 1N Loss of the data bus Mission loss	1	Add resistors of limitation (in series on the lines) to the level of the receivers
U2	Over voltage (U2 power supply)	Loss of the equipment 1N Loss of the data bus Mission loss	1	Protection of the transmitter and other receivers against over voltage Possibility to disconnect 1N
U3	...			

Criticality: 1 = Mission Loss , 2 = Degraded Mission, 3 = Minor

3 PRA

The Preliminary Risks Analysis (PRA) purpose is to identify risks at the early steps of design so as to be capable of controlling them.
Such identification results in a deductive approach which, on a complex system, is only really possible if the latter is preliminarily broken down in sections being sufficiently reduced to be correctly apprehended by a human spirit.
Such breaking down may naturally regard system functions, but may also concern the time allowance (critical phases), or an industrial process (tasks).

Identification of risks using functional breaking down…

Functional Arborescence	Apprehended events	Criticity	Actions for reducing risks	Action status
Product				
1. Function A				
2. Function B				
2.1.				
2.1.1. Elementary Function X	Untimely operation	1	Action A	Open
	Function loss	3	Action B	Closed
	Deteriorated operation 1	4	....	....
	Deteriorated operation 1	2	....	....
	....			
2.1.2.				

... or temporal breaking down

Temporal arborescence	Dreaded events	Criticity	Observed	Actions for reducing risks
Critical phases				
1. Phase A				
1.1. Sub-phase a				
1.1.1. Event x	No event	1	Signal X	Action A
	Untimely event	3	....	....
	....			
1.1.2. Event y	y before x	2	....	....

In the case of a functional analysis, the risks identification results from an interrogation about possibilities of absence, untimely or deteriorated operation of any elementary function, together with nuisances it may cause to environment (pollution, overheating, impact...). Such interrogation leads to a list of apprehended events.

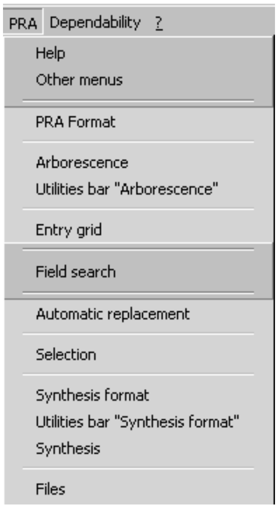
Depending on nature of risks and functions studied, the breaking down may be conducted more or less deeply in arborescence, according to analyst priority. In the case of critical phases, the latter attempts to know whether the event sequence may be disturbed (absent, untimely or wrongly ordered events,).

So identified apprehended events are subject to a classification according to a scale of gravity of consequences (or criticity), and actions for reducing risks may then be considered.

By setting up a data base combining risks and functions (phases or process) of product, rules of design with justification of certain choices, the PRA enables also to formalize the return of experience.

3.1 Main functionalities

FAILCAB helps user conduct PRA then operate it. It offers the following functionalities, accessible from menu PRA :



. Creating PRA format

. Performing the functional or temporal arborescence
(automatic management of arborescence references)

. Entering data fostering their standardization
(typing grid, field search, automatic replacement)

. Selection in PRA from multiple criteria

. Generating synthesis documents from personalized formats
(synthesis on symptoms observable by the example)

. Generating individual files per apprehended event

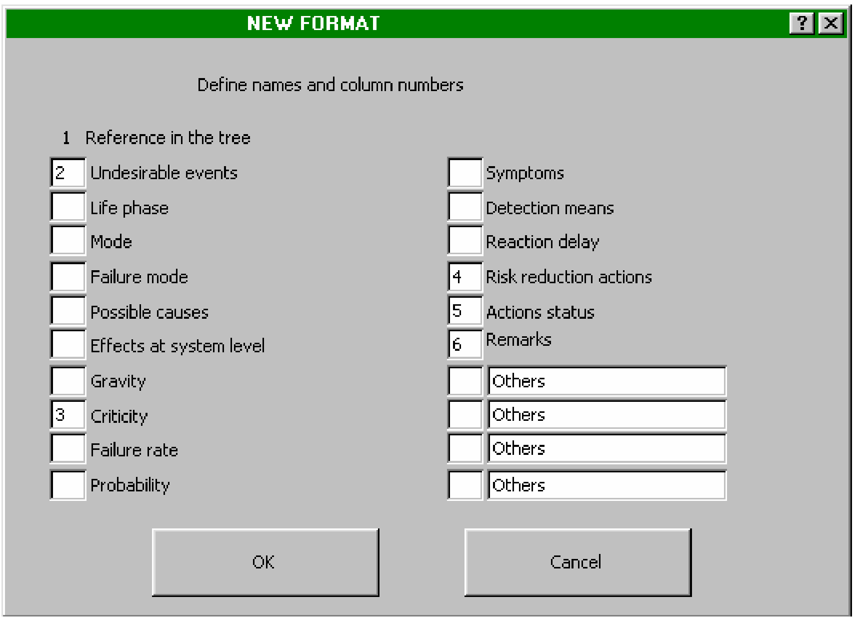
A simplified application example is shown below. More comprehensive examples are accessible using online help.

Functional Arborescence	Dreaded Events	Crit.	Observable Symptoms	Actions for Reducing Risks
1. Payload				
2. Orbit and attitude checkout				
3. Data Handling				
4. Telemetry / Remote Controls				
5. Heat Control				
6. Power supply				
6.1. Power generation				
6.1.1. Maintaining solar panels prior to spreading out	Untimely firing of a pyrotechnical squib			Specific protection
	Tie rod failure	2		Margin + tests
	Wrong behaviour on lauching	2		
6.1.2. Releasing Solar Generator (tie rods' cutting)	Pyrotechnic shear failure	1		Qualification
	Pyrotechnic squib failure	2		Redundancy
6.1.3. Solar generator spreading out	Stacking bush adhesion	2		
	Hooking of bush by a distorted tie rod after cutting	2	TM1	Design modification
	Hinge lock by bearing-way pollution	2		Cleaning action
	Stacking part mounted in the wrong way	1	TM7	Polarization + Procedures
	Insufficient motorization	2		Margin + tests
	Failure/distortion of panels or hinges	2		
6.1.4. Locking	Incorrect locking generating dynamic disturbances	2	TM2; TM3; TM5	
	Wrong behaviour to locking shock (hinge)	2		
	Failure of spreading out sensors	3		
6.1.5. Energy Generation (solar cells)	Cell pollution (propulsion, pyrotechnic ...)	4		
	Destruction due to micrometeorites	4		
	Insulation loss between network and a panel structure	2	TM4; TM6	
6.2. Solar generator orientation	Wrong checking	2		
6.3. Power control	Bar undervoltage	2		
	Bar overvoltage	1		Protection
6.4. Energy storage (batteries)	Heat dissipation (gradients)	3		
	Battery explosion	1		
	Battery electrolyte leakage	2		
6.5. Power distribution	Limiter loss	4		

Extract from the Preliminary Risks Analysis of a satellite

3.2 Creating the PRA Format

The command "PRA format" of menu PRA helps creating a new format, store the latter in a directory specific to user or recover a pre-stored format.
Requesting the creation of a new format generates the display of next menu in which a number of fields is offered to user in the French or English language.



NEW FORMAT

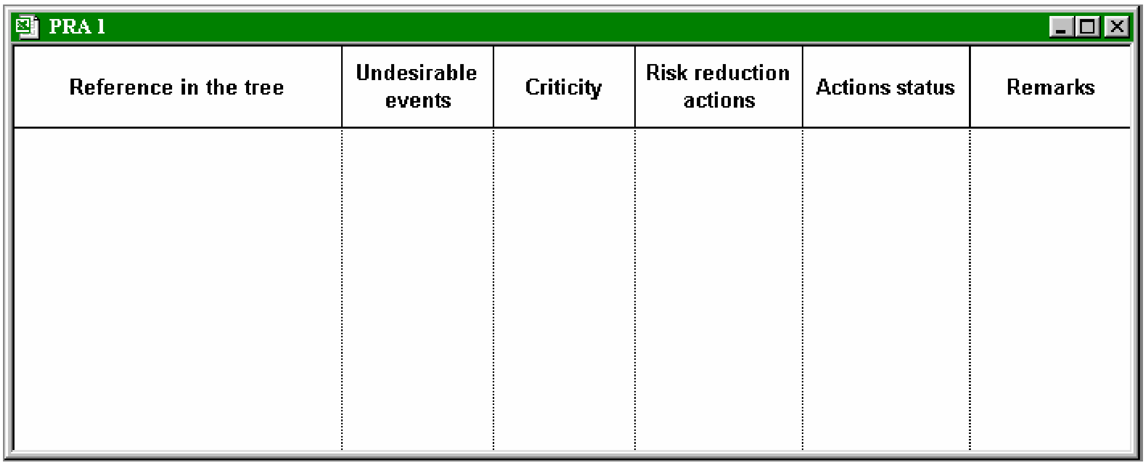
Define names and column numbers

1 Reference in the tree

2	Undesirable events		Symptoms
	Life phase		Detection means
	Mode		Reaction delay
	Failure mode	4	Risk reduction actions
	Possible causes	5	Actions status
	Effects at system level	6	Remarks
	Gravity		Others
3	Criticity		Others
	Failure rate		Others
	Probability		Others

User may choose among the latter by defining relevant column numbers, and possibly define other fields in the last four items offered.

Action on OK button generates the creation of requested format in a new sheet :



PRA 1

Reference in the tree	Undesirable events	Criticity	Risk reduction actions	Actions status	Remarks

So, modifying column width is possible by moving separation lines with mouse or performing manually other format modifications. The latter may be saved either immediately after creation, or from an informed PRA, so as to be reused.

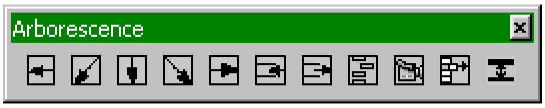
3.3 Constructing the Arborescence

Command "Arborescence" of menu PRA allows to create an arborescence, in the sheet of selected format or in a blank sheet, or recopy an arborescence already created in another format sheet.

A position in arborescence is defined by a series of numbers separated by dots. Each number features a breaking down order at a certain arborescence level and its position in the series defines the depth in this one.

0
1.
1.1.
1.2.
1.2.1.
...

The following utilities bar helps managing automatically such numbering. It is displayed or hidden using Command "Utilities bar".



Modifies initial position by incrementation at the immediately higher level :
1.3. → 2.

This command can be used directly on a selected part of the arborescence.

Inserts a new position by incrementation at a higher level :
1.3. → 2.

Inserts a new position by incrementation of initial position :

1.3. → 1.4.

Inserts an additional sub-level in arborescence from the initial position :
1.3. → 1.3.1.

Modifies initial position by incrementation at immediately lower level :
1.3. → 1.2.X.

This command can be used directly on a selected part of the arborescence. A coherence check inhibits certain untimely actions to prevent disruptions in arborescence.

Buttons and help insert or delete lines in document.

Recalculates automatically any arborescence numbering by indicating any possible incoherence.

Helps displaying arborescence at a chosen breaking down level. This one is initiated in a new document, which can be possibly saved.

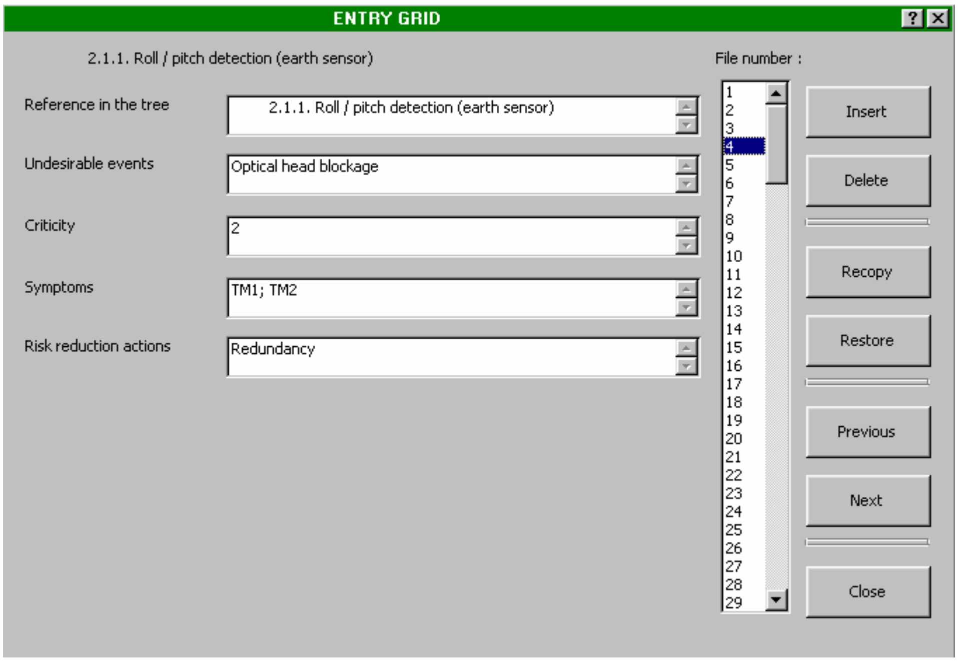
Allows adjusting the space generated by the program between the numbers of different arborescence levels.

1.
↔1.1.

Allows adjusting the height of cells in the sheet.

3.4 Typing Grid

Command "Typing grid" of menu PRA enables to display a grid to be informed which reassumes the different PRA fields (see example below).



ENTRY GRID

2.1.1. Roll / pitch detection (earth sensor)

Reference in the tree: 2.1.1. Roll / pitch detection (earth sensor)

Undesirable events: Optical head blockage

Criticity: 2

Symptoms: TM1; TM2

Risk reduction actions: Redundancy

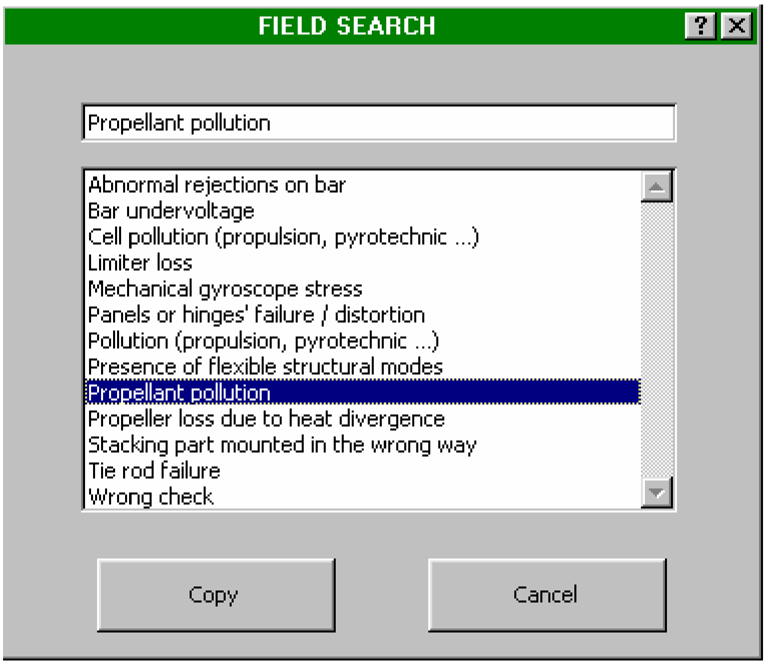
File number : 4

Such grid helps display different PRA files (corresponding to different lines of the latter) that user may select using cursor or buttons "Previous" and "Next". Position in arborescence is reminded in grid upper section.

Then, user may:
. insert or cancel files at desired positions (buttons "Insert" and "Cancel"),
. inform or modify a sheet then recopy it in PRA document (button "Recopy"),
. restore sheet in its initial condition, as soon as this one remains selected (button "Restore").

3.5 Field Search

Command "Field Search" of menu PRA helps display preliminarily-entered information in all cells of selected column.



Propellant pollution

Abnormal rejections on bar
Bar undervoltage
Cell pollution (propulsion, pyrotechnic ...)
Limiter loss
Mechanical gyroscope stress
Panels or hinges' failure / distortion
Pollution (propulsion, pyrotechnic ...)
Presence of flexible structural modes
Propellant pollution
Propeller loss due to heat divergence
Stacking part mounted in the wrong way
Tie rod failure
Wrong check

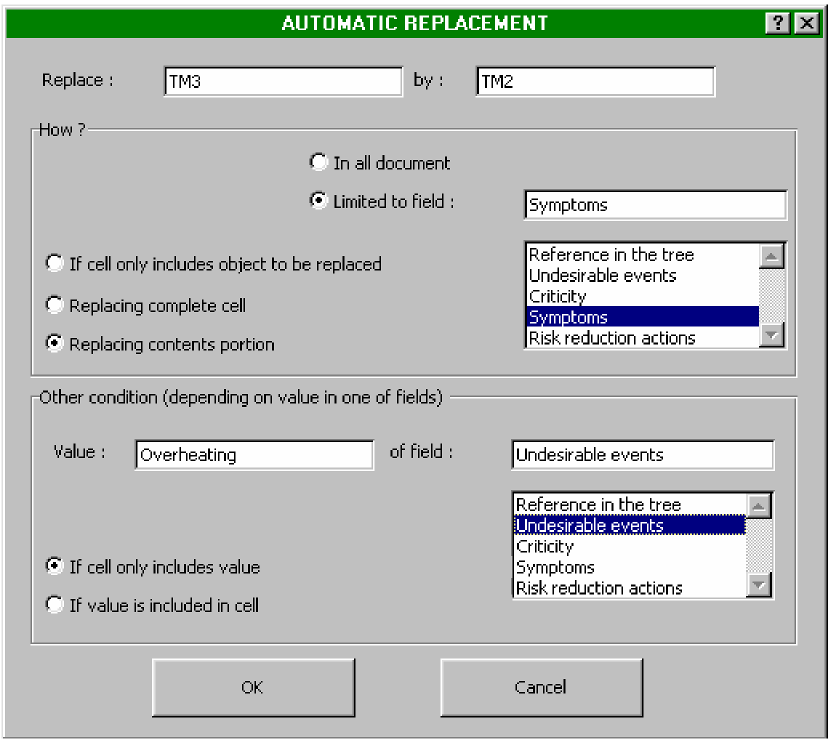
Such information is sorted out in alphabetic or increasing order in dialog box, and a cursor helps facilitating the search thereof.
Selected information, which is displayed in dialog box top section, may then be recopied in cell selected by simply acting on button "Copy".

Such functionality prevents from reentering already saved information and helps standardize this one in order to facilitate subsequent selection thereof through multi-criteria sorting.

3.6 Replacing Automatically

Command "Replacing Automatically" of menu PRA allows modifying terms used in PRA depending on different criteria, as shown in dialog box of next page.

In this example, telemetry TM3 is replaced by TM12 in field "Observable Symptoms" only when a overheating is apprehended. Other informed telemetry applications in this field are not affected by such modification.



AUTOMATIC REPLACEMENT

Replace : TM3 by : TM2

How ?

○ In all document

● Limited to field : Symptoms

Reference in the tree
Undesirable events
Criticity
Symptoms
Risk reduction actions

○ If cell only includes object to be replaced

○ Replacing complete cell

● Replacing contents portion

Other condition (depending on value in one of fields)

Value : Overheating of field : Undesirable events

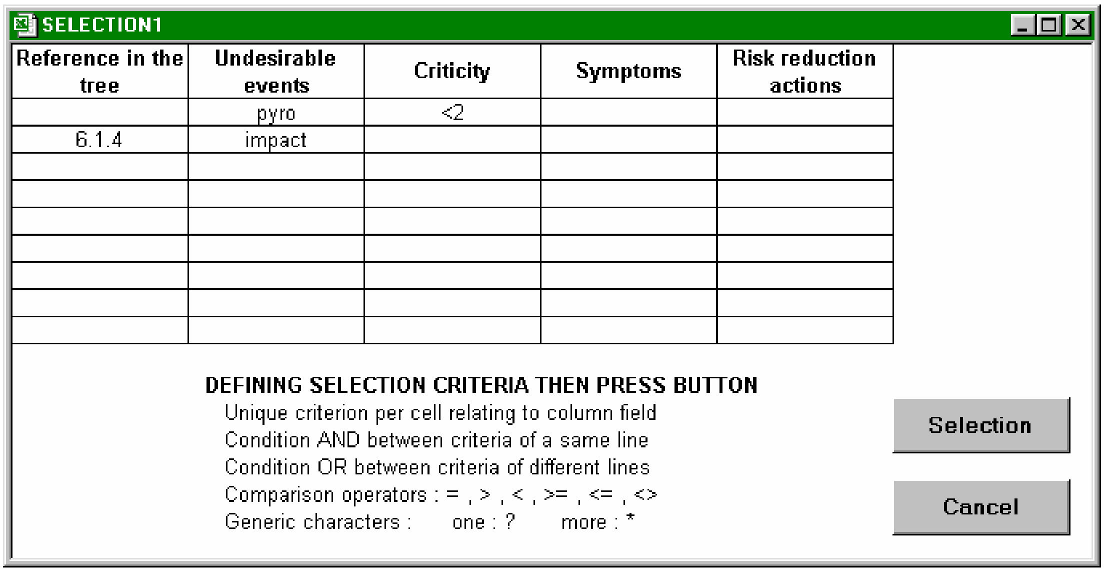
Reference in the tree
Undesirable events
Criticity
Symptoms
Risk reduction actions

● If cell only includes value

○ If value is included in cell

3.7 Selection

Command "Selection" of menu PRA helps perform searching in analysis document from multiple criteria.
Initiating such command displays a selection table in which user finds out again different fields of his document.



SELECTION1

Reference in the tree	Undesirable events	Criticity	Symptoms	Risk reduction actions
	pyro	<2		
6.1.4	impact			

DEFINING SELECTION CRITERIA THEN PRESS BUTTON
Unique criterion per cell relating to column field
Condition AND between criteria of a same line
Condition OR between criteria of different lines
Comparison operators : = , > , < , >= , <= , <>
Generic characters : one : ? more : *

So, he defines his criteria as follows :

. Each table cell only includes one criterion relating to relevant-column field.
. A condition AND is considered between criteria of a same line.

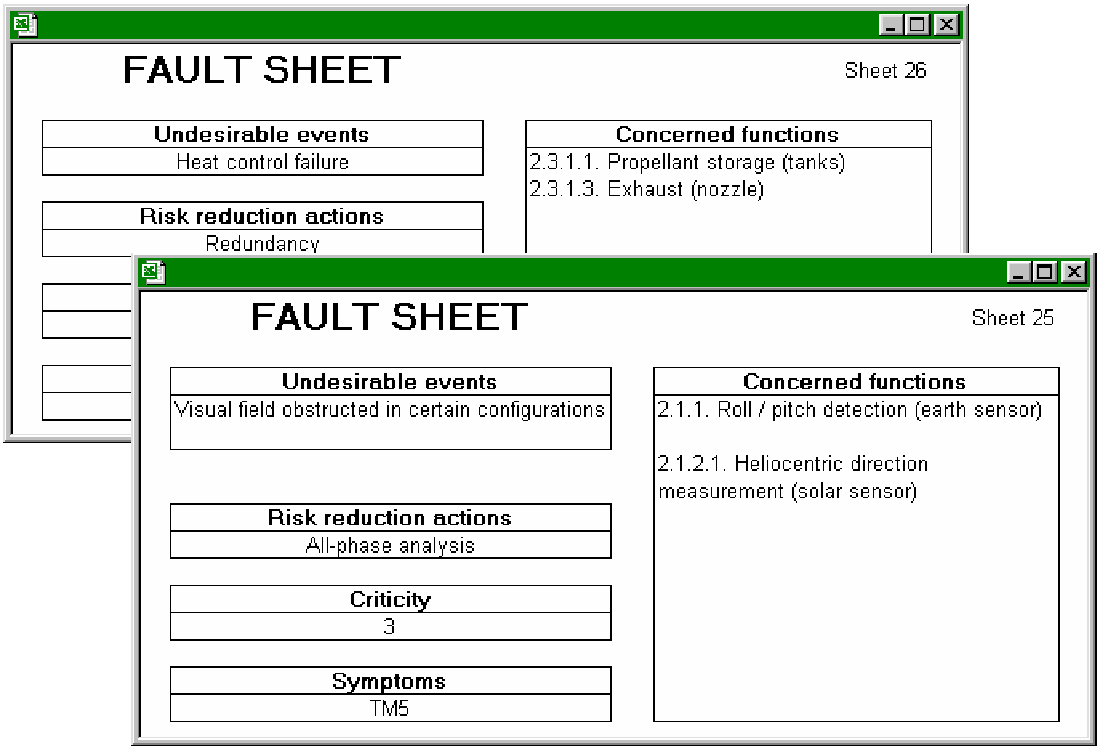
. A condition OR is considered between criteria of different lines.

So, previous example leads to searching apprehended events relating to pyrotechnics with criticity lower than 2, and those relating to impacts for product function whose reference in arborescence begins with 6.1.4.
Selection criteria may require comparison operators (= , > ,< , >= [higher or equal], <= [lower or equal]) and generic characters (? [a whatsoever character], * [many whatsoever characters]).

After defining his criteria, user commands selection by pressing button "Selection" located close to table.
So, search results are displayed on sheet together with selection criteria.

3.8 Synthesis

Command "Synthesis" of menu PRA helps performing automatically a PRA synthesis document, as that shown below, from a user predefined format.



FAULT SHEET

Sheet 26

Undesirable events
Heat control failure

Risk reduction actions
Redundancy

Concerned functions
2.3.1.1. Propellant storage (tanks) 2.3.1.3. Exhaust (nozzle)

FAULT SHEET

Sheet 25

Undesirable events
Visual field obstructed in certain configurations

Risk reduction actions
All-phase analysis

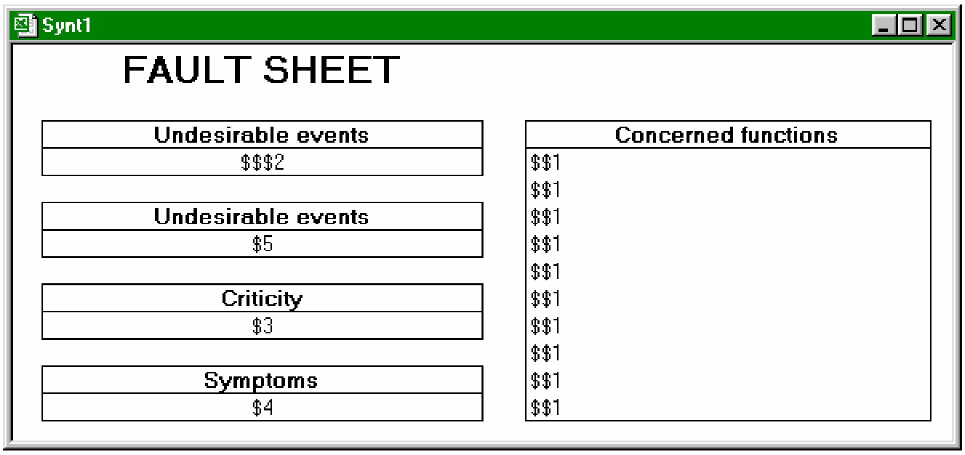
Criticity
3

Symptoms
TM5

Concerned functions
2.1.1. Roll / pitch detection (earth sensor) 2.1.2.1. Heliocentric direction measurement (solar sensor)

In addition to a synthesis depending on apprehended events, the generated document may e.g. concern criticity, so as to set a hierarchy in actions for reducing risks, or observability, for informing system instructions manual on possible causes of probable hazards.

Synthesis format corresponding to such example is shown below :



Synt1

FAULT SHEET

Undesirable events
$$$2

Undesirable events
$5

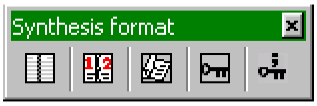
Criticity
$3

Symptoms
$4

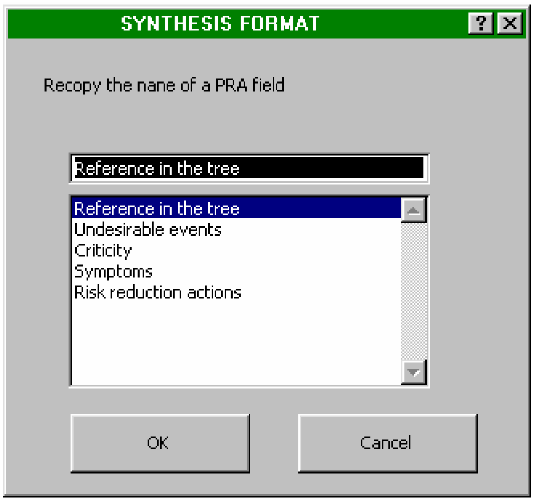
Concerned functions
$$1
$$1
$$1
$$1
$$1
$$1
$$1
$$1
$$1
$$1

Command "Synthesis Format" enables to create such format, save this one in a directory specific to user or recover a pre-saved format.

Creating a new synthesis format is carried out from a blank format sheet that the user documents using the following utilities bar :



Allows recopying in any sheet cell the name of one PRA field using a scrolling menu as that shown below.



SYNTHESIS FORMAT

Recopy the nane of a PRA field

Reference in the tree

- Reference in the tree
- Undesirable events
- Criticity
- Symptoms
- Risk reduction actions

Allows entering, in any sheet cell, the reference of a PRA field using a scrolling menu similar to previous one.
During synthesis, this reference (of type $ + field No.) will be automatically replaced by the information entered in this field for any page of document.

Allows to enter, in one vertical cell table located any place in sheet, the reference of a PRA field using a scrolling menu similar to previous one.
During synthesis, this table (the reference of which is of type $$ + field No.) will be automatically replaced by the list of information entered in this field for any page of document.

Allows to enter, in any sheet cell, the reference of the PRA field on which the synthesis will be carried out (activation field).
A synthesis sheet will be generated as many times as different information will have been entered in cells of this field. Such reference (of type $$$ + field No.) will also be replaced by relevant information.

Differs from previous button due to the fact it is used for fields capable of including a list of information separated by semicolons (e.g. : TM1; TM2; TM12).
A synthesis sheet will then be generated for any different information. Reference used is of type $$$$ + field No.

This utilities bar may be displayed or be hidden using command "utilities bar "Synthesis format" ".

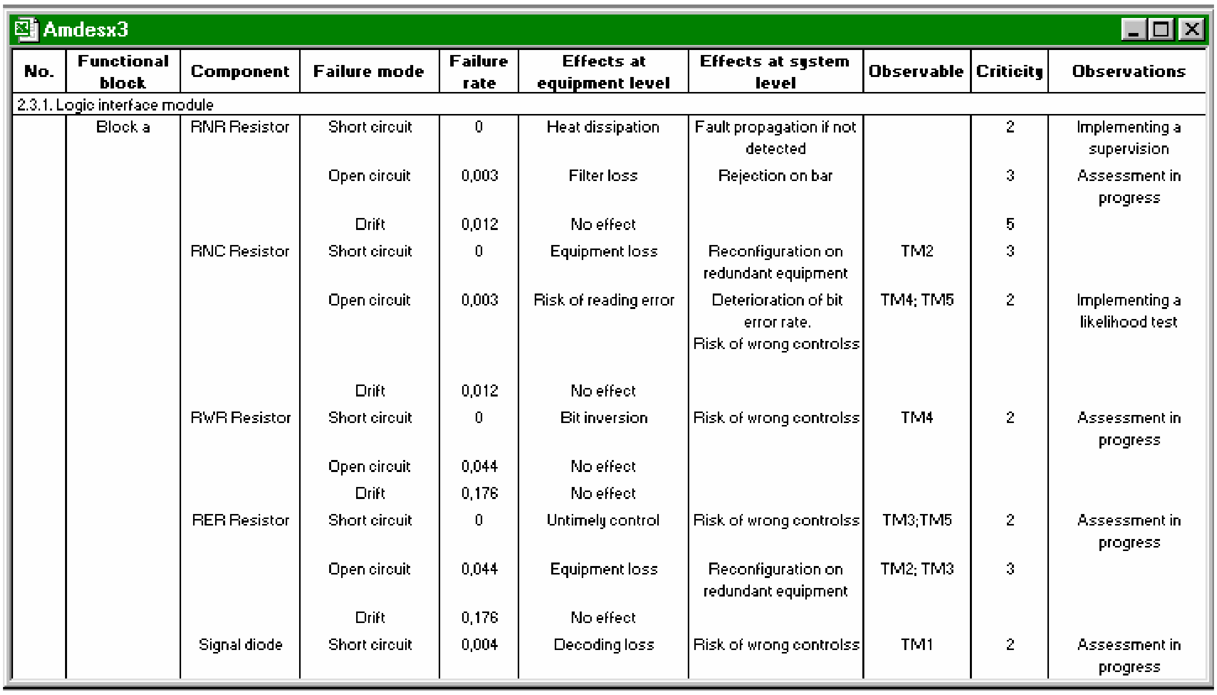
During synthesis, selection table according to various criteria is offered to user to possibly limit the synthesis to a PRA portion.

3.9 Sheets

Command "Sheets" of menu PRA helps performing automatically a document for printing which reassumes the different PRA sheets according to same format as that proposed by the entry mask. Such document may cover the whole PRA or only certain sheets.

4 FMECA

The Failure Mode Effect and Criticity Analysis (FMECA) consists in searching the effects at equipment level then at system level of elementary-component faults (see example below).



No.	Functional block	Component	Failure mode	Failure rate	Effects at equipment level	Effects at system level	Observable	Criticity	Observations
2.3.1. Logic interface module									
	Block a	RNR Resistor	Short circuit	0	Heat dissipation	Fault propagation if not detected		2	Implementing a supervision
			Open circuit	0,003	Filter loss	Rejection on bar		3	Assessment in progress
			Drift	0,012	No effect			5	
		RNC Resistor	Short circuit	0	Equipment loss	Reconfiguration on redundant equipment	TM2	3	
			Open circuit	0,003	Risk of reading error	Deterioration of bit error rate. Risk of wrong controlss	TM4; TM5	2	Implementing a likelihood test
			Drift	0,012	No effect				
		RWR Resistor	Short circuit	0	Bit inversion	Risk of wrong controlss	TM4	2	Assessment in progress
			Open circuit	0,044	No effect				
			Drift	0,176	No effect				
		RER Resistor	Short circuit	0	Untimely control	Risk of wrong controlss	TM3;TM5	2	Assessment in progress
			Open circuit	0,044	Equipment loss	Reconfiguration on redundant equipment	TM2; TM3	3	
			Drift	0,176	No effect				
		Signal diode	Short circuit	0,004	Decoding loss	Risk of wrong controlss	TM1	2	Assessment in progress

Fault modes considered may be defined at component or functional unit level (a few components providing an elementary function) and are deriving from standards or databases specific to user or project concerned.

4.1 Main Functionalities

FAILCAB helps user conduct FMECA and then operate it. It offers the following functionalities, accessible from menu FMECA (see next page) :

. Creating formats (FMECA, parts list, fault mode lists)
. Entering material product arborescence
. Creating FMECA document (database)
. Entering data fostering their standardization
(entry grid, field searching, replacing automatically)

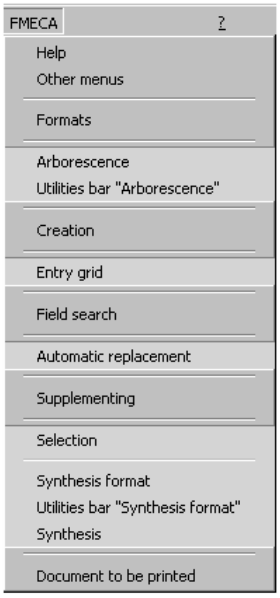
. Supplementing automatically the FMECA from :

- Parts lists (list of components, functional units, fault rates ...)
- Fault mode databases (at component or functional unit level)
- Syntheses of effects (from equipment to system)
- Any other databases imported on Excel

. Selecting in FMECA from multiple criteria

. Generating synthesis documents from personalized formats
(synthesis on symptoms observable using the example)

. Formatting prior to printing



Menu "FMECA"

4.2 Creating Formats

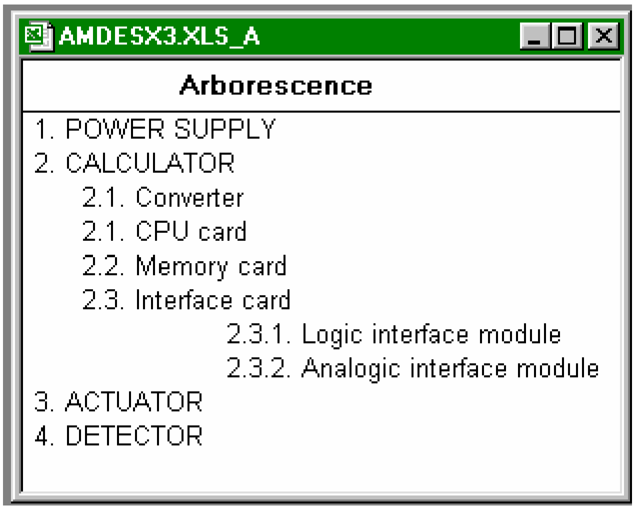
Similar to that of menu PRA, command "Formats" of menu FMECA helps creating formats for various documents (FMECA, Parts Lists, Lists of fault modes...) in the French or English language.

It also allows obtaining standard formats defined in standards X 60-510, CEI 812-1985 and MIL-STD-1629A.

It is also used to save such formats in a directory specific to user or recover pre-saved formats.

4.3 Entering Product's Material Arborescence

Command "Arborescence" of menu FMECA allows entering the material breakdown as in example below.



AMDESX3.XLS_A

```
              Arborescence
1. POWER SUPPLY
2. CALCULATOR
     2.1. Converter
     2.1. CPU card
     2.2. Memory card
     2.3. Interface card
                    2.3.1. Logic interface module
                    2.3.2. Analogic interface module
3. ACTUATOR
4. DETECTOR
```

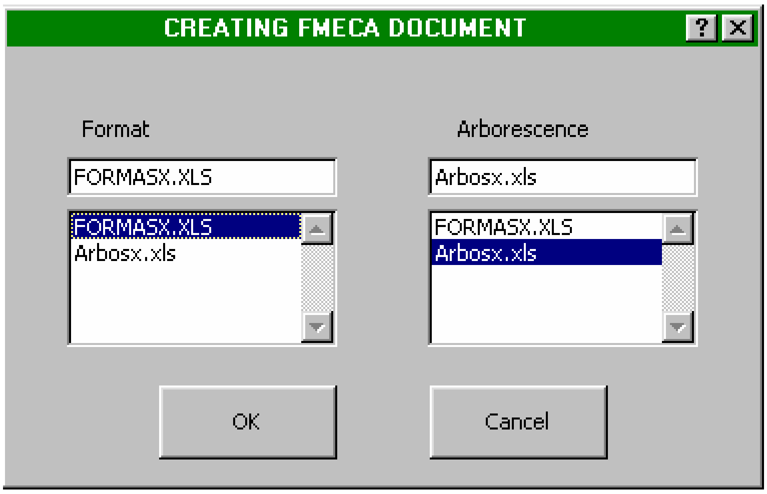
Initiating such command generates the creation of a new document where user may enter the arborescence using dialog boxes and same utilities bar as that used for the PRA (see PRA section of manual).

Such utilities bar is displayed or hidden using command " Arborescence utilities bar".

4.4 Creating FMECA Document

Command "Creation" of menu FMECA helps creating FMECA from a document format and material product arborescence.

Its activation generates the display of the following dialog box in which user specifies the concerned documents among all opened documents (format and arborescence).



CREATING FMECA DOCUMENT

Format: FORMASX.XLS

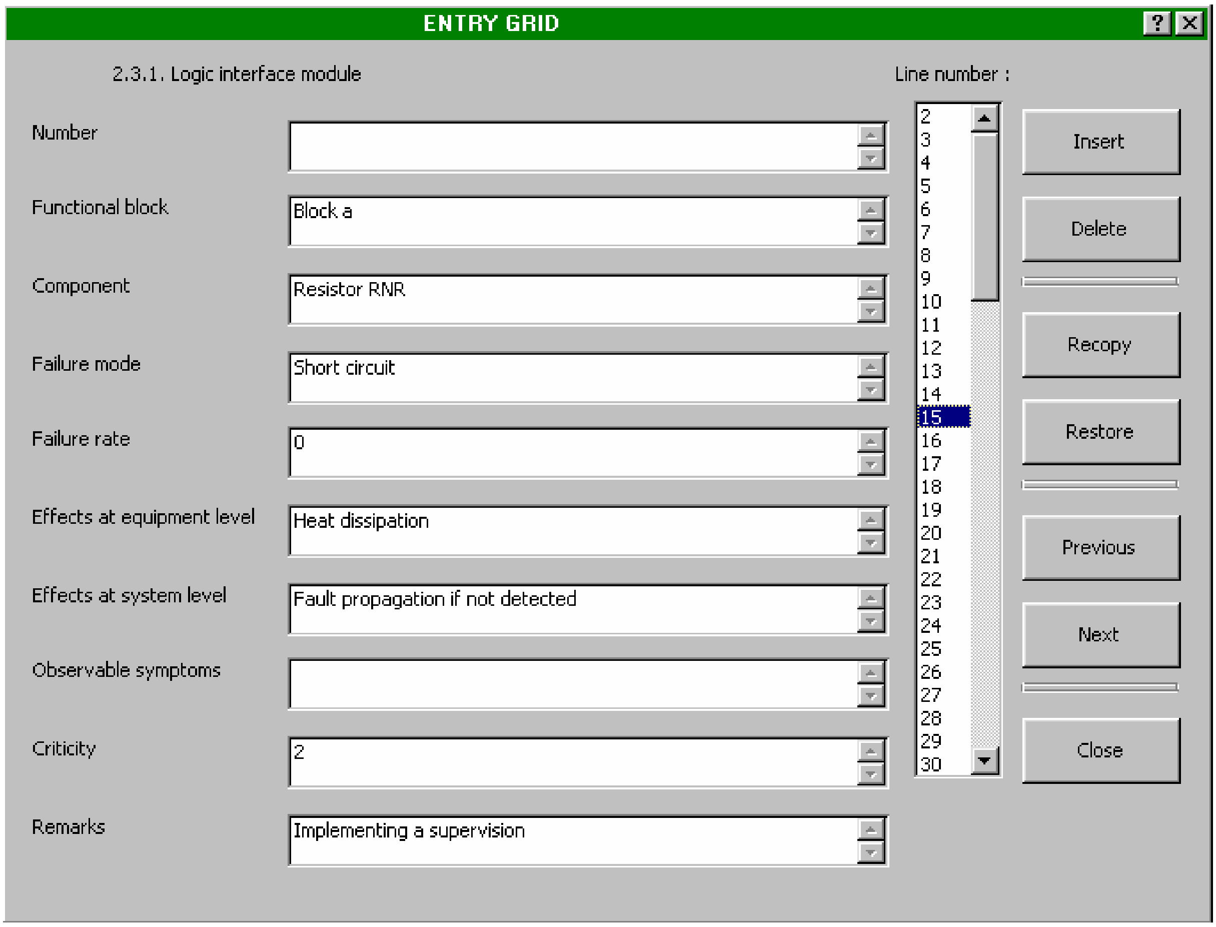
Arborescence: Arbosx.xls

Acting on button OK results in creating a document as that shown below.

Number	Functional block	Component	Failure mode	Failure rate	Effects at equipment level	Effects at system level	Observable symptoms	Criticity	Remarks
# 1. POWER SUPPLY									
# 2. CALCULATOR									
# 2.1. Converter									
# 2.1. CPU card									
# 2.2. Memory card									
# 2.3. Interface card									
# 2.3.1. Logic interface module									
# 2.3.2. Analogic interface module									
# 3. ACTUATOR									
# 4. DETECTOR									

4.5 Entry Grid

Same as that of menu PRA, command "Entry grid" of menu FMECA allows to display a grid to be informed which reassumes the different FMECA fields (see example below).



ENTRY GRID

2.3.1. Logic interface module

Number

Functional block: Block a

Component: Resistor RNR

Failure mode: Short circuit

Failure rate: 0

Effects at equipment level: Heat dissipation

Effects at system level: Fault propagation if not detected

Observable symptoms

Criticity: 2

Remarks: Implementing a supervision

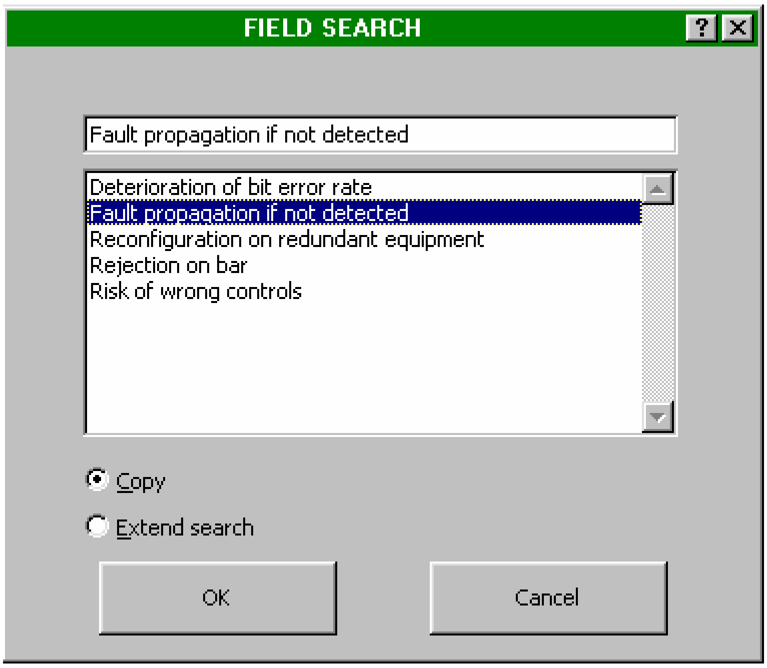
Line number : 15

Such grid helps displaying different PRA sheets (corresponding to different lines of the latter) the user may select using a cursor or buttons "Previous" and "Next". Position in arborescence is reminded on top of grid.

So, the user may:
. insert or delete sheets at desired locations,
. inform or modify one sheet then recopy in document PRA,
. restore sheet to its initial condition, as long as this sheet remains selected.

4.6 Field Search

Command "Field search" of menu FMECA helps displaying preliminarily entered information in cells of column selected. It looks like to that of menu PRA, but displayed information is limited to the arborescence portion in which selected cell can be found.


FIELD SEARCH

Fault propagation if not detected

- Deterioration of bit error rate
- Fault propagation if not detected
- Reconfiguration on redundant equipment
- Rejection on bar
- Risk of wrong controls

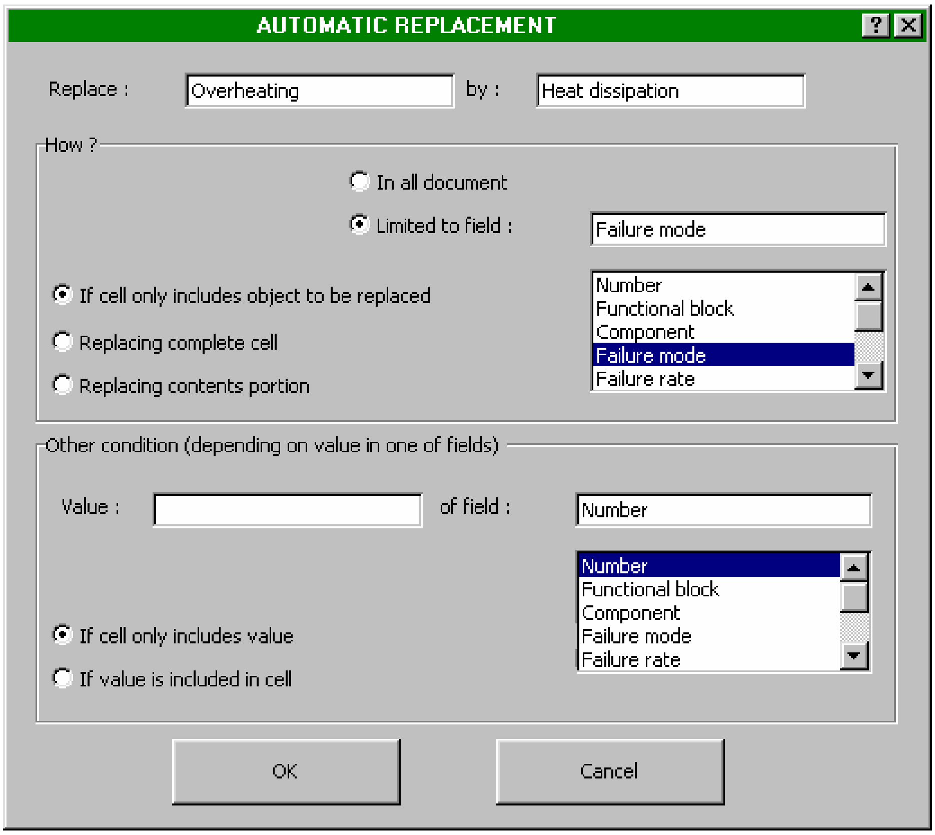
● Copy

○ Extend search

However, user may extend search by going progressively up in arborescence.

4.7 Replacing Automatically

Same as that of menu PRA, command "Automatic replacement" of menu FMECA allows to modify terms depending on different criteria, as shown in following dialog box.


AUTOMATIC REPLACEMENT

Replace : Overheating by : Heat dissipation

How ?

○ In all document

● Limited to field : Failure mode

- Number
- Functional block
- Component
- Failure mode
- Failure rate

● If cell only includes object to be replaced

○ Replacing complete cell

○ Replacing contents portion

Other condition (depending on value in one of fields)

Value : of field : Number

- Number
- Functional block
- Component
- Failure mode
- Failure rate

● If cell only includes value

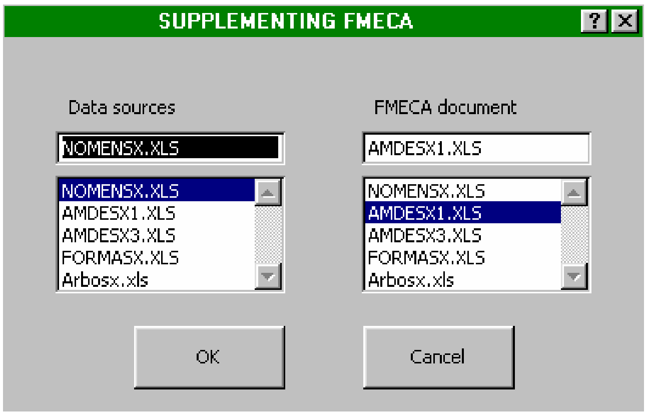
○ If value is included in cell

4.8 Supplementing FMECA Automatically

Command "Supplementing" of menu FMECA allows to supplement automatically FMECA from various databases.

Such supplementing may be performed from
. Parts lists (list of components, functional units, fault rates ...),
. Fault mode lists (at component or functional unit level),
. Syntheses of effects (from equipment to system),
. Any other databases imported on Excel™.

Same as for command "Creation", initiating command "Supplementing" generates the display of a dialog box in which user specifies concerned documents among all opened documents.



SUPPLEMENTING FMECA

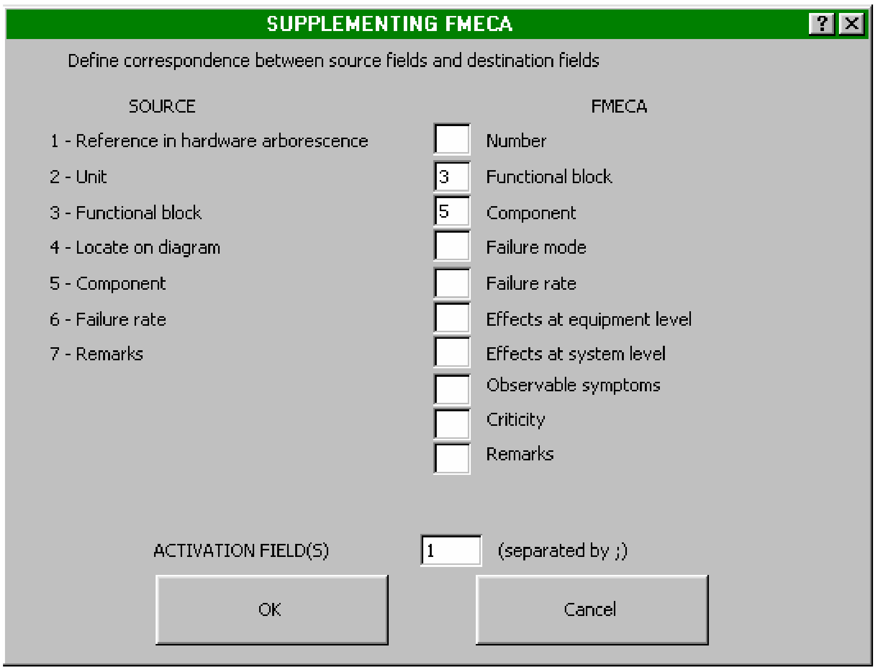
Data sources: NOMENSX.XLS

NOMENSX.XLS
AMDESX1.XLS
AMDESX3.XLS
FORMASX.XLS
Arbosx.xls

FMECA document: AMDESX1.XLS

NOMENSX.XLS
AMDESX1.XLS
AMDESX3.XLS
FORMASX.XLS
Arbosx.xls

Acting on button OK generates the display of a second dialog box in which user finds fields of both selected documents.



SUPPLEMENTING FMECA

Define correspondence between source fields and destination fields

SOURCE		FMECA
1 - Reference in hardware arborescence		Number
2 - Unit	3	Functional block
3 - Functional block	5	Component
4 - Locate on diagram		Failure mode
5 - Component		Failure rate
6 - Failure rate		Effects at equipment level
7 - Remarks		Effects at system level
		Observable symptoms
		Criticity
		Remarks

ACTIVATION FIELD(S) 1 (separated by ;)

So it indicates correspondence between source document fields and those of FMECA together with one or more activation fields, before running supplementing procedure.

Recopying source field information to the fields to be supplemented is then carried out each time correspondence between activation fields of both documents may be established. So, in this example, supplementing is performed as follows :

Reference in hardware arborescence	Unit	Functional block	Locate on diagram	Component	Failure rate	Remarks
2.3.1	Logic interface module	Block a	R1	Resistor RNR		
			R2	Resistor RNC		
			D1	Diode signal		
		Block b	C2	Capacitor CKR		
			D2	ZENER Diode		
			Q1	Switching transistor		
			U1	Quartz		
2.3.2	Analogic interface module	Block c	R1	Resistor RNR		
			R2	Resistor RNR		
			C1	Capacitor CKR		
			C2	Capacitor CLR		
			Q1	Linear transistor		
		Block d	R5	Resistor RJR		
			R6	Thermistor RTH		
			Q1	Switching transistor		

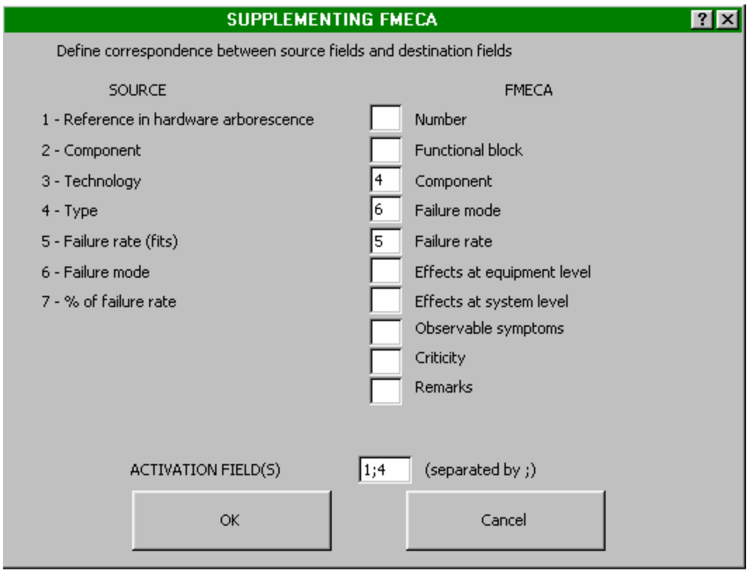
Source document (parts list)

Number	Functional block	Component	Failure mode	Failure rate	Effects at equipment level	Effects at system level	Observable symptoms	Criticity	Remarks
# 2.3. Interface card									
# 2.3.1. Logic interface module									
	Block a	Resistor RNR							
		Resistor RNC							
		Diode signal							
	Block b	Capacitor CKR							
		ZENER Diode							
		Switching transistor							
		Quartz							
# 2.3.2. Analogic interface module									
	Block c	Resistor RNR							
		Resistor RNR							
		Capacitor CKR							
		Capacitor CLR							
		Linear transistor							
	Block d	Resistor RJR							
		Thermistor RTH							
		Switching transistor							

FMECA after supplementing

The activation field corresponds here to reference in material arborescence (1). Information located in Functional Unit (3) and Component fields (5) were recopied in FMECA at different positions of arborescence stated in source document.

Example below shows how this operation is performed with various activation fields. It regards a supplementing application from a list of fault modes.



SUPPLEMENTING FMECA

Define correspondence between source fields and destination fields

SOURCE		FMECA
1 - Reference in hardware arborescence		Number
2 - Component		Functional block
3 - Technology	4	Component
4 - Type	6	Failure mode
5 - Failure rate (fits)	5	Failure rate
6 - Failure mode		Effects at equipment level
7 - % of failure rate		Effects at system level
		Observable symptoms
		Criticity
		Remarks

ACTIVATION FIELD(S) 1;4 (separated by ;)

Reference in hardware arborescence	Component	Technology	Type	Failure rate (fits)	Failure mode	% of failure rate
2.3.1	Resistor RNR	Metal layer	*RNR*	0,015	Short circuit Open circuit Drift	0% 20% 80%
2.3.1	Capacitor CKR	ceramics	*CKR*	0,09	Short circuit Open circuit Drift	35% 20% 45%
2.3.1	Switching transistor		*switching* *transistor*	0,06	Short circuit Open circuit Drift	60% 40% 0%
2.3.1	Switch SPDT		*Switch* *SPDT*		Blocked in ON position Blocked in OFF position Intermediate position	
2.3.1	Switch DPDT		*Switch* *DPDT*		Blocked in ON position Blocked in OFF position Intermediate position	
2.3.1	Quartz		*Quartz*	20	Short circuit Open circuit Drift	

Source document (list of fault modes)

Information located in Failure Mode (6) and Fault Rate (5) fields will be recopied in FMECA as soon as one type of component (4) is recognized in FMECA Component field and correspondence with Reference in arborescence (1) is established.

Generic character *, which replaces any number of characters, is used to recognize the type of component in a chain of characters.

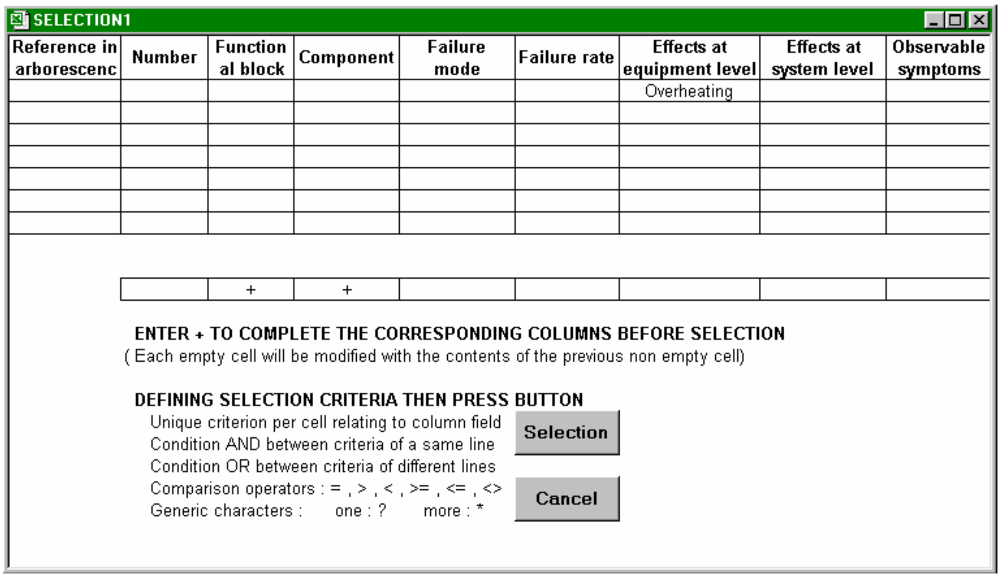
A field of source document defining positions in arborescence should be called with the word "arborescence" in its name. So, supplementing application regards here only section 2.3.1. of arborescence.

Number	Functional block	Component	Failure mode	Failure rate	Effects at equipment level	Effects at system level	Observable symptoms	Criticity	Remarks
#	2.3.1. Logic interface module								
	Block a	Resistor RNR	Short circuit Open circuit Drift						
		Resistor RNC	Short circuit Open circuit Drift						
		Diode signal							
	Block b	Capacitor CKR	Short circuit Open circuit Drift						
		ZENER Diode	Short circuit Open circuit Drift						
		Switching transistor	Short circuit Open circuit Drift						
		Quartz	Short circuit Open circuit Drift						
#	2.3.2. Analogic interface module								
	Block c	Resistor RNR Resistor RNR Capacitor CKR Capacitor CLR Linear transistor							
	Block d	Resistor RJR Thermistor RTH Switching transistor							

FMECA after supplementing

4.9 Selection

Command "Selection" of menu FMECA is used as that of menu PRA though selection table contains an additional line making it possible for user to specify whether fields should be informed by the program during selection (enter sign +).



Reference in arborescenc	Number	Function al block	Component	Failure mode	Failure rate	Effects at equipment level	Effects at system level	Observable symptoms
						Overheating		

	+	+					

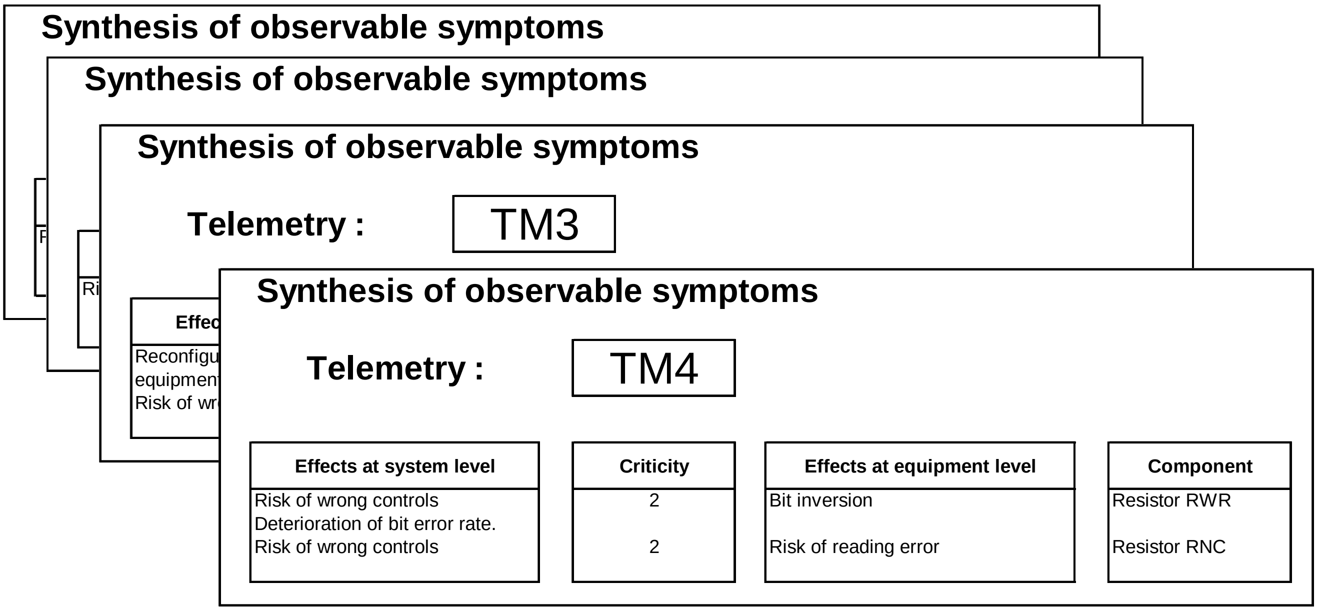
ENTER + TO COMPLETE THE CORRESPONDING COLUMNS BEFORE SELECTION
(Each empty cell will be modified with the contents of the previous non empty cell)

DEFINING SELECTION CRITERIA THEN PRESS BUTTON
Unique criterion per cell relating to column field
Condition AND between criteria of a same line
Condition OR between criteria of different lines
Comparison operators : = , > , < , >= , <= , <>
Generic characters : one : ? more : *

So, in previous example, all fault modes leading to an overheating will be informed with, for each of them, the name of component and that of relevant functional unit. Selection criteria are initiated on results sheet right section.

4.10 Synthesis

Same as that of menu PRA, command "Synthesis" of menu FMECA helps performing automatically a synthesis document, as that shown below, from a user predefined format.



Synthesis of observable symptoms

Synthesis of observable symptoms

Synthesis of observable symptoms

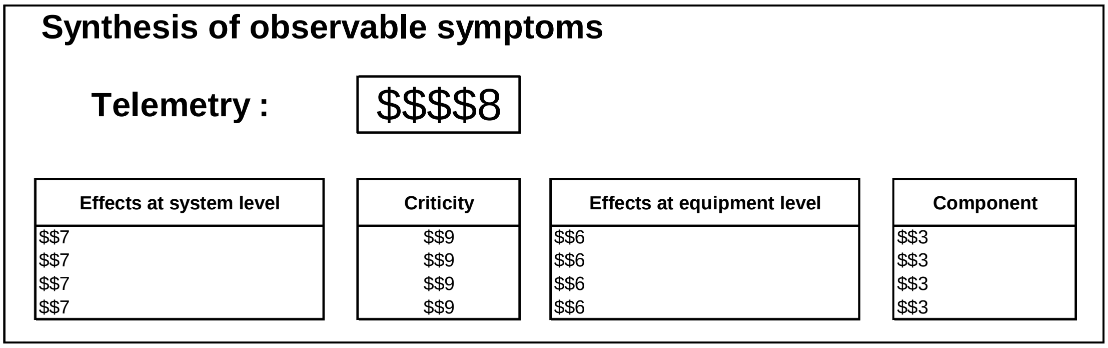
Telemetry : TM3

Synthesis of observable symptoms

Telemetry : TM4

Effects at system level	Criticity	Effects at equipment level	Component
Risk of wrong controls	2	Bit inversion	Resistor RWR
Deterioration of bit error rate.			
Risk of wrong controls	2	Risk of reading error	Resistor RNC

Synthesis format used in this example is as follows :



Synthesis of observable symptoms

Telemetry : $$$$8

Effects at system level	Criticity	Effects at equipment level	Component
$$7	$$9	$$6	$$3
$$7	$$9	$$6	$$3
$$7	$$9	$$6	$$3
$$7	$$9	$$6	$$3

It was created from command "Synthesis Format" which allows to generate a blank format sheet the user informs using utilities bar "Synthesis Format ", already shown in PRA section.

During synthesis , the selection table is offered to user for possibly limiting the synthesis to an FMECA section. The user should specify whether fields should be informed by program during selection (enter sign +).

4.11 Formatting before Printing

Command "Document to be printed" of menu FMECA generates a document similar to analysis document (active sheet) in which names of different fields are reminded on top of each page.
A page jumping is systematically inserted between each arborescence element.
User, using command «Formatting» of spreadsheet, before initiating document printing, may add a specific heading.

OPERATING LICENCE AGREEMENT

OF FAILCAB SOFTWARE PACKAGE

ARTICLE 1 : SUBJECT

The purpose of this Agreement is to define the conditions in which the CAB INNOVATION Company grants the customer with a non-transferable, non-exclusive and personal right to use the software package referred to as "FAILCAB" and whose features are specified in user's manual.

ARTICLE 2 : SCOPE OF THE OPERATING RIGHT

The customer may use the software package on one single computer and on a second one provided that the second computer does not operate at the same time as the first one. The customer can only have one software package copy maintained in a safe place as a backup copy.

If this license is regarding a performance on site, the customer may install the package software on a server, while scrupulously complying with purchase conditions stated on specific conditions especially defining the maximum number of users authorized to use the software package from their terminal and the maximum number of users authorized to use it simultaneously. The customer is therefore authorized to perform a number of software package documentation copies equal to the maximum number of users allowed to use it..

CAB INNOVATION will be in a position to perform inspections, either itself or through a specialized entity purposefully authorized by CAB INNOVATION, at customer premises to verify if customer has met its requirements : number of software package copies used, location of such copies, etc... Parties will agree as regards the practical modalities of performance of such inspections so as to disturb minimally customer's activity.

ARTICLE 3 : DELIVERY, INSTALLATION AND RECEPTION

The software package and attached supplies will be delivered to the customer on mail reception date. The customer installs, at its own costs, the software package using relevant manual delivered by CAB INNOVATION.
The customer performs the inventory and shall inform CAB INNOVATION, within three working days of the delivery, of any apparent nonconformity with respect to the order. The customer is liable for any loss or any damage caused to supplies as from the delivery.

ARTICLE 4 : TESTING AND GUARANTEE

Guarantee is effective as from the mail delivery date set forth in Article 3 and has a three-month validity.
During the guarantee validity, if the customer experiences a software package operation trouble, he should inform CAB INNOVATION about it, so as to receive any helpful explanations with the purpose of remedying such trouble. If the trouble is continuing, the customer will return the C.D. ROM to CAB INNOVATION, at CAB INNOVATION's Head Office, at his own expense and with registered mail with acknowledgement of receipt, by specifying exactly the troubles encountered.

Within the three months of reception of consignment set forth in preceding paragraph, CAB INNOVATION will deliver, at its own expense, a new product version to the customer. This new version will be benefiting of the same guarantee as benefited the first version.

The customer looses the benefit of the guarantee if he does not comply with the instructions manual recommendations, if he performs modifications of configuration set forth in Article 2 above without obtaining a prior written consent from CAB INNOVATION, or if he performs modifications, additions, corrections, etc... on software package, even with the support from a specialized service company, without obtaining a prior written consent from CAB INNOVATION.

ARTICLE 5 : PROPERTY RIGHT

CAB INNOVATION declares to be holding all the rights provided for by the intellectual property code for FAILCAB package software and its documentation.

As this operating-right granting generates no property-right transfer, the customer abstains from :
- any FAILCAB software package reproduction, whether it is wholly or partly carried out, whatever the form assumed, excepting the number of copies authorized in Article 2 ;
- any FAILCAB software package transcription in any other language than that provided for in this Agreement (see Appendix), any adaptation to use it in other equipment or with other basic software packages de base than those provided for in this Agreement.

To ensure this property protection, the customer undertakes especially to

- maintain clearly visible any property and copyright specifications that CAB INNOVATION would have affixed on programs, supporting material and documentation ;
- assume with respect to his staff and any external person any helpful information and prevention step.

ARTICLE 6 : USING SOURCES

Any FAILCAB software package modification, transcription and, as a general rule, any operation requiring the use of sources and their documentation are exclusively reserved for CAB INNOVATION.
The customer holds the right to get the information required for the software package interoperability with other softwares he is using, under the conditions provided for in the intellectual property code.
In each case, an amendment of these provisions will set out the price, time limits and general terms of performance thereof.

ARTICLE 7 : LIABILITY

The customer is liable for :
- choosing FAILCAB software package, its adequacy with his requirements, precautions to be assumed and back-up files to be made for his operation, his staff qualification, as he received from CAB INNOVATION recommendations and information required upon its operating conditions and limits of its performances set forth in user's manual;
- the use made for results he obtains.

CAB INNOVATION is liable for the software package conformity with his documentation. The customer shall prove any possible non-conformity.
CAB INNOVATION does not assume any whatsoever guarantee, whether explicit or implicit, relating to the software package, manuals, attached documentation or any supporting item or material provided and, especially, any guarantee for marketing of any products relating to software package or for using software package for a determined use, any guarantee for absence of forgery, etc...
Under no circumstances CAB INNOVATION could be held responsible for any whatsoever damage, especially loss in performance, data loss or any other financial loss resulting from the use or impossibility to use the FAILCAB software package, even if CAB INNOVATION was told about the possibility of such damage.
In the event where CAB INNOVATION liability is retained, it is expressly agreed upon that the total amount of compensation to be paid by CAB INNOVATION, all cases taken together, could not in any way exceed the initial-royalty price reduced by 25 % per period of twelve months elapsed as from the mailing delivery date.

ARTICLE 8 : DURATION

This Agreement is entered into for an undetermined period of time as of the date set forth in Article 3.

ARTICLE 9 : TERMINATION

Each party may terminate this Agreement, by registered mail with acknowledgement of receipt forwarded to the other party, for any breach by such party of its obligations, despite a notice remaining unresponsive for 15 days, and this occurring with no prejudice to damages it could claim and provided that the last paragraph of Article 7 above, be enforced.

At end of this Agreement or in case of termination for whatsoever reason, the customer will have to stop using FAILCAB software package, pay all sums remaining due on date of termination and return all elements composing the software package (computer programs, documentation, etc ...) without maintaining any copy of it.

ARTICLE 10 : ROYALTY

As a payment for the operating-right concession, the customer pays CAB INNOVATION an initial royalty the amount of which is determined in specific conditions.

ARTICLE 11 : PROHIBITED TRANFER

The customer refrains from transferring the software package operating right granted personally to him by these provisions. The customer also abstains from making documentation and supporting material (CD ROM), even free of charge, available to a person not expressly set forth in second paragraph of Article 2.

ARTICLE 12 : ADDITIONAL SERVICES

Any additional services will be subject to an amendment of these provisions, possibly through an exchange of letters, so as to specify the contents, modalities of achievement and the price.

ARTICLE 13 : CORRECTIVE AND PREVENTIVE MAINTENANCE

The corrective and preventive maintenance may be subject, upon customer's request, to a separate Agreement attached to these provisions.

ARTICLE 14 : ENTIRETY OF THE AGREEMENT

The user's manual defining the FAILCAB software package features is appended to these provisions.
The provisions of this Agreement and his Appendix express the entirety of the Agreement entered into between the parties. They are prevailing among any proposition, exchange of letters preceding its signing up, together with any other provision stated in documents exchanged between the parties and relating to the Agreement's subject matter.
If any whatsoever clause of this Agreement is null and void with respect to a rule of Law or a Law in force, it will considered as not being written though not involving the Agreement's nullity.

ARTICLE 15 : ADVERTISING

CAB INNOVATION could mention the customer in its business references as a FAILCAB software package user.

ARTICLE 16 : CONFIDENTIALITY

Each party undertakes not to disclose any kind of documents or information about the other party that it would have been informed of on the Agreement's performance and undertakes to have such obligation fulfilled by the persons it is liable for

ARTICLE 17 : AGREEMENT'S LANGUAGE

This Agreement is entered into and drawn up in the French language.
In the event where it is translated into one or more foreign languages, only the French text will be deemed authentic in case of any dispute between the parties.

ARTICLE 18 : APPLICABLE LAW - DISPUTES

The French Law governs this Agreement.
In the event of any disagreement over the interpretation and performance of any whatsoever provision of this Agreement, and if parties fail to reach an agreement under an arbitration procedure, only Toulouse’s Courts will be competent to settle the dispute, despite the plurality of defendants or the appeal for guarantee.