

Risk Analysis
Of
Paperless GMP Software

TITLE :	
AUTHORING GROUP :	
DATE ;	
SUPERSEDE PROTOCOL NO. :	

TABLE OF CONTENTS

Sr. No.	Contents		Page No.
1.	Introduction		
	1.1	Document Review	
	1.2	References	
	1.2.1	Project References	
	1.2.2	Standard and regulatory References	
2.	Risk Analysis		
	2.1	Intended use	
	2.2	End users	
	2.3	Foreseeable misuse	
	2.4	Characteristics Affecting Safety	
	2.5	Software classification	
	2.6	Risk analysis and evaluation	
	2.7	Risk traceability matrix	
	2.8	Overall assessment of residual risks	

1 Introduction

1.1 Document overview

This document covers the risk analysis of XXX device, designed in Paperless GMP software development project.

It contains:

- The risk analysis,
- The risk assessment report,
- The risk traceability matrix with software requirements.

1.2 References

1.2.1 Project References

#	Document Identifier	Document Title
[R1]	ID	Add your documents references. One line per document

1.2.2 Standard and regulatory References

#	Document Identifier	Document Title
[STD1]		Add your documents references. One line per document

Add the standard references to the table above. It may include ISO 14971, ISO 13485, IEC/TR 80002-1, IEC 62304, amongst others.

2 Risk Analysis

2.1 Intended use

Paste here intended use

2.2 End users

List the end users of the device: patients and/or medics and/or paramedics and their level of knowledge.

2.3 Foreseeable misuse

Add here the reasonably foreseeable misuses, like use outside the intended use

2.4 Characteristics Affecting Safety

Add here a table with questions found in Annex C of ISO 14971 and the answers about your medical device.

The table shall look like this.

#	Question of Annex C of ISO 14971	Answer
1	Intended use	See intended use
2	Question 2 ...	Add here answer

If your device is a networked device or a PEMS device, add here a second table with questions found in section Annex H.7.2 of IEC 60601-1, supplementing questions of annex C of ISO 14971 (see also section 14.13 of IEC 60601-1). This is recommended but not mandatory.

The table shall look like this.

#	Question of Annex H.7.2 of IEC 60601-1	Answer
1	Is connection to the network inconsistent with the intended use of each constituent PEMS?	Add here answer
2	Question 2 ...	Add here answer

2.5 Software classification

Given the intended use, the answers to questions above, and the software functional requirements (may add reference to a doc, like statement of work), the classification of the software is defined below:

Class	Justification	XXX Device
A	No injury or damage to health is possible	
B	Non serious injury is possible	
C	Death or serious injury is possible	

Add a cross in the classification of your device.

Justify your choice. Read the IEC 62304 standard to help you write the justification.

The justification shall be based on risk to the patient / user. Roughly if your software bears or mitigates:

- No risk or negligible risks, it is class A,
- Moderate (acceptable) risks, it is class B,
- Unacceptable risks, it is class C.

Note 1: the risk level is the one before software mitigation action.

For example: If there is an unacceptable risk before mitigation, that becomes acceptable after mitigation, and if the mitigation is made through software, then the software is class C (unacceptable risk before mitigation).

[Note 2: Read the IEC 62304, some components of your software may be of different class.

2.6 Risk analysis and evaluation

The matrix below contains the risk analysis table, used for the study of the risks associated with the device.

Add here a matrix with risk analysis.

Given the variety of risk analysis methods, the matrix may have different forms. The risk analysis method shall be described in the risk management plan.

If you use FMEA method, your matrix may look like this

1	2	3	4	5	6	7	8	9
ID	FUNCTION	FAILURE MODE	EFFECT OF THE FAILURE	FAILURE CAUSE	RISK	CAPA And/or PROOF OF THE RISK MASTERING (REFERENCE)	R.A. M.A.	RESI- DUAL RISK
1	EXAMPLE: To compute the drug dose	Can't compute the drug dose	Drug not delivered to patient or longer time to deliver drug	Missing input data or input data out of range	5	List mandatory data in instruction for use and their range, add a section about mandatory data in training session templates. Display a warning to user when data is missing and stop computation.	N/A	3
2	EXAMPLE: To compute the drug dose	Wrong computation of the drug dose	Wrong dose delivered to patient. Patient enema. Potential severe injury	Wrong input data	5	Add a picture with the silhouette of the patient matching the input data (sex, weight, age).	3	3

3	EXAMPLE: To compute the drug dose	Wrong computation of the drug dose	Wrong dose delivered to patient. Patient enema. Potential severe injury	User confounds a picture with another	5	Use silhouettes, which can be easily distinguished and different colors by ages (red=babies, orange=children, yellow=teens, green=adults).	N/A	3
---	--------------------------------------	------------------------------------	---	---------------------------------------	---	--	-----	---

Column 1: risk ID, assign an ID to each risk, risk IDs are referenced in this doc and in other docs

Column 2, 3, 4, 5 : FMEA analysis result

Column 6: risk level before mitigation. The values presented here are fictive. You shall implement your own scale of risk level.

Column 7: risk mitigation actions

Column 8: **RAMA = risk arising from mitigation action**. If a risk arises from the mitigation action, add here the IDs of those risks.

Column 9: risk level after mitigation (same comment as column 6)

In risk #2 of this fictive example, a system of pictures is used to prevent the use of wrong input data by displaying the silhouette of a patient matching the data. If the user is in a hurry (often the case) then he/she may not see the silhouette. A new risk arises from the mitigation action: risk #3.

If you use a method other than FMEA, your risk analysis table may look like this.

ID	RISK	FAILURE CAUSE	EFFECT OF THE FAILURE	RISK	CAPA And/or PROOF OF THE RISK MASTERING (REFERENCE)	R.A. M.A.	RESI- DUAL RISK
1	Missing input data	User skips mandatory input data	Drug not delivered to patient or longer time to deliver drug	5	List mandatory data in instruction for use and their range, add a section about mandatory data in training session templates. Display a warning to user when data is missing and stop computation.	N/A	3

You can also expand the risk level computation to some more columns, for example, if you compute risk level as:

- Risk criticality = Probability of occurrence x Consequence, with
- Probability of occurrence ranges from 1 (very low) to 5 (very high)
- Consequence ranges from 1 (remote) to 5 (catastrophic)

Then your risk analysis table may look like this:

ID	RISK	FAILURE CAUSE	EFFECT OF THE FAILURE	PROB	CONS	RISK	CAPA And/or PROOF OF THE RISK MASTERING (REFERENCE)	R.A. M.A.	RESI- DUAL PROB	RESI- DUAL CONS	RESI- DUAL RISK
1	Data out of range	User inputs data out of range	Drug not delivered	5	4	20	The mitigation action	N/A	1	4	4

You can also split the risks table by categories, eg:

- Operational/Functional use
- Maintenance
- Data (corruption, input data, loss of data ..)
- Software environment, like OS limits
- Usability engineering/ Human Factors Engineering (UE/HFE)
- Labelling, instructions for use
- Alarms, warnings
- Combination with other device
- ... any category which fits your organization

Note on UE/HFE: if you do a UE/HFE study (for example like what is recommended in IEC 62366) then risks detected in this study SHALL be added to the risk analysis table.

2.7 Risk traceability matrix

The risk traceability matrix below contains the connections between the risk analysis, software requirements and test plan. A risk is deemed mitigated when the test status is set to PASSED in the test report.

Traceability is a central activity of software design. The best way to ensure that a risk is mitigated, is to add a requirement in the software requirement specification (SRS). The requirement will be tested by one or more tests according to the test plan. When all the tests are PASSED, we have the proof that the risk is mitigated.

Some risks may be mitigated by other elements than software requirements, for example warnings in the instruction for use. These requirement about non-software elements can nonetheless be added to the SRS. See my SRS template for some samples.


ID	RISK	SRS REQUIREMENT ID	SRS REQUIREMENT TITLE	TEST ID	TEST TITLE	COMMENT
1	Data out of range	[entre SRS REQ id here]	Ranges of Data	[enter test id here]	Verify ranges of Data	Three requirements and four tests to mitigate the risk #1
1		[entre SRS REQ id here]	Display warning when data out of range	[enter test id here]	Verify that soft displays a warning when data out of range	
1		[entre SRS REQ id here]	List of mandatory data in instruction for use and training presentation	[enter test id here]	Verify that list of mandatory data is present in instruction for use	
1				[enter test id here]	Verify that list of mandatory data is present in training presentation	

Most of times, there is a one-to-many relationship between risks, mitigation requirements, and tests verifying requirements. The example above shows that 3 requirements were defined to mitigate the risk and that 4 tests are necessary to prove that the risk is eventually mitigated.

The risk traceability matrix below contains the connections between the risk analysis and software architectural or detailed design.

ID	RISK	SOFTWARE ELEMENT	SOFTWARE UNIT	COMMENT
1	Data out of range	Data Reader Module	Reader Controller	Mitigation of risk 1
1	Data out of range	Data Reader Module	Reader GUI	Mitigation of risk 1
2	Failure to display alarm	Alarm GUI		Alarm GUI bears the risk; hardware mitigation by alarm buzzer, see hardware specification.

Most of times, there is a one-to-many relationship between risks and software elements or software units. Quote the relevant element/unit that bear or mitigates the risk, or quote all elements/units. This depends on your software architecture
Risk #2 is an example of risk of software failure mitigated outside software.

	Risk Analysis of Paperless GMP Software	PROTOCOL NO.
		EFFECTIVE DATE:
		PAGE NO.:

2.8 Overall assessment of residual risks

Many residual risks present in a device may result in an unacceptable level of risk. The unacceptable level of risk shall be defined in the risk management plan (eg more than 10% of residual risks have a level higher than X).

Add a justification here about the overall assessment of residual risk showing that:

- They don't quantitatively break the rules about acceptable risk level defined in the risk management plan
- The qualitative assessment of residual risk by domain experts led to a favorable conclusion about the acceptable risk level

The qualitative assessment may be also based on bibliographic research about equivalent devices. Especially no residual risk can be linked to unacceptable adverse events, which occurred with equivalent devices.