Safety analysis
P. BRUNET

1. INTRODUCTION

Nowadays, People's safety is one of the main concern, but has different impact depending on the environment. While a car crash is almost common, an accident with a public transport is on all front pages.

Every 8 days POMA and OTIS companies move the population of the world with cable systems. Each day, the life of hundred of people relies only on one cable.

Of course, given this high responsibility, and the huge number of people transported, POMA-OTIS decided to give preemptive priority to safety. To reach this goal, safety analysis are performed for each of our systems. We keep track of possible dangerous situations from the beginning of the studies to the start up. These analysis are based on proven methods.

Moreover, a public or private APM commercialized on the world wide market must face to the lack of standard too, especially regarding cable systems.

The safety process must be in accordance with most of the national standards available in different countries.A corresponding ranks table must be established between all the safety levels defined in the existing standards.

One of the means to reach the required safety level, is the preliminary hazard analysis. We use these analysis to show to the checking authority that all hazards are reduced owing to appropriate solutions at least as safe as before (GAMAB, in France).

P. BRUNET, POMA-OTIS, Route des Rauches,74330 Sillingy
Tél : (33).450.22.39.08 Fax : (33).450.22.38.83
Email : Brunet@POMA-OTIS.POMAGROUP.COM

2. PRINCIPLE

2.1 METHODOLOGY

The safety study is based upon 3 main steps which lead to write three different documents.

- The first one consists in identifying and assessing the hazards taken into account.
- The second one consists in defining the risk level of each sub - systems which are involved in reducing or canceling hazards..
- The third one consists in a conception checking in order to ensure that the allocated risk level is reached.

2.2 REMINDER OF SOME DEFINITIONS

Component	The smallest part (electrical or mechanical part) of a unit. A sub - system is made of several components
Sub - system	The whole components used for a specific function of the equipment The whole equipment is composed of several sub - systems.
System	The whole equipment
Precaution	Undertaken safety measures to reduce hazards. There are three main kinds of precautions : • Device integrated in the system at the conception step • Action the equipment must run in a given hazardous situation , • Implementation of procedures (of maintenance, of intervention, of using...)
Hazard	A condition that is prerequisite to a mishap
Accident	Injury or damage to health
Hazardous situation	Any circumstance in which persons are exposed to a hazard.
Risk	Hazard evaluation unit resulting from the combination between the probability of occurrence of a mishap and the severity of its worst consequence.
Risk level	Classification of the elements in three categories taking into account the acceptable hazard and the relevant precautions (redundancies, procedures, constructive devices ...)
Hazard severity	Consequence of the worst credible accident that could be caused by a specific hazard
Probability	Frequency of occurrence of an accident.

3. PRELIMINARY HAZARD LIST

3.1 PRINCIPLE

In order to reduce the risk of injury or damage to health, it is necessary to identify the hazardous situations that can lead to an accident. This identification relies on the hazard list in paragraph 4 EN 292-1 Standard « System safety »

Then, hazardous situations are classified by risk level of each situation. The risk level table is the following one :

3.2 HAZARD SEVERITY CATEGORIES

3.2.1 SEVERITY CATEGORIES

The hazard severity categories are the following :

Severity	Category	Injury or damage to health
Catastrophic	1	Death
Critical	2	Severe damage to health with hospitalization for death risk and/or permanent handicap
Marginal	3	Minor damage to health, hospitalization without after-effects
Negligible	4	Less than minor damage to health or injury

3.2.2 PROBABILITY LEVELS

The level of occurrence probability is defined :

Level	Description	Specific Individual Item
A	Frequent or probable	Likely to occur frequently or several times in the life of the system.
B	Occasional	Likely to occur some time in the life of the system
C	Remote or improbable	Unlikely but possible to occur, or so unlikely, it can be assumed occurrence may not be experienced.

3.2.3 RISK EVALUATION

The combination of severity and frequency of occurrence quantify the risk associated with the hazard :

Severity →	1	2	3	4
Probability ↓				
A	HR	HR	MR	MR
B	HR	HR	MR	LR
C	MR	MR	LR	LR

HR = High Risk
MR = Medium Risk
LR = « Low » Risk

The HR and MR risks are unacceptable. Nevertheless, the measures to be undertaken to reduce them are more important for the HR risks than for the MR ones. The LR risks are acceptable.

Depending on the level of the risk to be reduced, it is decided of the precaution to be taken to eliminate or reduce identified hazards to an acceptable level.

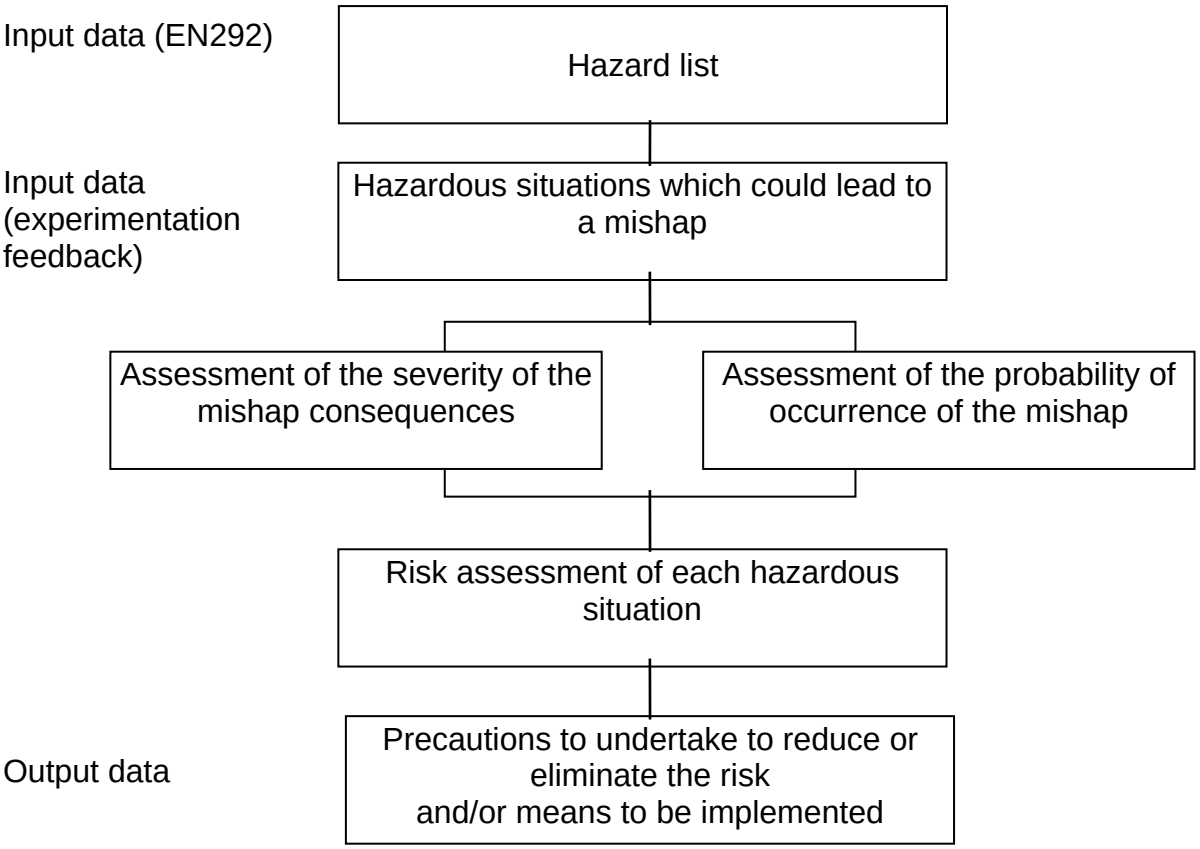
3.2.4 RISK REDUCTION

Identified hazards are eliminated or associated risks reduced by :

- the system design,
- the installation of protections,
- the implementation of operating procedures and/or maintenance procedures,
- the use of safety elements (mechanical sizing, manufacturing process, defined procedures, tests, etc.).

3.3 PROCEDURE SCHEME

We can find in the following document called « preliminary hazard list» the whole analysis and evaluation of those hazardous situations.



Each hazardous situation is thoroughly studied, and the implementations are worked out according to the level of the risk to reduce.

4. PRELIMINARY HAZARD ANALYSIS

4.1 PRINCIPLE

According to the severity and the frequency of occurrence of a mishap for a given risk, some sub - systems are more or less vital for the users and staff safety.

The preliminary hazard list is analyzed in order to validate the undertaken precautions, and to determinate the required risk level of each sub-system of the system according to the risk to be reduced, to the existence or not of redundancies, periodical controls ...

4.2 RISK LEVEL ASSESSMENT OF A SUB-SYSTEM

There are three risk levels : High Level (HL), Medium Level (ML) and Low Level (LL).

The relation between the risk level of an hazardous situation and the required rank (called risk level) of a sub-system is given in the following table :

Hazardous situation Risk Level	Precaution Risk level	Characteristics
HR	HL	High level of risk in case of failure => High Level element
MR	ML	Medium level of risk in case of failure => Medium Level element
LR	LL	Low level of risk or no risk in case of failure => Low Level element

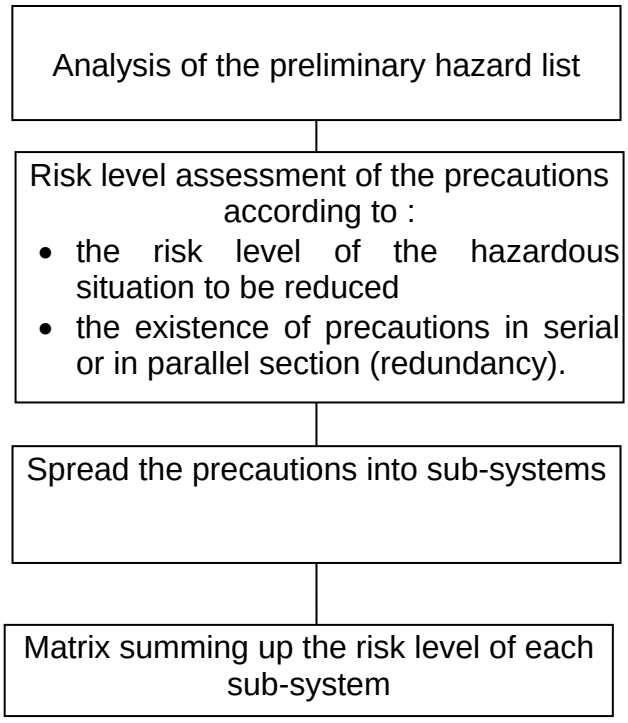
Probability of failure of equipment is decreased by specific requirements of quality during selection, design, manufacturing eventually installation. Of course, these requirements are in accordance with the risk level to be reached. Therefore, requirements for HL components or sub systems are much more accurate and much higher than LL ones.

Because the probability of failure of such components is reduced accordingly to the risk level of the hazardous situation, the probability, and therefore the risk level of occurrence of the associated mishap is reduced to an acceptable level.

The existence of a redundancy allows to decrease the risk level of the sub system of one unit.

4.3 PROCEDURE SCHEME

Input data



Output data

5. DETAILLED ANALYSIS OF EACH SUB-SYSTEMS

5.1 PRINCIPLE

During the design and component selection phase, designer always have in mind the required risk level of the sub - system they are studying.

During the design, sub systems are split in more simple sub systems, and most of the time directly into components.

This detailed analysis is used to determined the required risk level of each components to ensure the global risk level of the sub system is achieved.

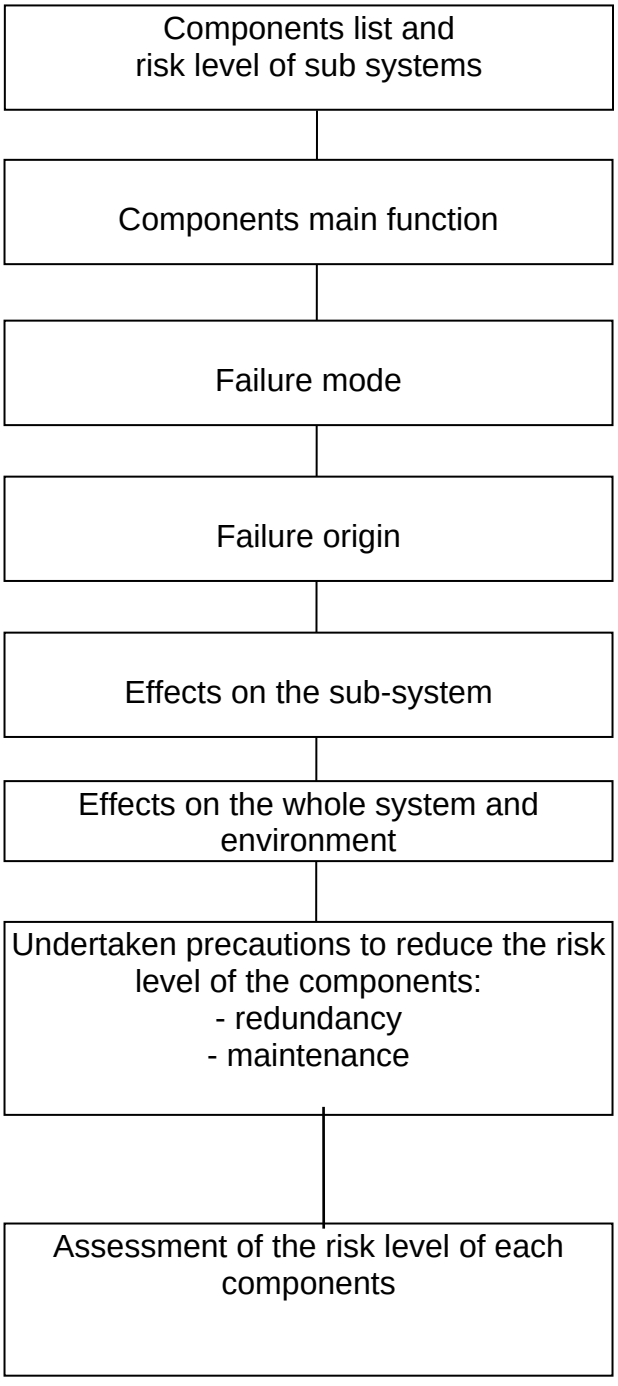
5.2 RULE TO DETERMINE THE REQUIRED RISK LEVEL OF A COMPONENT

The risk level required for a component is equal to the risk level of the sub system it belongs to, unless a risk level reduction applies (because there is a redundancy, a periodic check enabling to change the component before it is responsible for an accident...).

During this analysis, we checked that each components do not introduce a new hazardous situation (relative to the sub system it belongs to, or to the other sub systems) whose level is greatest than the global risk level of the sub system itself, or that was not taken into account in the preliminary hazardous situations analysis.

5.3 PROCEDURE SCHEME

Input data



Output data

6. CONCLUSION

For POMA-OTIS, the whole procedure described will be used :

- As a guide to take the relevant conception choice,
- To identify the most sensitive parts of the system regarding safety to pay a particular attention to them,
- To define the requirements in terms of quality, reliability and test of the components, in order to ensure the safety of the system according to the risk level of the hazards to be eliminated or reduced.