



3rd IAASS Conference

AN APPROACH FOR RISK ASSESSMENT: THE BRAZILIAN CASE

Durante, E., Leme, F. M. , Niwa, M., Marujo, E. C.



INTRODUCTION



- **Brazilian Space Agency (AEB)**
 - coordinator of the National System of Space Activities (SINDAE) .
 - regulations for commercial space activities in Brazil.

- **Launch safety regulations objectives:**
 - ensure public safety
 - ensure public and private property protection
 - ensure environmental protection
 - ensure compliance with international agreements, specific to this area, to which Brazil is a signatory



THE RISK MANAGEMENT PROCESS

NBR 14959

Risk Management

process used to systematically and continuously :

- Identify;
- assess;
- reduce or accept;
- and watch the full spectrum of risks .

goes throughout all the system lifecycle

part of the regular activities of a project



THE RISK MANAGEMENT PROCESS

NBR 14959

Step 1

Setting the risk management policy:

- definition of risk management policy
- preparation of risk management plan.

Step 2

Risk Assessment :

- identified each of the risk scenarios,
- determining risk magnitude,
- ranking



THE RISK MANAGEMENT PROCESS

NBR 14959

Step 3

Decision and Action

- risk analysis
- options for reducing risk , and
- risk reduction strategy

Step 4

Control, Communication and risk acceptance

- periodic reviews
- residual risks are reported
- formal acceptance of residual risk



THE RISK MANAGEMENT PROCESS

NBR 14959

Brazilians safety regulations

a new element

- submission process
- formal approval by the Safety Operator of Launch Center supported by a certification authority

IFI duty

- critically analyze plans and results of activities of risk management in defined intervals
- assess the adequacy and effectiveness of the ongoing process
- support for the authorization decision of a launch operation.



BASIC METHODOLOGIES TO RISK ANALYSIS

Two approach
quantitative methods

- try to evaluate the risks by a probability or a failure rate

qualitative methods

- identify all potential hazard and acidental events, associating each failure to a risk estimate



BASIC METHODOLOGIES TO RISK ANALYSIS

quantitative methods

- may not represent the reality.
- Some parameters are very difficult to quantify (insufficient data or little experience on the reliability of components).
- difficulties in identifying causes of risk (probability of human error, in particular).

qualitative methods

- validate concepts;
- prioritize risks
- compare proposed solutions for a determined problem
- quantify the relative weight of a certain parameter in the overall risk assessment



BASIC METHODOLOGIES TO RISK ANALYSIS

According to the Brazilian General Rules of Safe Space, to overcome any difficulties in applying quantitative methods, it is acceptable to use a qualitative approach.

The method used should be submitted to the Safety Operator of Launch Center for acceptance, during the submission process.



BASIC METHODOLOGIES TO RISK ANALYSIS

Quantitative methods

- procedure for classification of severity
- Preliminary Hazard Analysis

A risk matrix diagram with 'Frequency/consequence' on the vertical axis and five levels (1-5) on the horizontal axis. The levels are: 1 Very unlikely, 2 Remote, 3 Occasional, 4 Probable, 5 Frequent. The matrix is color-coded: Green for Low Risk (rows 3-5, columns 1-3), Yellow for Moderate Risk (rows 1-3, columns 4-5), and Red for High Risk (rows 1-2, columns 4-5). Arrows point from the labels 'High Risk', 'Moderate Risk', and 'Low Risk' to their respective regions in the matrix.

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	Yellow	Red	Red	Red	Red
Critical	Green	Yellow	Yellow	Red	Red
Major	Green	Green	Yellow	Yellow	Red
Minor	Green	Green	Green	Yellow	Yellow

- Hazard and operability study (HAZOP)
- Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Criticality Analysis (FMECA)



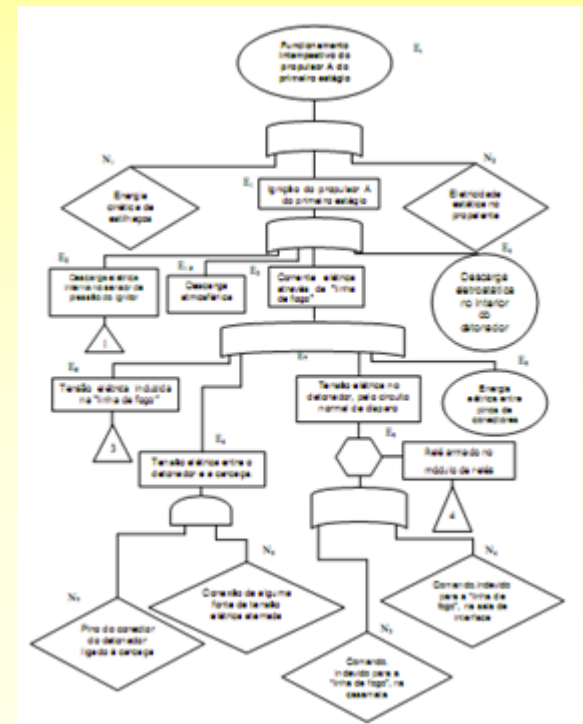
BASIC METHODOLOGIES TO RISK ANALYSIS

Quantitative methods

Probabilistic Risk Assessment (PRA)

A discipline that uses tools like FMEA, FTA, Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), Reliability Block Diagrams (RBD) or others to quantify risk

- Fault Tree Analysis





THE RISK BY BRAZILIAN SPACE SAFETY REGULATIONS

Five categories

- Catastrophic: may cause death of people.
- Critical: may cause severe personal injury and/or cause major damages to property and/or the environment
- Major: may cause mission loss (not considered in the safety field).
- Significant: can cause personal light injury, small damage to property and/or to the environment.
- Negligible: without consequences to people, property or the environment.



THE RISK BY BRAZILIAN SPACE SAFETY REGULATIONS

Safety goals

Severity	Consequence	Groups Affected	Maximum Acptable Value of Occurrence
Catastrophic	Death	Population	10^{-7} /operation
		Over flown Population	10^{-7} / launch
		Lunch center operational staff	10^{-6} /operation
Critical	Severe personal injury	Population	10^{-6} /operation
	Major damages to property and/or the environment	Any ground system potentially dangerous	10^{-6} / operation
		Other facilities	10^{-4} /operation
Significant	Personal light injury, small damage to property and/or to the environment	Everything that does not have any project goals accepted by the Safety Operetor	10^{-2} /year



THE RISK BY BRAZILIAN SPACE SAFETY REGULATIONS

From these set of goals, then, the high risk region of a risk matrice could be define and the selection of methodologies to be used in the risk management process can be structured. Thus, these methods can be applied at each project stage to the achievement of these objectives.



SUBMISSION PROCESS

Phase 0 - Feasibility

linked to feasibility studies and to identification of components or elements classified as potentially hazardous. At this phase risks derived from the project conception must be identified.

Phase 1 - Definition

linked to system definition. At that phase system elements that generate the risks identified in the previous phase must be detailed.



SUBMISSION PROCESS

Phase 2 - Development and production

linked to system fabrication and qualification. At this phase the results of the development and qualification stages must be presented to ensure that the elements identified in the previous phase meet the stated project requirements.

Phase 3 – Operation

linked to system operation at launch center. At this phase, plans and procedures to be used at launch center for safe operation of the system elements identified as potential risk generators must be submitted.



SUBMISSION PROCESS

- The risks should reduce to an acceptable level by:
- an intrinsically system safe design and/or
 - a proper operational procedure

Risk management

Phase	Activities
0	System and operational preliminary risk analysis.
	Identification of risks considered critical for safety in system level.
	First quantitative evaluation of risk levels to the possible technical design solutions.
	Presentation of project safety goals
1	Identification of risks.
	Study of risk reduction measures.
2	Finalization risk analyses
	Compliance demonstration with safety goals set.
	Management of critical safety parameters.
3	Development of procedures to be applied in critical activities identified previously



SELECTION OF RISK ASSESSMENT METHODS FOR BRAZILIAN PROJECTS

Phase 0:

In this phase the submission process starts. The use of PHA to identify the critical risks to the system and the project stakeholders and the definition of a Risk Matrix is recommended.

Phase 1:

In this phase tools that can show mitigation of risks identified in the previous phase are necessary. Besides the PHA, the FTA and FMEA tools could be used for this step.



SELECTION OF RISK ASSESSMENT METHODS FOR BRAZILIAN PROJECTS

Phase 2:

In the qualification stage the safety requirements have to be verified and safety goals have to be accomplished in the submission process. In this Phase the use of FMEA and FTA to the vehicle and use the HAZOP tool for risk assessment of the operations of integration and testing operations in a campaign launch are recommended.

Phase 3:

In the launch operation all the risks should have been mitigated so, the risk management in this phase have to monitor system operation and system elements identified as potential risk generators .



Application of Risk Assessment methods inside safety requirements compliance verification performed by an independent assessment organization

- Qualification process

- an extensive verification and validation process is needed.
- limited resources
- mechanisms to select which activities should have a detailed attendance could be used

Risk management

- a possible mechanism for planning the activities of independent assessment of safety requirements compliance.



CONCLUSION

- Risk is inherent in any activity
- Risk should not be taken as a problem, but as an understanding of the danger level due to a potential problem.
- Risk assessment sets up as an important discipline to the achievement of safety goals.
- The application of qualitative methods associated with quantitative methods can contribute strongly to project decisions and to final design quality. But without historical data to serve as basement to quantitative methods, like in the Brazilian case, the application of qualitative methods in the first projects could bring more reliable results.



CONCLUSION

With more realistic outcomes this process can be used, then, in other fields like independent conformity assessment process planning that have to cover an extensive system verification and validation process. Finally, with the improvement of the risk assessment discipline in the country it is expected to be possible apply all of existent risk management methods and even develop new ones