



White Paper 2015-11

How to Manage Low Probability, Catastrophic Risks: Industrial Risk Management

Low probability, high consequence risks (called in this White Paper 'catastrophic risks') are very significant when one looks at the history of major project-driven organizations. At the single project and at the portfolio level, a single occurrence can change the fate of entire organizations and even industries. Yet these risks are not properly covered by conventional Project Opportunity and Risk management process. In this White Paper we describe some adequate approaches and methods that have been proven to be particularly effective to prevent these risks.

Catastrophic events might not happen often, but when they do happen, their impact is tremendous on the organization touched, on the execution of the project impacted, other projects using the same resources, and sometimes even on the entire industry.

Avoiding catastrophic events is, on the long term, a key competitive advantage for individual Project organizations; and for the industry as a whole. It is easy to lose in one single event (and its consequential effects, in particular when key assets are involved) the entire profit of one year of business, which will take a long time to recover; often catastrophic events will even wipe out an entire company. Sometimes events such as massive pollutions or massive asset destruction with significant loss of lives will change an entire industry as new regulations are introduced or certain activities get banned.

The limits of insurance for projects

Let us first debunk the myth that those risks can be covered by insurance. Insurance markets only exist where there are a sufficient number of people or organizations that want to be insured for that particular risk so that insurance companies can average out their exposure over the entire market. There also has to be enough knowledge on the risk for insurance companies to derive meaningful statistics that allow them to fix the value of the relevant premiums and still protect themselves, their business and their other clients.

In the field of project management, the market is limited and it is difficult to calculate probabilities of occurrence. Hence insurance availability is limited and insurance policies have significant exclusions. In particular, consequential risks (such as loss of revenue, etc.) are generally not covered. Deductibles are also quite significant as a way to make sure that only major events will have to be investigated by loss adjusters.

In any case, should a catastrophic event happen, while some direct cost might be recoverable through insurance, consequential effects on the project portfolio won't. And of course, the impact of a catastrophic event on reputation cannot be insured.

Preventing catastrophic events is, on the long term, a key competitive advantage for all organizations involved in Project execution

Principles of prevention of catastrophic risks

Preventing catastrophic events always implies minimizing their probability and/or their consequence:

- Minimizing probability through the concepts of redundancy (allied with the concept of diversification), reliability management (including testing and preventive maintenance), and safety features in control systems,
- Minimizing consequence through the concepts of multiple barriers/ lines of defence and mitigation.

These two routes can be used jointly using well proven methods.

In the current condition of technology development, except in rare unavoidable instances (such as heavy lift), most catastrophic events will require multiple failures to develop simultaneously to happen. These failures can be either technical or human (and, increasingly, human failures play a major role in catastrophic events). Thus, the prevention of these events must consider these simultaneous failures

Introduction to Industrial risk management

We will call 'industrial risk management' the discipline that seeks to prevent catastrophic risks. This discipline is not commonly placed under the same organizational umbrella than general 'Project Opportunity and Risk'; it is sometimes managed by the Engineering function, or the Health & Safety function. However because catastrophic events can have a huge impact on Projects as

well as entire organizations, even if their probability is relatively low, Project Managers must make sure that the subject is addressed within their Project.

Most commonly used technical risk methods are not adequate to prevent catastrophic risks

When one thinks about technical risk, commonly used methods generally come to mind such as FMEA (Failure Modes and Effect Analysis) and its cousin FMECA adding prioritization (Failure Modes and Effect Criticality Analysis); or a similar method used in process fields, the HAZOP (HAZard and Operability analysis). These are

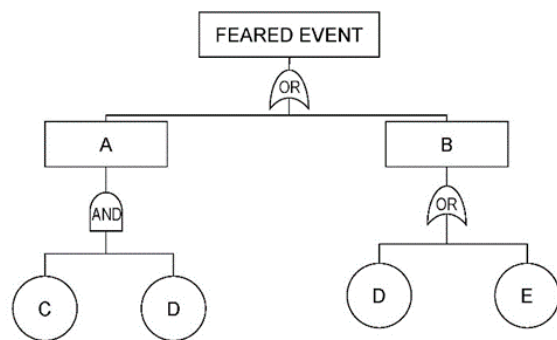
inductive methods: a failure is assumed and the consequences are inducted.

While these methods, if used thoroughly, are very effective at improving reliability of technical systems, they are not adequate to prevent catastrophic events because they only consider single failure modes, and not combined failure modes.

The power of deductive methods such as Fault Tree Analysis

Deductive methods are generally more difficult to apply than inductive methods but are much more powerful to prevent catastrophic risk. It is the case in particular of the Fault Tree Analysis. The method starts with the identification of a particular catastrophic event that is sought to be prevented. The possible causes are then identified through logical relationships with AND and OR gates. This forms a tree of possible events leading to the catastrophic failure. Common causes of failure can be readily identified if some events appear several times in the overall tree leading to the ultimate catastrophic failure.

The vast majority of catastrophic events result from the unlikely combination of two or more simultaneous independent failures



Example of a fault tree

In this example, D is a common cause of failure

Lessons learnt systems are essential to prevent catastrophic failures

There is a saying that making a mistake is not a big deal as long as one learns from it and does not do it twice. Unfortunately, lessons learnt systems and catastrophic event near-misses information sharing systems are not very developed in the project industry (contrary to industries deemed high risk such as the aerospace or nuclear industries). It is essential to foster exchange of lessons learnt and candid root cause analysis of near misses to prevent catastrophic risks. This should be a mandatory complement all industrial risk analysis methods

Conclusion

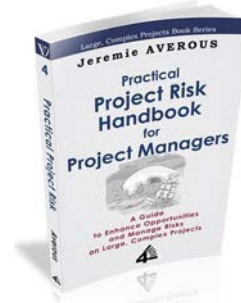
Preventing catastrophic events is, on the long term, a key competitive advantage for all organizations involved in Project execution. Insurance is not a sufficient protection as in particular it does not cover consequential impacts to the organization.

Common methods to analyse possible events (such as FMEA and HAZOP) have limits, and the most dramatic is that they don't allow considering the combination of independent faults, which is almost always at the root of all catastrophes. Other methods such as Fault Tree Analysis do exist in high reliability industrial organizations that can be used in Project execution environments to prevent the most catastrophic events to happen. These methods need to be supplemented by a robust and transparent lessons learnt and root cause analysis process.

Catastrophic event prevention methods have been successfully used by Project Value Delivery in a number of instances in Project execution contexts, leading to structural changes in the way some construction activities were undertaken.

Find all these principles of Project Opportunity and Risk exposed in a comprehensive manner in our new Handbook, Practical Project Risk Handbook for Project Managers

(now published, available in [Paperback](#) and [Kindle](#) versions!)



[all links to Amazon.com]



We Empower Organizations to be Reliably Successful in Executing Large, Complex projects.

Discover more on
www.ProjectValueDelivery.com