THE USE OF TRIZ IN BUSINESS CONTINUITY PLANNING

Jack Hipple  
Innovation-TRIZ  
Tampa, FL

Steve Elliott  
Elliot Consulting  
Tampa, FL

Abstract

The principles of TRIZ continue to find applications in fields outside their original application in engineering and technical problem solving. The past few years we have reported applications in management and organizational problem solving, ergonomics and human factors, and consumer product design. This year we want to review an application of TRIZ and its normal algorithms and tools, as well as its “reverse” version in an important new area—business continuity planning (BCP). TRIZ in “reverse”, sometimes called Predictive Failure Analysis™ or Anticipatory Failure Determination™, inverts the traditional algorithm and provides a mental process for identifying potential failure mechanisms that may not be found via normal “check list” processes, in wide spread use, such as HAZOP (Hazardous Operations Analysis) or FMEA (Failure Modes and Effects Analysis). Predictive Failure Analysis™ (PFA) has identified failure routes that were not able to be identified via these processes in the banking, chemical, and food processing industries. PFA and its application to business continuity planning (BCP) are discussed. BCP is a particularly important current concern given present day severe weather and terrorist concerns.

I. Business Continuity

When a business considers the broad topic of business continuity, it is considering what is involved in maintaining all aspects of its business through any emergency or disaster in a transparent and seamless way to its markets and customers. If this is done correctly, a customer would never know that a disaster ever occurred or that it had any affect on its supplier. This would be a TRIZ definition of an ideal result—the business continues without any interruption of any sort at any time.

When a business considers its response to disaster situations (weather, epidemic, terrorism, sabotage), the usual immediate concern is for potential loss of personnel and equipment and how to replace them or their functionality on a short term basis. Temporary facilities, collaborative supply relationships, and emergency assistance are normally the primary basis for this planning. Time frames of days are normally considered. Occasionally, planning around time frames of hours or weeks may be considered. However, as hurricane Katrina taught us, months and years may be more appropriate. Then there is the issue of scope. If we look solely at the headquarters building or the primary manufacturing plants, we are certainly looking at core concern areas, but hardly the entire scope of business continuity. Business continuity includes not only manufacturing and sales, but product delivery and customer service, warranty
response, cash management, and a myriad of other issues. Let’s consider all the elements of analyzing maintaining business continuity, not just short term survival. We will note how some basic TRIZ concepts can be integrated into the thinking

A. Risks and Vulnerability Assessment. Vulnerability depends on the nature of the business, the nature of the disaster that occurs, and the vulnerability of that business to many different potential crises. It is critical to distinguish between general vulnerability such as building impacts, equipment damage, and loss of operating personnel vs. the functions necessary to maintain a business. In the TRIZ community, we are accustomed to thinking in terms of functions rather than equipment or devices and this same thinking applies in the BCP area as well. For example, when we think of vulnerabilities, are we describing the vulnerability of our order processing center computers or the ability to provide information on customer orders? If our orders are processed outside of our main computer facilities by a third party, then our risk and vulnerability assessments are totally different compared to vulnerabilities if they are contained within our primary building. For example, our headquarters building may be located in a flood prone area, but the third party order processing may be in a tornado or earthquake prone area. The vulnerabilities are quite different. If we put on our TRIZ hats, we might ask:

1. How can the vulnerabilities identify themselves?
2. What resources are required to minimize risks? Have we considered both our internal and external sources?

Vulnerability can also time related. If the local McDonald’s fast food store is closed for a few days, customers are likely to return. If it is closed for several months, it is highly likely that its former customers will have tried other places to eat and possibly find another “favorite” place and never return as steady customers. What resources are required as a function of time? What is the ideal way of handling retail store closure over an extended time? How can the business sustain itself?

Then there is the functional nature of the vulnerability. For example, if a business sales force works entirely out of individuals’ homes away from a headquarters facility and uses only cell phones for communication, then this function may be virtually unaffected by a physical disaster at headquarters, but highly vulnerable to specific local conditions where the sales people live or the destruction of a cell phone tower. It is also possible that, in a major metropolitan area, that cell phone communication may be totally disrupted by an electromagnetic pulse, while conventional land line communication is unaffected. The vulnerabilities of a given business and its functions are a strong function of how, when, and where its functions are carried out.

B. Crisis Management and Mitigation. No matter what the nature of the emergency, an enterprise needs to deal with the immediate situation, no matter
whether it is loss of utilities, flooding, or flu outbreak. Again, many organizations have not adequately thought through even these short term responses. If a facility handles hazardous materials, crisis management also includes proper community communication.

From a TRIZ perspective, how can the crisis manage itself? What resources are required? What contradictions must be dealt with?

C. Communication. In times of crisis, communication is paramount. This includes communication to employees, customers, suppliers, and surrounding neighbors and governmental agencies, especially if the crisis involves any kind of a safety or hazardous material issue that might affect public welfare. Dealing with communication issues can be quite different if the enterprise workforce is dispersed. Instead of a large centrally located communication group, we could have reservation and sales agents working out of their homes around the country, such as with Jet Blue Airlines.

What resources can be used in a crisis? How can the communication occur automatically to the extent needed and wherever it is needed?

D. Risk Management. This is different than crisis management. This involves assessing and mitigating the physical and financial risks that are potentially involved in a crisis and its aftermath. It is not possible to eliminate all risks, but intelligent planning can minimize the potential risk. The types of risks will vary not only with the degree of the hazard, but the nature of the business. It is also greatly affected by the physical nature of an organization’s infrastructure. A business such as Starbucks with a café on every corner needs to have a quite different risk management program (with say, food contamination) compared to that of Amazon.com which operates no storefronts but has a huge one-location warehouse from which all shipments are made in response to Email orders.

What previously not thought about resources might we used to minimize risk? Have we considered the entire list of possible resources—Materials? Time? Before? During? After? People? Fields? Function conversions? Space? Examples of each of these could be backup disks, pre-planning time, contractors, paper to electronic record copies, loss of power triggering automatic responses and results.

E. Business Recovery. How does a business recover after a crisis or emergency? That depends a great deal on how well it has prepared ahead of time. From a TRIZ ideality standpoint, the customer would never realize that their supplier had ever had any kind of crisis or business interruption in the first place. An example of not doing this properly was provided with a recent major outage of fiber optic cable service in Florida when a construction crew cut a major fiber optic cable providing TV and Internet service to much of the state and the “back up” plan was in place, but the back up service was via a cable through New Orleans which had
not been repaired from hurricane Katrina’s impact. Customer service was interrupted for over 8 hours.

In our recovery plans, have we considered all the resources that might be available? Have we challenged the availability of these resources? What contradictions might prevent their use?

II. The “reverse” TRIZ Algorithm (Predictive Failure Analysis™) and how it can assist in this process

Though there are many versions of the basic TRIZ/ARIZ algorithm, let’s consider the most basic of these as it is more than sufficient to deal with most business continuity cases we have considered:

1. Define the focus for problem solving (Note: this in itself can be a long effort in itself and has its own algorithm)
2. State/envision the ideal result
3. Identify and use existing resources
4. Resolve contradictions that prevent an ideal state (possibly through the use of TRIZ 40 principles and separation principles

If we invert this algorithm for business continuity, we get this:

1. Define the ideal result (we desire the business to continue through any conditions)
2. Invert this ideal result (we do not want the business to continue during a crisis or emergency)
3. Exaggerate the inverted ideal state (we never want the business to survive under any crisis condition
4. Identify resources and conditions that would allow and assist this in happening
5. If contradictions are identified that may prevent a negative impact, how would they be resolved to allow them to happen?

Let’s quickly review some applications where this saboteurial thinking has been applied. The details of some of these applications are confidential, but the general nature of the application can be easily understood. In a banking application, a normal commercial bank and its Internet subsidiary was having excessive electronic bank fraud. This technique was used to identify routes of access and compromise not identified by normal check listing techniques. In a chemical plant release scenario, a toxic gas release situation was analyzed providing breakthrough ideas not provided by conventional HAZOP analysis. In a food Lysteria bacteria contamination problem, routes for contamination were identified, minimizing future potential poisonings and liability. Lastly software code analysis was improved through the use of saboteurial thinking and providing improved user reliability.

III. Application of PFA™ to Business Continuity
Let’s now look at how this inverted TRIZ algorithm can be used to improve the elements of business continuity planning discussed earlier. They are currently being applied with clients concerned with hurricane and weather vulnerabilities.

**A. Risks and Vulnerability Assessment.** When we apply the TRIZ algorithm in reverse, we ask “how can we make the enterprise vulnerable at all times under all conditions? How would we make sure that our business was always vulnerable? Going through the entire list of resources (from a TRIZ perspective), how could we use each of them to make our business and enterprise more vulnerable and the risks higher?

**B. Crisis Management and Mitigation.** How would we make sure that no one was informed of the nature of the crisis? That everyone assumed the worst because they had no information? The press reported erroneously because they had no information? How would we make sure this happened?

**C. Communication.** How can we make sure that there is no communication to anyone in a time of crisis? How would we accomplish this? That this communication is highly inaccurate and causes the wrong response of emergency response agencies? Our employees to do the exact opposite of what we would like them to do?

**D. Risk Management.** How can we make sure, with all the resources we have available, that we have no control over risk? That we have no knowledge of the extent of potential risk? That we have insured against all the wrong risks?

**E. Business Recovery.** How can we make sure the business never recovers? What resources do we need to accomplish this? Are they available? Where could we find them? If so, how can their impact be maximized?

Another way of using this process is to challenge a developed business continuity plan using PFA™. Business continuity planning (BCP) today consists primarily of check listing against known areas of concern:

1. Client locations, type, functions performed
2. Business processes and tolerance for both downtime and data loss
3. For each business process, a definition of software required, support environment, necessary internal staff
4. Hardware support required—internal, external, on site, off site, both? How managed?
5. Identification of critical data
7. Supply chain. Delivery methods, lead times, contact process, Vendors’ BCP plan? What alternative sources or materials may be usable and available?
8. Maintenance of customer service. Phone? Fax? Text messaging?

For each of these audit areas and a developed plan, we would use the PFA™ process to analyze it and determine how to make sure that it is not functional. This analysis would then be used to further improve the quality of the business continuity plan. TRIZ tools such as substance field modeling and cause and effect diagramming, potentially involving commercial TRIZ software products, or paper and pencil versions of them, can be very useful in group settings in the outline of a business continuity plan.

Conclusions
The area of business continuity planning (BCP) has become a highly important new focus area for virtually all major enterprises. TRIZ has many tools that can assist in greatly improving and achieving seamless business continuity.

References

1. Hipple, Jack “Using TRIZ in Reverse to Analyze Failures”, Chemical Engineering Progress, May 2005

www.innovation-triz.com
www.ideationtriz.com

™Predictive Failure Analysis is a registered trademark of Innovation-TRIZ
™Anticipatory Failure Determination is a registered trademark of Ideation International