Return To Previous Page

# Reversing TRIZ for Business Continuity Planning

By Jack Hipple and Steve Elliot

## Abstract

TRIZ principles continue to find applications in fields outside their original application in engineering and technical problem solving. Applications in management and organizational problem solving, ergonomics and human factors, and consumer product design have been demonstrated in the past few years. This article will focus on a review 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 inverts the traditional TRIZ algorithm and provides a mental process for identifying potential failure mechanisms that may not be found via normal checklist processes in wide spread use such as hazardous operations analysis (HAZOP) or failure modes and effects analysis (FMEA). Using TRIZ in reverse identifies failure routes that were not identified via these processes in the banking, chemical and food processing industries. Reverse TRIZ in business continuity planning (BCP) is particularly important given current present-day severe weather and terrorist concerns.

## Business Continuity

When a business considers the broad topic of business continuity, it considers 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 will never know that a disaster ever occurred or that it had any affect on its supplier. This is the TRIZ definition of an ideal result – the business continues without any interruption at any time.

When a business considers its response to disaster situations (weather, epidemic, terrorism, sabotage), the usual immediate concern is about the 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 time frames timeframes of 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, customer service, warranty response, cash management and a myriad of other issues. All of the elements are involved in the analysis for maintaining business continuity, not just short term survival. Some basic TRIZ concepts can be integrated into this planning.

### *Risks and Vulnerability Assessment*

Vulnerability depends on the nature of the business, the nature of the disaster and that company's vulnerability to 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, thinking usually occurs in terms of functions rather than equipment or devices and this same thinking applies to BCP. For example, when thinking of vulnerabilities, is it the vulnerability of 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 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 different. Using TRIZ, the following questions may arise:

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 also can be time related. If the local McDonald's fast food restaurant is closed for a few days, customers are likely to return. If it is closed for several months, it is likely that its former customers will have tried other places to eat, found 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 a retail store's 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 the company's sales 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, cell phone communication may be 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.

### *Crisis Management and Mitigation*

No matter what the nature of the emergency, an enterprise needs to deal with the immediate situation – whether it is loss of utilities, flooding or flu outbreak. Many organizations have not adequately thought through 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?

### *Communication*

In times of crisis, communication is paramount. This includes communication to – and with – employees, customers, suppliers, 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, reservation and sales agents may be 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?

### *Risk Management*

This is different than crisis management. This involves assessing and mitigating the physical and financial risks that may be involved in a crisis and its aftermath. It is not possible to eliminate all risks, but intelligent planning can minimize 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 different risk management program (including, for example, 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 online orders.

What previously not thought about resources might be used to minimize risk? 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.

### *Business Recovery*

How does a business recover after a crisis or emergency? That depends 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 a crisis or business interruption. As an example, there was a major outage of fiber optic cable service in Florida when a construction crew cut a primary fiber optic cable providing TV and Internet service to much of the state. 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 more than eight hours.

Have all the resources that might be available been included in recovery plans? Has the availability of the resources been challenged? What contradictions might prevent their use?

## Using The "Reverse" TRIZ Algorithm

Though there are many versions of the basic TRIZ/ARIZ algorithm, the most basic of these is sufficient to deal with most business continuity cases:

1. Define the focus for problem solving (Note: this in itself can require significant effort 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 the 40 inventive principles and separation principles)

By inverting this algorithm for business continuity, the questions change:

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 can they be resolved to allow them to happen?

Thinking and planning like a saboteur has helped more than one organization. A normal commercial bank and its Internet subsidiary were dealing with excessive electronic bank fraud. This saboteur planning was used to identify routes of access and compromise not identified by normal check listing techniques. In a chemical plant release scenario[1], 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.

## Application to Business Continuity

The inverted TRIZ algorithm is being applied to business continuity planning for clients concerned with hurricane and weather vulnerabilities.

### *Risks and Vulnerability Assessment*

Ask how we can make the enterprise vulnerable at all times under all conditions? How can we make sure that our business is always vulnerable? Going through the entire range of resources (from a TRIZ perspective), how can we use each of them to make our business and enterprise more vulnerable and the risks higher? How can our inventory be a liability?

### *Crisis Management and Mitigation*

How can we make sure that no one is informed of the nature of the crisis? That everyone assumes the worst because they have no information? The press reports erroneously because they have no information? How can we make sure this happened?

### *Communication*

How can we make sure that there is no communication to anyone in a time of crisis? So that communication is totally inaccurate and causes the wrong response of emergency response agencies? So that our employees do the exact opposite of what they should?

### *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?

### *Business Recovery*

How can we make sure the business never recovers? What resources do we need to accomplish this?

Are they available? Where can we find them? How can their impact be maximized?

Another way of using this process is to challenge a developed business continuity plan using TRIZ thinking in reverse. Business continuity planning (BCP) today[2] consists primarily of checklists 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; managed how
5. Identification of critical data
6. Nature of manufacturing operations – utility reliability, site access
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
9. Accounting – order entry, billing and invoicing, purchasing, banking relationships

For each of these audit areas and for a fully-developed plan, use TRIZ in "reverse" to analyze it and determine how to make sure that it is not functional. This analysis can 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 (involving commercial TRIZ software products, or paper and pencil versions of them) can be useful in group settings in the outline of a business continuity plan.

## Conclusion

Business continuity planning (BCP) has become an 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," , May 2005.
2. Elliot, Steve, Business Continuity Strategies, .

## Resources

1. Edwards, Aton, *Preparedness Now!*, Paragon Press, 2006.
2. Kaplan, Stan, et. al., *New Tools for Risk and Failure Analysis*, Ideation International, 1999.
3. *Process Safety Process*, monthly publication of the American Institute of Chemical Engineers and the .

### *About the Authors:*

Jack Hipple is a principal with Innovation-TRIZ. He is the TRIZ instructor for AIChE/ASME and does TRIZ

workshops for ASQ, PDMA and the Human Factors and Ergonomics Society. He has written TRIZ articles for The TRIZ Journal, Quality World, Mechanical Engineering, World Futures Quarterly, Creativity and Innovation Management's inaugural TRIZ issue, as well as a special three-part series on TRIZ for Chemical Engineering Progress. Contact Jack Hipple at jwhinnovator (at) eartlink.net or visit http://www.Innovation-TRIZ.com.

Steve Elliot founded Elliot Consulting Services in 2003 after a highly successful career as a global account manager, corporate trainer and senior sales executive from the communications and high-tech industries. Steve's broad professional experience includes sales, marketing, business development, operations, project management, business continuity planning, emergency preparedness and disaster recovery positions with AT&T, Control Data, Westinghouse and ABC/Capitol Cities. During his tenure at AT&T, Mr. Elliot's responsibilities included the management of large global enterprise accounts. He focused on performing detailed assessments of the technological and communications needs of his clients, and then proposing solutions to help them operate more efficiently and effectively. He is a Certified Business Resiliency Manager (CBRM), and FEMA-certified in Emergency Management, Incident Command System (ICS) and the National Incident Management System (NIMS). Contact Steve Elliot at selliot (at) elliot-consulting.com or visit http://www.elliot-consulting.com.



---

**Return To Previous Page**