

Application of Problem Inversion to Cascading Critical Infrastructure Failure

Ivan Taylor

Abstract Between 1994 and 2013, over 6800 natural disasters have occurred worldwide, claiming 1.35 million lives. Flooding accounted for over 40 % of these disasters displacing nearly 2.5 billion people. Storms were the second most frequent type of disaster: killing more than 240,000 people and costing over US\$900 billion in damage to infrastructure. It is commonly felt that the number of severe natural disasters has been increasing in recent years because of climate change. However, the problem of climate change may not be solved in the near future. So governments need to prepare for frequent future natural disasters and find ways to mitigate the potential death and destruction they cause. This chapter will discuss a novel method for making preparations to avoid the problem of cascading disasters created by a single natural event. This approach will adapt a knowledge based technique from manufacturing, called Ideation Failure Analysis™, to correct deficiencies in critical infrastructure. The technique involves a number of approaches that are combined into a comprehensive process. First, a simple direct approach is attempted with the assistance of a knowledge base. If the problem can not be resolved in the direct manner, then an indirect approach is suggested. A detailed Failure Analysis Questionnaire is used to assist in model building. A model of the failure network is developed. However, instead of working directly towards failure correction, an inversion process is conducted. That is, in order to facilitate greater creativity, the analysis team is asked to imagine ways to produce the failure. The creative work is then assisted by a knowledge base. The analysis team is able to prioritize the likelihood that a cause might have resulted in the failure. The next step is to find ways to prevent, eliminate, or reduce the impact of the failure. Again to assist the creative process, a knowledge base provides suggestions for correction techniques that can be prioritized in a hierarchical fashion. Finally, the results are evaluated to avoid negative side-effects or drawbacks in the suggested ways to correct the failure. This chapter will conclude by providing some recommendations and an evaluation of the potential of this technique.

I. Taylor (✉)
Policy Dynamics, New Hamburg, Ontario, Canada
e-mail: Ivanwtaylor@gmail.com

Keywords Critical infrastructure • Cascading failure • TRIZ • Ideation failure analysis

1 Introduction

Between 1994 and 2013, 6873 natural disasters have occurred worldwide, claiming 1.35 million lives. Flooding accounted for 43 % of these disasters displacing nearly 2.5 billion people. Storms were the second most frequent type of disaster: killing more than 244,000 people and costing US\$936 billion in damage to infrastructure [1]. It is commonly felt that the number of natural disasters has been increasing in recent years because of climate change. However, the problem of climate change may not be solved in the near future. So governments need to prepare for frequent future natural disasters and find ways to mitigate the potential death and destruction they cause.

“Red Teaming” has been used by military planners for many years [2]. In this type of analysis, a war game is simulated in which one group of players called the “red team” try to sabotage or otherwise disrupt the plans of the so-called “blue team”. By this challenge method of counter-analysis, plans can be tested under severe conditions to ensure they will hold up when used in real-life.

The author has adapted a version of the Nominal Group Technique [3] which is referred to as structured brainstorming. In a number of cases, this technique has been used with event planners [4]. The planners are asked to generate creative ideas to answer the question: “In what ways could the event fail?” This allows the planners to imagine the worst-case scenario and thus take appropriate actions beforehand to avoid the imagined problems. Klein [5] has used this technique successfully in project management. He appropriately named his approach a “pre-mortem”.

The software package, called Ideation Failure Analysis™ [6], employs a similar problem inversion process to enhance the creativity of an analysis team trying to find the root cause of a manufacturing failure. This chapter will discuss the potential of problem inversion to find the reasons for cascading critical infrastructure failure caused by natural disasters. In this paper, we will use the knowledge based technique from manufacturing in the Ideation Failure Analysis™ software. However, we recognize that the knowledge base could be adapted to correct deficiencies in the design of critical infrastructure that lead to cascading failures.

It will be shown that a comprehensive application of the Ideation Failure Analysis™ to correct the failure could prove overwhelming to an individual analysis team or even a team of analysis teams. So, a prioritization technique based on the Analytical Hierarchy Process [7] is suggested to allocate effort optimally in the processes of failure diagnosis and correction.

The Ideation Failure Analysis™ process is quite time consuming when conducted in its full form. Therefore, a “short-cut” direct approach to the failure analysis is suggested that might resolve simple problems. Section 2 will describe

this direct approach to the problem of finding the root cause of a cascading infrastructure failure caused by a natural disaster. Although this direct approach is not new, the Ideation Failure Analysis™ software supports the process by providing an extensive knowledge base of typical failure modes to facilitate the creative process conducted by the analysis team.

In Sect. 3, it is assumed that the direct approach did not lead to satisfactory results. Then the analysis team, using the Ideation Failure Analysis™ software, begins an indirect approach by completing a detailed Failure Analysis Questionnaire to support model building. We will provide two models that were developed using the software. These models are similar to network models that attempt to describe the interconnected process in a cascading critical infrastructure failure. These models are used to invert the problem of failure analysis. Using the software, the creative process is facilitated by asking the analysis team to suggest ways the failure could be produced.

The software provides “Directions” for investigation by the analysis team. Each of these Directions also comes with so called “Operators” which are specific examples and case studies of how the Direction might occur. Using this knowledge base of Directions, Operators and Case Studies, the analysis team is encouraged to develop ideas on the root cause or causes of the failure. In Sect. 4, this process is examined.

The process of determining how the failure can be corrected is described in Sect. 5. In this section, the Directions and Operators that are provided by the software to prevent, eliminate or reduce the impact of the failure are outlined.

In Sect. 6, the final steps in the Ideation Failure Analysis™ process are described. These steps involve the methods that can be employed to avoid negative side-effects or drawbacks of the solutions that were developed by the analysis team.

Section 7 provides a brief summary, some concluding remarks, some recommendations and an evaluation of the potential of the Ideation Failure Analysis™ for use by government agencies.

2 The Direct Approach

In the Ideation Failure Analysis™ process, the analysis team should begin by taking a direct approach to finding the root cause of the failure. The first step in this direct approach is to describe the situation in “everyday language” avoiding the use of professional terminology. It is believed that this will result in the problem being “generalized,” thereby the analysis team will be able to suggest more methods for solving it.

We can describe the problem situation as follows: “How do we avoid a cascading failure in the critical infrastructure of a city when a natural disaster occurs?”

The analysis team can now apply the knowledge base provided in the software directly. Below is a list of typical failures:

- (a) Explosion,
- (b) Combustion,
- (c) Corrosion,
- (d) Malfunction of electric or electronic device,
- (e) Deformation or destruction,
- (f) Disappearance of a useful object or material,
- (g) Appearance of a harmful object or material,
- (h) Disruption of useful system functioning, and
- (i) Appearance of a harmful effect in the system.

Of course, more than one of these typical failure modes might be applicable. Then some process of prioritization could be conducted. One way this could be done is using the Analytical Hierarchy Process [7]. In this case, pair-wise comparisons of the importance of each of these failure modes could be turned into percentage values. These percentage values can then be used to allocate effort to resolving these failure modes starting with the failure mode with the highest percentage value. Table 1 shows the results of an example run of the Analytical Hierarchy Process for these typical failure modes.

The investigation of these failure modes by the analysis team is supported by a knowledge base in the Ideation Failure Analysis™ software. One of the features of the knowledge base is that it is highly hierarchical. In the next paragraph, we will outline the types of information available in the knowledge base by looking at the particular failure mode of an explosion.

The knowledge base contains detailed information of the potential causes of chemical, thermal and mechanical explosions. If none of these types of explosions seem applicable, the analysis team need not stop there. The knowledge base outlines how some object or material might enter the system to create an explosion. There are two aspects that need to be considered to make this happen: a driving force and a transport path. The knowledge base contains specific details on how large or small objects could enter the system to cause an explosion as well as how liquids or gases could enter the system to create an explosion. One way small objects, liquids or gases could enter the system is on “carriers” like system inputs or

Table 1 Prioritization of typical failure modes

Typical failure mode	Priority value (%)
Explosion	21
Combustion	16
Corrosion	0.1
Malfunction of electric or electronic device	10
Deformation or destruction	12
Disappearance of useful object or material	4
Appearance of harmful object or material	13
Disruption of useful system functioning	5
Appearance of a harmful effect in the system	19

auxiliary materials such as lubricants or coolants, through small openings like cracks, broken or damaged seals or through porous materials. As an example of the extensiveness of the knowledge base for the direct failure modes, below is an excerpt concerning damage to connections:

Damage to connections between parts (movable or stable, permanent or dismountable junctions) can result from: Inappropriate connections such as wrong connection method, wrong dimensions, tolerance, and fit of connecting elements, excessive or insufficient fastening pressure, excessive or insufficient fastening elements (clamps, clasps, clips, bayonet plugs, sockets), excessive distance between fastened locations, wrong material for connecting elements, wrong method of welding, soldering, gluing, riveting, wrong connecting material (glue, solder, electrode material, wire); Impacts to the junction during operation (load, shocks, vibration, temperature deviation) that can cause deformation or shift in the elements that in turn damages the junction; Impacts from the medium on the material of the connected parts – corrosion, impurity saturation, abrasive wear, pollution; Harmful impact from other system parts – in particular, electro-chemical corrosion and diffusion due to the contact of different materials, thermal stress during deviations in temperature; Impact from repeated assembly and disassembly – deformation of parts, part damage; and, Adhesive effects (elements adhering to each other). Additional causes of junction damage are due to the fact that junctions are often inadequately protected from environmental impacts. Any barrier is subject to cracks or micro-cracks, either initially or due to various impacts.

This discussion outlines the high level portions of the knowledge base for the explosion failure mode. For each of these elements, the analysis team can look deeper into the knowledge base to obtain more details and creative ideas.

If this direct approach helps the analysis team identify root cause of the failure, they can look into the knowledge base to find ways to correct the failure.

There are details in the knowledge base on how to eliminate an energy source or a material from the system to correct the failure. Here is an excerpt from the knowledge base:

The analyst should consider the possibility of preventing the energy supply that causes the harmful effect by: preventing energy production; reducing the energy flow parameters to the point where the harmful effect is eliminated; dividing the energy flow into harmless flows; creating insulation against an undesirable energy; redirecting the energy flow; creating an energy flow that will oppose the undesirable flow of energy; absorbing the undesirable energy. If the energy that causes the harmful effect also serves some useful function, he or she should attempt to find a simple way to resolve the contradiction.

Also there are suggestions on how to separate the cause of the failure from the system in space or time. The analysis team is encouraged to look at specific conditions that might be present to create the failure mode. By removing these specific conditions, the failure mode might be eliminated. There are suggestions in the knowledge base on how to eliminate or reduce the impact of the failure mode or the likelihood of the failure or reduce the negative consequences of the failure.

If after examining these failure modes directly, the analysis team finds that the problem is not typical, the analysis team should perform the following steps.

- (a) Complete the Failure Analysis Questionnaire;
- (b) Conduct Failure Analysis Modeling;

- (c) Develop Failure Mode Prioritization;
- (d) Failure Mode Correction Prioritization; and
- (e) Evaluate Results.

3 The Failure Analysis Questionnaire

The Failure Analysis Questionnaire allows the analysis team to systematically examine the failure situation, and then build a model to describe it. There are two parts to the questionnaire: information about the system, and information about the failure.

It is important to identify the system in which the failure occurs. The first step is to name the system in a descriptive but concise manner. For our problem, the system can be thought of as “a city”. The next step is to describe the main parts of the system. The main parts of a city are its people, its institutions such as the government, financial systems and the emergency services, and finally its infrastructure such as its transportation systems, its water system, its gas and oil system, its electrical system and its communication system. Of course, with a little imagination the analysis team could identify other important systems or sub-systems that would need to be considered. However, for demonstration purposes this list will be enough with which to start.

Then the system environment should be outlined. This environment can be thought of as the super-system that surrounds the system and of which the system is a part. The super-system could be the country or region in which the city is located.

The next aspect of the system that needs to be identified is its primary useful function. The primary purpose of a city is as a place in which people can live and work efficiently. This primary useful function may be supported by other useful sub-functions that should also be listed. The sub-functions of a city are shelter, wealth generation and storage, medical care and social events to name just a few.

The final part of the system description is the potential harmful functions that are created by the system. The potential harmful functions of a city are waste and pollution, and possibly excessive energy and resource use. High levels of population density might also be considered to some extent a harmful function of a city.

It is useful at this point to describe why the failure could not be solved using the direct method. The reason that the problem has not been solved already has many parts. The main reason the problem might not have been solved already is related to the expense in terms of private and public investment in prevention of critical infrastructure failure that is not considered affordable.

The analysis team should answer the question “What about the failure is unclear?” The nature of interconnectedness of the critical infrastructure might be one of the things that is most unclear about the problem.

Another important element of the description is determining what events are associated with the failure. What are the historic events prior to the failure? And

what are the reasons they occurred? There are many examples of natural disasters causing failure of critical infrastructure. Most of the recent ones have been analyzed extensively by many national and international agencies.

The analysis team should consider whether other attempts have been made to solve this problem. It is believed that although many attempts have been made to solve this problem, none have been completely successful. However, there have been many useful partial successes created by the general awareness of the need. Too often these successes come after a critical infrastructure failure caused by a natural disaster rather than before. Another result is that as time passes without another natural disaster occurring, the successful strategies are forgotten and the problems return.

Localizing the failure is also an important step. The analysis team should try to determine the specific circumstances in which the failure occurred. The analysis team should identify the last event before the failure occurred. Also the analysis team should identify any concurrent events that happened with the failure or specific conditions associated with the failure. Different cities are susceptible to different types of natural disasters but the most common ones are floods and storms. The most common occurrences to storms and floods are in coastal regions or near rivers. Inland cities might also be commonly susceptible to tornadoes and occasionally susceptible to earthquakes. One of the specific conditions of critical infrastructure failure is lack of preparation and planning and possibly poor architectural design of buildings, ports and roads.

With the answers to the Failure Analysis Questionnaire, the analysis team should then be able to develop a system model. Figure 1 shows a simplified model of the

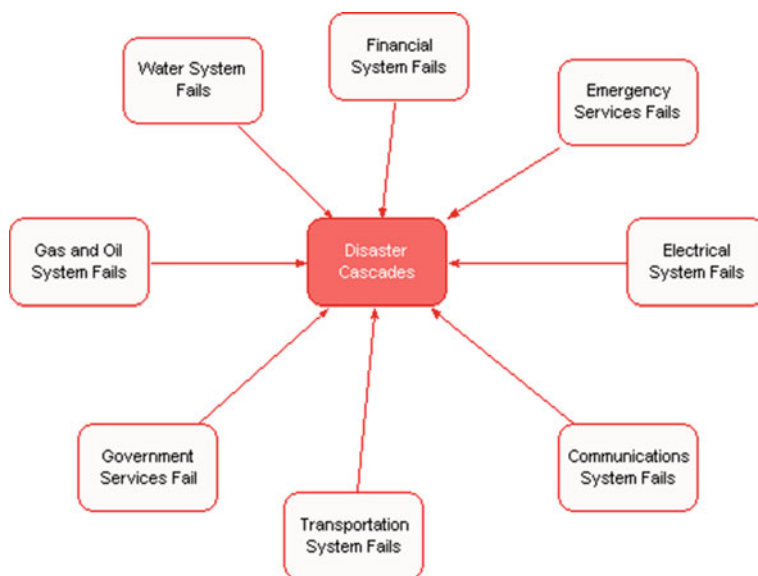


Fig. 1 A simple model of cascading critical infrastructure failure

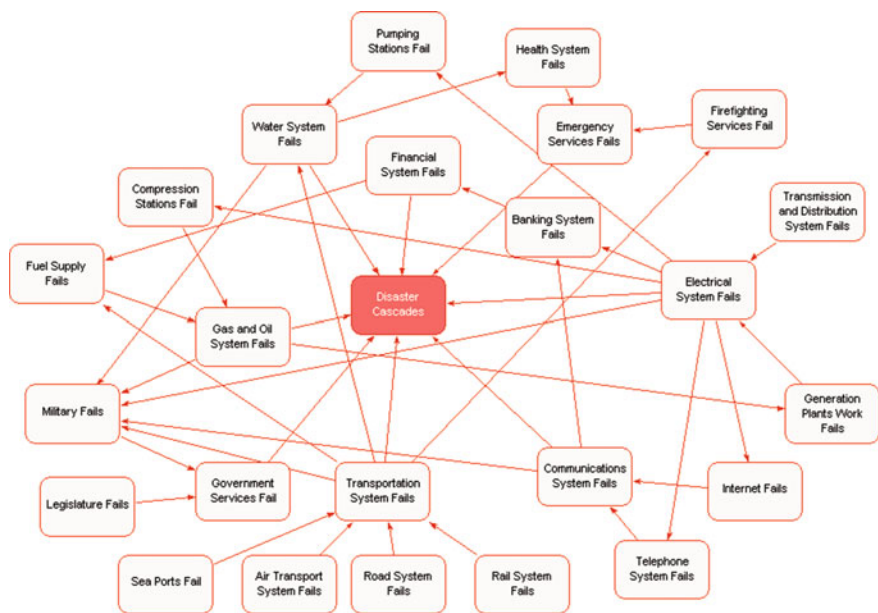


Fig. 2 A more complex model of cascading critical infrastructure failure

problem of cascading failure of critical infrastructure while Fig. 2 shows a more complex model of the problem.

Using this model, the problem can be inverted. The analysis team is encouraged to “find a way to produce the failure”. The analysis team then uses an embedded knowledge base of Directions, Operators and Illustrations to create possible causes of the failure. A Direction is a statement that represents how the model can be used to suggest ways to create the failure. Each model can be used to suggest many Directions towards the failure.

Below is a complete list of the Directions created by the software for the inverted problem suggested by the simple model in Fig. 1:

1. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Gas and Oil System Fails).
2. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Government Services Fail).
3. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Transportation System Fails).
4. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Communications System Fails).
5. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Electrical System Fails).
6. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Financial System Fails).

7. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Emergency Services Fails).
8. Consider opportunities for providing [the] (Disaster Cascades) with help of resources of [the] (Water System Fails).

For the more complex model shown in Fig. 2, the software generated 25 similar Directions for consideration by the analysis team.

4 Hypothesizing Failure Modes

At this point, it might be worthwhile to divide the problem into its particular sub-problems and employ a number of analysis teams, one for each of the sub-problems. For example, the analysis team could be broken into analysis sub-teams for the gas and oil system, the government services, the transportation system, the communication systems, the electrical system, the financial system, the emergency services system and the water system. It is recommended that these sub-teams for each of these sub-problems be augmented by experts in each of these fields.

There are two possible ways to conduct the analysis from here. One approach involves a top-down comprehensive method of identifying all possible ways to create the failure. This strategy allows for an exhaustive set of possible causes. A second method, involves considering the most promising way to create the failure. Then the process is repeated with the next most promising way, and so on. For each possible cause, the question is whether the necessary resources are available for the cause to be feasible.

As one could imagine, the exhaustive method would take a great deal of time. However, it is the recommended way to conduct the analysis. The second method would seem more efficient although could still be quite time consuming. We will again prioritize the inverted failure modes using the Analytical Hierarchy Process (see Table 2). Then we will look in some detail at one failure mode.

Let’s look at the knowledge base concerning the search of resources related to the Gas and Oil System Fails to determine if this cause could create the cascading

Table 2 Prioritization of inverted failure modes

Inverted failure modes	Priority value (%)
Gas and oil system fails	4
Government services fail	11
Transportation system fails	8
Communications system fails	9
Electrical system fails	7
Financial system fails	2
Emergency services fails	43
Water system fails	15

disaster. The question that needs to be answered is: “Are there sufficient resources in or near the Gas and Oil System so that if it fails, a cascading critical infrastructure failure will occur?” Using the Ideation Failure Analysis™ knowledge base, the analysis sub-team who are particularly knowledgeable about the gas and oil system would begin with a direct approach to finding resources.

4.1 *Finding Resources Directly*

For this purpose, the knowledge base contains information on available: materials resources, energy resources, time resources, space resources, structural resources, functional resources, and information resources. Table 3 shows a subjective prioritization using the Analytical Hierarchy Process that could be used to allocate effort towards the search for these resources. With this allocation in mind, the analysis team would use the knowledge base to look in more detail at each of these resources.

There is extensive information in the knowledge base concerning each of these resources. Here is an excerpt from the knowledge base concerning energy resources:

The analyst should consider as a resource any kind of energy available in the object or process that might help to provide existing functions or operations, or to perform new ones. The analyst should consider mechanical impacts of solid-state objects, mechanical impacts of liquids and gases, thermal impacts, chemical impacts, electrical fields, magnetic fields, radiation impacts. Mechanical impacts of solid-state objects can be used for: creating a desired shape, creating a dynamic shape, transportation, control of transport, protection, slackening an undesired action, obtaining information, energy accumulation. Mechanical impacts of liquid or gases can be used for: retaining objects, transporting liquids and gases, creating a support, reducing resistance to movement, destroying solid-state objects, sealing, heating, or temperature control. Thermal impact can be used for: changing material properties, creating phase transitions, destroying an object, generating force, joining parts, transporting an object, or controlling chemical processes. Thermal impact can be used to change material properties. In particular, the following can be changed: structure, composition, magnetic properties, mechanical strength, color, shape and dimension. Thermal impacts can be used to create phase transitions, in particular, for: melting – solidifying, evaporation – condensation, sublimation, changing crystal structure. Chemical impacts can be used for: creating a material, changing properties, joining objects, creating force, process

Table 3 Prioritization of failure resources

Typical failure resources	Priority value (%)
Material resources	15
Energy resources	38
Time resources	19
Space resources	19
Structural resources	5
Functional resources	2
Informational resources	2

activation, obtaining information, transferring information. Electrical fields can be used for: transporting liquids or light objects, separating objects, changing an object's structure, changing an object's properties, material decomposition, process control, generating permanent forces, creating shocks, obtaining information. Magnetic fields can be used for: joining parts, integrating powder or granules, creating force, developing a particular structure, material separation, obtaining information about an object. Radiation impacts can be used for: destroying, heating, generating an electrical field, comparing and distinguishing objects, making objects visible, developing a non-visible image, marking parts, image transformation, or documenting information. If the analyst cannot find energy resources within the object or process, he or she needs to consider the resources within the nearby environment. In particular, he or she should consider the energy of the super-system of which the object or process forms a part.

We will briefly go through the steps of determining the various resources required for the gas and oil system to be the cause of the failure.

The analysis team should consider any kind of material available in the system. Obviously, the oil and gas system contains flammable material that could result in explosions. In this case, the analysis team would need to look for material that could act as an igniter. This igniter might be found in the energy resources which will be discussed below.

The analysis team should consider any kind of energy available in the system. The analysis team should consider mechanical impacts of solid-state objects, mechanical impacts of liquids and gases, thermal impacts, chemical impacts, electrical fields, magnetic fields, radiation impacts. Table 4 provides a subjective prioritization of these energy resources using the Analytical Hierarchy Process that can be used to allocate effort to the further analysis of these energy resources.

Mechanical impacts of solid-state objects might include the transportation system of trucks that are used to move the gas and oil. Mechanical impacts of liquid or gases might include the pumping stations and piping that moves the gas and oil to the city. Thermal impact might be the destruction of some parts of the system caused by fires created by explosions. Electrical fields can be used to create sparks from short circuits that cause the ignition of gas and oil in the system. Radiation impacts can be used for heating which might be related to the ignition of a gas or oil system explosion.

Table 4 Prioritization of energy resources

Energy resource	Priority value (%)
Mechanical impact of solid-state objects	20
Mechanical impacts of liquids and gases	18
Thermal impacts	27
Chemical impacts	10
Electrical fields	21
Magnetic fields	2
Radiation impacts	2

The analysis team should consider the time intervals in the system in particular, time before delivery of the gas and oil such as the time in refiners or compressors, time during the delivery such as the delivery of gas and oil in ships, trucks and pipelines, time after the delivery has ended such as at the facilities of the gas and oil users.

Free space might be available in the object. This space can involve the co-location of parts of the gas and oil system with other facilities or the distance that must be traveled between the sources of the gas and oil and the final destination of the gas and oil.

The analysis team should consider the structure of the system. In particular, they should consider the location of subsystems such as the refineries being near coast lines of oceans, lakes or rivers or gas and oil generators being co-located with electrical energy plants.

The analysis team should consider how part of the process could perform additional functions in particular, useful functions, such as heat or energy generation; and harmful functions such as pollution or contamination of water supplies.

The analysis team should consider any information about the system such as rate of flow on pipelines, shiploads, truckloads and barrels of oil and gas delivered.

After this thorough examination of resources, the gas and oil analysis team might conclude that all the resources required for this failure mode exist near the gas and oil system. Then this failure mode needs to be addressed. Or the analysis team may conclude that none of the resources are available near the gas and oil system. Then they can rule out this failure mode. Finally, the analysis team might conclude that some but not all resources are in or around the system. Then the analysis team can find new resources. For the sake of this example, we will examine the process of finding new resources using the Ideation Failure Analysis™ knowledge base.

4.2 *Obtaining New Resources*

The analysis team should consider the methods for changing or modifying the system under consideration in order to obtain: new material resources, new energy resources, new space resources, modifying time, modifying structure. Table 5 shows a prioritization of the various types of new resources that need to be examined by the analysis team.

Table 5 Prioritization of new failure resources

New failure resources	Priority value (%)
Material resources	24
Energy resources	57
Space resources	8
Time resources	8
Structure resources	3

Here is an excerpt from the knowledge base concerning new material resources:

To obtain new material resources, the analyst should try to modify material available within the object. He or she should consider the following ways of modifying available material properties: material transfer, obtaining new material resources through physical effects, or obtaining new material resources through chemical effects. New materials can be obtained in a system via transfer from another system. The analyst should consider applying the following transfer mechanisms: using a flow of liquid or gas, "capturing" elements, electro-transfer. The analyst should consider the following physical effects capable of changing or modifying material properties and obtaining material resources: by thermal treatment, by fractionating, by decomposition, by mixing, by introducing additives, by ionization/recombination, by using specific effects. Treatment with heat or cold can change the initial properties of a material. In particular, the following can be changed: hardness, shape, aggregate state. Fractionating a material can provide it with new properties, in particular, mobility or controllability. The decomposition or transformation of a material to a mobile state can help in removing the material after it has fulfilled its desired function. Mixing materials can provide several new properties such as the ability to: connect, affix. Additives introduced into a material can provide new properties such as the ability to provide: insulation, expansion. Ionization (recombination) can change material properties to provide: electrical resistance, stages of aggregation.

We will briefly go through the process of looking for new resources in the gas and oil system.

For new material resources in the gas and oil system, there are many ways that the material resources could be transformed such as through additives, decomposition and mixing. Broken piping could allow harmful outside materials to enter the system and interact with the gas and oil. Refining chemicals could initiate harmful material interactions in the gas and oil system.

For new energy resources, the analysis team should consider transferring or delivering energy through the transportation system of ships, trucks and compression systems. New electrical energy could come from downed power lines. The knowledge base provides many more energy sources that could be used to develop analogies about new energy resources.

For new space resources, the team should consider the movement through space such as the space in and around the transportation network. Leaks from the gas and oil system might occur in these new spaces.

For new time resources, the analysis team should consider modifying available time in the processes of the system. The gas and oil system might try to adapt to the natural disaster using time resources. Another way the time resources might be affected is through an interruption of service that creates a cascading failure of the critical infrastructure.

The analysis team should consider ways of changing the structure of the oil and gas system such as integrating two processes. For example, the gas delivery system could interact with the oil transportation system to enhance the failure. Or the failure could be enhanced by the transportation of oil by ship, ocean and port being connected to the transportation of oil by truck and road.

In addition, the analysis team should consider the specific failure resources available in the system as shown below.

4.3 *Specific Failure Resources*

Table 6 shows an example Analytical Hierarchy Process prioritization that could be used to allocate effort in the search for specific failure resources.

As an excerpt from the knowledge base, the following is a description of possible human errors or malicious acts that should be considered:

Human errors and malicious acts are often resources for system failure. Unpleasant as it is, we must recognize the existence of people who will intentionally damage a system to serve their own interests. Unintentional failures can be caused by humans as well. A person can be dangerous due to his/her specific characteristics or habits, including: a physical or mental disorder such as poor motor coordination, low intelligence, delayed reactions; mental instability that manifests as lack of self-confidence (easily influenced by others), or aggressiveness; a habit of under-estimating the level of risk such as belief that a failure will never take place, a habit of relying on the competence or wisdom of others, a habit of taking risks; the acceptance of harm as an “unavoidable evil” such as remaining passive in a dangerous situation, not learning from accidents; tendency to act “by rote” in an emergency such as following customary (familiar) instructions regardless of the situation, mimicking the actions of others when individual decisions are necessary, relying on personal, everyday experience; tendency to apply a creative approach to any routine situation such as disobeying instructions “for good reasons”, perfectionism; having a “guilty conscience” that manifests as illegal actions, anti-social behaviour. An “ordinary” person can be transformed into a source of danger for the system he/she is dealing with due to the following unfavourable conditions: poor professional background such as lack of professional knowledge, lack of attention to auxiliary operations and elements, violating safety regulations, disregard for complicated devices or processes; stressful environment such as life/health threatening environment, stress due to frequent changes, high level of responsibility, repeated failure; fatigue caused by repeated irritation/annoyance, monotonous working conditions, specific physical, biological or chemical impacts; hindered control of a situation such as diverting

Table 6 Prioritization of specific failure resources

Specific failure resources	Priority value (%)
Intentional actions or spontaneous events	8
Differences in some parameter or characteristic	4
Specific characteristics and properties of a system	3
Harmful structures	11
Small failures and disturbances	2
Dangerous adjacent systems or elements	29
Faulty control devices	10
Faulty counter-failure systems	10
Human errors and malicious acts	22
Exhaustion of the useful resources	1

attention, erroneous or incomplete information; misunderstanding due to non-specific words or gestures, cultural differences, falsified information; poor written instruction that are impractical, lack of recommendations for emergency situations, including unreasonable restrictions, conflicting with other recommendations, unclear to the user, modified or appended many times; automatic reaction; irresponsible environment impacting a person's behaviour; group egoism causing a person to intentionally misrepresent information, providing special privileges to certain people, imposing unreasonable restrictions on others, neglecting community interests when making decisions; lack of training for extraordinary situations, not taking protective measures beforehand, lack of training regarding the use of protective means.

The analysis team should consider the consequences of changed location and speed such as in delivery systems for gas and oil. Pressure differentials caused by leaking of gas or oil pipelines might be considered here.

The analysis team should consider harmful structures. In particular, they should consider either in space or in the supply schedules if the gas and oil supply system is disrupted. They should consider specific characteristics of the subsystems such as when sub-systems of the gas and oil system can have large harmful effects. They should consider small failures and disturbances that tend to lead to more dangerous consequences such corrosion in pipelines. They should consider elements that become unfit or harmful under irregular circumstances. In particular, they should consider inflammable materials and toxic materials.

Faulty control devices or protection systems can be sources of danger. In particular, the analysis team should consider electrical or electronic measuring devices located at system inputs/outputs such as pressure monitoring systems. Faulty counter-failure systems, protective means, safety measures can be the sources of high-risk. In particular, the analysis team should consider faulty controlled or automatic valves or emergency switching mechanisms.

Harmful resources can appear by the exhaustion of the useful resources. For example, the gas and oil system could run out of useful transportation services.

5 Correcting Failure Modes

The failure correction stage involves using the model and knowledge base to prevent, eliminate or reduce the harmful effects of the failure.

5.1 Preventing the Failure by Averting Its Causes

For this purpose, the analysis team should identify the events prior to the failure. They should consider going back and modifying the events such as in our case, diversifying the fuel supply system, or hardening or providing backups for the compression stations. These measures might be costly to implement but it might be worthwhile if this would avoid cascading failure of the critical infrastructure.

5.2 *Eliminating the Failure's Harmful Effects*

The harmful effect might be eliminated by: removing or changing the source of harm; modifying the harmful effect; counteracting the harmful effect; isolating the system from the harmful effect; increasing the system's resistance to the harmful effect; modifying or substituting the effected object. Table 7 provides a prioritization of these ways to eliminate the harmful effects that was developed using the Analytical Hierarchy Process.

To get a feeling for the nature of the failure correction knowledge base, below is an excerpt on isolating the system from the harmful effect:

The analyst should consider isolating the system from the harmful effect. In particular, he or she should try to isolate the system from: wear, fire, explosion, ambient oxygen, evaporation, thermal impact. To make the isolation more effective, he or she should consider inventive ways to introduce an isolating material. The analyst could consider the following ways of introducing an isolating material: use available materials; use selectively permeable isolation; use an easily-destroyed intermediate layer; transform a mediating element. The analyst could consider using materials available in the system or process as isolating materials. In particular, he or she could make use of materials: involved in causing the harmful effect; available in the system or produced by it; that are inexpensive. The analyst should pay particular attention to the possibility of easily replacing the isolating material if and when it is destroyed. If you need to isolate a system from the environment but also need to maintain access to the system, the analyst should consider using an isolating material or arrangement such as foam, a layer of liquid, gas or air, or a grating (to separate large particles from smaller ones). If two adjacent components that will have to be separated adhere too tightly to each other, the analyst should consider using an intermediate layer. The intermediate layer should hold the two components together but should be easily removed or destroyed.

The analysis team should try to remove the source of danger. For example, hardening of the gas and oil refineries and delivery systems would make the process more secure. They should consider modifying the harmful effect. If the harmful effect takes place at a point, the analysis team should consider changing the point contact to a multiple points of contact. This might involve having many smaller gas and oil storage sites rather than one large site. They should consider using another effect. For this purpose, they should consider neutralizing the harmful effect with a countering effect such as hardening of the gas and oil system. They should consider isolating the system. The analysis team could use available materials such as open spaces.

Table 7 Prioritization of ways of eliminating the failure mode

Ways of eliminating the failure mode	Priority value (%)
Remove or change the source of harm	25
Modify the harmful effect	3
Counteract the harmful effect	7
Isolate the system from the harmful effect	30
Increase the system's resistance to the harmful effect	30
Modify or substitute the effected object	4

5.3 Stopping the Harmful Effects of the Failure

The analysis team should try to make the system more resistant. In particular, they should decrease the sensitivity to a harmful effect by for example providing hardening, backup systems, multiple supply lines, and a diversity of sources of supply. An alternative would also provide in advance for immediate restoration of the system by replacing or repairing portions that are destroyed or damaged. This could involve dedicating resources to come into effect in the case of a natural disaster.

If it is impossible to protect the system, the analysis team should consider substituting the system. In particular, the analysis team could look into substituting the gas and oil system with electrical energy systems or replacing the trucking of gas and oil with pipelines.

If the analysis team has not found a way to resolve the problem, they should try to reduce its harmful effect by: localizing its harmful effect; reducing the effect; facilitating detection; or “sugar coating the pill”.

To show the extent of the knowledge base to support the stopping of the harmful effects, below is an excerpt from the knowledge base:

If it is impossible to eliminate a harmful effect, the analyst should consider the possibility of localizing it. This will help to protect other parts of the system and to assess damage as well. For this purpose, the analyst should consider: confining the effect to a definite location or time interval, or sheltering a material inside another material. The analyst should consider reducing the harmful effect at a specific location and for a specific period of time. In particular, he or she could distribute or dilute the harmful result. If a local defect can not be eliminated, the analyst should consider multiplying this defect so a pattern develops which hides the defect. He or she should see if there is a way to utilize, even temporarily, a harmful material, energy or undesirable system parameter. If it is impossible to eliminate a harmful effect that leads to a search (for lost or damaged systems or for individuals responsible for the harm), the analyst should consider making provisions in advance that will facilitate the search. If it is impossible to eliminate or reduce the harmful effect, the analyst should consider achieving some partially compensating positive effect. This might make things easier to accept, at least.

The analysis team should consider confining the effect to a definite location, or in this case creating smaller gas and oil storage facilities. The solution of many smaller facilities would also have the possibility of reducing the harmful effect. They should consider implementing detection systems such as pressure monitors on pipelines. They should consider providing shelters for citizens to move to in case their gas and oil heating systems fail.

6 Evaluating the Results

The analysis team would now select the most promising of the possible solutions. The most promising possible solutions would be considered “Good, that is, the failure would be completely prevented or eliminated”. However, the analysis team

should not stop there. Even solutions that can prevent or eliminate the failure might have adverse side-effects. The solution should be examined for adverse side-effects using a simplified form of the Ideation Failure Analysis™ and then these adverse side-effects should be prevented, eliminated or reduced.

The second most promising solutions might be considered “Good, but..., that is, there are one or more minor problems with correcting the failure”. Again these minor problems should be avoided, eliminated or reduced. The knowledge base provides specific suggestions that can be used to separate these minor problems from the potential solutions. Thus the “Good, but” solution has a known defect while the so-called “Good” solution has no known defects until the simplified Ideation Failure Analysis™ is conducted on it.

To provide an example of how this might work in practice, we will consider as an example the “Good” solution of replacing the gas and oil system with an electrical energy system. We will consider the “Good but” solution as diversifying the gas and oil supply, storage and delivery system. This solution has the known drawback that it might be more costly.

6.1 Simplified Ideation Failure Analysis™

The “Good” solution completely solves the problem. However, unpleasant surprises can arise. Therefore, the analysis team should conduct a simplified Ideation Failure Analysis™: step 1, invert the problem; step 2, invent possible failures; step 3, prioritize failures to be eliminated.

In step 1, the analysis team should “invert” the problem as follows: “It is necessary to produce all possible failures to [critical infrastructure] and/or its environment with the help of [an electric energy system]”.

In step 2, the analysis team can then imagine possible failures that use the following resources: systemic resources; change resources; differential resources; inherent resources; organizational resources; small failures and disturbances; dangerous elements; control devices; protection systems; human errors and malicious acts; exhaustion of useful resources.

It is likely that a natural disaster that is harmful to the gas and oil system would also be harmful to electric energy system. For example, cables might be broken, generators could fail or be over loaded, fires or explosions could be created by short-circuits.

In step 3, the analysis team should list possible problems with the solution. Then they should prioritize the problems based on their consequences and likelihood and determine which problems should be eliminated. It is likely that electric energy generators would fail during a natural disaster such as a flood or a severe storm. Overhead transmission wires and cables would probably break and fall possibly causing fires or explosions.

The analysis team should consider various ways to resolve the problems as shown in Table 7. These drawbacks in the electric energy system might be eliminated by having generator backups and running cables underground instead of overhead.

6.2 *Resolve the Contradictions*

If the solution contains some known drawbacks, the analysis team should formulate a contradiction such as “The concept [of diversifying the supply, storage and delivery system for gas and oil] should provide [avoidance of a cascading failure of the critical infrastructure in the city] ... but should avoid [the problem of being costly]”. Then using the separation principles they should try to resolve this contradiction.

To demonstrate how the knowledge base can support the resolution of the drawbacks of the potential solutions, the following excerpt from the knowledge base is provided.

The analyst should try to separate the contradictory requirements: in space, in time, between a whole object and its parts depending on different conditions. The analyst should try to separate opposite requirements in space. For this purpose, he or she should partition the object or assign each contradictory function or condition to a different part. The analyst should try to separate opposite requirements in time, that is, schedule operation so that conflict requirements or functions take effect at different times. The analyst should try to separate opposite qualities between the whole object and its part. For this purpose, he or she should: assign one of the contrary functions or conditions to one or more parts, while the whole object retains the remaining functions and conditions; separate the part(s) with the undesirable qualities from the rest; isolate the part(s) of the system or process that has the undesirable qualities; consider making use of the special properties or features of the object. The analyst should determine what action will manifest these properties or features and apply that action and try to identify a parameter or condition that can change to allow the system to meet one requirement under one condition and the opposite one under another condition.

The analysis team should try to avoid the contradiction: in space, in time, between a whole object and its parts depending on different conditions. For example, one way to separate the contradiction in time is to shift the solution into the future. As the centralized gas and oil system ages and replacement is being considered, steps could be taken to diversify the system, making storage sites smaller and distant from each other in space.

7 **Concluding Remarks**

In this chapter, we have shown how problem inversion can be used to enhance creativity in failure analysis. We have looked at an example of the problem of cascading infrastructure failure in a city caused by a natural disaster such as a flood or a storm. We have also demonstrated how the processes and the knowledge base in the Ideation Failure Analysis™ software could augment this problem inversion process.

We have demonstrated that solving this problem using this method would take a great deal of effort. The allocation of effort could be distributed to teams of experts because the process breaks the problem into its individual parts and the knowledge base has been developed in a highly hierarchical manner. We suggested that a prioritization method be applied to the allocation of effort to make the process more efficient. In particular, in our example, we used the Analytical Hierarchy Process in this allocation of effort. The Analytical Hierarchy Process seems to be an excellent way to allocate effort because it provides the prioritization in percentage terms where the total amount of effort can be broken down into its separate components. Also although not all of the components will get the same allocation of resources, none of the components will be completely overlooked. Each component will receive some amount of effort allocated to it even if it is small. This is important because failure analysis is often affected by small problems that have big impacts.

This approach does not come without some serious reservations that must be considered. First, as we have already mentioned is the time and effort required to complete the process in an exhaustive manner. The second is the fact that analysts using the knowledge base as a checklist might stop their creative process after finding just one potential failure mode or correction technique for the particular Direction or Operator. It is imperative to push the creative process to attempt to exhaust the ideas that can be generated from each Direction and Operator. The third concern relates to the applicability of the knowledge base in the Ideation Failure Analysis™ software. It could take a great deal of effort to adapt the knowledge base to make it more applicable to the problem of cascading failure of critical infrastructure. Associated with this problem with the method is the availability of expertise. Getting teams of experts together to work through the issues for a great length of time might be difficult or costly. Also it is likely that the solutions found by this method have already been ruled out because they are too costly to implement. If they were not too costly, they would probably have already been implemented. Finally, there may be security concerns. If the failure modes became widely known to the public, there would be a great deal of negative publicity that there are a large number of failure modes being considered by government agencies. There are also the obvious security concerns of keeping this knowledge of the numerous failure modes out of the hands of enemy forces because this method and its results could facilitate sabotage or terrorism.

None of these reservations would seem to be sufficient to discount the value of further analysis of the inversion technique for solving the problem of cascading failure of critical infrastructure caused by a natural disaster.

References

1. Center for Research on the Epidemiology of Disasters (2015) Human cost of natural disasters: a global perspective. World Health Organization. http://emdat.be/human_cost_natdis. Accessed 24 Nov 2015

2. Mateski M (2009, June) Red teaming; a short introduction. Red Team J. [http://redteamjournal.com/papers/AShortIntroductiontoRedTeaming\(1dot0\).pdf](http://redteamjournal.com/papers/AShortIntroductiontoRedTeaming(1dot0).pdf). Accessed 24 Nov 2015
3. Evaluation Research Team (2006, Nov) Gaining consensus among stakeholders through the nominal group technique. Evaluation Brief No. 7, Department of Health and Human Services, Center for Disease Control and Prevention. <http://www.cdc.gov/healthyyouth/evaluation/pdf/brief7.pdf>. Accessed 24 November 2015
4. Taylor I (1996, Apr) An extension of structured brainstorming using the six thinking hats. Directorate of Logistics Analysis, Research Note 9603. <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc42/p498627.pdf>. Accessed 24 Nov 2015
5. Klein G (2007, Sept) Performing a project PreMortem. Harvard Business Review. <https://hbr.org/2007/09/performing-a-project-premortem>. Accessed 24 Nov 2015
6. Kaplan S, Visnepolschi S, Zlotin B, Zusman A (1999) New tools for failure and risk analysis anticipatory failure determination (AFD) and the theory of scenario structuring. Ideation International Corporation. <http://www.ideationtriz.com/new/materials/AFDNewToolsbook.pdf>. Accessed 24 Nov 2015
7. Saaty TL (2008) Decision making with the analytic hierarchy process. Int J Serv Sci 1(1):83–98. http://www.colorado.edu/geography/leyk/geog_5113/readings/saaty_2008.pdf. Accessed 24 Nov 2015

Disaster Forensics

Understanding Root Cause and Complex Causality

Masys, A.J. (Ed.)

2016, XVII, 409 p. 41 illus., 30 illus. in color., Hardcover

ISBN: 978-3-319-41847-6