MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

The Importance of Misalignment to Reduce Risk and Prevent Disasters

Mark Galley*
ThinkReliability
Pearland, Texas 77584, USA (Houston)
*Presenter E-mail: mark.galley@thinkreliability.com

Abstract

Large incidents are a combination of different factors. Any of those factors on their own would not have produced the incident, but together can be catastrophic. This unfortunate alignment is the nature of all disasters. Understanding how each piece came together to produce that incident provides important insight for reducing risk and preventing future incidents from occurring. Some organizations within the energy, aviation and healthcare industries cite James Reason's Swiss cheese model of accident causation to explain this confluence of events. The holes in each slice align just right for the incident to occur. Moving just one of the slices can prevent a negative outcome. If more than one slice is misaligned, the risk can be made even lower. This is also known as defense in depth and layers of protection—approaches used across high-risk industries.

The straight-line slices of cheese overlook the important interconnections within complex issues. An incident consists of multiple cause-and-effect relationships that all come together in a particular way. Digging into these causes provides opportunities to misalign an incident, reducing the risk of the system in the future. Highly reliable organizations dissect their operations to pinpoint where simple verifications and checks can make the likelihood of an incident significantly lower.

This presentation uses a few historical disasters, including the 2005 Texas City refinery explosion, to explain how a complex incident can be analyzed starting with just a few basic cause-and-effect relationships. That simple analysis can then be expanded into a much more detailed explanation revealing how simple miscommunications like shift change, were causally related to the disaster. Changing one item would have changed that incident. Improving the way people communicate details within an incident improves the way they mitigate risk and prevent incidents going forward.
Keywords: Incident Investigation, Risk Management, Risk Assessment, Process Safety Information and Knowledge, Operational Integrity, Human Factors and Errors

1 Introduction

The way problems are explained affects the way they're solved. An accurate and thorough representation of an issue is essential for understanding the different ways risk can be reduced. There can be disconnects in the way people discuss problems depending on the tool or model people use. These miscommunications can distort the analysis and obscure the solutions. Avoiding communication roadblocks doesn't require adding another tool, but rather going back to the basics—a first principles approach.

2 Right-Answer Versus System Problems

From our earliest school years, we learn that solving problems is about finding the right answer. Twelve or more years in school focused on providing the right answer on homework, tests and college entrance exams has an effect—it creates a bias for the one, right answer. That right-answer approach from school becomes our default model for all problems. It reinforces the idea that there is a silver bullet, cure-all, panacea or root cause to solve whatever the problem might be.

But there are two fundamentally different types of problems with your operation. There are *right-answer problems* that have one answer and there are *system problems* that have a range of different solutions. Many of the daily problems people encounter in their jobs have one right answer. In these cases, the right-answer approach works well. How many people were on the crew? What's the volume of the tank? What's the flash point of that product? What is the planned start date? Which valves need to be closed to isolate this system? All these questions have a one right answer.

System problems, on the other hand, don't have a right-answer. A system problems naturally break down into parts. Because they're multifaceted there is a range of solutions. Different people working on the same problem can propose completely different ways to solve it. Solutions to a system problem vary by complexity as well as effectiveness. Some solutions are better than others. There are also trade-offs and constraints. Sometimes a high risk, potentially catastrophic problem can have a solution that is simple, yet extremely effective.

Just as risk and reliability are probabilistic, system problems are too. The concepts of a cumulative reduction in risk, layers of protection and defense in depth are based on the *degree* to which the probability and consequence can be lowered. Like the concept of six-sigma, preventing a system problem is also a matter of degree. There's not one right answer. Safety within a company, whether it's for personnel or process, strives for zero incidents by making the risk extremely low. Operations and equipment issues are system problems—as are all issues related to human performance and human error. Improving training and procedures to prevent errors also has a spectrum of solutions, instead of a right answer.

Distinguishing between right-answer and system problems is important because the approach and language for solving them is different. Right-answer problems have one right answer. The words *right* and *wrong* apply. This question, "What is 3 x 5?," has one answer: 15. Someone may believe

it's 18, but their answer is wrong. It's appropriate discuss these types of problems in terms of right and wrong.

Questions like, "Why did the equipment fail?," "Why did the tank overfill?," and "Why did that injury occur?" require some digging. There is not one answer to those questions. The explanation of why something happened naturally uncovers more and more questions. The same question may be answered differently by different people. Each person may explain a different part of the overall problem since they see the incident from their different points of view. Engineering, operations and maintenance don't see problems the same way, but that doesn't mean there's necessarily a conflict either. With a system problem, different people can provide different answers to the same question, yet both can be telling the truth. This point is demonstrated in the case studies in this paper (see Section 6).

3 How the Search for the Root Cause Distorts Problems

One of the most common mistakes people make when investigating a problem is trying to apply right-answer thinking to a system problem. This right-answer bias leads people to mistakenly attribute an incident to a special cause, commonly referred to as the "root cause." A root cause is usually defined as the one factor that if removed would have prevented the incident from occurring. This model assumes that some causes are more important than other causes. The less important causes, those that cannot produce the issue on their own, are known as contributing factors. In this model, the identification of the root cause is key to eliminating the problem.

This mental model is appealing to those who think in terms of right-answer, but it is evidence of how people are biased to their own points of view. People select and emphasize the information that supports their agenda and ignore what doesn't. For an incident to have occurred, every cause of that incident had to happen. The fire triangle is one example of this. Changing any one of the causes changes the incident. Those who believe a root cause is a special type of cause, use the same argument: if the root cause wouldn't have occurred the incident never would have happened. This point may be true. But right-answer thinkers fail to recognize that same point applies to all the other causes of the incident in the same way. When a right-answer thinker tests one of the causes, they can mistakenly conclude that they're right without testing other causes. Their argument for that cause is accurate, valid and true, but it is not "right." It's not the cause. It's one of the causes. This is a known as confirmation bias. People test their root cause to confirm they're correct. If they tested their argument on any of the other causes, they would notice each of those causes satisfies the same argument. This is confirmation bias because people only test their preferred cause to confirm they are correct. It reflects how strong right-answer bias can be.

These are perceived less important causes are typically labelled as contributing causes or secondary causes and may not even be considered for solutions. By differentiating causes organizations can be missing opportunities to find better solutions. Focusing only on root causes artificially restricts the analysis, thereby limiting the set of available solutions. Ideas and insights from others can inadvertently be stifled if the group is mandated to focus only on the important causes – the root causes. Another unfortunate characteristic of root cause logic is it inadvertently aligns with a blame mentality. By looking for just one cause, blamers want to know the person or

group who caused the problem. They don't want to look at the system. Blamers want to know the person or group responsible. The right-answer model of root cause analysis often mistakenly reinforces the language of blame.

Understanding that the root is a system of causes that branch out in different causal paths, all of which had to occur to produce the incident, provides an accurate and thorough explanation of an incident. The concept of conducting a root cause analysis to identify that system is based on simple cause-and-effect, and so is the Swiss cheese model.

4 How the Slices of Swiss Cheese Align

The Swiss cheese model (see Figure 1) of accident causation developed by James Reason provides an easy way to visualize how multiple breakdowns result in a problem. The Swiss cheese model has become popular across industries from refining to healthcare. It provides a conceptual framework that a problem is consists of multiple factors that all came together and aligned in the right way to produce the unwanted incident. Reason uses latent and active failures. He says the latent failures are built into the system, whereas the active failures are behaviors of individuals.

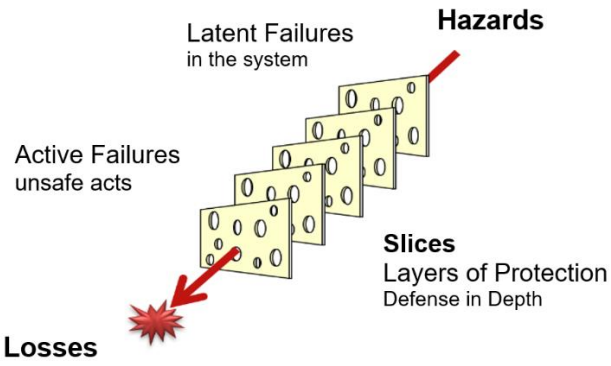

Figure 1 – James Reason's Swiss cheese model

Within the model, each slice of cheese is meant to represent an organizational defense. The holes in a slice are weaknesses where the defense can be breached. The model demonstrates that organizations put systems and processes in place that are designed to prevent a problem. When all the slices align in such a way that there's straight line passing all the way through the negative event happens. All the breakdowns are required.

The point is multiple items must align for the incident to happen. Meaning, if we misaligned just one slice the problem is avoided. Misaligning more than one slice makes the likelihood of occurrence even lower. This is the layers of protection logic that helps reduce risk in many organizations.

When a problem does occur, an investigation identifies all the different slices–the systems that broke down. For the incident to have occurred, all the slices had to align in a particular way. In retrospect, it can seem incredible how everything came together the way it did. But they had to come together in that specific way, or the incident wouldn't have happened.

What people sometimes don't realize about their organization is that multiple slices are aligning every day. Every day 2 of 5, 3 of 5 or 4 of 5 slices are lining up, but because they don't all align, there hasn't been a major problem. Everything within the company's operations look fine because there are not big problems, but there are several little problems occurring. These little problems may be considered minor because they have low consequences. But in reality, these low consequence items are essential pieces of the large problems that haven't happened yet. Improving the way an organization works the seemingly small, low consequence items lowers the risk of larger incidents. Concerns like, "Why are we even spending time on this issue, nothing happened," may happen. We're spending time on it because there's an inherent value of prevention.

This point of misaligning one slice isn't a unique insight, it's simply the nature of cause-and-effect. It is the same lesson for root cause analysis logic. All the causes must happen for the incident to occur. Changing or misaligning any one of the slices changes the issue. The lesson from the Swiss cheese model is a lesson in basic cause-and-effect.

Because the individual slices of Swiss cheese are always shown in a straight line, it leads people to believe that the breakdowns are linear. Because the model is linear people often conclude the incident is linear. Incidents, also known as a system problems, are nonlinear. The incident is nonlinear, but the cause-and-effect relationships between the different breakdowns (slices) can be linear or nonlinear. The Swiss cheese model provides no information about the cause-and-effect relationships within the incident. Conceptually, the lesson of misalignment within the Swiss Cheese model is valuable and it works well to introduce the idea. But the Swiss cheese model ignores important cause-and-effect relationships within the incident that are essential for revealing different options to lower risk. A problem analysis starts linearly, but it expands to be nonlinear in order to provide a complete explanation of what happened.

Rather than considering the slices of Swiss cheese to be inadequate defences, they can simply be thought of as causes. This provides a more thorough explanation because it includes what Reason called "conditions." He differentiated between causes and conditions in his explanation of the Swiss cheese. The distinction between types of factors that produce an issue is not necessary. The active and latent factors are causes. One isn't more causally related to an incident than the other. The latent failures occur along the same causal path as active, but farther upstream. For example, how the equipment was designed occurred before how it was operated. One is not more or less important than the other because both are required for the incident to occur. The valuable insights people share using the Swiss cheese model regarding breakdowns and alignment are simply lessons of cause-and-effect.

Cause-and-effect is not a problem-solving technique, it's a fundamental principle of the different techniques. The repeatability requirement of science is simply producing the same effects with the same causes regardless of who performs the experiment. There is no secret method to explaining how or why something occurred. Cause-and-effect is how things work on the farm, in the mechanic's garage, in the refinery, in the hospital and at an airline. People who know a particular discipline, field or hobby well can describe the detailed cause-and-effect relationships within the function. Those who don't understand a task or process can't explain its causes and effects. To them, it just happens.

Cause-and-effect may seem too simple for complex problems. But it only seems simple because it's fundamental. Cause-and-effect applies equally to small, large, simple and complex problems in safety, operations, equipment and human performance. It's works the same for explaining why something went badly as it does for explaining why something went well. It doesn't change from incident to incident. The case studies below show how the analysis of a problem can begin basically, then expand as necessary. Cause-and-effect thinking *is* the critical thinking and troubleshooting skills that so many organizations aspire to develop among their team members.

Each of the case studies in this paper show how a bias for a right answer can inadvertently confuse the way people explain a problem. But these miscommunications have no bearing on the incident. They don't change the incident in any way. If an investigation remains focused on identifying cause-and-effect relationships supported with evidence, a complete explanation of the incident will emerge. The cause-and-effect analyses in these examples begin as simple linear 3-to 5-Whys. They then expand into as much detail as needed to thoroughly explain the issue. By taking a first principles approach, people's biases will be flushed out to provide a clear, accurate and thorough explanation of the issue.

6 Texas City Refinery Explosion 2005

On March 23, 2005, a massive explosion at the Texas City, Texas, refinery 40 miles southeast of Houston resulted in a catastrophic disaster with 15 fatalities and more than 180 injuries. A simple summary of the incident is that too much liquid was added to a tower resulting in a release to atmosphere that ignited.

The incident can be explained many ways. Some of the different points of view of why the disaster happened are:

- The level instrument on the tower displayed the wrong level. The instrument indicated a lower level of 9 feet and dropping. The 165-feet-tall tower should not have been filled above 10 feet. The liquid level in the tower ultimately reached 158 feet without operations realizing it. (Instrument)

- The valve on the bottom of the tower was in the closed position. The standard operating procedure (SOP) for startup of that system states that the bottom valve should be 50% open. That procedure was not followed. (Procedure)

- The experience of the control room operator was inadequate. During startup of this isomerization unit, a qualified operator must be on the board in the control room. In cases where a less experienced operator is on the board, a senior technical representative must accompany them. Due to an unplanned family emergency, the senior technician badged out of the facility at 10:47 a.m. The less experienced operator on the board continued with the startup. (Experience)

- The blowdown drum, D-20, that the overfill of the tower flowed into was vented to atmosphere. Once the large volume of liquid left the raffinate tower, it overwhelmed the capacity of the blowdown drum, which was vented out a stack instead of a flare that could have handled the excess flow more effectively. (Design)

- There was a miscommunication on shift change that morning. One of the day supervisors missed the shift change meeting after the night crew had already filled the bottom of the tower to the required level. The plan discussed in that meeting was to not add any more liquid to the tower. (Miscommunication)

Each one of the explanations above is accurate. But none of them are individually the right answer. None of them are *the root cause* of the issue. But all are causes. The next question to ask for each one of these arguments is, "Why?"

The cause-and-effect relationships in the five bullets need to be diagrammed. The last word in each of the bullets shows how that information would typically be labeled. Organizations frequently use broad terms to categorize an incident. The intent is to provide a simple summary of what happened, but it can oversimplify and distort the issue. A thorough explanation requires an incident to be broken down into parts.

Figure 2 a simple cause-and-effect analysis for the Texas City refinery disaster. This 1-Why is accurate, but it is not a complete explanation of the incident. There are many cause-and-effect relationships that need to be added.

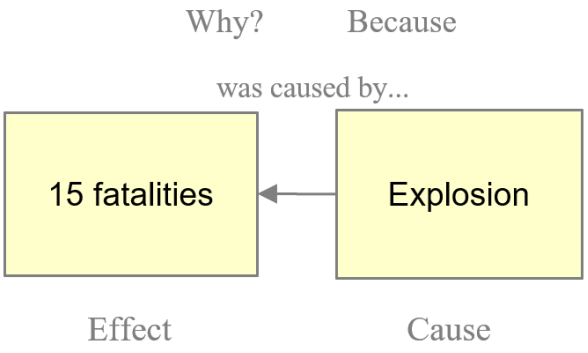

Figure 2 – A 1-Why analysis of the Texas City refinery explosion investigation.

Here's a 5-Why for the first bulleted item–instrument failure (Figure 2). This cause-and-effect analysis is linear.

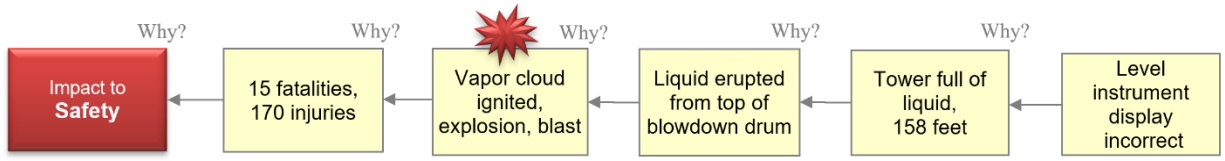

Figure 2 – An accurate, 5-Why to begin the Texas City refinery explosion investigation.

But the different perspectives listed in the bullet points allow for multiple 5-Whys. See the different 5-Whys in Figure 3 below.

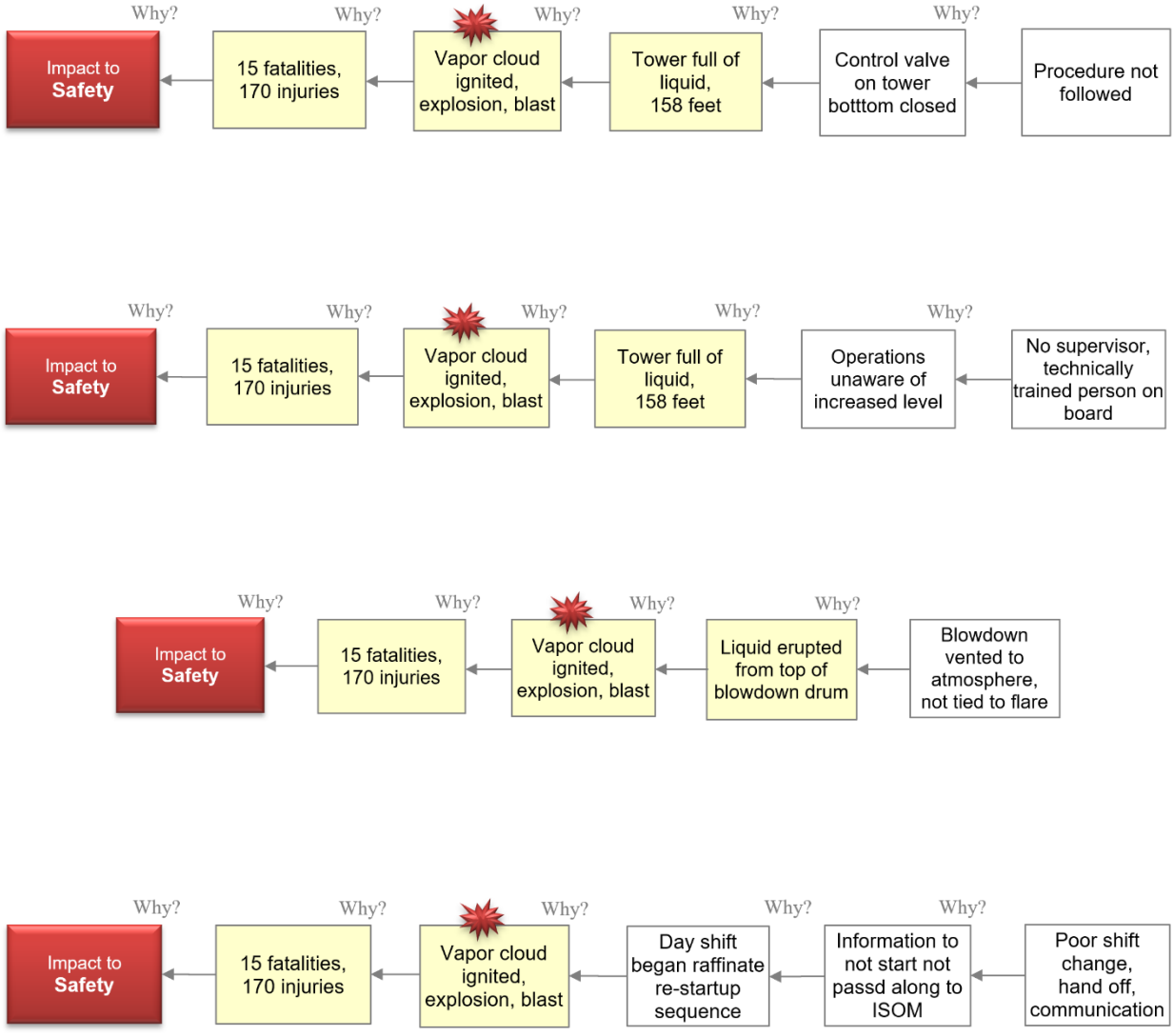

Figure 3 – Different 5-Whys. Each is accurate and can be used to start the investigation.

The 17-Why below (See Figure 4) shows how the five different linear analyses can combine into one more complete explanation with parallel cause-and-effect relationships. This is the nonlinear nature of incidents that the Swiss cheese model doesn't reflect.

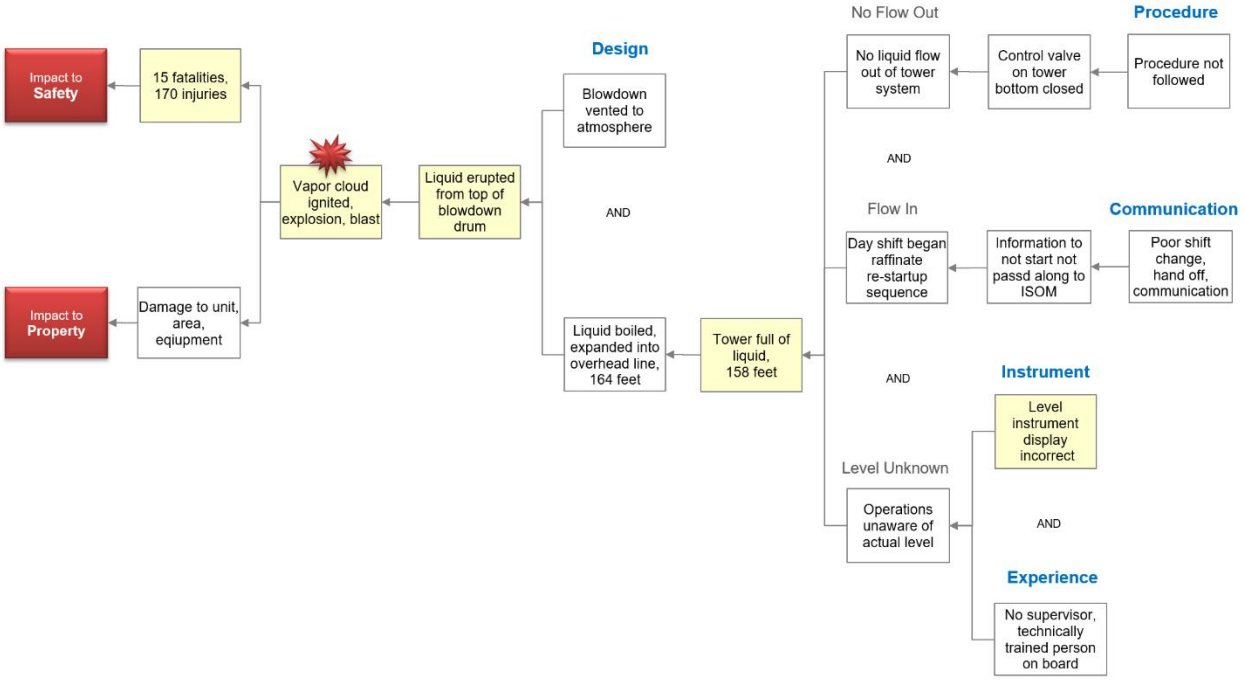

Figure 4 – The 17-Why shows how multiple 5-Whys can combine into one analysis.

All the causes in this analysis had to occur for this incident to happen. This is analogous to the multi-layered breakdowns of the Swiss cheese model that all must align for the negative outcome to occur. Each causal path in the diagram reveals an independent, linear chain of events that results in the loss of life and impact to property. Reviewing a single path can make it seem as though that path alone caused the incident. People usually believe their particular linear explanation is the right one. This is the flaw in linear, right-answer, root cause thinking. All the different paths are the root of this incident.

The Texas City disaster is shown below as a 125-Why (included in Figure 5 to show how the structure develops). An incident contains all its causes. The investigation can reveal a 1-Why, 5-Why, 17-Why or more Whys. The level of detail depends on how much the organization wants to know about the incident. Executive summaries show one level of an investigation, but they can exclude important details. The intent of root cause analysis is to dig into those details to an appropriate level to find the best solutions.

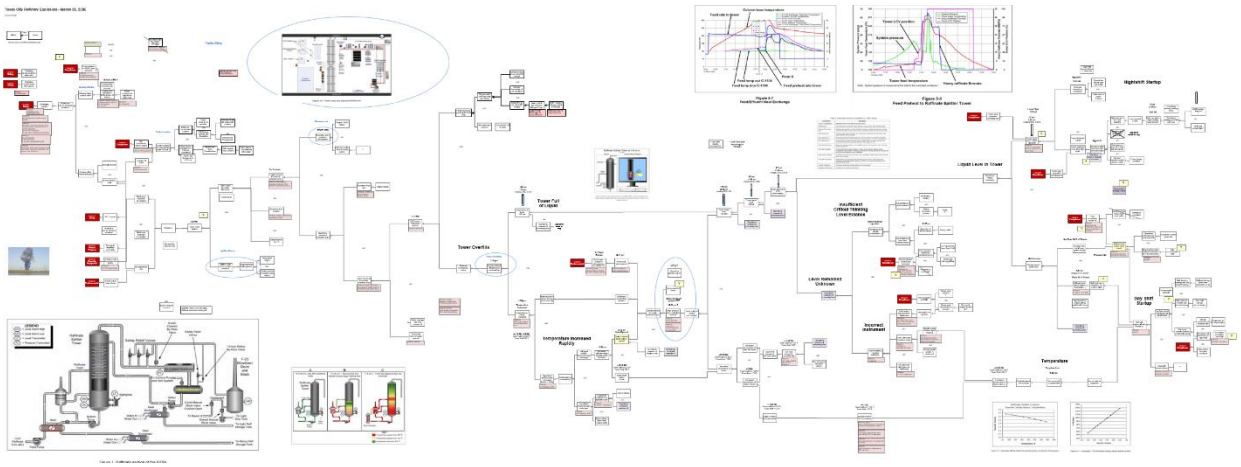

Figure 5 – The structure of the expanded 125-Why Texas City refinery explosion investigation.

Making a cause-and-effect diagram improves the way people communicate the details of what they know. The right-answer bias of conventional root cause analysis becomes difficult to support with this diagram. Verbally, root cause logic seems to make sense, but visually, its flawed logic is easier to see. Controlling (or misaligning) any one of the causes reduces the risk of a similar incident occurring. By controlling multiple causes, the risk can be reduced significantly. This basic-to-detailed approach of cause-and-effect analysis can be applied to any issue to improve communication and reduce risk.