Root Cause Analysis Tools A Complete Guide

INFRASPEAK

Table of Contents

What Is Root Cause Analysis?

The expression “root cause analysis” is an umbrella for different methods that allow us to analyse failures and fix them, or at least troubleshoot.

This means that a root cause analysis isn’t one particular method but rather a set of tools that examines errors in security, manufacturing, internal processes, assets or systems.

What are the main Root Cause Analysis Tools?

There are dozens of tools to perform a root cause analysis. Each has its own advantages, disadvantages, and applications. It’s not the first time we discuss how significant analysis tools are for effective maintenance, so in this ebook we’ll dive into five tools that are particularly valuable in this field:

- 5 Whys Analysis
- Fault Tree Analysis
- Ishikawa Diagram
- FMEA
- Data Analysis

Needless to say, none of them are mutually exclusive. You can employ different tools according to criticality, and occasionally even use more than one at the same time.

The 5 Whys Analysis

The Five Whys (also styled 5 Whys) is one of the many methods to find the root cause of a failure. It is an interrogative technique, in which you explore cause-effect by repeatedly asking "why?" until you find the root cause. Anecdotal evidence suggests that 5 times is enough to find the answer you're looking for, hence the name "5 Whys".

The big advantage of the "5 Whys" technique is recognising that there is a series of events that precede failure. More often than not, failure will arise from a chain of cause-effect reactions, or a domino effect, and not from the single event that immediately precedes it.

The 5 Whys analysis is a simple and quick problem-solving tool to uncover the root cause, and it applies to several contexts. In maintenance, the goal of any root cause analysis is fixing the original error.

Plus, it helps managers implement new strategies to avoid similar failures, and establish internal processes that minimise the probability of failures at any point.

Who developed the 5 Whys method?

Whenever we're looking at root cause analysis tools, it's always interesting to understand how they came about. The 5 Whys exercise was developed by Sakichi Toyoda, Toyota's founder. According to Toyoda's principles, machines "stop when there is a problem".

Asking "why" 5 times helps to find out the origin of that problem – and thus the solution becomes clear. The concept was integrated into Toyota's production process during the company's expansion, and it is still a part of its lean methodology to this day.

How does the 5 Whys technique work?

Imagine that you have a fever. Surely you'll take an antipyretic to relieve your symptoms, but that's not a cure. To cure yourself, you need to ask why you have a fever. "Why do I have a fever?" ⇢ viral infection ⇢ "Why do I have an infection?" ⇢ I contracted the influenza A virus ⇢ "Why did I contract a virus?" ⇢ I was in close contact with an infected person.

See, we did not even need the 5 questions to figure out what happened!

From then on, it's easy to figure out that not only do you need an antiviral, but the way to avoid reinfection is to keep your social distance. Of course, this is a rather simplistic example – we all know we get sick because we were close to an infected person – but it wouldn't be so obvious if someone hadn't already questioned "why?".

Please note that we can't always follow a linear train of thought to figure out the root cause. In some cases, there are several potential root causes, which force you to explore different answers to each "why".

Here’s an example where there are multiple potential answers: The car won’t start. → Why? → The car battery is dead. → Why has the car battery died? → The headlights stayed on overnight. → Why did they stay on? → There was no alarm sound or warning light on the control panel.

Here’s when the diagram breaks down into two possibilities:

→ Why wasn’t there an alarm? → The sensor failed. → Why? → The sensor was never replaced.
→ Why wasn’t there any warning light on the panel? → There was an electrical problem. → Why? → The fuses are damaged.

When the 5 Whys analysis branches out into many different possibilities, it’s almost always a symptom of insufficient quality control and failure detection methods.

Never forget that you’re analysing the process, not the people, so never accept “human error” as the root cause. Surely, there is a quality control process that wasn’t performed, even if it is a simple checklist. In more complex analysis, organise all the answers in an Ishikawa diagram (also known as fishbone diagram). Combining both methods will help you visualise better all the hypotheses.

How do you run a 5 whys analysis?

1. Bring together a team.
Root causes analysis should not be performed by a single person. Bring together a team with a good know-how of the asset – but who is willing to look at things with fresh eyes and explore all the answers.

2. Define the problem.
It's preferable if everyone in the team can testify and see the failure for themselves. Every single team member should agree on a description. For example, they must agree that the most appropriate definition for the failure is "the car won't start" (rather than "the ignition won't start") because that would trigger different questions going forward.

3. Start asking "why"?
Now that everyone is "on the same page", it's time to start asking "why?". The answers must match the facts, and not suppositions about what happened. Not all team members will likely offer the same answers, so they must debate until the team reaches a consensus.

4. Learn to stop.
Be wary of stopping too early – try to go through 5 rounds of "why?" questions – but you also need to learn when to stop. When answers are not useful to understand failure anymore, or when they don't shed light on possible solutions, it's time to stop. If you cannot find a root cause, try another root analysis tool, like the fault-tree analysis (FTA) or Failure Modes and Effects Analysis (FMEA), which you can learn about later in this ebook.

5. Adapt your maintenance plan.
After finishing the analysis, the team should suggest measures to avoid similar failures. During this step, it is useful to review all the answers to establish new quality control procedures.

When should you use the 5 Whys analysis?

In maintenance, the 5 Whys analysis may be used for root cause analysis, troubleshooting or problem-solving. It tends to be very efficient, and quick, to discover the root cause of failures with low to moderate criticality. Besides, it has great applicability as a quality improvement tool, within a lean methodology.

Unlike other tools, the 5 Whys analysis cannot be used at a conceptual stage. Its use is limited to finding the cause of problems that already occurred, or analysing failures that indeed compromise functionality. On the bright side, you won't "waste time" with hypothetical questions.

What are the limitations of the 5 Whys method?

The main limitation of the 5 Whys method is self-evident: since it tends to follow linear logic, it can only find a single root cause. It's not practical when there are several lines of investigation or when there might be more than one root cause.

Besides, since it only assesses events that already occurred, and it's merely qualitative, it's not suitable for a probabilistic risk assessment. It depends on your team's know-how to work out the root cause. If there was an unexpected failure mode, you may never consider that answer – and never reach a conclusion.

Your team might have a biased view, which might compromise the results of the analysis. The team might ask biased questions or offer biased answers that confirm their suspicions or theories. It's not always easy to set "symptoms" and "causes" apart or to know when to stop. Occasionally, you might stop before you have time to execute a deep and thorough analysis.

Fault Tree Analysis (FTA)

A Fault Tree Analysis (FTA) is a systematic approach to problem-solving, troubleshooting and identifying a failure's root cause using a diagram. A fault tree analysis can either be used to explore a single failure or systematically examine a group of components, which makes it a versatile tool for a root cause analysis.

What is the purpose of a fault tree analysis?

- to diagnose the root cause of a failure
- to understand how the system can break down
- to determine inherent risks
- to identify measures to minimise risks
- to estimate the frequency of safety breaches

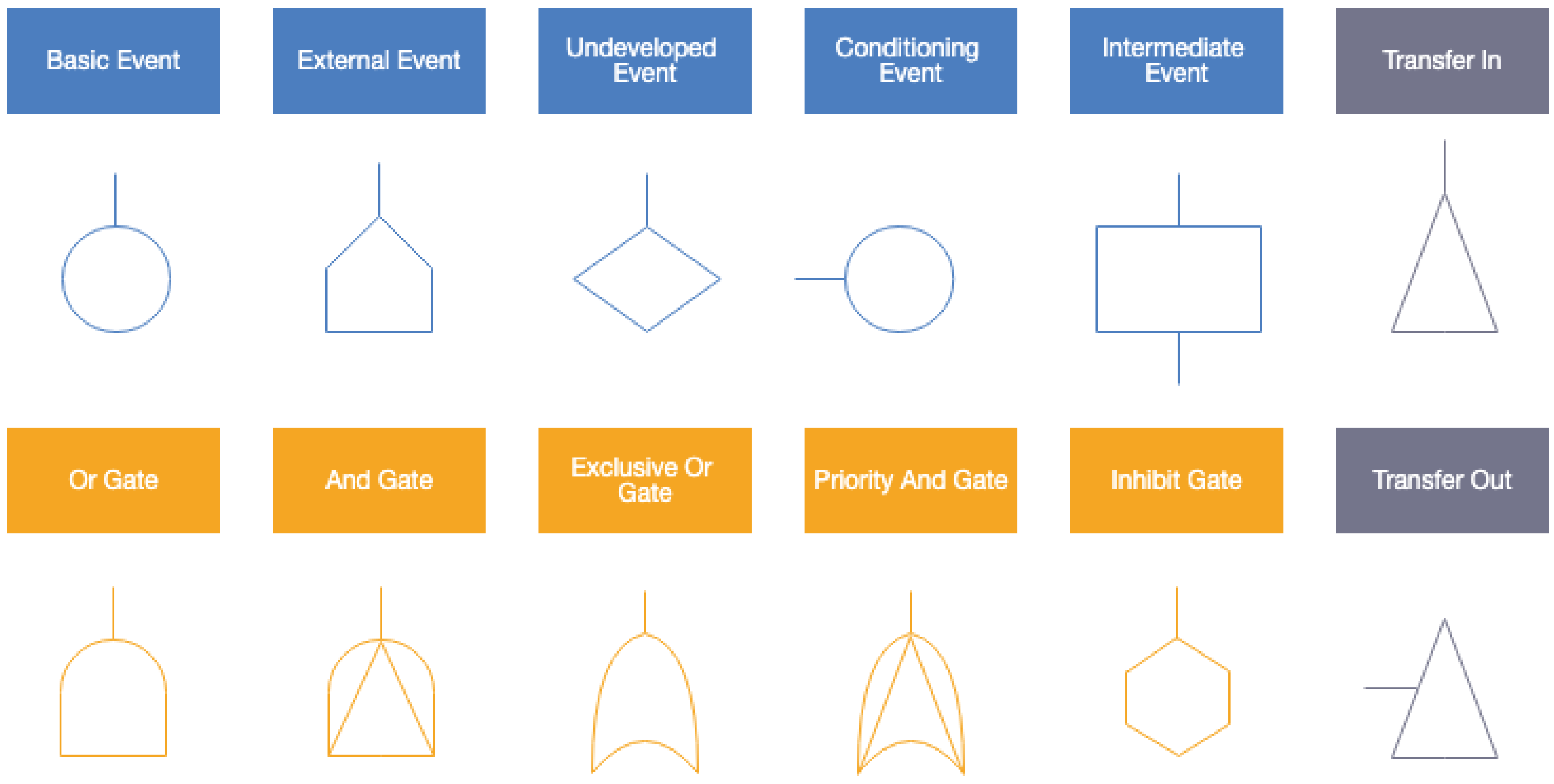
What are the advantages of performing a fault tree analysis?

- improve compliance with safety regulations
- map the correlation between failures and subsystems
- establish priorities for the system as a whole
- implement changes in product or system design to minimize risks
- carry out a probabilistic risk assessment (PRA)

How to create a fault tree analysis diagram

Your starting point for a fault tree analysis diagram is the failure itself. From that top event onwards, the diagram should grow following a logical sequence – until you determine root cause.

The fault-tree analysis diagram applies boolean logic. It employs symbols to represent each event that might have caused or contributed to the breakdown, including external and conditioning events. The gate symbols ("and", "or") that connect them establish the relationship between input and output events. Here's a list of all the symbols in an FTA:



Source: Caccoo.com

You can also structure the diagram using a reliability software, in which gate symbols equal 1 or 0. Most software will integrate the information with statistical probabilities, which turns FTA into a quantitative method.

Because of these characteristics, an FTA is a common method for safety assessments and probabilistic risk assessments (PRAs). A PRA is a systematic approach to risk and reliability analysis, which estimates risk, the likelihood of failure, and the magnitude of the consequences.

When to use FTA in maintenance

We've already established that an FTA can be used for a PRA, which makes it appropriate for high hazard industries, including aerospace manufacturing, nuclear, chemical, petrochemical, and pharmaceutical industries. In software engineering, FTA is a cause-elimination technique for debugging.

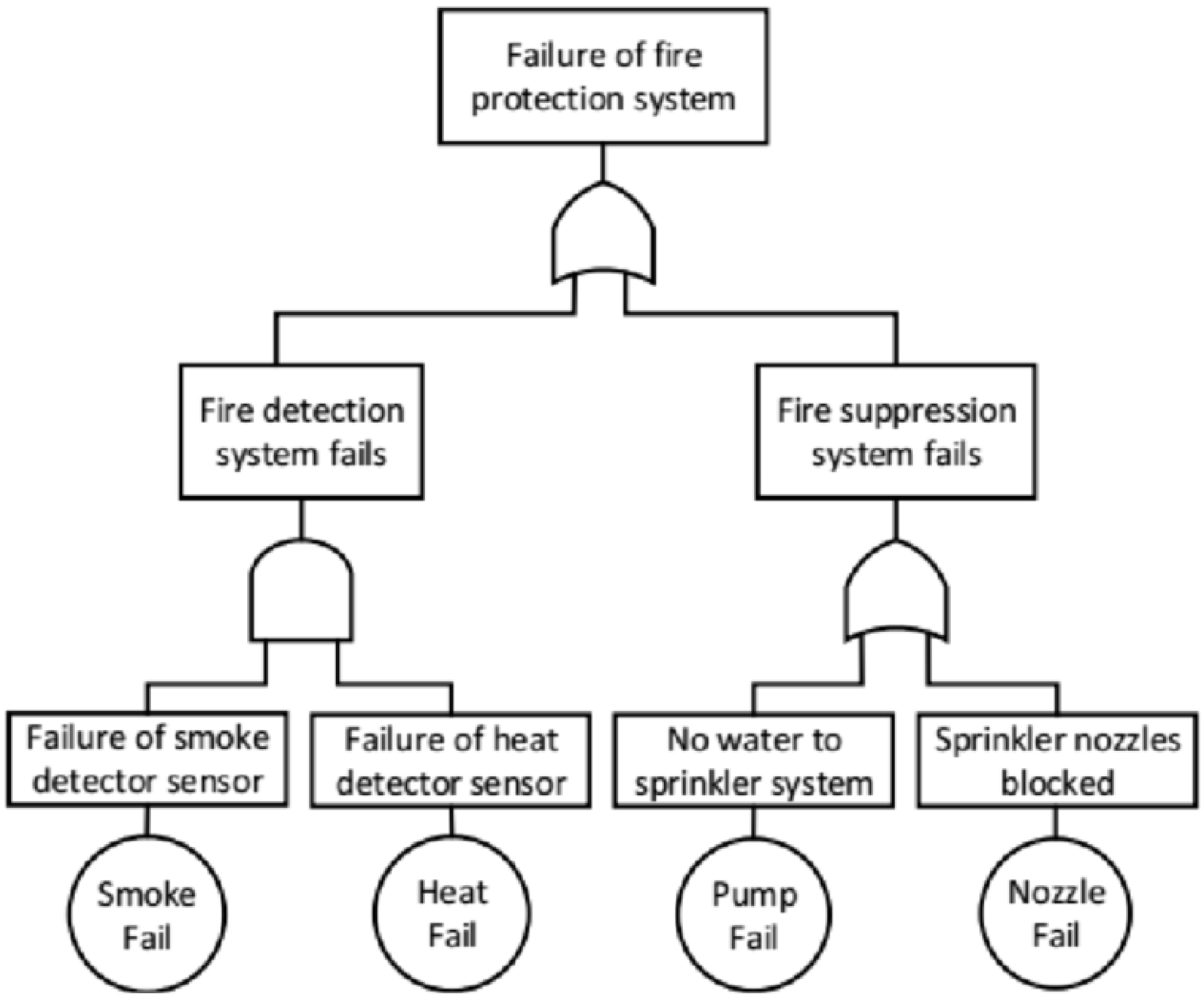
As a curiosity, NASA preferred an FMEA analysis for the Apollo missions – which took the Man to the Moon for the first time – because the probability of returning safely to Earth was too low according to an FTA. After the Space Shuttle Challenger disaster in 1986, which disintegrated only 73 seconds after liftoff, NASA began using a combination of FMEA and FTA analysis.

Now, flip the page and let's get straight to the point...

How do you use FTA in maintenance?

When there's an unexpected breakdown or a failure that almost leads to one, it's good policy to perform a fault tree analysis to get to the root cause. Otherwise, a failure will happen again.

For example, if the fire protection system fails, there are two possible failure modes: either (hypothesis A) a failure occurred in the fire detection system or (hypothesis B) the fire suppression system failed.



Original Source

If the fire detection system failed, it means that the fire detectors failed and so did the heat detectors (both mechanisms must fail). On the other hand, if it was the fire suppression system, it means that there was not enough water in the system or that sprinklers were blocked (any of the two would be enough to cause failure).

If we conclude that the problem was not enough water, then we've found our root cause. Your fault tree analysis may stop here because you've found the "base event" (marked with a circle).

However, as a maintenance manager, you might wonder why the water pump failed. For example, whether it was lack of maintenance, wear out or insufficient capacity for the building's needs. You can either continue with the diagram or turn to an alternative method, like the 5 Why's analysis.

Investigating the root cause is, ultimately, what allows you to make the right changes in the maintenance plan, implement new safety rules, and assess risk. Consequently, both the asset's availability and reliability increase over time. And this is how you can use fault tree analysis in maintenance.

Although it is not used systematically outside the industries we mentioned, the fault tree analysis is a very useful tool to determine root cause(s) and improve any company's maintenance strategy. You can use it almost in any context, from simpler failures to more complex systems. Plus, it showcases how several events might contribute to the outcome.

What are the limitations of fault tree analyses?

There is not a single foolproof root cause analysis. FTA too has its limitations:

- It's a unidimensional model. FTA doesn't take into account time or the asset's useful life, which may be a problem when you're in the product development stage.

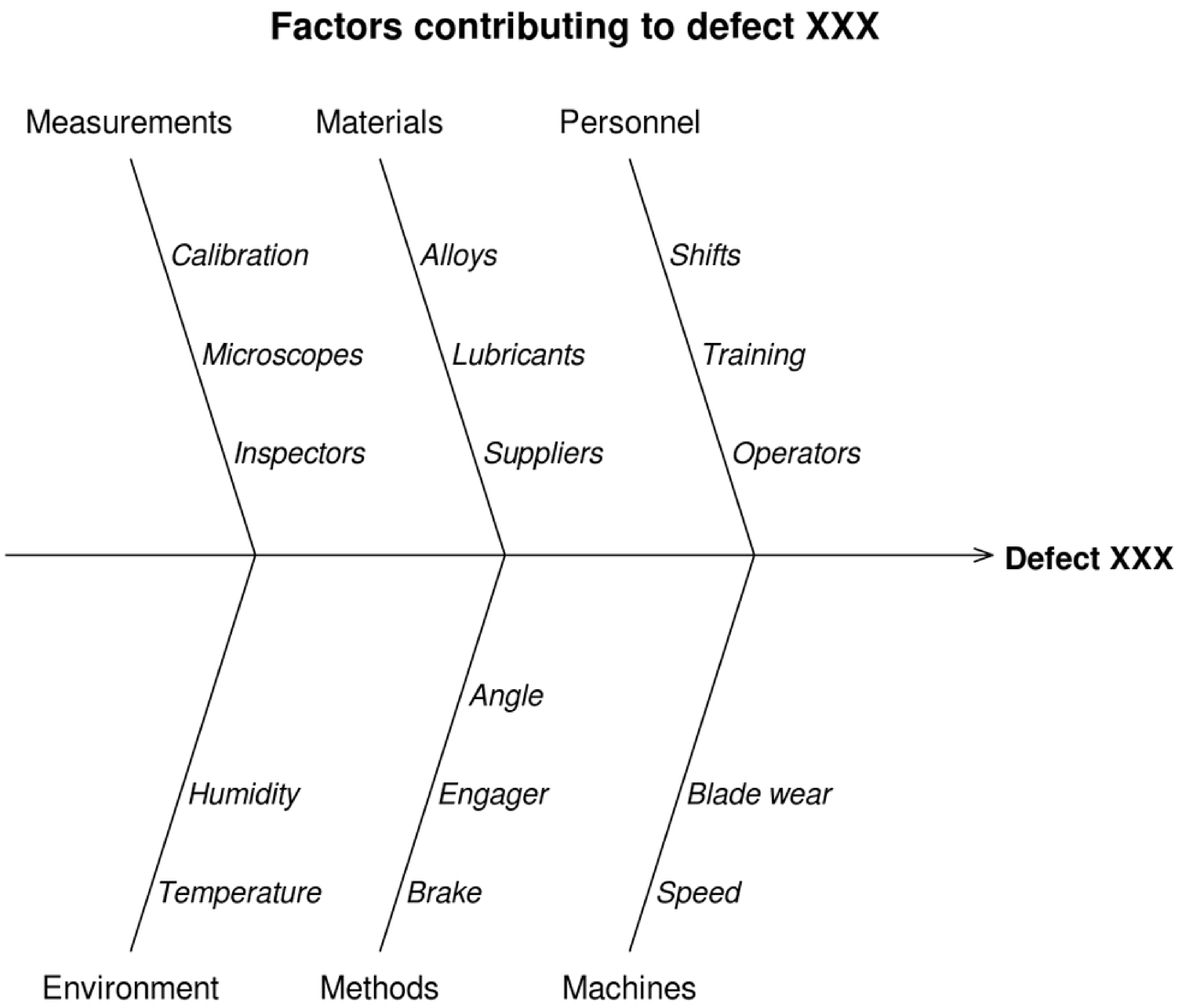
- FTA is a binary system. Each hypothesis is either validated or not, making it roo rigid for assets with conditional failures (failures that only happen under certain conditions, i.e. low temperatures) or partial failures.

- It is not always possible to determine the probability of failure, which invalidates FTA as a quantitative method.

Ishikawa Diagram

The Ishikawa diagram (also known as the “fishbone diagram”, for its shape) consists of organising causes and effects in a diagram, split into 6 categories, until we find the root cause. The categories are as follows:

- Measurements
- Materials
- Personnel
- Environment
- Methods
- Machines.



Original Source

This root cause analysis tool highlights the relationship between the company's different departments. As a result, it's suitable for solving failures that don't have a single root cause. Suppose a factory produces a defective lot after manufacturing thousands in good condition. What could have happened? Was there an issue with the raw materials? Human error during production? Why wasn't it discarded after quality control? Is there more than one root cause to explain it?

The Ishikawa diagram has applications in maintenance but also in marketing and management, making it extremely versatile. The "fishbone" will improve internal processes, promote team spirit and expose nonconformities. On the other hand, it can "diffuse" your attention or complicate the root cause analysis unnecessarily.

Next up, is Failure Modes and Effects Analysis. Keep reading!

Failure Modes and Effects Analysis

For a FMEA (the acronym for Failure Modes and Effects Analysis), we will define a “failure” as a loss of functionality, while “failure mode” is how the failure itself happens. It is one of the most common tools for root cause analysis due to its versatility.

FMEA is sometimes known as DFMEA (which stands for Design Failure Mode and Effects Analysis) or PFMEA (which means Processes Failure Mode and Effects Analysis). These are used to analyse potential failures in product design or in the processes of a business unit, respectively.

Here’s a simple example to understand the difference between a failure and a failure mode — if an automatic payment terminal stops printing paper receipts (failure), it might be because the paper roll is not set properly (failure mode #1) or because its compartment is not closed (failure mode #2).

Failure modes are our way to the root cause. However, FMEA goes even further. After signaling failure modes (and, by extension, potential root causes), it then evaluates the effect and impact of each failure.

To understand what this means, we’ll use a more complex example. Imagine there’s a failure because the fan was operating with too many vibrations (failure mode). What happens in the aftermath? The piece of equipment stops momentarily (failure effect), which leads to production losses.

Different failure modes may lead to different effects, with various outcomes for the company. That’s why FMEA is often combined with a criticality analysis. When both are performed at the same time, it’s known as FMECA (Failure Modes, Effects and Criticality Analysis).

What are the main purposes of FMEA?

And now, a little bit of history. The United States army developed FMEA in the 50s. Shortly after, the aviation industry and NASA adopted it, and NASA went on to use it for the Apollo missions, the Viking program, and the interstellar Voyager missions. FMEA is also prevalent in the automotive and oil industries.

As mentioned, FMEA is suitable for several contexts. It can analyse function, processes (PFMEA, focused on manufacturing and assembly processes) or project design (DFMEA). It's advisable to carry out an FMEA every time a new product is released or there are any significant changes – new manufacturing processes or regulations, for example – and when your client's feedback denounces a recurring problem.

What are the advantages and benefits of FMEA?

The main goal of an FMEA is to improve the asset's output, reliability and safety. However, there are many other benefits of going through this process, such as:

- Developing a work method that will, in all likelihood, be well-succeeded, safe and reliable.
- Assessing failure modes and their impact, so that you can prioritise them according to criticality and likelihood (especially if you carry out an FMECA). Setting priorities improves your maintenance plan.
- Identifying failure points and verifying system integrity – whose security should not be compromised – even if you need to introduce new safety measures.
- Trying out changes and adjustments in product design (for example, testing if the probability of failure has decreased).
- Faster troubleshooting, given that failure modes and their respective causes are all well-described.
- According to the failure modes, defining criteria for try-outs and inspections that should be included in the preventive maintenance plan.

What are the disadvantages and limitations of FMEAs?

On the other hand, FMEAs also have some weaknesses:

- FMEA is not suitable for systems in which several failures may occur at once, since it doesn't take into account the correlation between them.
- As we'll see below, severity, probability and detection have the same impact on risk assessment, which is a simplified approach.
- FMEAs rely on your team's expertise to list failure modes, making it a time-consuming process that requires a lot of professionals.
- An FMEA needs constant updating, because your knowledge about an asset increases with experience, time and use; you'll likely discover new failure modes your team hadn't considered from the get-go.
- In case you fail to consider a failure mode, you'll underestimate the risk associated with the asset. On the other hand, going into painstaking detail will take your attention away from critical problems and is a waste of resources.

How to perform a Failure Modes and Effects Analysis

The biggest challenge in a Failure Modes and Effects Analysis is being thorough regarding failure modes, its causes, and impacts. Usually, you'll organise the information on a table divided into 7 columns, one for each of the steps below.

1. Define failure modes
The first step of an FMEA analysis is defining all possible failure modes for each component. To achieve this, consider previous experiences with similar assets.

FMEA and FMECA are regularly used in high-risk industries, in which safety is the top priority. Yet, for the purposes of this article, we'll use a much more mundane example: a poorly prepared dish at a restaurant.

We're dealing with an unfortunately common failure mode, finding a hair on the plate. Our inner Michelin inspector can also think of at least 3 other failure modes – finding an insect in the food, not enough salt, and food poisoning. Obviously, a real restaurateur would think of many more. It's the greatest challenge in FMEA: if you forget failure modes, you are already compromising risk assessment.

2. Failure effect

The second step to make an FMEA is describing clearly the failure's effect because this will determine its severity. Try to be as specific as possible with the description to determine severity ranking on step 3. What's the effect of our failure mode? Well, in the short term, sending it back to the kitchen. In the long term, not coming back.

3. Severity

The severity rating is a scale from 1 and 10, according to the impact of each failure:

- 1 minor risk: faults are almost imperceptible
- 2-3 low risk: failures are perceptible, but cause only minor annoyance
- 4-6 moderate risk: the consequences of failures are noticeable (even for customers) and affect asset performance
- 7-8 high risk: the operation is totally compromised, which disrupts schedules
- 9-10 very high/critical risk: the asset is completely compromised and there are high security risks.

We don't know about you, but for us, the asset "dish with human hair" is completely compromised, with great safety and hygiene risks. We give it a 9 (we're saving that 10 for salmonella).

4. Potential root cause

The same failure mode can have several root causes. For example, if a lift stops between floors, it might be a wrong configuration or an electrical problem. If you list all the potential root causes beforehand, it's easier to test, troubleshoot, and correct failures when they happen.

In our example, the root cause is evident: the kitchen personnel are not wearing hair caps. If we had found an insect in the salad, for example, there would be more potential culprits: improper storage; failure to wash properly; infestations, and so forth.

5. Occurrence

Occurrence represents the expected frequency of the failure, again based on asset history or that of a similar piece of equipment. Usually, occurrence is a rating from 1 to 10, in which 1 is "extremely unlikely" and 10 means "extremely likely" or "inevitable".

Based on our personal experiences, we estimate the frequency of our failure mode to be a 2.

6. Detection

In this column, you should propose measures to detect potential failures. The detection rating – or the ability to detect the failure – consists of a scale from 1 to 10, in which 1 stands for "extremely likely" and 10 "extremely unlikely".

In our case, the proposed measure to avoid the specific failure mode would be to visually inspect the dish before serving it to customers. But visual inspections are somewhat unreliable – which is why we only noticed it too late. So, not wanting to delve further into these bad experiences before lunch, we estimate a detection ranking of 4, "somewhat likely".

7. Calculate Risk Priority Level (RPN)

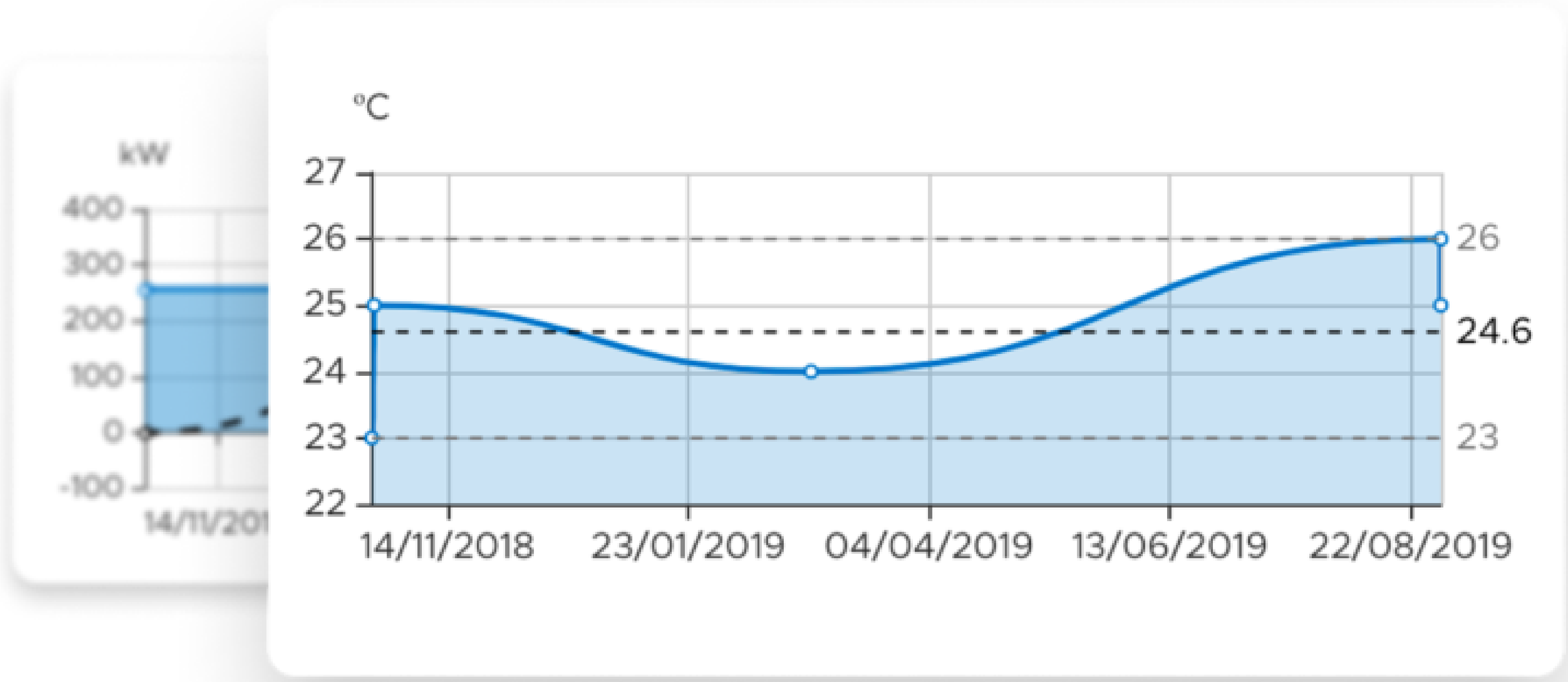
Finally, we can calculate the risk priority. The RPN equals severity (which we calculated in step 3) x occurrence (step 5) x detection (step 6). The bigger the risk level, the bigger the need to search for improvements.

The risk level of our dish, according to the scores we gave it, would be 9*2*4 = 72. If we had given a 10 to that salmonella, with the same frequency and likelihood of detection, its risk level would be 80 – which means it would have greater priority, which sounds about right!

Data Analysis

Lastly, but not any less important or effective, there's data analysis. As the name suggests, it consists of collecting, modeling and processing information in a way that allows managers to obtain valuable insights about what is underperforming. This task becomes simpler if you're using a CMMS or an Intelligent Maintenance Management Platform (IMMP) to streamline and manage all of the data: assets, maintenance plan and executions.

Inserting the data "religiously" into the software helps calculate indicators such as the compliance rate, planned maintenance percentage, and scheduled maintenance in a heartbeat. It also gives you a global perspective about the history of each asset and, after a failure, it may help pinpoint the exact moment when maintenance failed.



Source: Infraspeak

In a way, all of the methods we've listed depend on data analysis. So, it can (and should) be a part of any root cause analysis tool of your choosing.

Do you want to know how Infraspeak's data analysis features can help you with root cause analysis?

Learn all about our Intelligent Maintenance Management Platform today.

Schedule a Demo Now

INFRASPEAK