Learning from Engineering Disasters

An Online Continuing Education Course for Engineers

Course Number: F-1003

Credit: 1 Hour / 1 PDH / 1 CPD

Learning from Engineering Disasters

Jared W. Jensen, P.E.

Things break. This is the simple fact of engineering and the reason that failure analysis has been a critical skill for every engineer in every discipline since the first humans began designing simple tools to make the lives of their tribe better. Critical thinking skills are the cornerstone of everything an engineer does, and the ability to learn from failure sets the successful engineer apart from the rabble of tinkerers.

Respecting this need to learn from failure, Admiral Hyman G. Rickover declared: "Success teaches us nothing; only failure teaches."[1] Success can breed arrogance and a reliance on the individual rather than proven processes and methods. This in turn breeds vulnerability which can lead to severe failures in the unforgiving engineering arts. To avoid this, prudent engineers cultivate a sense of humility and respect for natural forces through regular study of failure.

This course will introduce you to a simple process that may be used to analyze any engineering failure from simple missteps to major disasters. Large or small, complex or straightforward, every engineering failure can teach a lesson to engineers of all kinds. An organized approach will enable quick learning from case studies and current events equally so that the mistakes of the past are not repeated.

The learning objectives for this course are as follows:

1. Identify major subsets of failure types
2. Introduction to root cause analysis
3. Learn a formal approach to identify lessons learned from engineering failures outside the learner's core expertise
4. Introduce nomenclature and methodology through basic case studies

Nomenclature will be introduced first. We will then define the major types of engineering failures, the most likely points at which they develop during the engineering process, and the major sources of each. Lastly, a process to analyze engineering failures and disasters with a goal to find broad engineering lessons is presented. At the end of this last section will be a short quiz.

Though examples of engineering disasters are presented throughout, this course is presented at a survey level. For those who are interested in delving deeper into this subject, additional courses are available on this website that will build on this foundation. Each will apply the techniques

[1] Address to the US Naval Postgraduate School, 1954.

taught here to major engineering disasters and highlights the multi-discipline lessons that may be learned from notable engineering disasters across several disciplines.

Disaster examples detailed in this course are drawn from many different industries, geographic regions, and time periods to highlight an important point that should be your first lesson: Any engineer can learn something from every major engineering disaster in history regardless of the particular circumstances or discipline. This basic fact rests in the assertion that engineers of all disciplines are masters of the physical world and rely just as much on a shared critical thought process as their particular skill specialty to understand the world and solve the problems they face.

Nomenclature

The following terms will be used throughout this course and other lessons dealing with specific case studies. In order to avoid confusion, terms used frequently are defined here. Refer to this section regularly during this course.

Critical Flaw

A critical flaw is the single fundamental physical deficiency in a sub-system driving the overall engineered system to fail catastrophically. Catastrophic failures resulting from critical flaws can be pinpointed to an existing physical defect that was present before the onset of the event resulting in the failure. This marks a critical flaw as different from failure modes that develop during the event which may be tied to improper operation, exceeding design limits, or damage caused at the onset of an event that resulted rapidly in catastrophic failure. Inherent material flaws, controlled manufacturing variability, and similar defects that are within the design tolerance of the system are not critical flaws.

When multiple physical components fail in parallel to cause a larger overall accident, multiple critical flaws may be present. This occurrence is rare; to be considered critical flaws, the multiple physical failures must be pre-existing, fundamental to the accident's final severity, and completely independent of each other. The key point in determining whether two critical flaws are present is that both critical flaws must exist *before* the onset of the accident. They may only become apparent as the accident progresses, but their source must be outside the conditions of the accident. Be sure to understand if this is the case or if one critical flaw drove two or more portions of the system to failure under the stress created by the original failed component.

Sidebar – Nature vs. Man

Natural disasters typically cause more widespread and severe effects than engineering disasters due to the awesome power of nature. The US Gulf Coast presents a stark example. The Katrina Hurricane in 2005 caused widespread damage to the entire US Gulf Coast but particularly in Louisiana & Mississippi where it caused 1,833 deaths, displaced over 1 million people and resulted in about $170 billion in damages. By comparison, an engineering disaster—the Macondo blowout—five years later resulted in 11 deaths and about $65 billion in direct damages—mostly due to the cost of clean-up and lost economic output. Though it was the worst oil spill ever in the petroleum industry, the Macondo blowout had a measurably smaller impact when compared to the Katrina hurricane.

Disaster

This is an engineering failure that has broad consequences either geographically or politically. With very few exceptions, more than just the end users of the failed engineered system are directly affected by the consequences of a disaster. Most disasters yield significant learning points for the applicable industry. These result in modified engineering processes, the emergence of new technology, revised or completely new regulations, and shifts in public opinion. These major accidents are the most severe engineering failures and should be used as important learning points for engineers of all disciplines.

Engineered System

The engineered system is the product, assembly, structure, or combination of man-made components forming the complete process or product under examination. This may be something as simple as a single manufactured product like a power drill or something as complex as an extra-planetary probe and its launch system. At the onset of any investigation into an engineering disaster, it is important to maintain a broad view of what to include in the engineered system until evidence proves otherwise. By focusing too narrowly on a failure early in the investigation, important lessons may be lost and the true root cause may be obscured.

Failure

In the context of this lesson, a failure occurs when an engineered system entirely ceases to perform its primary function or is so severely impaired that it must be shut down. For the purposes of this lesson, engineered systems that function at less than ideal performance levels are not necessarily failures unless continued operation exacerbates damage to the point of ultimate failure or rapidly results in personnel harm.

Initiating Event

Each failure starts somehow. The initiating event is the first link in the chain of events that leads to system failure. These events are typically simple in themselves—like a bird strike during aircraft takeoff or a tree falling across a power line. Whatever the case, the initiating event is the decision, force, or factor that begins the accident. Although the initiating event may not be

something that can be prevented, it is important in any analysis to identify and learn from the circumstances that started the engineering disaster under consideration.

Load

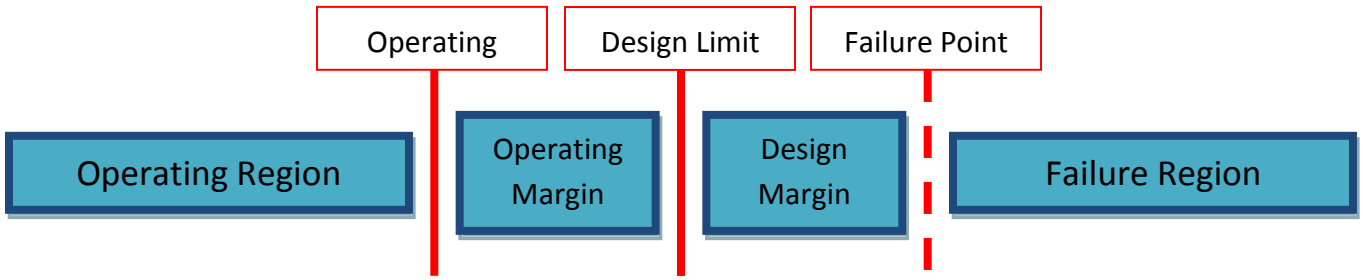
Engineered systems are designed to accomplish specific functions. The output is often designed to support a particular resistance or force; this is specified as the load. For example, a heat exchanger may be designed and sized to carry a specific thermal load to maintain a target system at a specific temperature. In this case, the load is specified by a quantity of thermal power. Common types of loads include pressure, electrical, structural, tensile, and thermal.

Margin

Margin is the available capacity between the intended operating point of the engineered system and the actual failure point of the system and its components. Engineered systems all have margin, but the type and amount of margin varies based on the design approach used and the regulatory environment applicable to the engineered system. Most systems will have multiple sources of overlapping margin, but most of these may be grouped into two subsets.

Design margin is typically built into a system either by intentionally de-rating the materials used in manufacture or designing for higher loads than will actually be encountered during operation. Often, this type of margin will be used to prevent failure in the regions where analysis uncertainty cannot clearly define the ultimate point of failure for a material property, complex geometry, or physical phenomenon that is difficult to model.

Operational margin is added by reducing the load imposed during operation of the engineered system to a lower point than that allowed by design. Where design margin avoids failure near performance limits that are difficult to define due to uncertainty, operational limits provide a cushion between normal operating modes and design capacity. This buffer allows the engineered system to tolerate variability during operation such as vibration, momentary overload, shock loading, rough handling, and a host of other problems. Operational margin is also the easiest source of emergency capacity as it represents the difference between normal operation limits and those limits that have already been included in the original design process.

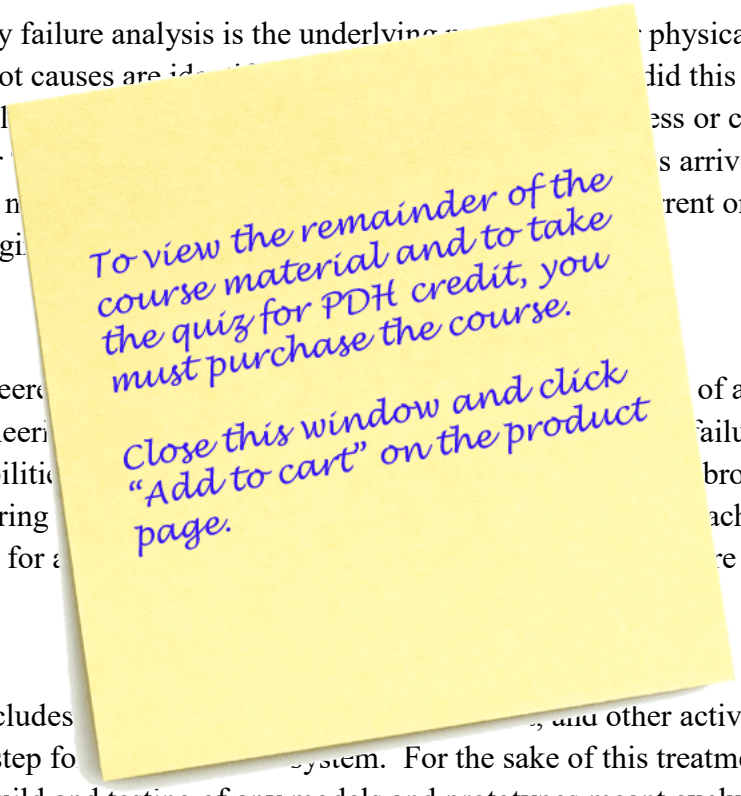


Process Flaw

Unlike a critical flaw, a process flaw results from the engineering and operational decisions made in developing, producing, and using the engineered system. This is not a physical defect but rather a defect in process, judgment, or knowledge of the engineered system or the environment in which it is used. Process flaws will sometimes lead to physical defects, but the underlying cause of the problem, the true flaw, is the process. Examples of process flaws include poor design review procedures, absence of clear operating instruction, and quality control practices that fail to detect manufactured defects.

Root Cause

The root cause in any failure analysis is the underlying [illegible] physical defect that led to eventual failure. Root causes are id[illegible] did this occur" is a statement of physical [illegible]ess or condition, a personal decision, or [illegible]s arrived at the "root" of a failure chain when n[illegible]rent one can be uncovered. Most engi[illegible]



Most times an engineere[illegible] of a few categories that enable the engineeri[illegible]ailure and alert others to potential vulnerabiliti[illegible] broadly tied to a phase in the engineering [illegible]ach providing a separate opportunity for a[illegible]e directly as a process flaw.

Design Phase

The design phase includes [illegible], and other activities that precede the first fabrication step fo[illegible]ystem. For the sake of this treatment, the design phase includes the build and testing of any models and prototypes meant exclusively for gathering information and refining the final design. For simple engineered systems, third party material manufacture and procurement processes may be considered together with the rest of the design phase. In this case, any component or process flaw originating with these out-sourced components is treated generically as a procurement failure. A more rigorous failure analysis separates these steps from each other, placing requirement definition, quality control and procurement steps into the design phase while the sub-contracted manufacture is part of the overall production phase.

Design Trade-off

Design trade-offs are a significant part of any engineered systems. An entirely separate discussion can be built around the trades made between the three basic constraints on prosecuting a successful engineering goal: Time, Money, & Quality. The important point here is that a