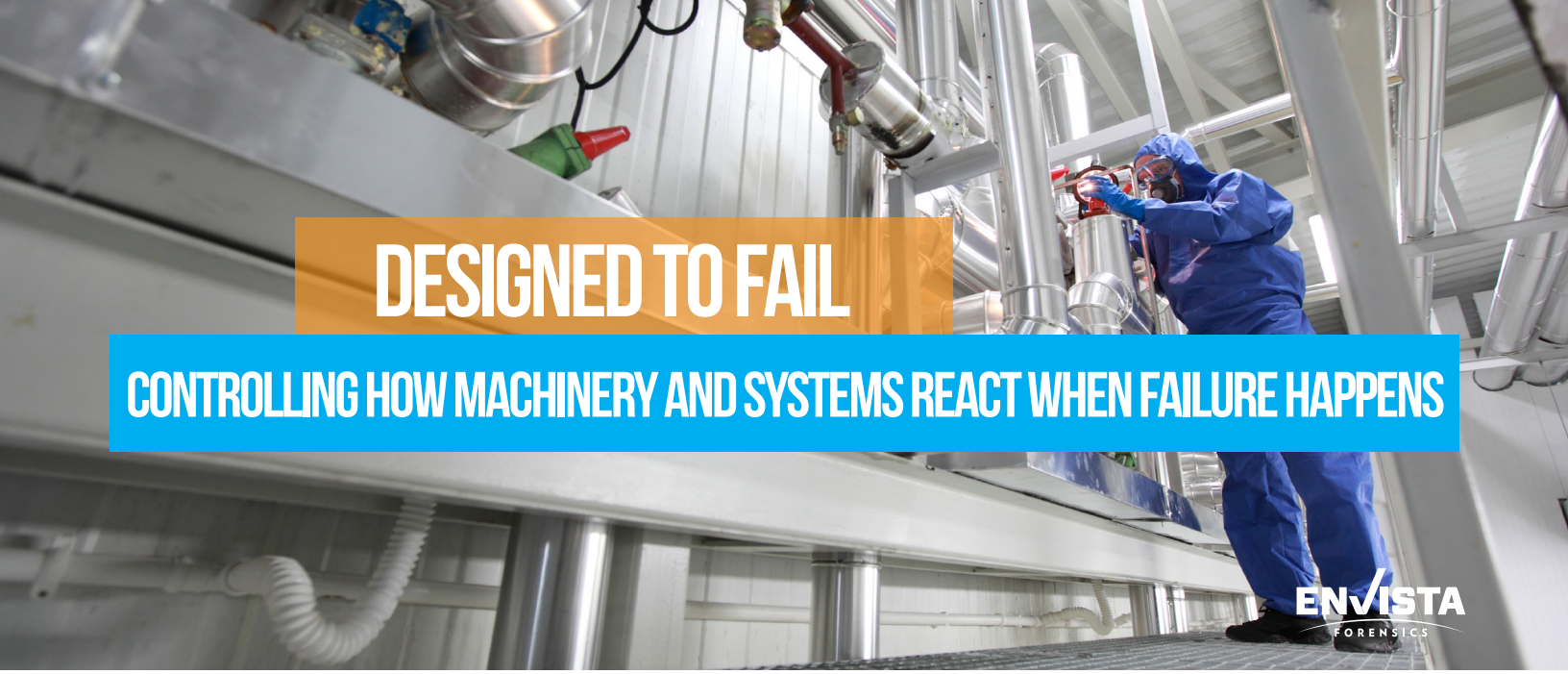

DESIGNED TO FAIL

CONTROLLING HOW MACHINERY AND SYSTEMS REACT WHEN FAILURE HAPPENS

Author: Melissa Simpson, P.E., Project Engineer, Envista Forensics

Although the phrase "failure is not an option" may be a common philosophy, the prudent engineer will consider the effects of failure and the preferred outcome in order to mitigate dangerous or undesirable results. Though the future cannot be predicted with certainty, the certainty of failure is assured.

When it comes to the design of machinery or systems, there is a reasonable expectation for engineers to render a design with careful consideration to operation in both ideal and less-than ideal circumstances. Following industry standards and best practices are implicit in responsible engineering.

Highlights

- Foundation for Responsible Engineering
- Nature of Failures
- Physical vs. Functional Failures
- Single Point, Cascade, and Widespread Failures
- Probability and Possibility of Failures
- Practical Design Applications
- Anticipating Failure

A Foundation for Responsible Engineering

There are many large organizations that serve as a foundation for responsible engineering for various industries and applications. For example, the International Code Council (ICC) has developed extensive requirements relevant to the construction of buildings and building systems. In addition, the American Society for Testing and Materials (ASTM), American Petroleum Institute (API), and International Electrotechnical Commission (IEC) have established best practices for the design and construction of raw materials and components.

Other organizations have a more unique audience, such as an association for fabricators, manufacturers, or operators, that have publications to address specific concerns regarding failure and safety of a given application relevant to their areas of expertise. Guidelines, recommendations, videos, or case studies may be available that highlight the known risks involved in the design and operation of specific types of machinery.

Eliminating or mitigating the effect of known risks is a cornerstone of responsible engineering. The use of safety factors to deliver a more robust design than ideal circumstances require is one way to reduce the probability of a particular failure mode. However, the magnitude of the safety factor is unique to each situation and can be determined from a number of sources, such as engineering standards, rules of thumb, education, or experience. Since it is typical for the cost of a design to increase based on the factor of safety, determining a reasonable safety factor for a given application is affected by economics and the experience of the engineer. A prudent engineer will render a design that both reduces the probability of known failures reasonable to expect in a particular application and reduces the risk of failures that are not

known or expected. Therefore, the safety of a particular design is limited by the designer's knowledge of the application and environment in which the machinery operates.

The Nature of Failures

For the purpose of engineering design, a failure is considered a situation when a component, machine, or system ceases to function in the manner intended by the designer, owner, or operator. The failure may be physical or functional in nature. What differentiates a physical failure from a functional failure is that a physical failure requires the underlying nature of the item to change. For example, a rod is still a rod if it becomes bent, even if the change in characteristics means that it ceases to function as an appropriate rod for a particular application without repair or replacement. However, if a rod has fractured into two pieces, the nature of the component is no longer that of a rod for any application and would require replacement. For reference, the chart below lists examples of physical versus functional failures.

Physical Failure	Functional Failure
Cracked bracket	Bent bracket
Fractured bearing	Bearing out of round
Valve frozen in place due to corrosion	Check valve stuck due to debris
Tire tread separation	Tires with worn treads

Physical vs. Functional Failures

The most common examples of physical failures relate to material fractures and corrosion. For that reason, a responsible engineer expends significant resources to select an appropriate material for a given application and to estimate the expected service life of the component, machine, and system.

The physical or functional failure of one component may remain a single point of failure that can be identified and repaired during periodic inspection. However, unidentified or unrepaired component failures may contribute to the subsequent failure of additional components, the machine, or system. For example, worn bearings may contribute to accelerated wear and tear of other components since the imbalanced movement of the bearings in the races can cause increased vibrations. Therefore, the components identified by their potential as single points of failure should also be considered when defining inspection requirements and replacement intervals.

In some situations, the chemical compatibility, conductivity, or combustibility of materials may be as important as the mechanical properties of a material or its performance at different temperatures. The potential for exposure to temperature differentials, chemicals, vibration, cyclic loading, or impact should also affect the material selection process. When a selected material, such as an elastomer hose, is expected to degrade at a higher rate than others in a given machine or system, the component should be considered consumable with recommended inspection requirements or replacement intervals in order to mitigate the risk of failure.

Single Point, Cascade, and Widespread Failures

There are situations when the damage to machines or systems is more widespread or severe than anticipated as a result of a particular failure. This may be the result of a cascade failure that resulted from unanticipated interactions between components, machines, or systems under a particular set of operating conditions.

Redundancy is the traditional method used to reduce the potential of single point failures that may lead to cascade failure. The redundancy may be similar or dissimilar in nature. A secondary or backup system that automatically engages when the primary system fails is an example of a similar redundant system. One example of dissimilar redundancy is a relief valve set at 3,000 psi and a rupture disc designed to burst at 3,300 psi both installed to protect a pressure vessel in the event the relief valve becomes stuck or does not have sufficient flow to reduce the pressure to a safe amount without the assistance of another device. Triple redundancy and dissimilar redundancy are common in applications when the outcome of a particular scenario is severe, such as the aviation and space industries.

Some extreme conditions, such as power loss, fire, or explosion may result in the simultaneous failure of multiple components. Multi-point failures often increase the severity of an incident or result in conditions that are difficult to predict. Also, safety systems are subject to failure themselves or may be insufficient for the magnitude of the incident they are designed to prevent. One example of an insufficient safety system would include installation of a level III or IV lightning protection system in a region with a high probability of strikes with maximum currents above 100kA.

Probability and Possibility of Failures

Reasonable measures to prevent an incident are predicated upon scenarios considered common or with a high probability of occurrence. However, all possible scenarios should be considered when the outcome of a catastrophic failure could result in injury or death. The severity of an incident is directly related to the level of scrutiny a design will receive after an incident.

Professional engineers are bound by law and creed to protect the public health, safety, and welfare in deference to the impact that engineering has on the lives, property, economy, and security of residents and the national defense.[1] When appropriate according to the law, licensed professional engineers are responsible for the design of machinery and systems.

Practical Design Applications

There are industry standards that address design practices for machines to prevent injury, such as the International Standards Organization (ISO) 12100 and American National Standards Institute (ANSI) B11. Guards are often included as part of a machine's design or incorporated in its installation in order to protect people from hazards. However, it is prudent to consider when and why a specific guard may be removed, such as removal of a heat shield or physical barrier during maintenance, since a guard alone may not be sufficient to prevent an incident without secondary measures in place.

Other organizations, such as the American Petroleum Institute (API), American Society of Mechanical Engineers (ASME), or the International Code Council (ICC) publish standards that address design and installation practices to prevent or mitigate the risk of injury or economic loss.

There are procedural, mechanical, and electrical means to incorporate safety into the design of a machine or system. Procedural means include those that rely on a person to respond in an appropriate manner to prevent injury or avoid damage such as the certification or training of operators, posted warning signs, and alarms. Although useful and practical in most situations, it is not prudent to rely on the awareness and response of an individual when an oversight or mistake would result in severe injury or significant damage.

1 Texas Engineering Practice Act and Rules Concerning the Practice of Engineering and Professional Engineering Licensure. §1001.004.a and §1001.004.b.1

As the severity of a potential incident increases, the design should incorporate more permanent means of protection.

Procedural	Mechanical	Electrical
Operator certification, training	Valves	Automation
Warning signs	Level indicator on chemical tank that may overflow	Ground Fault Circuit Interrupter (GFCI)
Alarms	Insulation on hot surfaces	Sensors

In a system that involves pressurized fluid, valves are an example of a permanent, mechanical means to design for failure in order to prevent injury or damage to equipment. Valves are subject to damage from wear and tear, environmental, or process-related conditions so the design engineer should evaluate the effect of such failures and select valves that fail in an ideal manner. Depending on the application, actuated valves that fail-open, fail-closed, or fail-safe may be more appropriate than manual valves that fail in place since they require an external force applied by an electronic, pneumatic, or hydraulic signal that causes the valve to return to its normal position when the signal is removed or interrupted.

Common Valve Design Types	
Fail-Open (Normally Open)	An actuated two-way valve that requires an external force to remain closed, also referred to as normally open valves
Fail-Closed (Normally Closed)	An actuated two-way valve that requires an external force to remain open, also referred to as normally closed valves
Fail-Safe	An actuated multi-way valve or a valve with a bypass that directs the process flow into a safe direction. This term may also be applied to actuated two-way valves that fail-open or fail-closed when the valve response to a signal interruption does not create a hazard.
Fail in Place	A manually operated valve that remains in place until manipulated by an operator

There are electronic devices that may be incorporated into the design to automate the steps of a process within a machine or system. Whether to ensure appropriate guards are in place or ensure activities happen in the correct order, using switches and sensors in the design is an appropriate means to automate a safe response in situations when it is not prudent to rely on a person to input the appropriate signal in time to prevent an incident. For example, a selector switch may be incorporated into an electrical circuit to either force the process to stop when a proximity sensor detects motion or prevent an operator from performing the next task.

Anticipating Failure

Designing machinery and systems in such a way that anticipates probable or possible scenarios leading to injury or damage requires a systematic approach, experience, and imagination. A Failure Modes and Effects Analysis (FMEA) is a method of recording the potential scenarios, risks, severity, and follow-up actions. The most developed, comprehensive lists of failure scenarios come from teams of people with varying perspectives, expertise, and experience levels.

Approaching the design of machinery and systems with the expectation that something will go wrong provides the opportunity to incorporate reasonable measures to control how machinery and systems will react when failure happens. The probability of injury or damage to machinery increases when probable or possible scenarios are not anticipated, the severity of a potential incident was not considered, and readily available design features are not incorporated.

Although safety devices or precautions may be in place at the time of failure, injuries may still happen for a number of reasons. Safety protocols might not be followed, safety devices may not be operable or effective, or the incident may be more severe than anticipated. After a failure has happened, experts delve into the details of the incident to identify the contributing factors and evaluate whether or not reasonable measures were taken to prevent the incident. Forensic engineering experts are obligated to report the facts that form the basis of their opinions and be prepared to support their opinion during subsequent litigation.

By considering how machinery and systems react when they fail, engineers can evaluate and design reasonable means to control the effects of failure in an effort to prevent further damage or injury.