Fail-Safe and Safe-Life Designs
And Factor of Safety

Factors of Safety (a.k.a. Safety Factor)

The factor of safety is usually expressed as a ratio of the "load carrying capability" of the structure to the expected loading. Loading may be static, impact, fatigue, wear, et cetera. The purpose of using a safety factor is to assure that the design does not fail in the event of unexpectedly high loads or the presence of material/design defects. Factors of safety are applied to decrease the probability of failure, or in more positive terms, they increase the probability of success. They are applied in part due to inherent ignorance present in all designs. Ignorance stems from natural variability in materials and manufacturing processes, maintenance, and what the design really experiences in its lifetime. Lower factors of safety may be required if the following are true, larger ones are justified if these are less true:

High quality and consistency of materials, manufacturing, maintenance and inspection
Good control or knowledge of the actual loads and environment
Highly reliable analysis and/or experimental data

The commercial airplane business has extremely rigorous control over airplane structures and systems from fabrication and assembly through inspection and maintenance. The environmental effects and maximum loads airplanes experience are also well understood. Extensive fatigue and static testing is conducted on components and systems. Therefore, relatively low factors of safety are applied (around 1.3) even though safety is at stake.

The degree of ignorance is not the only element that the engineer should use to determine appropriate factors of safety. The potential harm that failure can produce is also important. If failure would result in a mere inconvenience, then a small factor of safety may be acceptable. If failure would be expensive or even life threatening, then a larger factor of safety is justified.

How does an engineer determine an appropriate factor of safety? In some instances, such as pressure vessels, minimum factors of safety are mandated by codes and standards. But this is not often the case. Experience with similar designs is often the best method. Typically, factors of safety range from a low of 1.3 to around 5.

Fail-Safe and Safe-Life Designs

Aerospace engineers, for designs involving fatigue loading, developed safe-life and fail-safe philosophies. The concept of fail-safe designs is extended here to include all designs that mitigate the harm caused by failure.

What is meant by "Fail-Safe"?

Fail-safe designs are designs that incorporate various techniques to mitigate losses due to system or component failures. The design assumption is that failure will eventually occur but when it does the device, system or process will fail in a safe manner.

What is meant by "Safe-Life"?
Safe-life refers to the philosophy that the component or system is designed to not fail within a certain, defined period. It is assumed that testing and analysis can provide an adequate estimate for the expected lifetime of the component or system. At the end of this expected life, the part is removed from service.

When should either of these philosophies be employed?
The benefit of safe-life designs includes reducing the likelihood of unplanned maintenance and reducing the likelihood of any failure. Benefits of fail-safe designs include being able to manage the unexpected and mitigating damage if failure occurs.

There is no method to help determine which if either of these philosophies should be employed. Engineers must use their judgment on a case-by-case basis. The decision to use either of these philosophies is justified whenever the "cost" and likelihood of failure outweighs the "cost" of implementing either fail-safe or safe-life designs.

"Cost" of failure may include:
- Physical harm to people or the environment
- Loss or destruction of property or equipment
- Loss of productivity or use of the failed "system" or device
- Damaged reputation

Likelihood of failure
- The engineer should always consider how likely a certain failure will be. In so doing, it is important to consider all potential loading conditions – even abusive loads.

"Cost" of implementing can include:
- Increased expense and time for design and testing
- Increased production costs
- Decrease in product performance

There are no formulas to help determine when fail-safe or safe-life designs should be employed. Airplane designs employ both of these concepts, making air travel one of the safest modes of transportation. Yet, it is not possible to make aircraft completely safe. There are always conditions that are prohibitive to guard against.

Techniques for Safe-Life Design
Since it is imperative that the component or system not fail within the predicted life time, extensive testing and analysis is required. Safe-life designs involve a testing and analysis (typically fatigue analysis) to estimate how long the component can be in service before it will likely fail. Since no amount of analysis and testing can assure how long a particular part will perform without failure, a generous factor of safety should be included to prevent catastrophic failure. The product should be designed so that it can be easily inspected in service.

Techniques for Fail-Safe Design

Redundancies (avoid single point failures)

Back-up systems –If failure of a critical subsystem will cause severe losses, back-up systems are often employed. For example, commercial aircraft have a minimum of two engines. They are designed such that fully loaded airplanes can takeoff even if one engine fails.

Multiple load paths – if a structural element fails, the load it was carrying will be transferred to other members. Obviously, it is essential that the fracture be detected before multiple members fail.

Intentional "Weak Link"

An inexpensive and easy to replace component may be used to prevent damage to expensive or difficult to repair component. Fuses in electrical circuits are an example of this for electrical systems. Shear pins are used on boat propellers are a mechanical example. These are inexpensive and easy to replace pins that transmit power from the shaft to the propeller. If the propeller strikes an object, the shear pin is designed to fail before the propeller or shaft are damaged.

Physical Law

Designing a system in such a way that failure cannot be catastrophic based on how failure will occur. For example, nature gas pipelines are produced from sufficiently tough material so that it will fail in a ductile manner, rather than brittle. Ductile fractures propagate at about 600 ft/sec. Brittle fractures propagate at about 1500-2500 ft/sec. When a crack forms in a pipe, the gas will immediately begin to decompress. The decompression wave will travel down the pipe at about the speed of sound (1300 ft/sec). If the crack speed is faster than the decompression speed, the crack front will always remain under high pressure and the crack will grow indefinitely. Otherwise, the decompression wave will out run the crack, and the crack will stop growing.

Early Detection

When a structure is designed such that cracks will easily be detected before they reach critical length, it may be considered a fail-safe design. A critical element of this is the detection of the crack before it reaches critical length. It is very important that proper materials (high fracture toughness) be selected that can withstand large cracks before fracturing.

Fracture mechanics must be used:

- Determine minimum detectable crack length (how small of crack can nondestructive testing detect)
- Determine critical crack length for the maximum load
- Create a crack growth curve showing crack length as a function of number of cyclic loads
- Determine how much time is required from the crack to grow from the minimum detectable length to critical length.

Leak-before-break – pressure vessels use this method to prevent explosive failures. Pressure vessels are designed such that a crack will propagate completely through the vessel before it reaches critical length. Generally, the cracks will start at the internal wall and progress outward, radially. Leaks are generally easy to detect, and therefore, should be detected before the crack grows to critical length. See Figure 1

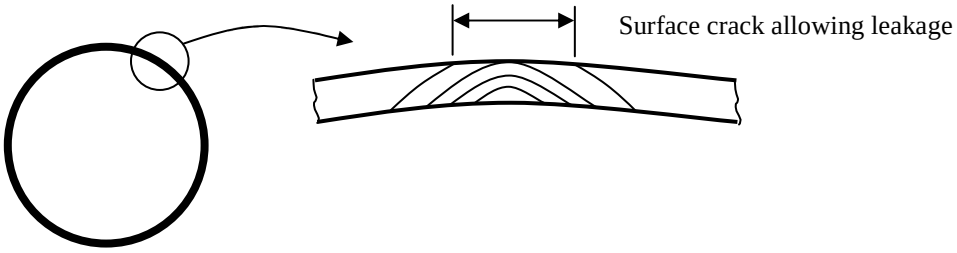

Figure 1 – Leak-before-break in a pressure vessel.

Crack Arresters – to prevent cracks that exceed critical length from fracturing the entire part, crack arresters may be added to the structure. In aircraft these are in the form of riveted straps added to the skin. This will contain the crack to a small area of the structure. See Figure 2.

Effectively, what is occurring is the crack tip stress intensity decreases as it approaches the arresters. The arresters start to carry more and more load, thus decreasing the load near the crack tip.

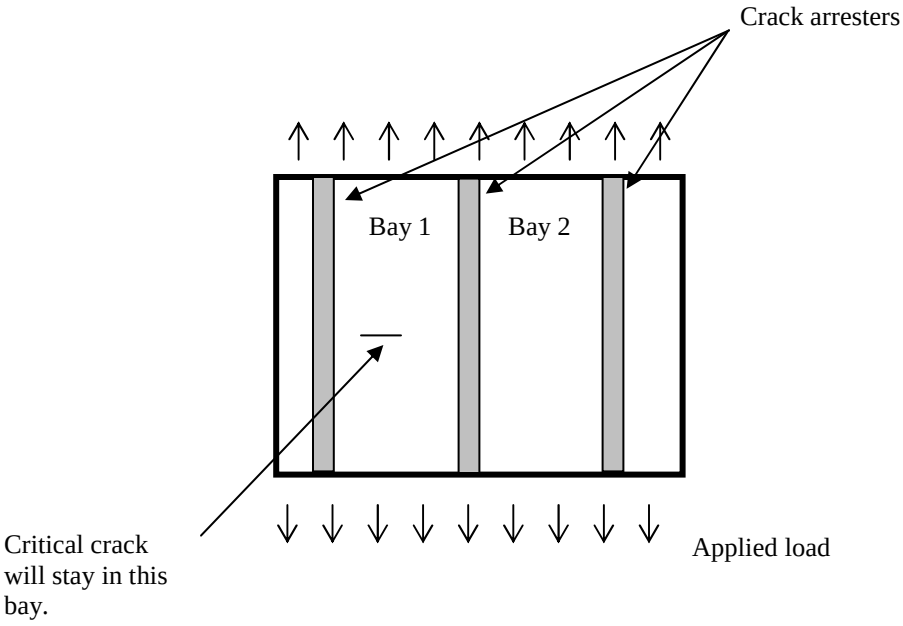

Figure 2 – crack arresters preventing extensive crack growth in a panel with axial loads.