Design philosophies

Throughout aviation history, design principles have been developed based on experience. Initially, structures were made strong enough to sustain certain loads, based on engineering judgement. Later, experience demanded that degradation during operation should somehow be considered.

This has led to the different design philosophies.

The first philosophy is generally referred to as “safe-life” or “safety by retirement”.

Safe life is the number of flights, landings, or flight hours, during which there is a low probability that strength will degrade below design strength.

This philosophy is based on the assumption that the likelihood of structural degradation leading to structural strengths below the design strength is very low. A pristine structure may degrade due to various circumstances, but before the structural strength would reduce to below a design strength, the aircraft would be replaced or discarded.

This degradation may be induced by phenomena like metal fatigue.

Hence along with the introduction of metallic structures in aviation, the safe life design principle developed.

In the early days, this philosophy worked fairly well. In most cases, end of life of aircraft was dictated by other factors than the likelihood of failure, in particular with most military aircraft.

There are, however, aspects that may cause issues with this safe-life design philosophy. For example, the lifetime is increased, because the operator wants to exploit the aircraft for a longer duration of time. Or in aircraft development and design, other methods or materials are introduced that effectively result in shorter lifetimes.

Consider, for example, replacing one aluminium alloy by a stronger alloy to improve the airframe strength. This stronger alloy could have poor fatigue properties, resulting in more rapid degradation of the structural strength.

Well known aircraft accidents associated with the safe-life design principle are the de Havilland Comet accidents in the 50’s of last century.

With two of these aircraft, the fuselage exploded during cruise at high altitude. Cracking occurred at window cut-outs imposed by the rather high stresses.

These accidents were not expected because fatigue was considered in the design. For example, the full-scale fatigue test resulted in failure after about 16,000 flights, while both aircraft accidents occurred near 1,000 flights.

This difference is attributed to the fact that the full-scale fatigue test was executed after the overload test was applied. This resulted in favorable stress redistributions relieving fatigue critical locations.

Repeating the test with an aircraft taken from service, resulted in only 3,000 flights until failure.

The second design philosophy is called “fail safe” or “safety by design”.

Fail safe is the attribute of the structure that permits it to retain required residual strength for a period of unrepaired use after failure or partial failure of a principal structural element.

This design principle emphasizes the use of multiple load paths. That is, multiple elements carrying the loads. This concept is based on the observation that critical components had limited service lives.

The concept assumes that failure of a primary member should not endanger aircraft safety, because other components still could carry the loads.

Structures, therefore, were designed to be more robust.

Aside from improving safety, this turned out to be more economically viable than the safe-life concept, because elements could be operated longer before retirement.

The concept is based on identifying all events and failure modes for which structural strength has to be established. An issue observed with this principle however, was that in reality events occurred that were not anticipated in design.

Another problem making this concept less effective, is the occurrence of multiple site damage.

If all load carrying elements slowly degrade or build up damage, then failure of one member may lead to the case where the remaining damaged members are no longer able to carry the load.

The third design philosophy is called “damage tolerant design philosophy” or “safety by inspection”.

Damage tolerance is the ability of a structure to sustain anticipated loads in the presence of fatigue, corrosion, or accidental damage until detection (via inspections or malfunctions)

So take the illustration left. With service time, damage slowly will develop, corresponding to a slow reduction of the strength.

Depending on the inspection method, damage of different sizes may be detected. Once damage is detected, regulations require that the structure is repaired, corresponding to the strength returning to its pristine strength.

When strength reaches the fail-safe requirement – design strength – then damage has reached its critical size.

The time window between detection and critical or allowable damage size is the time available for inspection, detection, and repair.

The damage tolerant design philosophy has been introduced in the certification requirements in 1978.

This change in design philosophy was not meant to replace the previous design philosophies, but added scheduled inspections to the existing practice.

In addition, strength assessment had to assume imperfections and manufacturing flaws present in the pristine structure from Day 1, which implies more emphasis on damage growth analysis, rather than structural life.

The scheduling of inspections assures the durability, although they should be economically feasible.

The previous graph, illustrating the restoration of strength when repairs are applied, illustrates a fundamental assumption in the damage tolerance design philosophy: repairs should restore the original strength of a structure.

Although the damage tolerant design philosophy significantly improved the durability of airframes, it does not guarantee safety in itself.

This is illustrated by the Aloha Airlines accident, where a Boeing 737 lost a significant portion of the upper fuselage structure.

This failure was caused by multiple site damage in the riveted longitudinal fuselage joints. These joints were susceptible to corrosion, because the aircraft operated in a warm humid maritime environment.

The operator was advised by Boeing to inspect these joints, but it did not perform the required structural inspection, resulting in failure.

The combination of fatigue damage with environmental influences has resulted in that airframes these days should be designed damage tolerant and with sufficient durability.

Here, durability is defined as the ability of a structure to sustain degradation from fatigue, corrosion, and accidental damage to the extent that they can be controlled by maintenance and inspection programs.

In practice, this means that every aircraft manufacturer should demonstrate damage tolerance through analysis supported by tests. Here, the pyramid left illustrates that most tests performed are coupon level tests. They are meant to generate material data.

The more detail added to the test, and the more the test panel represents the final structure, the more complex and expensive tests are. Because these component tests mostly serve the validation of analyses, less tests are needed.

The procedure on the right-hand side, illustrates that for each major element or component, the aircraft manufacturer must identify whether inspection is possible or not.

If not, the component is certified according to the safe-life design principles, whereas inspection means that damage tolerance principles are applied.

In case such structures comprise multiple load paths, it effectively follows the fail-safe philosophy with added inspections. Otherwise, it must be guaranteed that damage will grow very slow, leaving ample time to inspect, detect, and repair.