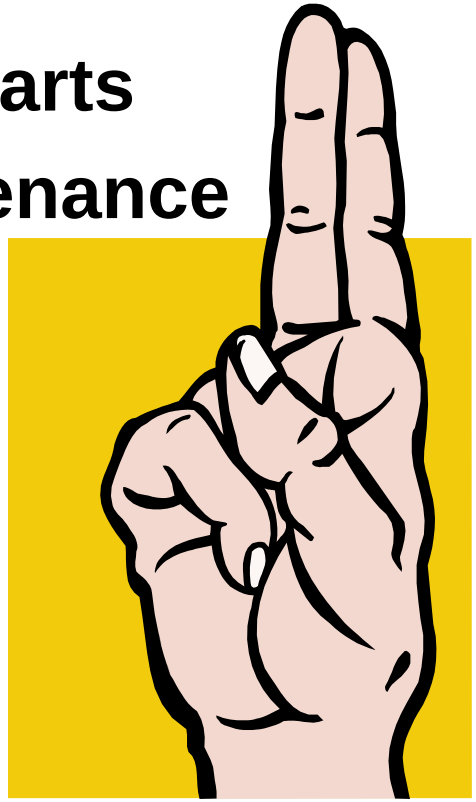
PHM Standards Panel 2012

By: M. Walz.

Date: 24-27 September , 2012

PHM Some Industry Promises

- **Increase Safety**
- **Increased usage of Life Limited Parts**
- **Reduction in Unscheduled maintenance**
- **Reduction in Fault Not Found**
- **Reduction in manual inspection**



Important Concepts

- **Credit:** To give approval to a HUMS application that adds to, replaces, or intervenes in industry accepted maintenance practices or flight operations.
- **END-TO-END:** The term "end-to-end" as used in the text is intended to address the boundaries of the Health Usage Monitoring System (HUMS) application and the effect on the rotorcraft. As the term implies, the boundaries are the starting point that corresponds with the airborne data acquisition to the result that is meaningful in relation to the defined credit without further significant processing. In the case where credit is sought, the result must arise from the controlled HUMS process containing the three basic requirements for certification as follows:
  - equipment installation/qualification (both airborne and ground),
  - credit validation activities, and
  - Instructions for Continued Airworthiness (ICA) activities.

THE FAA FAIL-SAFE DESIGN CONCEPT.

The Part 25 airworthiness standards are based on, and incorporate, the objectives, and principles or techniques, of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

The following basic objectives pertaining to failures apply:

(1) In any system or subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or

significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.

(2) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

THE FAA FAIL-SAFE DESIGN CONCEPT cont.

The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these

principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e., to ensure that major failure conditions are improbable and that catastrophic failure conditions are extremely improbable.'

(1) **Designed Integrity and Quality, including Life Limits**, to ensure intended function and prevent failures.

(2) **Redundancy or Backup Systems** to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(3) **Isolation of Systems**, Components, and Elements so that the failure of one does not cause the failure of another. Isolation is also termed independence.

(4) **Proven Reliability** so that multiple, independent failures are unlikely to occur during the same flight.

(5) **Failure Warning** or Indication to provide detection.

(6) **Flight-crew Procedures** for use after failure detect ion, to enable continued safe flight and landing by specifying crew corrective action.

(7) **Check-ability**: the capability to check a component's condition

(8**) Designed Failure Effect Limits**, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(9) **Designed Failure Path** to control and direct the effects of a failure in a way that limits its safety impact.

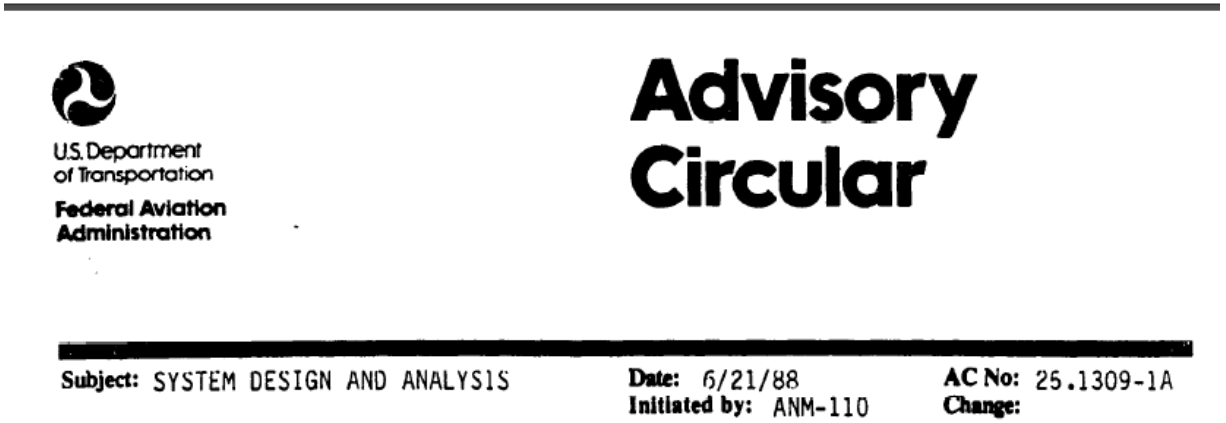
(10) **Margins or Factors of Safety** to allow for any undefined or unforeseeable adverse conditions.

(11) **Error-Tolerance** that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation, and

maintenance.

FAA Safety Analysis

All certification starts with a Functional Hazard Assessment ref AC 25-1309



U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: SYSTEM DESIGN AND ANALYSIS **Date:** 6/21/88 **Initiated by:** ANM-110 **AC No:** 25.1309-1A **Change:**

1. PURPOSE. This Advisory Circular (AC) describes various acceptable means for showing compliance with the requirements of § 25.1309(b), (c), and (d) of the Federal Aviation Regulations (FAR). These means are intended to provide guidance for the experienced engineering and operational judgment that must form the basis for compliance findings. They are not mandatory. Other means may be used if they show compliance with this section of the FAR.

Safety Defined Effects

- **Minor -** Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may. include, for example: a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants crew workload,

Safety Defined Effects

- **Major-** Failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be,

for example, --

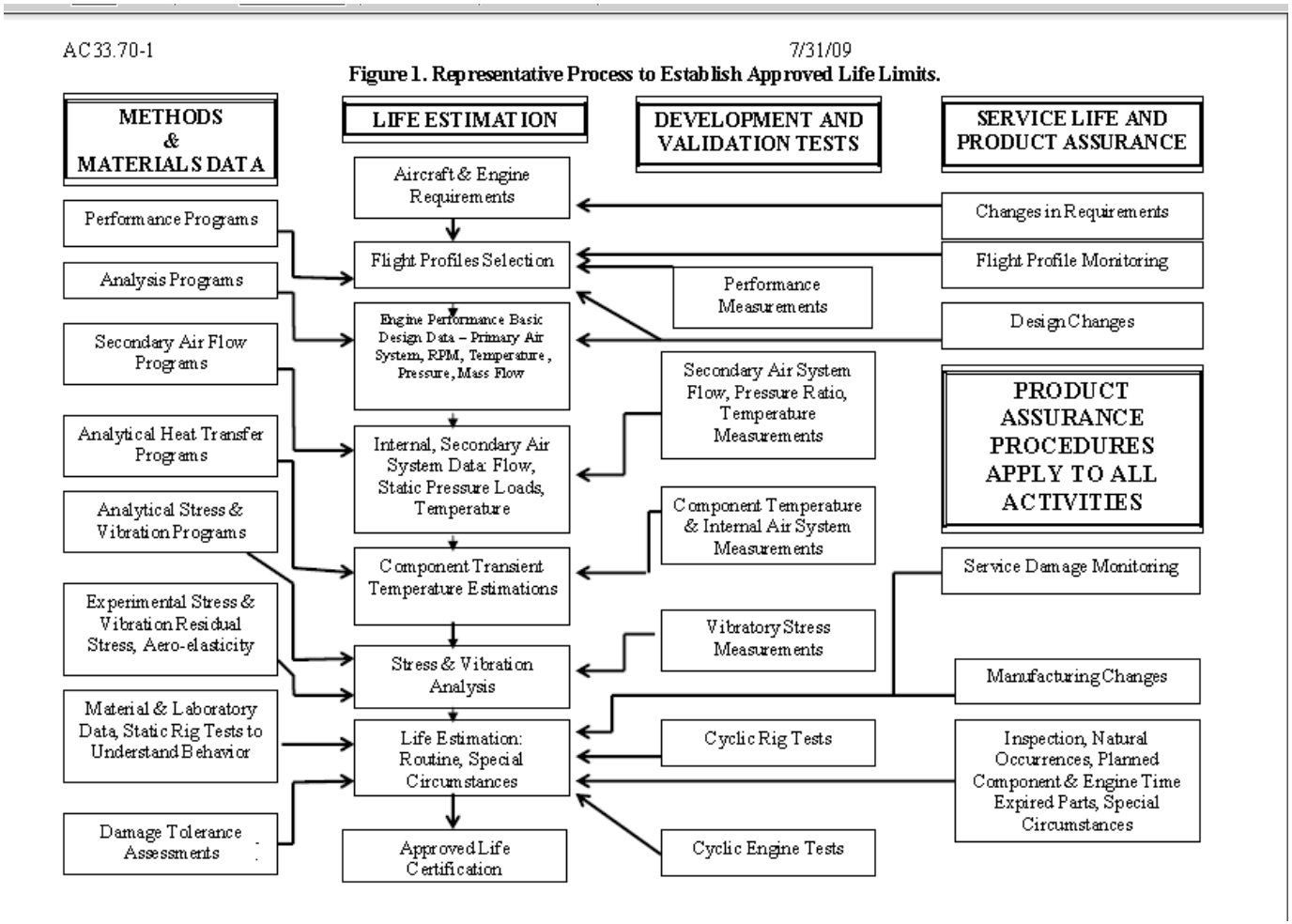
(i) A significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or some discomfort to occupants; or

(ii) In more severe cases, a large reduction in safety margins or functional capabilities, higher workload or physical distress such that the crew could not be relied on to perform its tasks accurately or completely, or adverse effects on occupants.

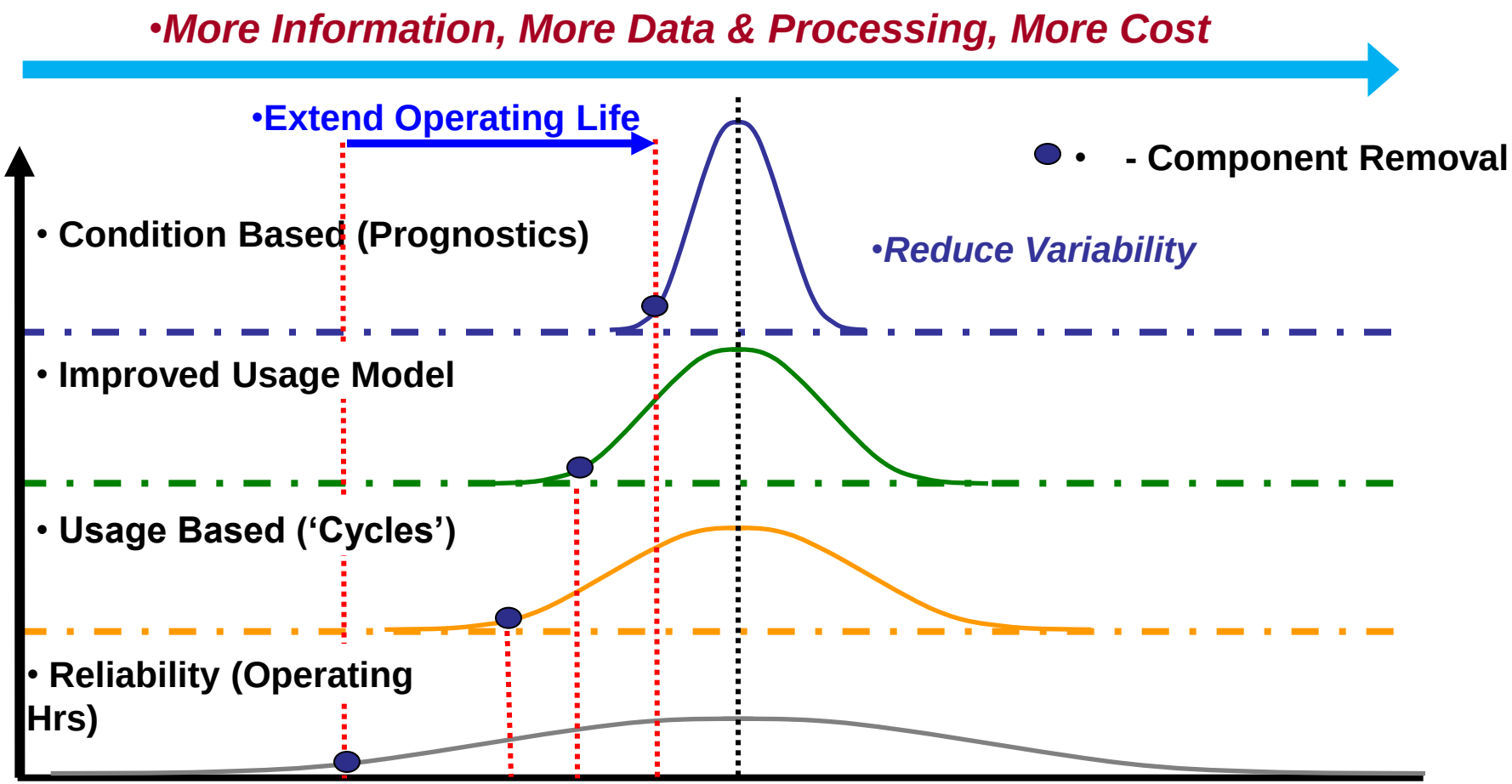
Safety Defined Effects

- **Continued Safe Flight and Landing**: The capability for continued controlled flight and landing at a suitable airport, possibly using emergency procedures, but without requiring exceptional pilot skill or strength. Some airplane damage may be associated with a failure condition, during flight or upon landing.
- **Catastrophic:** Failure conditions which would prevent continued safe flight and landing.

Life Limited Parts



Proposed Life-ing Improvement



•Life/Health Prediction can drive maintenance planning, vehicle operations planning, spares allocation, component/system overhaul ,…

A View of Prognostic systems

- Predictive health management typically **requires higher bandwidth data** which may include data from sensors such as an accelerometer

- Predictive health management typically **involves the capture and manipulation of large multi-dimensional 'windows'** of data onboard.

- Predictive health management typically **does not require real-time response**

- Predictive health management typically **requires maturation** during operational use including the capture of onboard data.

- Predictive health management can be **support critical, not flight/safety critical**

- An affordable approach to the maturation of flight critical health management can be **to implement it first as support critical and then promote it to flight critical status.** Requires flight critical hardware.

Questions?